Volpe National Transportation Systems Center

TTD No. RA 2068
Contract No. DTRS-57-89

Maglev System Concept Definition (SCD) System Safety Review

First Interim Report

Booz·Allen & Hamilton Inc.
4330 East West Highway
Bethesda, MD 20814-4455

in association with
Canadian Institute of Guided Ground Transport

January 7, 1993

TABLE OF CONTENTS

LIST OF EXHIBITS

LIST OF EXHIBITS (Continued)

1.0 INTRODUCTION

As part of the National Maglev Initiative (NMI), the Federal Railroad Administration (FRA) solicited proposals to conceptually define the technical feasibility, performance and costs of constructing and operating Maglev systems in the United States. Four teams were selected to prepare System Concept Definition (SCD) documents for their respective designs:

- Magneplane
- Foster-Miller
- Grumman
- Bechtel

The FRA requested support from the Volpe National Transportation Systems Center (VNTSC) to conduct a system safety review of each of the SCDs. Current FRA regulations are primarily technology-specific and based upon years of steel wheel, steel rail operating experience.

Because the design of maglev systems is still in the conceptual phase, detailed design information is not presently available. However, top level safety analyses can be prepared and were required as part of each contractor's SCD. FRA requirements for each SCD included definition of a system safety program and preparation of a structured hazard analysis. The system hazard analysis was to address the following[1]:

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

In addition, the following safety related criteria, listed in Exhibit 1-1, were referenced in the Request for Proposals (RFP) for System Concept Definitions.

---

1 Maglev System Concept Definition, Feb. 20, 1991, Section C, 5.3 DTFR53-91-R-00021

EXHIBIT 1-1
Maglev System Criteria
Related to Safety

SCD RFP S.O.W. SECTION C	SCD REQUIREMENTS RELATED TO SAFETY		
3.1.1(d)	Noise and Vibration	–	(DG) The noise and vibration produced by total system operation should be designed to meet existing Federal standards and industry practices, as appropriate, for stationary facilities such as maintenance areas and stations. Noise and vibration produced by the vehicle traversing the guideway should be minimized. Potential noise and vibration impacts and possible mitigation methods in urban areas should be given special attention.
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(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.
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.

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

EXHIBIT 1-1 (Continued)

SCD RFP S.O.W. SECTION C	SCD REQUIREMENTS RELATED TO SAFETY		
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(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(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			The contractor shall, as a minimum, address following elements:
3.2.1(a)	Vehicle	–	Levitation and guidance systems including magnet design and configuration, cooling, control system requirements, power requirements, and failure modes.
3.2.1(c)	Vehicle	–	Structural design considerations, including weight and crash worthiness considerations.
3.2.1(d)	Vehicle	–	Braking system, including regenerative, aerodynamic, mechanical or other suitable means.
3.2.1(e)	Vehicle	–	Active and/or passive banking, including the minimum horizontal and vertical radii of curvature as a function of vehicle velocity.
3.2.1(f)	Vehicle	–	Aerodynamics, including calculated internal and external noise intensities, and innovative design techniques to reduce drag and/or noise.
3.2.2(a)	Guideway	–	Civil structural elements, including piers, footings, columns, spans and materials used and adjustability of structure to maintain required alignment.
3.2.2(b)	Guideway	–	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)	Guideway	–	Alignment tolerances, and sources of disturbances (expansion gaps, thermal distortion, warpage, differential settlement of substructure, wear, etc.).

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

EXHIBIT 1-1 (Continued)

SCD RFP S.O.W. SECTION C	SCD REQUIREMENTS RELATED TO SAFETY	
3.2.2(d)	Guideway	– Entry/exit method, including maximum speeds, impact on headway, physical size and configuration.
3.2.2(f)	Guideway	– Power requirements, proposed distribution method, lightning protection and grounding.
3.2.2(i)	Guideway	– Instrumentation for sensing guideway integrity and vehicle positions.
3.2.3(a)	System Considerations	– Communications and control systems, including overall philosophy, principal elements, software hardware integration and verification and validation methodology.
3.2.3(h)	System Considerations	– 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

This report documents a review of the four System Concept Definitions (SCDs) with respect to the system safety process, hazard identification, hazard criticality assessment, mitigating measures and the proposed validation process to verify hazard resolution.

1.1 APPROACH TO THE SCD SAFETY REVIEW

The approach used for reviewing the safety programs and hazard analyses prepared by the SCD contractors was as follows:

- A generic process for implementing a system safety program during the conceptual design of a new transportation system was defined and compared to the programs outlined in the SCDs. Each approach was evaluated with respect to its system safety organization, safety process, and schedule for implementation.

  Each contractor's system safety approach is reviewed in the first section of each of the following chapters.

- Each SCD was reviewed to identify how the contractor addressed the required safety issues:
  - Loss of system power
  - Loss of control and/or communication system
  - Loss of levitation or guidance
  - Loss of guideway integrity
  - Guideway obstruction
  - Fire
  - Evacuation and rescue
  - Levitation/guidance/magnet failure
  - Operation restrictions
  - Manual override, security and training
  - Maintenance of safe headway.

  These safety issues are referred to as "baseline hazards". The "baseline hazards" were reviewed in a matrix format, as illustrated in Exhibit 1-2.

For each baseline hazard, the contractor's Preliminary Hazard Analysis (PHA) or similar analysis, was reviewed for accuracy and completeness, and the "resolution" or "control method" was documented. The remainder of the SCD was reviewed to:

- Identify the design features referenced by the PHA
- Identify the "resolution" or "control method" of hazards adopted by designers but not covered in the PHA

- Identify issues, such as hazards that were not addressed, hazard classifications that were inconsistent, or ambiguities that the FRA or contractor may wish to investigate.

The matrices and accompanying text is provided in the second section of each chapter.

EXHIBIT 1-2

Hazard Matrix

BASELINE HAZARD	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
RFP REQUIRED SAFETY ISSUES	HOW RESOLVED IN THE CONTRACTOR'S PHA	HOW RESOLVED IN OTHER SECTIONS OF THE SCD	OPEN ISSUES OR COMMENTS

- Additional safety issues were addressed as part of the SCD review:
  - Safety-related items from Exhibit 1-1
  - Vehicle/Guideway Dynamics
  - Electromagnetic Interference (EMI)
  - Guideway Maintenance Operations.

  These "additional hazards" are presented in a similar matrix in the third section of each chapter. Where contractors identified hazards not in either VNTSC list, they were included with the additional hazards.

- The emergency response strategy, design features, and advantages and disadvantages of each approach were reviewed and documented in the fourth section of each chapter.

1.2 SYSTEM SAFETY PROGRAMS APPLIED TO CONCEPTUAL 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 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.

To evaluate each contractor's system safety approach, a model system safety program, focused on the design phase activities, was defined. It encompassed 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 performance of the safety tasks in the program. It should further 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 very important that they are included because without formal management recognition and tracking of safety tasks, they are easily 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 mandated 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. Every system concept definition program should conduct a Preliminary Hazard Analysis (PHA). A PHA is usually the minimum level of safety analysis for an advanced design effort because the requirements for subsequent safety analyses are based on the categorization of hazards from the 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 – In some complex development programs, such as Maglev systems, it may be necessary to establish 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.

1.3 SAFETY ANALYSIS CONSIDERATIONS

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 primary analysis tools which are interrelated. 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 methodology contained in FAA Advisory Circular 25.1309-1A. The safety process described in this section is intended to be used as an engineering tool to help verify that a specific design architecture and its installation in the Maglev train is safe.

The relationship between these four tools is shown in Exhibit 1-3 and discussed in the following sections. Exhibit 1-4 identifies each design phase and corresponding analytical tasks and outcomes. Notice 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.

EXHIBIT 1-3

System Safety Analysis

Conceptual and Functional Relationships of PHA, FMECA, FTA and ZA

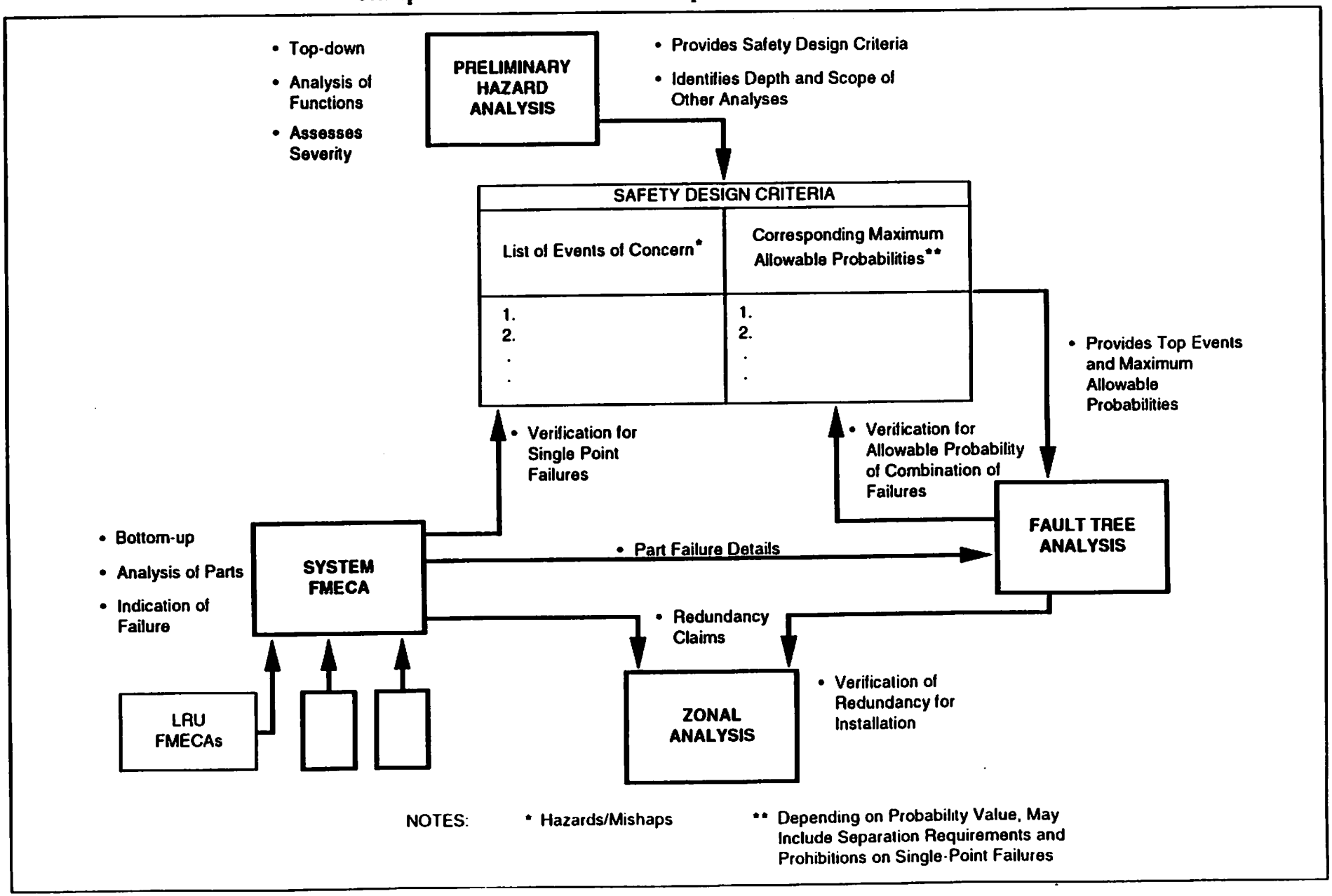


EXHIBIT 1-4
Outcome of Safety Analyses

PHASE	ANALYSIS TASKS	RESULT/OUTCOME
SYSTEM CONCEPT DEFINITION	• PHA • Independent Review	• For a new design: Safety events of concern & numerical safety criteria • For an existing design: safety criteria for design modifications
DEVELOPMENT 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)

1.4 SAFETY ANALYSIS TOOLS

Four safety analysis tools, useful during the design phase, are briefly discussed below. Each contractor's system safety program should contain a plan to conduct similar analyses.

1.4.1 Preliminary Hazard Analysis (PHA)

A PHA is a systematic, high-level examination of a proposed system's functions to identify and classify potential hazards to the Maglev system 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 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 or transit applications may provide sufficient information. For complex systems, a new formal PHA should be prepared to provide a thorough evaluation of the system.

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 functional failures and assigns hazard classifications for each.

1.4.2 Failure Modes, Effects and 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, a working document, should be continually refined to reflect the current status of the system design. The preparation of the analysis should begin early in the design stages and its refinement should parallel design progression.

1.4.3 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 serve as a mathematical model in 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 undesired event for the Maglev system called the "Top Event".

"Top Events" can be established from PHAs. Usually, Top Event candidates are derived from hazards/mishaps classified in the PHA as Category I or II. 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.

1.4.4 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 system installation. The ZA can substantiate the FMECA and FTA for the systems under consideration by verifying that design redundancies are reflected in the installation and are not violated by single undesired events, including cascading or common-cause events.

1.5 HAZARD CLASSIFICATIONS

The PHA is used to assign hazard classifications and safety criteria and establish what, if any, additional analyses are required. In order to assign hazard classifications, a definition of hazard classifications must be stated. MIL-STD-882B is the most widely used reference for definitions of hazard classifications. The Hazard Severity Categories identified in MIL-STD-882B are stated here:

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-882B cautions that *"these hazard 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."*

Each SCD states that their program will follow the overall approach of MIL-STD-882B. However, only one SCD provides an adaptation of the general hazard category wording in MIL-STD-882B. The definitions below are suggested as a standard to provide consistency in future Maglev safety reviews, and were used to suggest the classification of hazards when an SCD contractor did not.

The classification descriptions and design standards are derived from those set forth in FAA Advisory Circular 25.1309-1A. These classifications and standards apply to airplanes certified by the FAA under Title 14 of the CFR, Chapter I, Part 25 as well as those certified under the equivalent regulations of other countries. Adoption of Maglev terminology has been substituted for airplane terminology.

- **Class I (Catastrophic):** Hazards/Mishaps which would result in multiple fatalities, destruction of levitating vehicles, or damage to terminals or guideway segments such that the effected segments of the Maglev system cannot operate.
- **Class II (Critical):** Hazards/Mishaps which would reduce the capability of the Maglev system or the ability of operators to cope with adverse operating conditions to the extent that there would, for example, be a large reduction in safety margins or functional capabilities, extensive damage to Maglev system equipment, higher workload or physical distress such that the operators could not be relied upon to perform their tasks accurately or completely, or adverse effects on the traveling public, including up to a few severe injuries or, exceptionally, fatalities.
- **Class III (Marginal):** Hazards/Mishaps which would reduce the capability of the Maglev system or the ability of the operators to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, non-disabling damage to Maglev system equipment, a significant increase in operator workload or in conditions impairing operator efficiency, or some minor injury, discomfort or danger to the traveling public.
- **Class IV (Negligible):** Hazards/Mishaps which would not significantly reduce Maglev system safety, and which involve operator actions that are well within their capabilities. Negligible Hazards/Mishaps may include, for example, a slight increase in operator workload, such as manual train operation into a station on a line where trains normally operate automatically, or some inconvenience to the traveling public.

Note that a Catastrophic Hazard/Mishap (Category I) is not quite the same as the conventional definition of a fatal accident. The latter covers accidents in which as few as one person is killed (e.g. a fatality where a train strikes a person on the track). The Catastrophic Category as used here for system safety assessments is in effect a multi-fatality Hazard/Mishap. It is true that the definition also includes loss of a train or fixed line equipment, which might sometimes be non-fatal, but in practice usually involves fatalities.

The Critical Category (Category II) is intended to cover those Hazards/Mishaps for which the risk of escalation to a catastrophe is potentially high and also those in which a small number of persons may be seriously injured, or, in exceptional circumstances, killed.

1.6 STANDARD DESIGN CRITERIA

Maglev system functions should be designed and installed so that:

1) PROBABLE mishaps are no more severe than Class IV.
2) Class III and II mishaps are IMPROBABLE, wherein
   a) Class III mishaps are at least REMOTE, and
   b) Class II mishaps are at least EXTREMELY REMOTE.
3) Class I mishaps are EXTREMELY IMPROBABLE.

PROBABLE mishaps re those anticipated to occur one or more times during the operational life of each Maglev vehicle.

IMPROBABLE mishaps include REMOTE and EXTREMELY REMOTE mishaps.

REMOTE mishaps are those not anticipated to occur during the entire operational life of a single random Maglev vehicle. However, they may occur occasionally during the total operational life of all vehicles in use on a single system.

EXTREMELY REMOTE mishaps are those anticipated to occur rarely, if at all, during the total operational life of all Maglev vehicles on any one system, but nevertheless must be considered as possible.

EXTREMELY IMPROBABLE mishaps are those so unlikely that they are not anticipated to ever occur during the entire operational life of all Maglev vehicles in the system.

* * * * *

The following four chapters of this report review each SCD contractors safety program, hazard analyses and emergency response system. For ease of reference back to the SCD documents, paragraph numbers are included in parenthesis with an abbreviation of the contractor:

- MP – Magneplane
- FM – Foster-Miller
- GR – Grumman
- BE – Bechtel

2.0 SAFETY REVIEW OF SCD – MAGNEPLANE

This chapter contains a review of the Magneplane system safety program, their hazard analyses and related issues, and their proposed emergency response strategy.

2.1 SAFETY REVIEW OF SCD SYSTEM SAFETY APPROACH – MAGNEPLANE

The Magneplane safety approach is based on MIL-STD-882. Four hazard categories were developed to classify hazards in terms of severity (MP SCD 5.3.10.1). For each category, a numerical hazard rate goal was developed for safety related failures. In addition, the safety criteria are based on the following principles:

- No single point failure shall result in a Category I or II hazard
- Any single point failure that results in a Category III or IV hazard shall be backed up by a safe mode of operation.

The Magneplane SCD also defines general safety objectives and design requirements (MP SCD 5.3.10.1.2.2 and 5.3.10.1.2.3). These objectives serve to define activities that are required to identify, evaluate and eliminate hazards. The design requirements provide guidance during system design. The following precedence is established for resolving hazards:

1) Design for minimum risk
2) Incorporate safety devices
3) Provide warning devices
4) Develop procedures and training.

2.1.1 Organization Structure

Magneplane plans to establish a safety office, however, its prescribed duties do not include actually performing safety tasks, with two exceptions (MP SCD 5.3.10.1.3):

- Software Requirements Hazard Analysis (MP SCD 5.3.10.1.3.7) where the safety office is given responsibility to perform the analysis and develop software design and test requirements
- Training (MP SCD 5.3.10.1.3.5) where the safety office is given responsibility for conducting the training.

Magneplane plans to establish a safety office responsible for planning, tracking, describing, and documenting the following tasks:

- Preliminary Hazard Analysis (PHA) (MP SCD 5.3.10.1.3.1)
- System Safety Management (MP SCD 5.3.10.1.3.2)

- Hazard Tracking and Risk Resolution
- Software Requirements Hazard Analysis (MP SCD 5.3.10.1.3.7)
- Safety Compliance Assessment (MP SCD 5.3.10.1.3.6)
- Training (MP SCD 5.3.10.1.3.5).

2.1.2 Safety Process

The following issues were evident from the Magneplane SCD:

- System level Responses and Preliminary Hazard Analysis (MP SCD 5.3.10.2) – Two types of safety analyses were performed on the current design concept: System Level Responses to system level issues such as weather, braking obstacles and control system failures were identified, and a Preliminary Hazard Analysis was performed on 13 subsystems. The findings of these analyses are discussed in Section 2.2 of this report.
- System Safety Management (MP SCD 5.3.10.1.3.2) – System Safety Management is described as planning, providing, describing and overseeing the safety effort. An explanation is not provided to discuss what organization performs the tasks that ensure the design is safe.
- Hazard Tracking and Risk Resolution (MP SCD 5.3.10.1.3.4) – The process for Hazard Tracking and Risk Resolution is not adequately presented. No entity is assigned responsibility for finding the hazards nor is a procedure for transferring hazards to the hazard log provided.
- Safety Design Requirements (MP SCD 5.3.10.1.2.3) – Eight design requirements are listed (No. 9 is not a design requirement) but there are no program tasks that describe *how* they will all be accomplished. No design requirements mention designing to quantitative risk values. Except for a brief statement in MP SCD 5.3.10.1.2.5, no quantitative design analysis is identified.

2.1.3 Schedule

The Magneplane report states that the safety office is responsible for the timely completion of safety tasks throughout the program. However, a safety program schedule is not provided.

2.2 RESOLUTION OF BASELINE HAZARDS - MAGNEPLANE

Exhibit 2-1 outlines the Magneplane hazard analysis findings and references the SCD system description. There are several issues regarding the hazard analysis process used by Magneplane during SCD development. A review of the PHA demonstrates the following concerns:

- Understanding the purpose of PHAs
- Providing a systematic and exhaustive PHA
- Identifying and categorizing the effects of hazards
- Providing a closed-loop system safety design process.

2.2.1 Understanding the Purpose of the PHA

The purpose and content of Magneplane's PHA is unclear. Although guidelines for performing the PHA are well defined and are adapted from MIL-STD-882, the PHA provided does not adhere to the MIL-STD. For example, Magneplane identifies that the following items shall be considered by the PHA (MP SCD 5.3.10.1.3.2):

- Hazardous components
- Safety related interface considerations among various elements of the system
- Environmental constraints including the operating environments
- Operating, test, maintenance and emergency procedures
- Safety related equipment, safeguards and possible alternate approaches.

These items require a complete detail design which is not available during the concept design phase of development. The analysis performed by Magneplane more closely resembles a Failure Modes, Effects and Criticality Analysis (FMECA) than a PHA.

Performing a FMECA rather than a PHA during the concept design phase of development results in the following areas of concern:

- Without knowing the effect and severity of a hazard, it is not possible for the contractor to determine whether the design baseline is acceptably safe.
- Because the design is not complete, a complete FMECA is not possible.

EXHIBIT 2-1
Magneplane
Baseline Hazards

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of System Power	*MP SCD 5.3.10.2.2.12.b* Power System failure - Single 115V or 34.5 Kv line fails Resolution: 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. Resolution: 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. Resolution: 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 protector 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. Resolution: Provide differential current protection devices.		
Loss of Control System and/or Communic-ations System	*MP SCD 5.3.10.2.2.13.6* Global Communication Center - Loss of global communications Resolution: 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.

EXHIBIT 2-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Control System and/or Communic-ations 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 Class II hazard.
Loss of Levitation and/or Guidance	*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.	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 Class I 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.

EXHIBIT 2-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Levitation and/or Guidance (continued)	*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 claims that a complete failure is extremely improbable. An analysis is required to prove that the system meets the requirements.
	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. Magway 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.
	Provide box beam continuity span expansion joints and provide electrical signal to ensure magway 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.	

EXHIBIT 2-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity Including Debris, Snow, Ice, Misalignment and Entry/Exit.	MP SCD 5.3.10.2.1.c Magway Monitoring is defined under system level responses analyses – Magway Monitoring shall be provided to detect magway problems. 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. *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. *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 severe impact. The failure of the switch to operate does not constitute an independent hazard.	MP SCD 3.2.2. Magway monitoring shall be provided and include Closed Circuit Television (CCTV), power distribution monitoring, ride quality monitoring, fencing and visual inspections. MP SCD 3.2.2.g.5. Magway Surface wear and Heating. An analysis is provided to estimate the radiated energy of the magway above the ambient temperate. Magswitch monitoring is not discussed in the SCD.	CCTV, ride quality monitoring and visual inspections may not mitigate this hazard since these measures are creative rather than proactive. The analysis of Magway heating is based on 20 second headways. Levitation sheet induced current melting of snow may result in formation of potentially dangerous ice sheets during system non-operating periods if trough drainage is inadequate. This mitigation of this hazard requires a thermal analysis to ensure that all temperature conditions are considered. This is potentially a Class I hazard. Potential ice build-up on aerodynamic control surfaces is not addressed. Magswitch monitoring is not discussed in the SCD.

EXHIBIT 2-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		COMMENTS
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Guideway Obstruction	*MP SCD 5.3.10.2.1.d Magway Obstacle Foreign objects in magway* - 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 Magway Monitoring includes: CCTV, Power Distribution, vehicle ride quality, visual inspections and structures (fencing).	This is potentially a Class 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 which are reactive to the hazard and do not mitigate the hazard. Ferromagnetic debris on the track presents a serious hazard, potentially damaging the vehicle magnet.
Fire	*MP SCD 5.3.10.2.4 Fire Protection* -Passenger injuries are probable. 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.	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.	
Evacuation and Rescue Requirements with Attention to Elevated and Tunnel Sections	*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 emergency response section of this report.)	

EXHIBIT 2-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Levitation/ Guidance/ Magnet Failure	*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. Cryogenic transfer line failure will result in loss of cryogenic helium flow to the associated cryostats. Resolution: The cryostats will be valved off to maintain the thermal capacity in the superconducting state to allow the train to reach the next magport. *Distribution header cryostat failure* will result in loss of cryogenic helium flow to the associated cryostats. Resolution: The cryostats will be valved off to maintain the thermal capacity in the superconducting state to allow the train to reach the next magport. *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. 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.		The hazards effects are not discussed. The potential hazard associated with magnet quenching induced by severe vibration or excessive shock is not addressed. 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. Concerns regarding the possible release of cryogenic gas cloud should be addressed. (Risk of cryogenic burns).

EXHIBIT 2-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Operation Restrictions	*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, magway 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 magway 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.	
Manual Override, Security, and Training	Not addressed in PHA.	Not addressed in SCD.	
Maintenance of Safe Headway	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.	

- The purpose of a PHA is to address top-level hazards that affect the system. To resolve a top-level hazard, several subsystems may be involved. For example, mitigation of the "Guideway Obstruction" hazard may require interface between the guideway monitoring and train control systems. By analyzing single failures with each subsystem, the top-level hazard cannot be completely resolved. The PHA should create criteria that pertains to resolving hazards, rather than analyzing hardware specific failure modes.

2.2.2 Providing a Systematic and Exhaustive PHA

Magneplane did not analyze the system during all phases of operation and under all operating conditions. The following are examples which should be further investigated:

- Aerodynamic controls were analyzed for four possible failure conditions including:
  - actuator failure,
  - loss of vehicle power,
  - bird strike,
  - unexpected "Hardover" operation.

  Asymmetrical control surfaces is a potentially hazardous condition that was not addressed. In addition, the severity of control surface failures is dependent upon the speed at which the vehicle is traveling. The phase of operation was not discussed.
- Failure of the communication system should require an analysis to include all functions performed by the global and wayside systems. In particular, incorrect command transmission must be analyzed in detail and safeguards must be incorporated to assure that any incorrect command transmission is adequately mitigated.

2.2.3 Identifying and Classifying the Effects of Hazards

An important purpose for performing a PHA is to analyze and classify the effects of hazardous conditions. Although Magneplane defines hazard categories in detail, there appears to be confusion in addressing the hazardous effects. The following is a list of hazards in which no effects are stated:

- Vehicle Electrical System (MP SCD 5.3.10.2.2.3.b) – Three failure conditions are analyzed but no effects are described or classified.
- Magnetic Field Shielding (MP SCD 5.3.10.2.2.8) – Two failure conditions are analyzed but no effects are described or classified.

- Box Beam/Levitation Sheets (MP SCD 5.3.10.2.2.9) – This analysis does not analyze system hazards but rather provides a list of design features intended to prevent the kinds of failures that should be identified and classified.
- Magswitch (MP SCD 5.3.10.2.2.11) – The PHA defines the vulnerability of the vehicle to certain failures while passing through a switch that could result in a Class I hazard. However, this hazard is not defined. Presumably, the hazard is that "the vehicle departs from the guideway".
- Power System (MP SCD 5.3.10.2.2.12) – The effects of power failure on the vehicle is not defined or classified. The only failure case considered was power loss. However, overvoltage and reduced voltage conditions could also have hazardous effects.
- Communications (MP SCD 5.3.10.2.2.13) – The effects of failures are not defined or classified.

Without defining the effects and seriousness of hazards, it is not possible to determine if system designs are acceptably safe. This analysis, as prepared, is not a useful tool to guide the design of a Maglev system and definition system requirements.

2.2.4 Providing a Closed-loop to the Design Process

Although Magneplane's proposed design concept largely reflects the mitigating measures outlined in their PHA, the hazards are not categorized. Therefore, it cannot be determined if the resolutions are adequate to mitigate the hazard.

2.3 IDENTIFICATION/RESOLUTION OF ADDITIONAL HAZARDS – MAGNEPLANE

Exhibit 2-2 summarizes additional hazards identified by Magneplane. There are three significant findings that were uncovered during this review:

- The hazard associated with snow/ice accumulation has not been adequately mitigated.
- Magneplane does not consider failures of the landing gear system during normal operation.
- Magneplane considers unexpected deployment of the landing gear system as a Category IV hazard.

EXHIBIT 2-2
Magneplane
Additional Hazards

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Doors and Door Interlocks	*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.	
Seating Handrails and Steps	*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.	
Landing Gear and Emergency Brakes	*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. <u>Resolution:</u> 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.

EXHIBIT 2-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Weather	*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 magway will eliminate snow and ice. Operations will continue at reduced speeds. High Winds, Hurricanes, Tornadoes - The magway 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* Magway Surface Wear and Heating - An analysis is provided to estimate the radiated energy of the Magway above the ambient temperature.	The calculations for Magway heating is based on 20 second headway.

EXHIBIT 2-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PHA REFERENCE	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Magnetic Field Shielding	*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 Resolution: 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 Resolution: 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 of fields is not discussed in the SCD

2.3.1 Snow/Ice Accumulation

Magneplane's resolution for mitigating the snow/ice accumulation includes providing Magway monitoring and relying on the heating of the Magway during normal operation. Block interface monitoring straps will monitor the magway and detect expansion and contraction due to weather. Closed Circuit Television (CCTV) will also be used to detect the level of snow accumulation. The thermal analysis that estimates the heat radiated by the magway is based on 20 second headways, and since much longer headways are likely, does not prove that snow will not accumulate. Therefore, this hazard has not been adequately mitigated.

2.3.2 Landing Gear

The hazards associated with the landing gear system have not been fully addressed. The PHA mitigates hazards and failures of the landing gear system by initiating pre-flight inspections. The more significant hazard is a failure that occurs at high speed.

An unexpected deployment of the landing gear is considered a Category IV hazard. This assessment is based on the aerodynamic controls preventing the vehicle from losing control. A further analysis is required to show that the effects of this hazard are as minimal as claimed.

2.4 EMERGENCY RESPONSE

2.4.1 Vehicle Emergency Evacuation Overall Strategy

In passenger stations, substations, maintenance areas and other areas where normal door level platforms are provided, passengers and crew will egress through the vehicle's side doors and/or window panel emergency exits.

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 (MP SCD 3.2.1.c.1.2, Vol. 2). The vehicle doors are approximately 48 inches wide allowing for two-abreast emergency egress, if necessary (MP SCD Figure 55, Section 3.2.1, Vol. 2).

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 (MP SCD 3.2.1.c.3.15.3.8, Vol. 2). These emergency exits are specified as aircraft Type I which must have rectangular openings sized no smaller than 24 x 48 inches.

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 (MP SCD Section 3.2.1.c.1.4, Vol. 2) shown in Exhibit 2-3. The staircase shown in Exhibit 2-3 integrated with the hatch door to assist in emergency egress, is not included in the SCD design.

The track trough structure where the evacuated passengers/crew will walk is comprised of a fiber-reinforced plastic curved support structure for propulsion system LSM windings (MP SCD 3.2.2.b.5, Vol. 2 and Figures 31 and 32, Section 3.2.2, Vol. 2). This LSM winding support structure is designed to withstand considerable linear motor induced loading (MP SCD 3.2.2.b.4, Vol. 2) and thus will not be compromised by the additional loading of egressing passengers. The radius of the track trough cross section is 2.1 meters (MP SCD Figure 1, Section 3.1.2, Vol. 1). Accordingly, the local curvature of the trough walkway, shown in Exhibit 2-3, should not impede safe movement along the track. The track walkway height increase from the trough center to the edge of a nominally 0.5 meter wide "single-file walking right-of-way" is about 1.4 cm.

Evacuated passengers egress from the track trough to a safe location 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 track guideway. This hinged stairway will swing over the track trough, shown in Exhibit 2-4 (MP SCD Figure S-11, final page of Vol. 7B), to allow the passengers/crew to climb out of the track trough and over the track side box beams. Such hinged stairways and associated local emergency platforms will be provided "at intervals" along the guideway length (MP SCD 5.3.10.2.3, Vol. 5). The suggested maximum spacing between these egress locations and an emergency platform is specified by the SCD to be approximately 0.76 km.

The local emergency platform allows for transferring passengers/crew to a standard revenue system Maglev "rescue vehicle" (MP SCD 5.3.10.2.3, Vol. 5), either on the same track or an adjacent track, shown in Exhibit 2-4. 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 Exhibit 2-4, will provide access to the station platform.

A wider stairway "may be provided" from the local emergency platforms to ground level, shown in Exhibit 2-4. These stairways will be counterbalanced for self-stowing and will be normally inaccessible from the ground (MP SCD 5.3.10.2.3, Vol. 5).

The SCD does not address the issue of system reactivation activities; there is no mention of checking if guideway tracks 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 (MP SCD 3.2.2.i.3, Vol. 2).

EXHIBIT 2-3
Magneplane Proposed Vehicle Emergency Egress Means
Vehilce To Guideway Egress

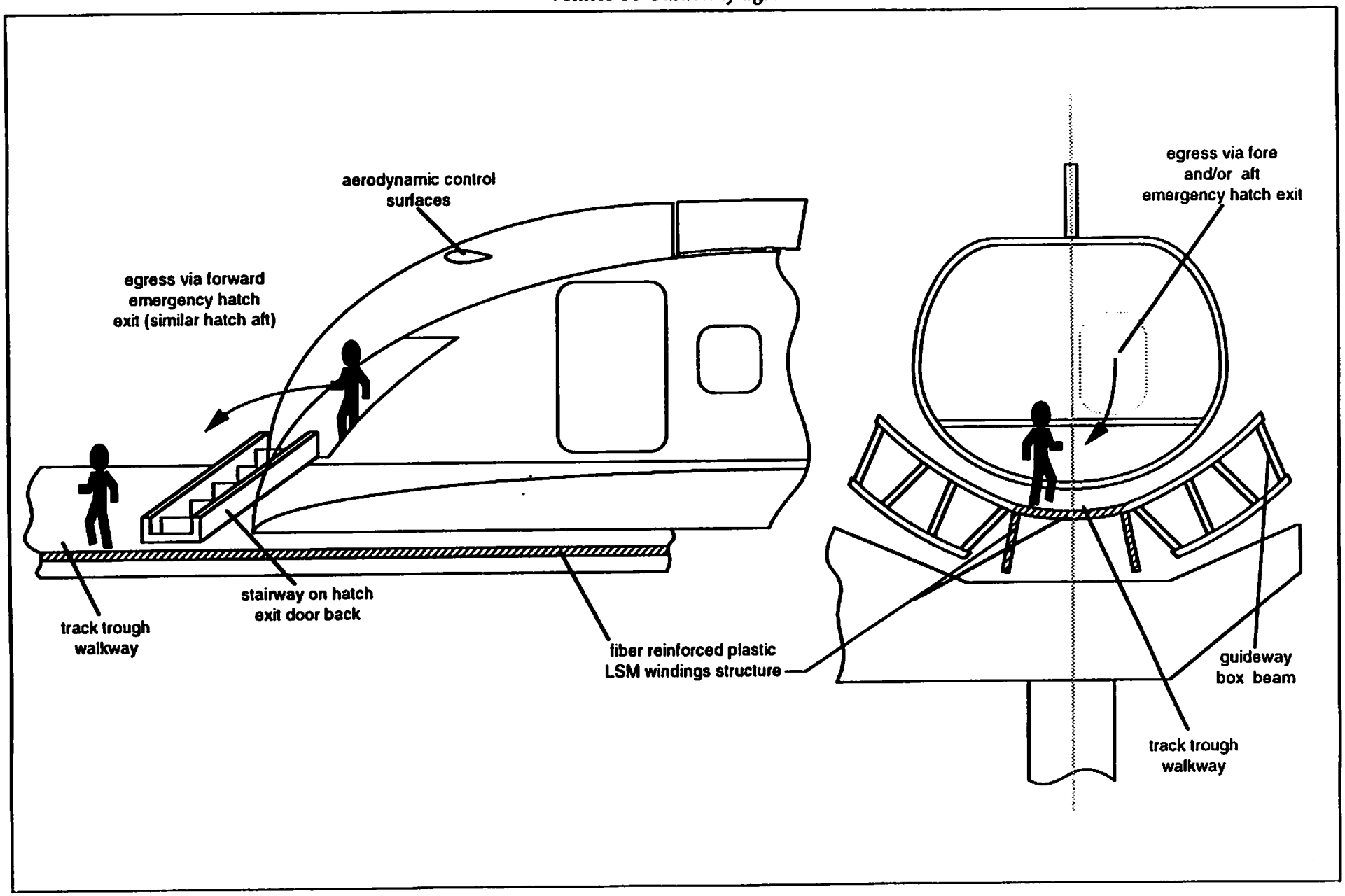
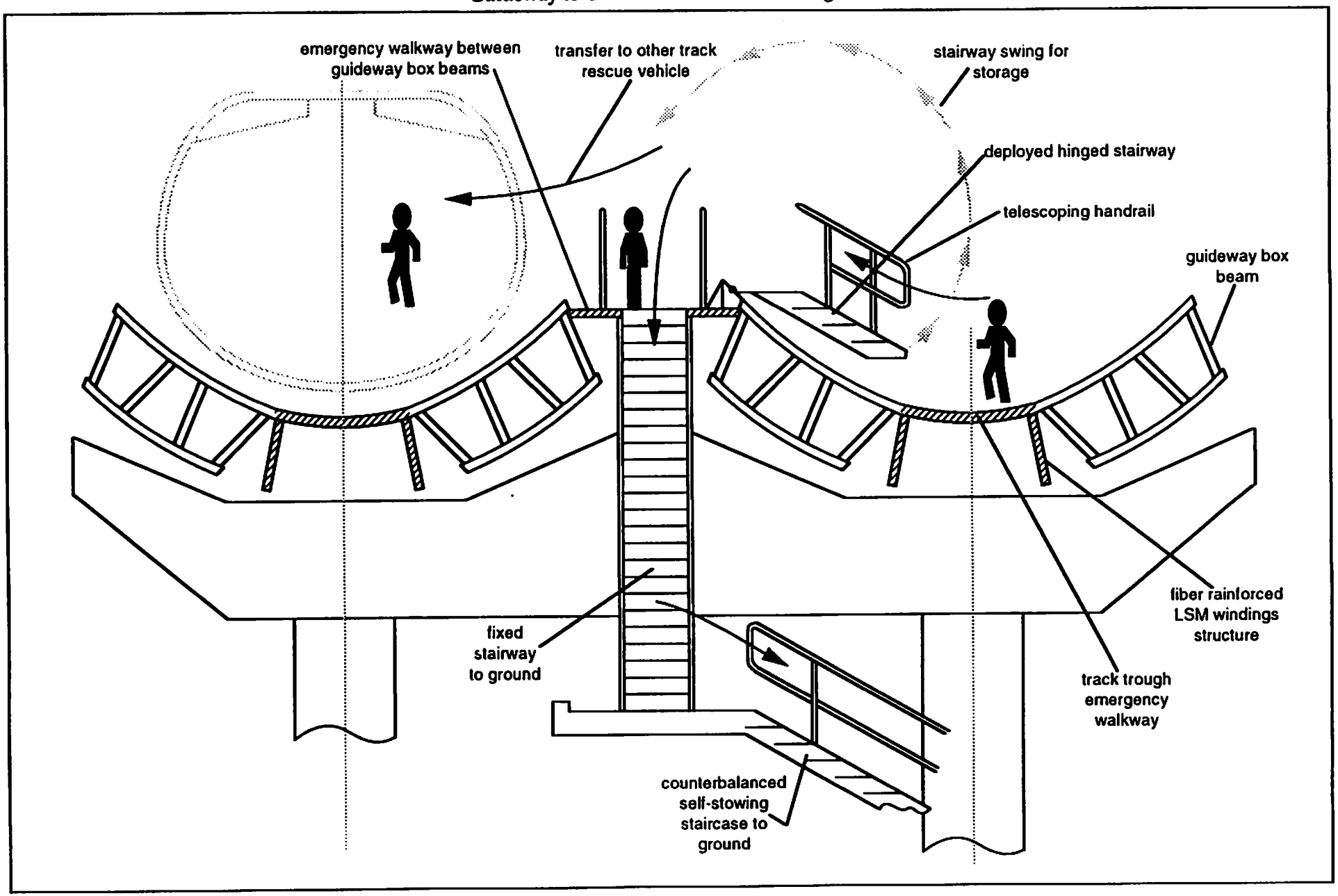


EXHIBIT 2-4
Magneplane Proposed Vehicle Emergency Egress Means
Guideway to Ground or Rescue Vehicle Egress



2.4.2 Vehicle Emergency Evacuation Within Guideway Switch Zones

The Magneplane system guideway switching concept widens the track trough by increasing trough flat bottom width to form a track side branch (MP SCD 3.2.2.d of Vol. 2). A vehicle traversing the switch section at speed is electrodynamically guided along either the switch-trough branch 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 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.

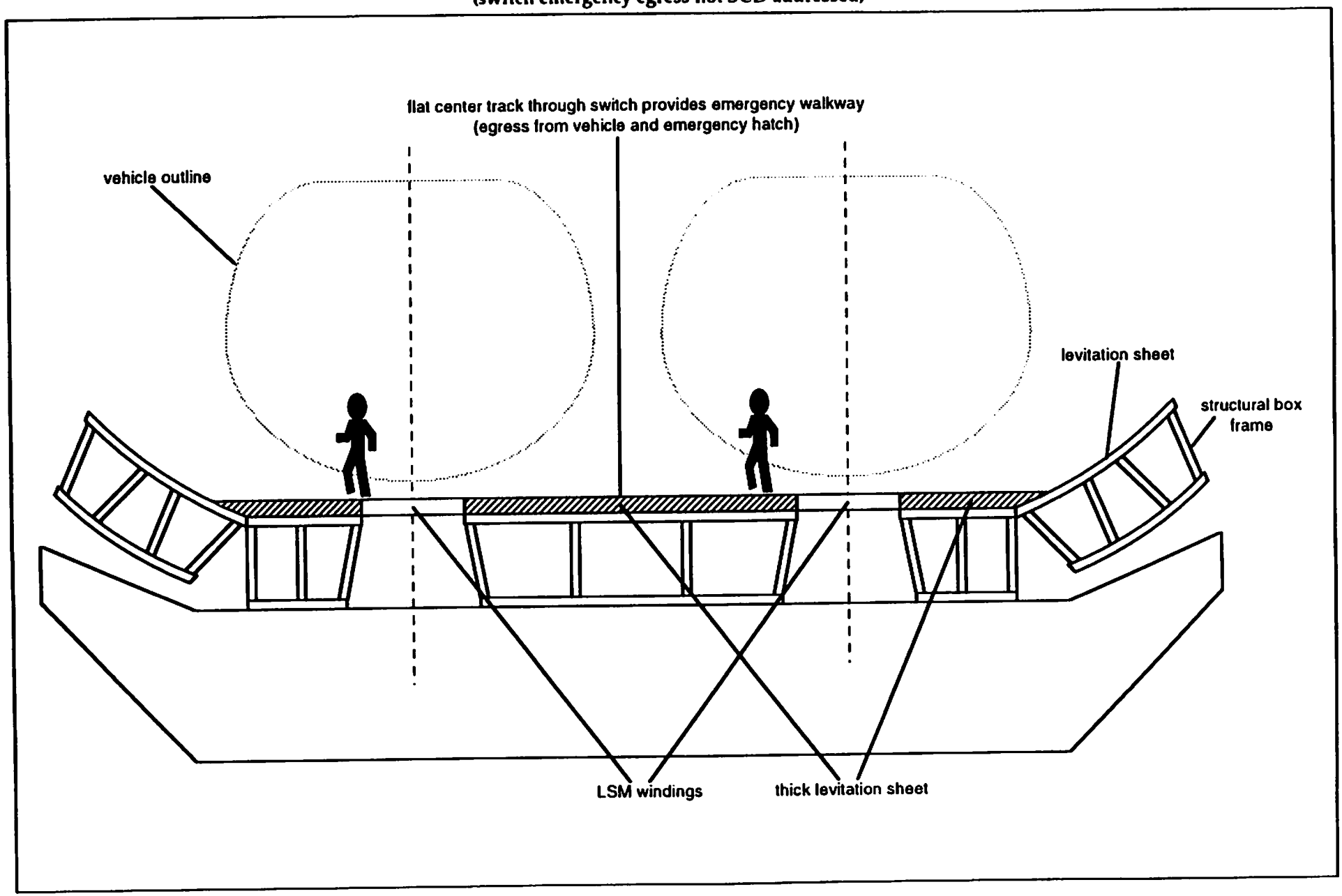
Spaces on each side of the embedded null-flux loops and LSM windings are completely filled with concrete to provide a flat running surface, shown in Exhibit 2-5. This flat surface is required for the air suspension pads which extend downward from the sides of the vehicle when it is traversing through 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 track 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.

2.4.3 Vehicle Emergency Evacuation Within Superelevated Track Guideway Curve Zones

The Magneplane vehicles are physically free to roll within the guideway track semi-circular trough when traversing curves, but are limited by electrodynamic side forces. The side forces tend to act about the vehicle roll axis to keep the vehicle propulsion magnets almost directly under the track LSM magnets (known as vehicle "keel effect") (MP SCD 3.2.2.g.4, Vol. 2). The guideway track troughs are effectively "superelevated" through current because the track's banking results in essentially zero lateral forces relative to the vehicle's fixed axis for trains traversing the curve at the designed speed (MP SCD 1.5 and 1.6, Vol. 1). The track effective "superelevation" through curves is implemented by means of the appropriate angular displacement of the LSM windings and the associated side levitation plate box structures about the center of the trough cross-sectional curvature.

During emergency stopping on a guideway track curve, the vehicle "keel effect" roll stiffness will progressively diminish as the speed decreases towards zero. This allows the vehicle to roll in toward a horizontal position using the pendulous action caused by gravity; the vehicle is supported on low speed air-lubricated landing pads which provide almost negligible resistance to vehicle roll motion. The pendulous action occurs because the vehicle's center of gravity is vertically below the center of the track trough cross-sectional curvature.

EXHIBIT 2-5
Possible Application of Magneplane Emergency Egress Means to Proposed Passive Lateral Switch Design Concept (switch emergency egress not SCD addressed)



Any vehicle stopped on a guideway curve will be horizontally level. A substantially level 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. For the tangent track case, the track walkway may be located on the track box structure levitation sheet portion of the track trough, and not on the LSM winding support structure if the superelevation induced track "bank angle" is high, such as the bank angle of a curve designed for high speed. However, this track levitation sheet walkway would likely not be perceived by evacuating passengers/crew to be any different from a tangent track LSM winding support structure walkway.

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

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. (MP SCD 3.2.1.c.3.15.3.8, p.72, Vol. 2).

A 90 second vehicle emergency evacuation duration is considered adequate for a Maglev vehicle where the risk of rapid fire spreading and/or explosion is lower than the risks associated with aircraft, due to the lack of large quantities of liquid fuel on-board. The Maglev vehicle fire protection requirements should be in accordance with aircraft requirements (MP SCD 5.3.10.2.4, Vol. 5).

The SCD proposes using only single vehicles in revenue service with 45 or 140 passenger capacity. System capacity will be attained by operating vehicles at very low headways relative to existing public guided ground transport system operating practice. The option of designing larger single vehicles for a larger eventual system capacity is also suggested for possible longer term upgrading of the system (MP SCD 1.8, Vol. 1).

Current vehicle passenger capacity design standards require each Magneplane vehicle fore and aft hatch-type exits to evacuate 23 or 70 passengers, respectively, within the specified 90 second evacuation duration in the event of an emergency (i.e., a maximum of one passenger every 1.3 seconds). Awkwardness of egress from the hatch-type exits, evident from Exhibit 2-4, makes realization of a 90 second evacuation unlikely, at least for a 140-passenger vehicle.

The FAA has proposed requirements for commercial aircraft that the maximum distance from any seat row to the nearest exit be 9 meters (30 ft.). This requirement is easily satisfied by the proposed Maglev vehicle cabin layout for normal entry/exit doors, but not for the emergency hatch exits.

2.4.5 Emergency Response Information Communication Means

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 (MP SCD 3.2.1.k.15, Vol. 2).

The SCD specifies the need for at least one attendant to be on-board each Maglev vehicle in transit (MP SCD 3.2.1.k.19, Vol. 2). 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 will be transmitted to the vehicle attendant. The attendant will notify the passengers via the on-board public address system or a provided megaphone (MP SCD 3.2.1.c.4, Vol. 2) 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 need to be addressed in subsequent program phases.

2.4.6 Provision for 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 (MP SCD 3.2.1.g, p.120, Vol. 2). 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.

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 very limited supply of emergency power. There should be sufficient thermal capacity in the superconducting magnet dewars to provide for electrodynamic suspension for the relatively short duration of 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 (MP SCD 3.2.1.d.2, Vol. 2). Presumably, low speed landing air pads can 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 can be realistically eliminated for the duration of vehicle emergency stop deceleration and urgent evacuation procedures without causing undue passenger discomfort.

It may be advisable for purposes of emergency evacuation and safety assurance, to provide a very modest capacity emergency battery power supply system aboard the vehicle, which is completely separate from the primary on-board battery supply subsystem.

2.4.7 Advantages of SCD Proposed Emergency Response Vehicle Evacuation Means

Emergency evacuation from a stopped vehicle onto the guideway track trough will be available over the entire guideway length, including track 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 track walkway to a "safe location" will be provided via a hinged staircase for egress over the track box beam onto a track-attached local emergency platform, then either via a staircase to ground level or from the platform into a Maglev rescue vehicle.

2.4.8 Disadvantages of SCD Proposed Emergency Response Vehicle Evacuation Means

In emergencies passengers and crew will egress onto the guideway track, not onto a dedicated walkway physically separated from the operational tracks. 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 number of passengers required to egress through the hatch-type exits at the front and rear of a vehicle may be too high to realize the 90 second goal, at least for the 140 passenger vehicle design.

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 disabled and/or elderly passengers.

3.0 OVERVIEW OF SCD - FOSTER-MILLER

This chapter contains a review of the Foster-Miller system safety program, their hazard analyses and related issues, and their proposed emergency response strategy.

3.1 OVERVIEW OF SCD SYSTEM SAFETY APPROACH - FOSTER-MILLER

3.1.1 Organization Structure

There is no discussion of a safety organization provided by Foster-Miller. A statement is made that safety and reliability plans will be provided in the final version of the report. However, DOT form DOT F 1700.7 says that the present report is the final report for this contract. Under the heading of "Reliability Considerations" an integrated analytical approach involving safety, reliability, and maintenance activities is described, but no organizational structure for implementing it is defined.

3.1.2 Safety Process

The following issues were evident from the Foster-Miller SCD:

- **Safety Assurance (FM SCD 7.1)** - Foster-Miller provides a general summarized discussion of their baseline design approach to Fire Control, Evacuation, Lightning Protection, Door Operation, Guideway Integrity, Human Factors, and Magnet Quench Prevention. Their overall safety strategy appears to deal with most critical failures and malfunctions by bringing the train to a controlled safe stop and evacuating the passengers onto a protected walkway. All other safety topics, including their version of PHAs, referred to as "Safety Hazard Screening," are covered under the heading of Reliability Considerations.
- **Integrated Analytical Approach (FM SCD 7.2.1)** - Foster-Miller describes an "Integrated Analytical Approach" which aggregates the treatment of safety, reliability, and maintenance activities during the design process. While there is much that can be said in favor of this approach, Foster-Miller does not address the organizational issues associated with such integrated efforts.

The proposed Mission/Safety MTBF Matrix is intended to relate the impact of failures on safety and system availability in a new and novel way. The matrix is a complex rearrangement of the Hazard Risk Index found in MIL-STD-882B using quantitative values instead of qualitative judgments about the allowable frequency of undesired events. It presents 25 possible rankings for such events, which are too many to be meaningful for design requirements. By comparison, MIL-STD-882B provides 20 rankings, and FAA Advisory Circular 25.1309-1A provides four, which is about right for design guidance purposes.

In the discussion of the source of the values used in the Mission/Safety Matrix there are two apparent errors:

- The quotation from the FAA Advisory Circular on Federal Aviation Regulation 25.1309 is from the obsolete version that was canceled in 1988 and replaced with AC 25, 1309-1A. The correct maximum probability for any catastrophic failure condition is 1×10^{-9} for each flight hour.
- The domestic fleet average delay and cancellation rate due to airplane-chargeable equipment failures is really on the order of 3%, three times greater than stated.

A brief discussion on the Foster-Miller philosophy for setting allowable failure rates for design indicates a misunderstanding of the subtle but critical differences between failure rates and probabilities and the role of each in designing safe system functions. A numerical value is shown for redundant aircraft engine control systems that is referred to as a failure rate but is more likely a probability. The number is presumably derived from an MTBF given for a single control system, but no calculations are given and the numbers are not reconcilable by any direct relationship.

- **Safety Hazard Screening (FM SCD 7.2.2)** - Foster-Miller describes "safety screening" of the design concept as roughly corresponding to a MIL-STD-882 Preliminary Hazard Analysis. The identified hazards (called "Causes" by Foster-Miller) are essentially high-level generic events of external origin. They are divided into three categories:
  - Human origin
  - Weather related
  - Miscellaneous.

There is no classification of the effect of the identified hazards to the Mission/Safety Matrix proposed by Foster-Miller. The safety screening results are of little value for showing how Foster-Miller has or will"...identify, assess, resolve, and follow-up potential safety-critical hazards and unsafe conditions for each Maglev system...". The system design descriptions provided elsewhere in the report are more useful than the safety screening results for understanding the safety features of their baseline design.

- **System Reliability (FM SCD 7.2.3)** - Under this heading, two case studies are used to demonstrate the Foster-Miller tradeoff analysis methodology. One is on mechanical versus electronic switching, and the other is on onboard versus batch mode refrigeration. The quantitative portions of both analyses are questionable as to correctness. The switch analysis, for example, uses generic source data that is known to vary widely in different applications, contains several mathematical errors, and states quantitative conclusions with no substantiation or derivation. These analyses also indicate that the Foster-Miller "integrated analytical approach" may be causing some confusion by mixing safety issues with reliability issues.

3.1.3 Schedule

There is no safety program schedule provided in the Foster-Miller Maglev Development Plan. There is a line item "Safety Testing" in the full-scale test program, and a "Safety/Egress/Fire Suppression" line item included in the system analysis task schedule.

3.2 RESOLUTION OF BASELINE HAZARDS – FOSTER-MILLER

Exhibit 3-1 outlines the Foster-Miller hazard analysis findings and corresponding references to the SCD design plan. The PHA methodology used by Foster-Miller during the hazard analysis process raises several issues:

- A systematic PHA process is not evident
- Methods for identifying and categorizing the effects of hazards are not included
- There is no closed-loop process which ensures that hazard resolutions are incorporated in design plans
- Excess burden is placed on maintenance actions for ensuring safety.

EXHIBIT 3-1
Foster-Miller
Baseline Hazard Resolution

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of System Power	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. Resolution: Provide redundant power station and system wide dynamic braking if power loss occurs.	*Section 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 Class II hazard. The resolution of this hazard is to provide redundant power stations, however, the SCD addresses a single string system. It is apparent that the author of the safety hazard analysis and the designers have not communicated to resolve this hazard. 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. Resolution: 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. Resolution: Design guideway to accommodate maintenance vehicles on guideway.		Maintenance vehicles on the guideway is 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. Resolution: Provide back-up power supply.	Section 5-4 System Power Utilization - Back-up power is not discussed.	Loss of back-up power is potentially a Class II hazard.

EXHIBIT 3-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Control System and/or Communication System	Table 7-2 - - p. 7-14 through 7-18. *Cut fiber optic wires to guideway coils* resulting in loss of propulsion control. Resolution: Make it difficult to get at wires and control braking by controlling bus voltage. Table 7-2 - - p. 7-14 through 7-18. *Collision with trains* resulting in damage to trains and fatalities. Resolution: Provide sensors to detect trains and stop trains before collision. Make trains crashworthy.	Section 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). Section 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.	Methods for installing fiber optics is 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, expected to operate in 933 MHz band. Loss of propulsion control is potentially a Class I hazard since the braking and propulsion systems are interrelated. A zonal, installation analysis is required.
Loss of levitation or guidance	Not addressed in hazard analysis		This is potentially a Class 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.

EXHIBIT 3-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity Including Debris, Snow, Ice, Misalignment, Entry/Exit	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.	*Section 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 Class I catastrophic hazard.
	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. Resolution: Guideway to train sensors to detect objects. Redundant train systems.	*Section 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 Class I catastrophic event. The resolution in the PHA does not adequately resolve the hazard.

EXHIBIT 3-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	ISSUES
Loss of Guideway Integrity Including Debris, Snow, Ice, Misalignment, Entry/Exit (continued)	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. Resolution: Isolate passengers from guideway similar to aircraft boarding.	Not addressed in SCD.	This is potentially a Class II hazard. The superconducting magnet cryostats are particularly prone to damage from ferromagnetic debris impact due to magnetic attraction.
	Table 7-2 - - p. 7-14 through 7-18. *Objects consistently and randomly found on guideway routes.* Resolution: Maintenance locate and remove objects. Develop public awareness programs.	*Section 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 Class 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. Resolution: Probe vehicle after maintenance.	Not addressed in SCD.	This is potentially a Class 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. Resolution: Reinforce front and remove windows.	Not addressed in SCD.	Design criteria should be developed that prevent objects from being hung in front of the train.

EXHIBIT 3-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity Including Debris, Snow, Ice, Misalignment, Entry/Exit (continued)	Table 7-2 - - p. 7-14 through 7-18. *Snow* - Impair visibility and build-up on guideway. Resolution: Slanted guideway surfaces.	Section 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. Resolution: Slanted guideway surfaces.	Not addressed in SCD.	This is potentially a Class 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. Resolution: 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 Class 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. Resolution: 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.
	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 low probability hazard.
Guideway Obstruction	See - Loss of guideway integrity including debris, snow, ice, misalignment, Entry/Exit (above)		

EXHIBIT 3-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Fire	Table 7-2 - - p. 7-14 through 7-18. *Train damage, chemical vapors, fatalities and injuries* Resolution: Fire detection and suppression system.	Section 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.	This is potentially a Class 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 Requirements with Attention to elevated Guideway and Tunnel Sections	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. Table 7-7 - - p. 7-28 through 2-29 *Handicap egress from train on elevated guideway.* Resolution: 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. Resolution: Provide air slides, fireman's tube, walkways on guideway. Repelling concept utilizing seat belts. Provide spring loaded ropes.	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.	

EXHIBIT 3-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Levitation, Guidance, Magnet Failure	Not addressed in Hazard Analysis		Loss of part or all magnetic suspension represents a significant safety issue. Hazards relating to magnet quenching due to vibration, impact, loss of coolant and cryostat vacuum failure need to be addressed.
Operational Restrictions	Not addressed in Hazard Analysis	Section 6.2 5- Major Failure Mode and Recovery - Two or more 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.	
Manual Override, Security and Training	Not addressed in Hazard Analysis		
Maintenance of Safe Headway	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.	Section 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 unlikely hazard. Software safety should be based on quality assurance, documentation of code, and verification/validation of software.

EXHIBIT 3-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Weather Conditions and Constraints	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 need to be addressed.

3.2.1 Providing a Systematic PHA Process

Foster-Miller proposes the use of a "Hazard Screening" process that approximately corresponds to a MIL-STD 882 type PHA. The Foster-Miller hazard screening process only considers hazards caused by external events. There is no mention of hazards that result from subsystem malfunction or human error. The hazards identified (called "Causes" by Foster-Miller) are essentially high-level generic events of external origin. Each "cause" has associated resolutions required to mitigate the hazard. These are not specific and do not relate to safety issues that apply to Maglev. For example:

- To mitigate an "automobile/truck collision with train at ground level" hazard, the Foster-Miller PHA suggests implementing grade crossing gates "similar to existing ones for railroads". Although Foster-Miller discusses the guideway and automobile roads on the same grade, for a train moving 134 m/s (300 mph), total grade separation is probably essential. A collision is potentially catastrophic and should have been classified properly.
- To mitigate a "snow" hazard, "slanted guideway surfaces" are proposed. But accumulation of snow on slanted surfaces is common and further analysis is needed.
- To mitigate a "cut fiber optic wires to guideway coils" hazard, the analysis recommends: "make it difficult to get at wires". Design and installation requirements to protect the fibers should also be addressed.
- To mitigate a "computer virus" hazard, "antivirus software" should be installed. Mitigating computer viruses are probably the least important element of a well structured software development process.

3.2.2 Effects of Hazards

The effects of identified hazards are not classified with respect to the Mission/Safety Matrix proposed by Foster-Miller. This results in an analysis that is of little value because it cannot be determined how Foster-Miller will "identify, assess, resolve, and follow-up potential safety critical hazards and unsafe conditions for each Maglev system."

3.2.3 Providing a Closed-Loop to the Design Process

There appears to be minimal coordination between the hazard analysis and the SCD design definition. The following examples demonstrate the lack of communication between the safety engineer and design engineers:

- The "Hazard Screening" resolution of the guideway obstruction hazard only addresses incorporating train sensors to detect objects. However, section 3.9 of the SCD defines four methods for identifying guideway obstruction, including:
  - Vehicle systems to record vehicle passage for deterioration, misalignment, excessive precipitation build-up, harsh weather and presence of object
  - Embedded fiber optic sensors to monitor guideway integrity
  - Security fencing, overhead shielding and video incident detection
  - Drone inspection of the entire route.
- The "Hazard Screening" resolution for a fire hazard only includes incorporating a fire detection and suppression system. However, section 7.1.2 of the SCD describes several steps for mitigating a fire hazard including:
  - Ensuring fire codes, as defined by the FRA, are achieved
  - Incorporating fire retardant materials into the design
  - Providing back-up power for emergency lighting and ventilation.

The design approaches recommended to control hazardous events are not specific. For example, they recommend some broad, general approaches such as "redundant train systems," "public awareness," "shielding methods," "backup power supply," etc. which are truisms for any design approach, but not helpful in assessing Foster-Miller's understanding of hazards in their baseline design.

3.2.4 Maintenance Actions to Ensure Safety

Throughout the PHA, Foster-Miller places the burden for ensuring safety on maintenance actions. For example:

- To mitigate "environmental corrosion of the guideway and train components", maintenance personnel will perform periodic inspections similar to aircraft. During the conceptual design phase of development, criteria should be developed to eliminate or control corrosion such as choosing non-corrosive materials, ensuring proper drainage of guideway and providing drain loops in vehicle wire bundles.
- To mitigate "objects consistently and randomly found on guideway routes" hazard, maintenance personnel will locate and remove objects. Maintenance cannot be expected to effectively perform this task over the entire guideway.
- To mitigate "magnetic dust/clay builds up on train/guideway magnets" hazard, maintenance personnel will perform periodic cleaning. Since the hazard severity is not identified, the interval of these inspections is not clear. If the frequency is too short, high maintenance costs may result. If the frequency is long, management controls must be put in place to ensure the cleaning is performed.

3.3 IDENTIFICATION/RESOLUTION OF ADDITIONAL HAZARDS - FOSTER-MILLER

Exhibit 3-2 outlines additional hazards identified by Foster-Miller. The findings/issues are similar to those discussed for the baseline hazards. Additional hazards are better discussed in sections of the SCD other than in the PHA "Hazard Screening" process. For example, Foster-Miller examines environmental issues, such as vibration, EMI and noise requirements in detail in Chapter 8, but they are not discussed in the PHA.

The PHA and SCD descriptions do not always agree. For example, the safety analysis recommends that maximum braking rates be limited to 0.2 gs. However, the SCD claims that braking levels may potentially reach deceleration levels as high as 0.25 gs. This demonstrates that Foster-Miller's "Integrated Analytical Approach" to the treatment of reliability, safety and maintenance may not be a closed loop process.

EXHIBIT 3-2
Foster-Miller
ADDITIONAL HAZARDS

ADDITIONAL HAZARD	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Vehicle Guideway Dynamics	Table 7-2 - - p. 14 through 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.	
Electro-magnetic Interference and Compatibility	Table 7-2 - - p. 7-18. EMI fields passenger and crew exposure. Communication control and data processing malfunctions. Resolution: Shielding methods and study effects on humans.	Section 8.3 discusses EMI in detail.	
Noise and Vibration	Not addressed in PHA	Section 18.1 discusses noise and vibration in detail.	External aerodynamic noise can represent a significant hazard
Magnetic Radiation	Table 7-2 - - p. 7-18. EMI fields and passenger exposure. Potential communication control and data processing malfunctions. Resolution: Shielding methods and study effects on humans.	Section 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.
Electrical Shock	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.	

EXHIBIT 3-2 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Braking	Table 7-2 - - p. 7-18. Passenger comfort and safety of seat belted and standings. Resolution: 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. Section 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 needs to be addressed.
Vehicle does not stop at station	Not addressed in PHA.	Not addressed in SCD.	
Doors	Not addressed in PHA.	Section 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.

3.4 EMERGENCY RESPONSE

3.4.1 Vehicle Emergency Evacuation Overall Strategy

The 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 (FM SCD 7.1.3).

Three options for emergency egress from stopped vehicles are listed:

- Lateral egress via the normal entry/exit doors onto a guideway supported emergency walkway, shown in Exhibits 3-3 and 3-4 for single and for dual track guideways, respectively. (Option A)
- 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 Exhibit 3-5. (Option B)
- 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 Exhibit 3-6. (Option C)

It should be noted, with respect to the fore/aft egress option, that the staircase shown in Exhibit 3-3 is integrated into the hatch door to assist in emergency egress from the vehicle and is not included in the SCD design. Also, in reference to the fore/aft egress option "B", the Foster-Miller vehicle design provides for emergency egress from one vehicle to another within a train set via vehicle end centered passageways which are partly surrounded by the train set articulated magnet bogies. Limiting crew and passenger access to inter-vehicle passageways to emergency situations eases the magnetic field shielding requirements for these passageways.

All three vehicle emergency egress options can accommodate passenger/crew egress from the guideway walkways to ground level via emergency staircases, shown in Exhibits 3-3, 3-4, 3-5 and 3-6. These staircases will be located at intervals along the length of the track.

Both the lateral and the fore/aft vehicle emergency egress options can also accommodate egress from guideway walkways to Maglev rescue vehicles, shown in Exhibits 3-3, 3-4 and 3-5. In the downwards egress option, movement from the below-track suspended walkway backup into a Maglev rescue vehicle on the same track is not practical because of safety risks associated with deploying the rescue vehicle floor hatch staircases or ladders onto the suspended walkway.

EXHIBIT 3-3
Foster-Miller Proposed Vehicle Emergency Egress Means
Option A: Preferred Vehicle Side Egress Option – Single Guideway

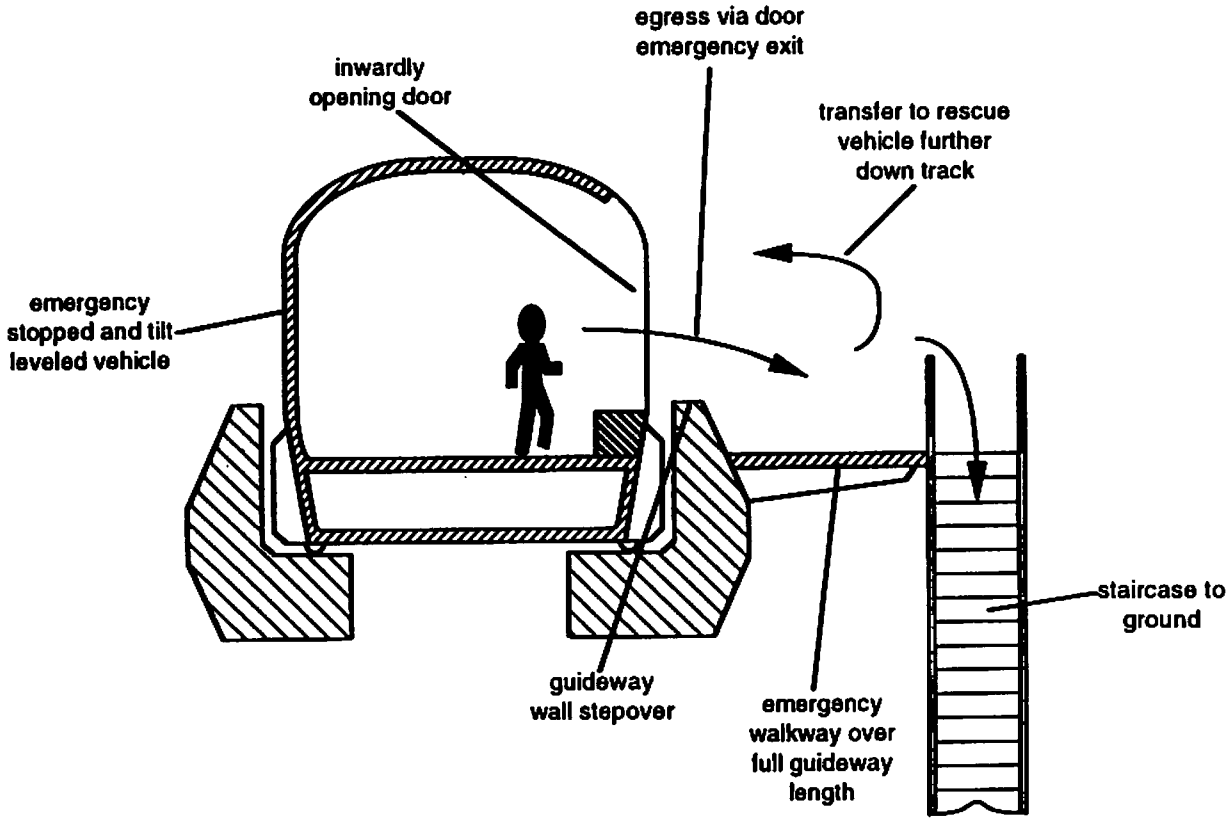


EXHIBIT 3-4
Foster-Miller Proposed Vehicle Emergency Egress Means
Option A: Preferred Vehicle Side Egress Option – Dual Guideway

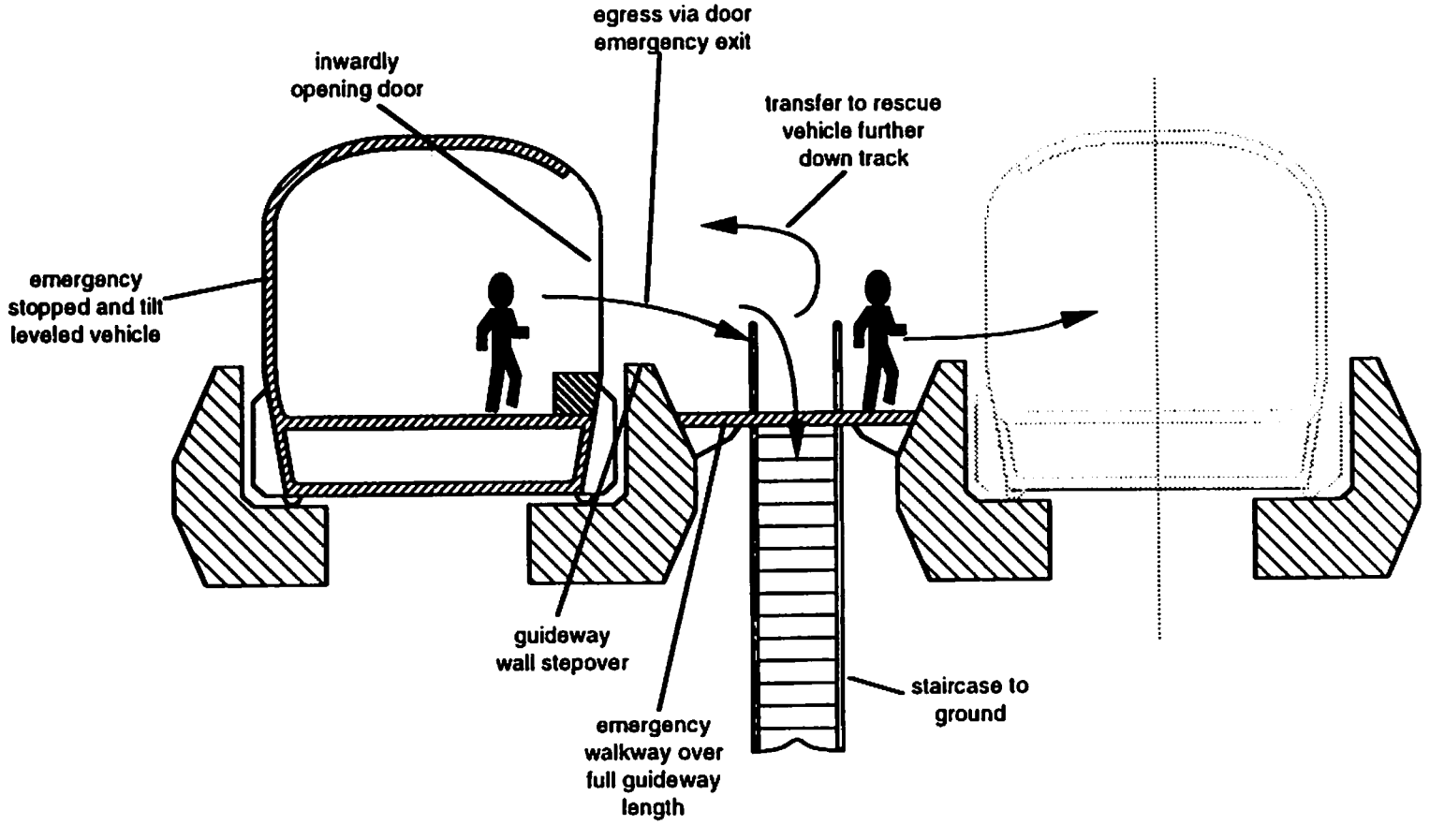


EXHIBIT 3-5
Foster-Miller Proposed Vehicle Emergency Egress Means
Option B: Vehicle Alternative End Egress Option

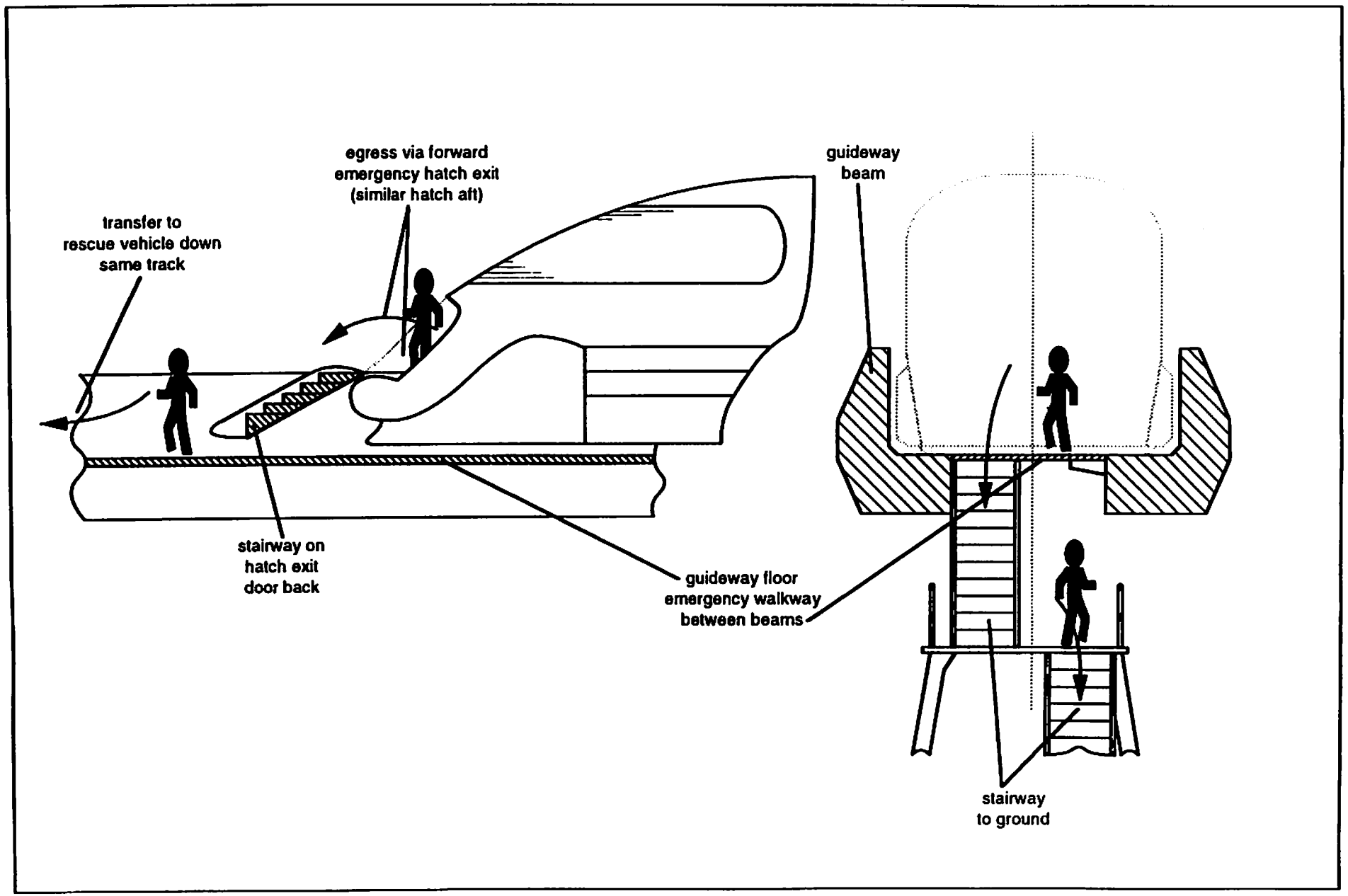
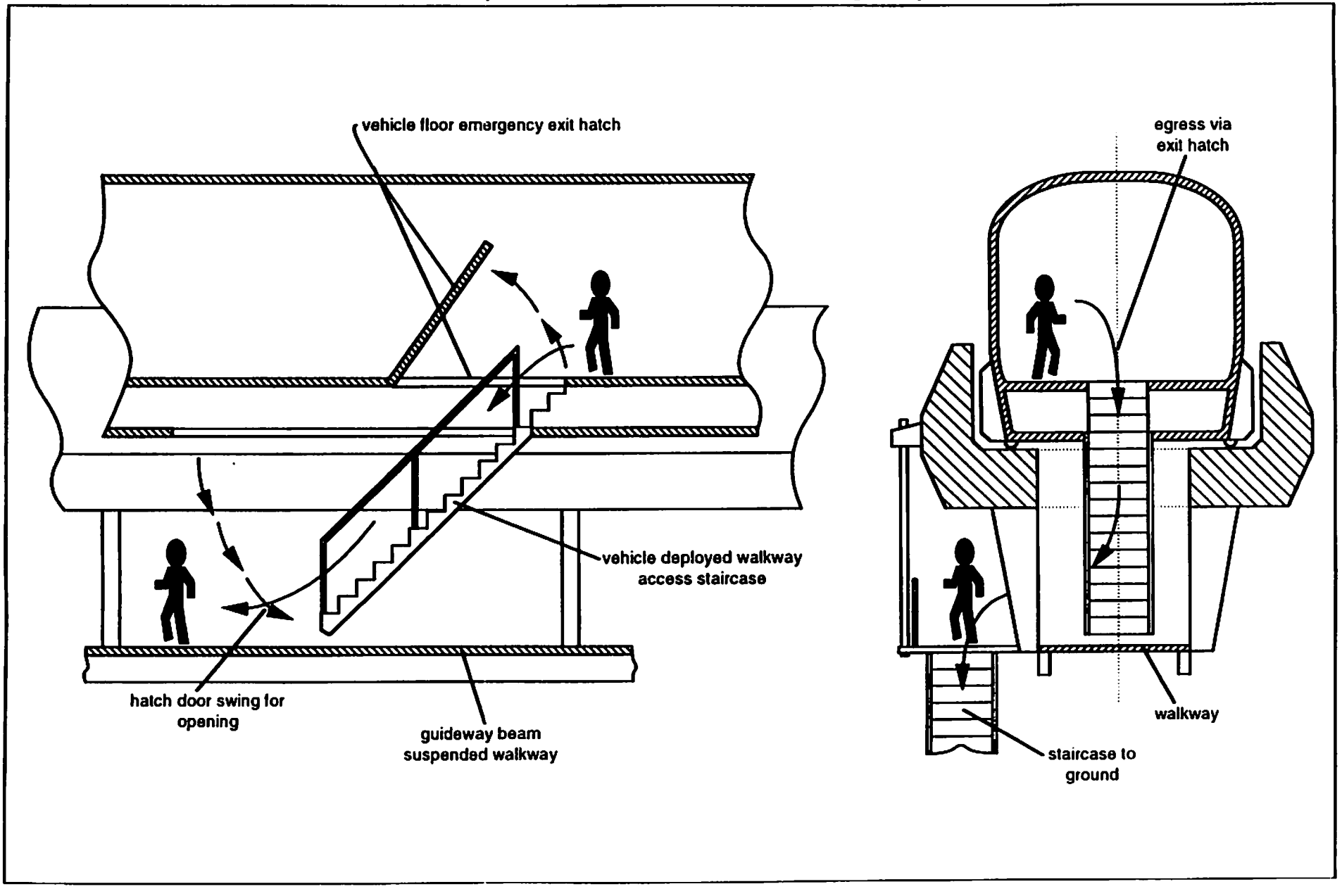


EXHIBIT 3-6
Foster-Miller Proposed Vehicle Emergency Egress Means
Option C: Vehicle Alternative Downward Egress Option



The SCD does not explain how the suspended walkway is configured to handle the obstruction caused by guideway pylons. One option is to split the top of the pylons into two columns, but this greatly complicates pylon design and increases capital cost.

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 (spaced at 5-6 meter intervals between the track structural beam sidewalls). Currently, the 1.4 meter square vehicle floor exit (FM SCD Figures 2-33 and 2-34) 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.

The SCD proposes standardized 24.7 meter 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 one door on each side near both the front and rear of the vehicle passenger cabin. The vehicle doors are 1.37 meters (54") wide allowing for two-abreast emergency egress, if necessary, for lateral egress option "A" (FM SCD Figure 2-3). As shown in Exhibits 3-3 and 3-4, the guideway track sidewall will constitute a 0.46 meter (18") high obstacle to lateral egress from the vehicle doors to the emergency walkway. Presumably, deployable steps with folding handrails will assist disabled and elderly passengers from the vehicle to the emergency walkway.

3.4.2 Vehicle Emergency Evacuation Within Guideway Switch Zones

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

- A vertical switch design, shown in Exhibit 3-7, used for high speed mainline application; designated as switch Type I
- A lateral switch design, shown in Exhibit 3-8, used primarily for intermediate speed off-mainline application (e.g., in the vicinity of stations); designated as switch Type II
- A lateral switch design, shown in Exhibit 3-9, 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 Exhibit 3-7, 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

EXHIBIT 3-7
Possible Application Of Foster-Miller Emergency Egress Means To Proposed Type I – High Speed Vertical Switch Design Concept (switch emergency egress not SCD addressed)

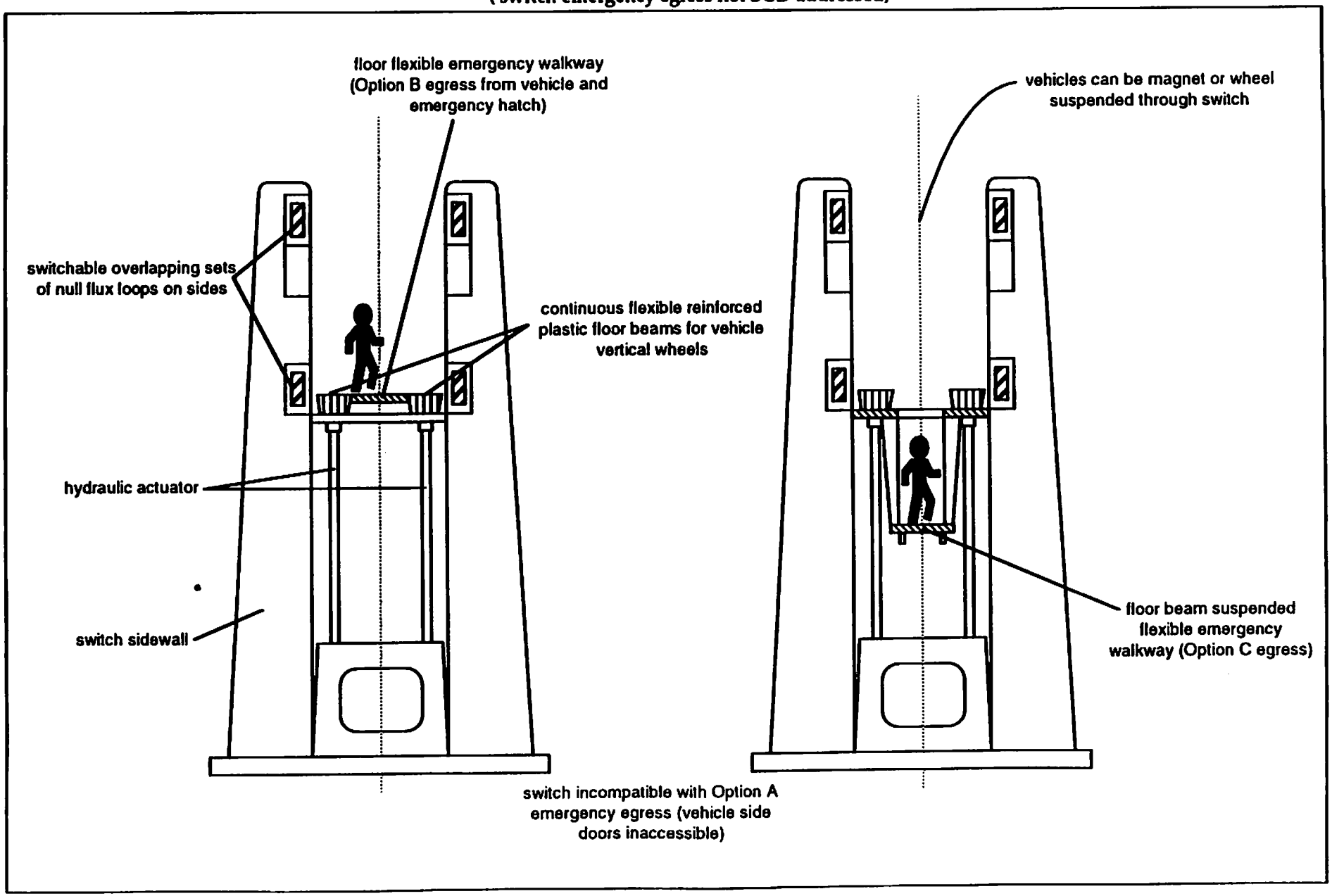


EXHIBIT 3-8
Possible Application Of Foster-Miller Emergency Egress Means To Proposed Type II – Low Speed Lateral Switch Design Concept (switch emergency egress not scd addressed)

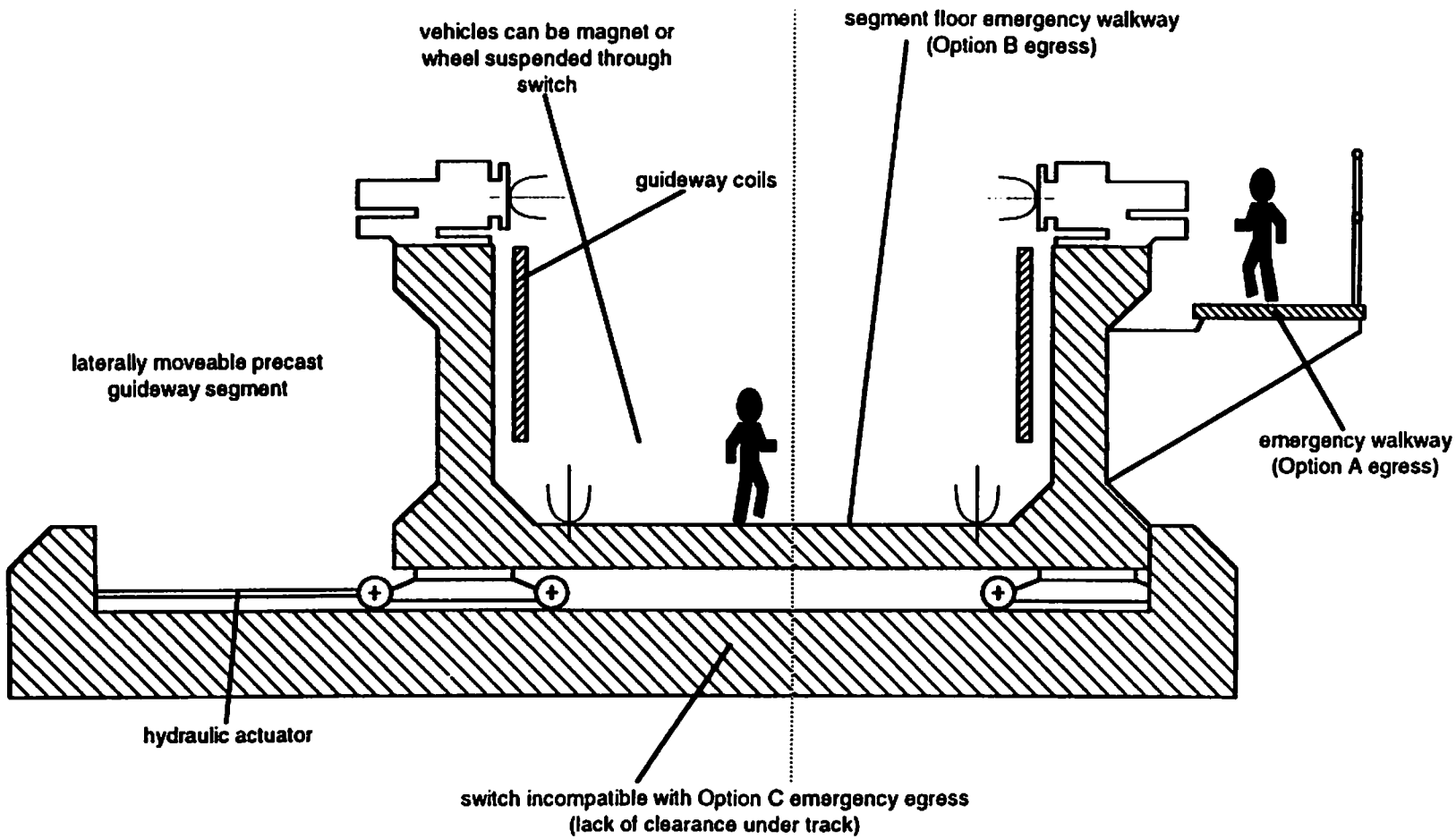
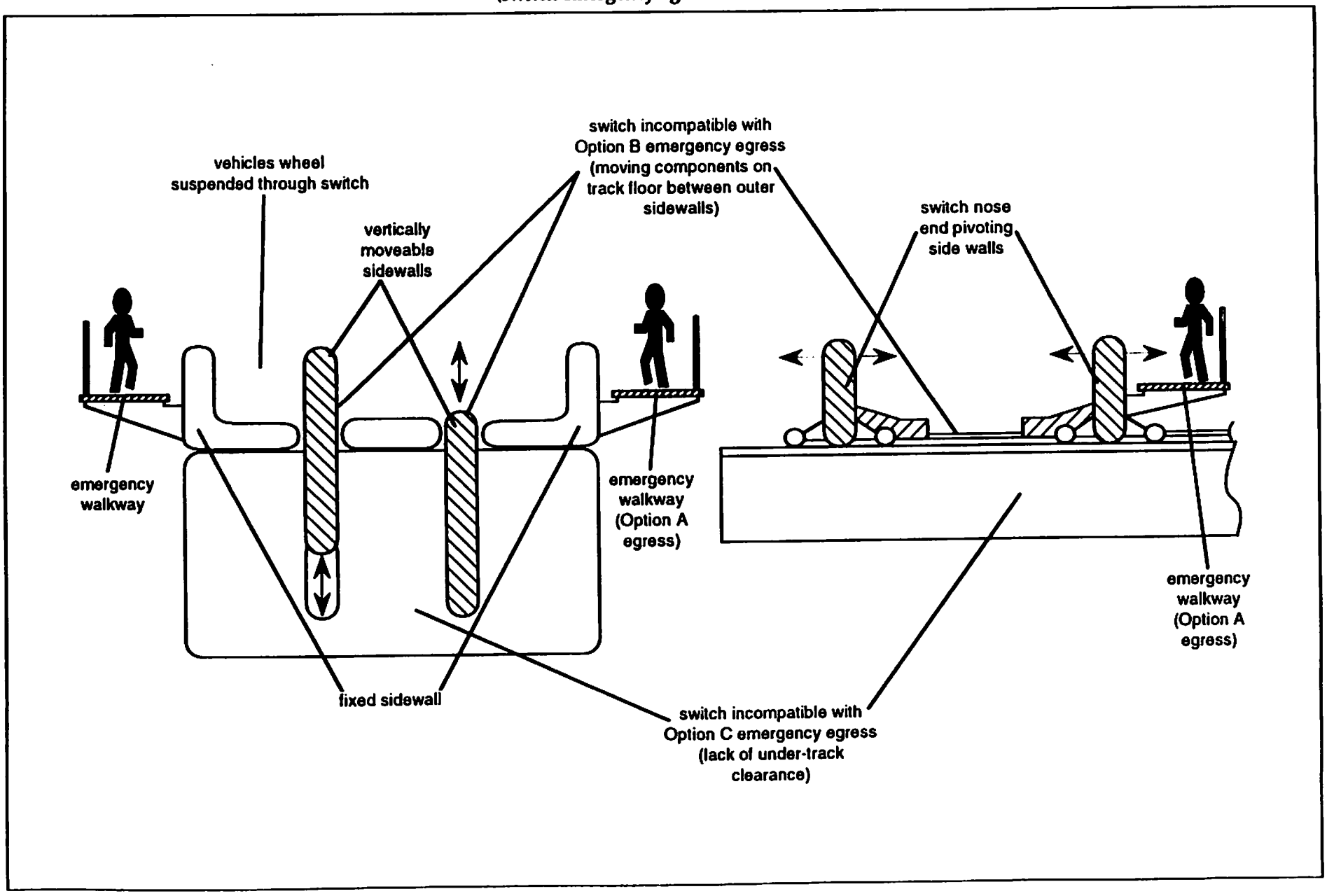


EXHIBIT 3-9
Possible Application Of Foster -Miller Emergency Egress Means To Proposed Type III – Low Speed Lateral Switch Design Concept (switch emergency egress not scd addressed)



either an upper or lower track branch. 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 Exhibits 3-3 and 3-4. This switch design could, however, incorporate an emergency walkway between or suspended below the landing wheel floor members, as shown in Exhibit 3-7; this walkway is required for the fore/aft or the downward emergency egress options shown in Exhibits 3-5 and 3-6, respectively. Switch walkways need to 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 Exhibit 3-8, incorporates the hydraulically actuated lateral displacement of multiple segmented length track sections supported by wheels running on laterally oriented rails (FM SCD Figure 3-63).

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 Exhibits 3-3 and 3-4. These walkways will be designed to be 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 Exhibit 3-8, 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 Exhibit 3-6.

The low speed switch, Type III, shown in cross-section in Exhibit 3-9 is only used for vehicle wheels-deployed operation and incorporates pivoted moveable sidewalls at the switch nose end together with vertically moveable sidewalls. These movable sidewalls are located between outside fixed sidewalls and can be raised above or retracted into the track floor (FM SCD Figure 3-64). Three sidewalls define possible switch track branches: angular movement of the switch nose end sidewalls, appropriately raised and lowered vertically moveable sidewalls and the outside fixed sidewalls.

This lateral switch design allows for placement of an emergency walkway along either laterally moveable sidewalls or the outside fixed sidewalls, shown in Exhibits 3-3 and 3-4, for the proposed first emergency egress option. The remaining two emergency egress options are not possible for this lateral switch design; the fore/aft and the suspended walkways seriously compromise passenger and crew safety because of potentially dangerous mechanical components. Exhibit 3-10 summarizes the feasibility of switch types with emergency egression options.

EXHIBIT 3-10

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
III	Yes	Safety Negated	No

3.4.3 Vehicle Emergency Evacuation Within Superelevated Track Guideway Curve Zones

The proposed vehicle's hydraulic active tilting system can tilt the vehicle up to 12 degrees from horizontal, and the guideway track beam superelevation may be angled up to 12 degrees from horizontal (FM SCD 2.5). Thus, vehicles with operative tilting systems stopped on a superelevated track 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 track 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 track curve and tilted to match the track superelevation angle. This tilting allows for deployment clearance 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 from the walkway; emergency egress onto the guideway walkway from vehicle side doors becomes difficult for elderly and disabled passengers. Downward egress becomes virtually impossible because of stairway/ladder clearance requirements.

3.4.4 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 practices. The cabin layout is based on 2 X 3 business class seating at 1.0 meter (39.4") pitch, 2 X 2 first class seating at 1.1 meter (43.3") pitch and 0.54 meter (21.3") aisle width (specified on Figures 2-12, 2-33 and 2-34 of the Foster-Miller report). 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.

The 90 second emergency evacuation duration is adequate for a Maglev vehicle where the risk of rapid fire spreading and/or explosion is less than the risks for aircraft. In this regard, the Foster-Miller Maglev vehicle fire protection is in accordance with aircraft practice and is consistent with the general aircraft oriented design approach of this SCD baseline design.

Four 1.37 meter (54") wide entrance/exit doors, two per vehicle unit side, are provided in each vehicle unit. Each unit also has one wheelchair station (FM SCD Figures 2-33 and 2-34). 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 Exhibits 3-3 and 3-4. The corresponding evacuation rate for evacuating 37 passengers in a 90 second duration is one passenger every 2.4 seconds. The requirement to emergency evacuate up to 50 passengers per available door for the Foster-Miller proposed vehicle design is consistent with aircraft practice.

Two 1.4 meter (55") square emergency floor hatch doors are provided in each of the proposed vehicle units (FM SCD Figures 2-33 and 2-34). 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 Exhibit 3-6. 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 exists will be required to evacuate up to 74 passengers for business class seating per vehicle unit within the specified 90 second evacuation duration (i.e., a maximum of one passenger every 1.2 seconds per consist trainset). The awkwardness of egress from the vehicle fore and aft emergency hatches, evident from Exhibit 3-5, makes the realization of complete evacuation within the specified 90 second duration unlikely, even for the baseline two-vehicle unit trainset configuration.

The FAA-proposed commercial aircraft requirements for maximum distance between any seat row and the nearest exit to be less than 9 meters (30 ft) is satisfied by the proposed Maglev vehicle cabin layout with respect 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 last case.

3.4.5 Emergency Response Information Communication Means

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 (FM SCD 6.1.3 and 6.1.5). 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 only mentions 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 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. 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.

3.4.6 Provision for 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 (FM SCD 2.7.4). 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 emergency on-board power battery subsystem is incorporated 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 (FM SCD 2.7.4).

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 in an emergency which requires vehicle landing and subsequent emergency evacuation. Additional discussion and detail should have been provided in the SCD.

3.4.7 Advantages of SCD Proposed Emergency Response Vehicle Evacuation Means

Emergency evacuation from a stopped vehicle onto a guideway-supported walkway, in accordance with either the lateral or the fore/aft alternate egress options, will be possible typically over almost the entire guideway length, except as noted below.

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 with Maglev rescue vehicle.

The system guideway capital costs associated with providing emergency evacuation paths from a stopped vehicle to an emergency walkway is minimal for the proposed fore/aft emergency egress option because the guideway track floor functions also as a walkway; these costs are limited to constructing egress staircases from the walkway to ground at determined intervals.

3.4.8 Disadvantages of SCD Proposed Emergency Response Vehicle Evacuation Means

Emergency evacuation from a stopped vehicle onto a guideway-supported walkway will not be available for three of the nine combinations of switch design and emergency egress options (see Exhibit 6-1) for 2 of the 3 combinations of highly superelevated track and the emergency egress options or for any of the three emergency egress options through superelevated curves when the vehicle tilting system is inoperative.

The capital cost of the guideway supported emergency walkway required for most of the guideway length for either the lateral or downward emergency egress options, will be significant, although such walkway cost was not estimated in the SCD report.

The downward vehicle emergency egress option appears to be flawed 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.

The proposed fore/aft vehicle emergency egress option requires significantly longer vehicle evacuation times for trains with more than two vehicle units when compared to the two alternate egress options of this SCD.

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 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.

4.0 SAFETY REVIEW OF SCD - GRUMMAN

This chapter contains a review of the Grumman system safety program, their hazard analyses and related issues, and their proposed emergency response strategy.

4.1 OVERVIEW OF SCD SYSTEM SAFETY APPROACH - GRUMMAN

4.1.1 Organization Structure

No discussion of the safety organization structure is provided. However, it is stated that the safety activities conducted to assess the Grumman Maglev conceptual design were essentially conducted by Battelle independently from the design team.

4.1.2 Safety Process

Grumman conducted a thorough PHA of their design concept in accordance with standard industry practice. The approach and hazard classification methodology is based on MIL-STD-882B. Approximately 150 hazards were identified, including the generic safety issues identified in the SCD statement of work. 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 with the hazard. These PHA entries have been checked against the appropriate system descriptions within the body of the SCD, providing evidence of a closed loop process.

The interfaces between safety, human factors, reliability, and maintenance activities were handled correctly. The reliability program conducted during the contract period made good use of the PHA data.

4.1.3 Schedule

There is no future safety program schedule provided. Grumman does not provide any planning information for future safety analysis work. The Safety Assurance Plan section of the report deals with the activities conducted under the SCD contract.

4.2 RESOLUTION OF BASELINE HAZARDS - GRUMMAN

Exhibit 4-1 shows the Grumman response to the Baseline Hazards identified in the statement-of-work. Grumman thoroughly understands the purpose and procedure for conducting a PHA. Each of the baseline hazards was subdivided into more detailed and concise events of concern. A proposed control provision was established for each event. Verification of control provisions was limited to Class I and II hazards. Very few potential hazards identified in the PHA were not addressed in the detailed design text.

EXHIBIT 4-1
Grumman
Baseline Hazards

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of System Power	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. (Class I) Control provisions provide for on-board emergency braking capability.	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. (Class 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. (Class 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.
	Power Discontinuity Between Guideway Sections (1.9-1.10) results in variation in train propulsion/braking. (Class 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 Class IV Minor event, therefore, design plan was not verified.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of System Power (continued)	Inability to Dissipate Energy During Braking (1.11-1.12) results in loss of braking. (Class 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. (Class 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. (Class III) Control provisions include use of highly reliable component and design in "fail-safe" manner	Hazard is defined as a Class 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. (Class IV) Control provisions include design control in "fail-safe" manner.	Hazard is defined as a Class IV Minor event, therefore, the design plan was not verified.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control	Hazard was subdivided into thirty-five hazards: Loss of or Insufficient Propulsion Commanded (to Inverters) (3.1) resulting in train running slower than desired or may stop. (Class IV) Control provisions include using redundant computers.	Hazard is defined as a Class IV Minor event, therefore, the design plan was not verified.	
	Excessive Propulsion Commanded (to Inverters) (3.2) resulting in overspeed or collision. (Class 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.	**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. **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.	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.
	Loss of or Insufficient Dynamic Braking Commanded (3.3) resulting in overspeed or collision. (Class I) Control provisions include utilizing "fail-safe" on-board emergency brake.	Same as Hazard 3.2	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR FOR MITIGATING HAZARDS	
Loss of Command and/or Control (continued)	Excessive Dynamic Braking Commanded (3.4) resulting in excessive deceleration causing minor injury. (Class 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. (Class 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. (Class 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. (Class I) Control provisions include designing comparison of command and actual speed function in substation computer in "fail-safe" manner.	Same as Hazard 3.2	
	Improper Generation of Speed Command (3.8) resulting in possible overspeed and/or collision. (Class I) Control provisions include designing speed command generation function in substation computer in "fail-safe" manner.	Same as Hazard 3.2	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control (continued)	Incorrect Route Integrity Data Received (e.g., Switch Position, Obstacles on Guideway) (3.9) resulting in possible collision with train or object. (Class I) Control provisions include designing route integrity subsystem in "fail-safe" manner; includes protection from nonconflicting routes and detection of obstacles on guideway.	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. (Class 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. (Class I) Control provisions include designing emergency brake control fuction 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	
	Incorrect Interpretation of Vital Train Operating Data (e.g., Location, Speed, Direction) (3.12) resulting in possible overspeed and/or collision. (Class I) Control provisions include designing functions which use this vital data in substation computer in "fail-safe" manner.	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	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control (continued)		Strategies employed to achieve these goals are: provide ground fault portection, 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. **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 fuctions 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.	
	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. (Class 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. (Class 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	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control (continued)	Start-Up Not Initiated (3.15) resulting in train not leaving station area or other location when desired. (Class 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. (Class 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	
	Train Not Stopped/Positioned Properly In Station (3.17) resulting in possible injury to passenger while boarding/deboarding. (Class 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. (Class 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.	**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	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control (continued)	Switching Commanded When Not Desired (3.19) resulting in possible train leaving guideway or suffer major damage. (Class 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	
	Incorrect Train Location Determined (3.20) resulting in possible headway violation and collision. (Class 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. (Class 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. (Class 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 villation and collision. (Class 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. (Class I) Control provisions include designing emergency brake control circuit to handle wayside command in "fail-safe" manner.	Same as Hazard 3.2	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control (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. (Class 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. (Class 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. (Class III) Control provisions include designing emergency braking within acceptable deceleration limits, and maintain proper guidance on guideway.	**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.	
	Critical On-Board Equipment Failure or Emergency Condition Not Acknowledged (3.29) resulting in possible overspeed, collision, or on-board fire. (Class 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	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control (continued)	Door Opening Not Commanded (3.30) resulting in passengers unable to egress vehicle, resulting in possible injury. (Class II) Control provisions include allowing passengers to open door in emergency.	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. (Class I) Control provisions include designing door control function (door closure) in "fail-safe" manner with passenger override capability in emergency.	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	
	Incorrect Speed/Movement Requests Made From Central (3.32) resulting in possible headway violation or overspeed resulting in collision. (Class I) Control provisions include designing substation control equipment in "fail-safe" manner to ensure safe operation.	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 restrictuve 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. (Class IV) Control provisions include designing vehicle monitoring in a highly reliable manner.	Same as Hazard 3.32	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Command and/or Control (continued)	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. (Class I) Control provisions include critical equipment failures of train or wayside should be handled by substation equipment in "fail-safe" manner. 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. (Class 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 Same as Hazard 3.32	
Loss of Communication System	Hazard was subdivided into fifteen hazards: 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. (Class I) Control provisions include designing substation computer in "fail-safe" manner to safely shutdown train when link is lost.	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.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of 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. (Class IV) Control provisons include designing encoder/decoder scheme in "fail-safe" manner.	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 portection, 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. 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 fuctions 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. 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.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Communication System (continued)		**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.
	Incorrect Encoding/Decodinng of Train Location, Speed, or Route Integrity Data in Substation (2.3) resulting in possible collision between trains, switch, or with object. (Class I) Control provisions include designing encoder/decoder functions to be "fail-safe".	Same as Hazard 2.2	
	Loss of Central to Substation Data Link (2.4) resulting in loss of scheduling capability. (Class IV) Control provisions include using redundant link.	Hazard is defined as a Class 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. (Class IV) Control provisions include using redundant link.	Hazard is defined as a Class 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. (Class IV) Control provisions include ensuring safety of system via wayside/on-board equipment.	Hazard is defined as a Class IV Minor event, therefore, the design plan was not verified.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Communication System (continued)	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. (Class IV) Control provisions include designing substation equipment for safe shutdown if problem exists.	Hazard is defined as a Class IV Minor event, therefore, the design plan was not verified.	
	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. (Class IV) Control provisions include designing substation equipment for safe shutdown if problem exists.	Hazard is defined as a Class 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. (Class I) Control provsions 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. (Class 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	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Communication System (continued)	Incorrect Encoding/Decoding of Vital Train Operating Data (e.g., Location, Speed) (2.11) resulting in collision or overspeed condition. (Class I) Control provisions include designing encoder/decoder in "fail-safe" manner (on-board and at substation).	Same as Hazard 2.2	
	Loss of Train Eqipment Status and Emergency Condition Data Link at Substation (2.12) resulting in improper speed command, resulting in overspeed or collision with another train. (Class 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. (Class I) Control provisions include designing encoder/decoder in "fail-safe" mannes(on-board and at substation).	Same as Hazard 2.2	
	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. (Class 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	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Communication System (continued)	Incorrect Encoding/Decoding of Substation to Train Vital Data (2.15) resulting in train emergency braking may not occur when needed; possible collision/overspeed. (Class I) Control provisions include designing encoder/decoder in "fail-safe" manner (on-board and at substation).	Same as Hazard 2.2	
Loss of Levitation/ Guidance and Levitation/ Guidance/ Magnet Failure	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. (Class 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. Loss of or Reduced Levitation/Guidance During Passenger Boarding/Deboarding (4.4) resulting in passenger injury while boarding/deboarding. (Class II) Control provisions include using multiple magnets per vehicle and configure in highly reliable manner.	**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. **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. **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. **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.	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

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN 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. (Class 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. (Class 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. (Class 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. (Class IV) No control provisions are recommended.	Hazard is defined as a Class IV Minor event, therefore, the design plan was not verified.	If passengers are unprepared or loading baggage overhead, effect might result in injury.
	Guidance Not Maintained During Emergency Braking (4.9) resulting in possible loss of train/guideway integrity, resulting in passenger injury. (Class II) Control provisions include consideration of means to maintain adequate train/guideway integrity during emergency braking	**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.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Levitation/ Guidance and Levitation/ Guidance/ Magnet Failure (continued)	Overheating Occurs in Superconducting Magnets (4.10) resulting in levitation decrease, resulting in possible undesired train/guideway contact and possible passenger injury. (Class II) Control provisions include separately cooling each magnet and make structurally reliable. Magnets Make Contact With Rails at Normal Speeds (4.11) resulting in undesired rail/magnet contact, resulting in possible injury. (Class I) Control provisions include designing magnet structure and connecting hardware in highly reliable manner.	**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. **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).	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.

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity, including Debris, Snow, Ice, Misalignment, Entry/Exit. (Debris, Snow, and Ice are addressed in "Guideway Obstructions" hazards).	Hazard subdivided into fourteen hazards: <u>Guideway Support Column Collapse/Shift (6.1)</u> results in train leaving guideway. (Class 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. **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. **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 activiles to ensure the integrity of the infrastructure, subsystems, and structural components.	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.

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity, including Debris, Snow, Ice, Misalignment, Entry/Exit. (Debris, Snow, and Ice are addressed in "Guideway Obstructions" hazards) (continued)	Collapse/Shift of Guideway (Lateral) Support Arm (6.2) results in guideway track(s) losing support and train leaving guideway. (Class 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. (Class I) Control provisions include designing and contructing according to appropriate standards.	Same as Hazard 6.1	
	Collapse of Guideway Track (6.4) results in train leaving guideway. (Class I) Control provisions include designing and constructing according to appropriate standards.	Same as Hazard 6.1	
	Improper Lateral Alignment of Guideway Track Sections or Rails (6.5) results in undesired contact between train and guideway; sudden stop could occur. (Class 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 Scetions or Rails (6.6) results in undesired contact between train and guideway; sudden stop could occur. (Class 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	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity, including Debris, Snow, Ice, Misalignment, Entry/Exit. (Debris, Snow, and Ice are addressed in "Guideway Obstructions" hazards) (continued)	Excessive (Longitudinal) Gap Between Guideway Track Sections or Rails (6.7) results in possible propulsion transients with little overall effect. (Class 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 Class IV Minor event, therefore, design plan was not verified.	
	Rail Separates From Guideway Track (6.8) results in undesired contact between vehicle and rail, resulting in injury or death. (Class 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. (Class II) Control provisions include to properly design coil placement.	**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. (Class 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.	**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.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity, including Debris, Snow, Ice, Misalignment, Entry/Exit. (Debris, Snow, and Ice are addressed in "Guideway Obstructions" hazards) (continued)		**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. (Class 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. (Class I) Control provisions include design switch mechanism and all connecting hardware to handle expected loads.	Same as Hazard 6.1	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity, including Debris, Snow, Ice, Misalignment, Entry/Exit. (Debris, Snow, and Ice are addressed in "Guideway Obstructions" hazards) (continued)	Switch Mechanism Does Not Move or Moves Too Slowly (6.13) resulting in collision with train or switch element. (Class 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. (Class 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 (Obstacles include debris, snow, and ice)	Obstacle Present On Guideway Track (6.21) results in collision with object, resulting in sudden deceleration or train leaving guideway; injury/death results. (Class 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. **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 Class I Catastrophic event. Unable to determine if obstacle detection system is designed with redundancy from the design text.

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Fire (Vehicle, ROW, facility adjacent to ROW)	Vehicle fire hazard was subdivided into two hazards: Fire Occurs On Train From Electrical Component/Subsystem Overheating (5.6) resulting in possible passenger injury. (Class 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.	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. (Class 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

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Evacuation and Rescue Requirements with Attention to Elevated and Tunnel Sections.	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). (Class 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. Emergency Egress Required From Guideway In Tunnels (6.18) resulting in passengers unable to leave guideway resulting in further injury or injury from exposure. (Class 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. Passenger Trips/Falls On Center Guideway (6.19) resulting in injury/death. (Class I) Control provisions include designing center guideway surface to provide appropriate traction for personnel. Emergency Condition Requires Response Personnel Access to Guideway (6.20) resulting in response personnel unable to access guideway. (Class 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. See Emergency Evacuation/Response Plan evaluation. See Emergency Evacuation/Response Plan evaluation. See Emergency Evacuation/Response Plan evaluation.	

EXHIBIT 4-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Operation Restrictions	Operation restrictions were recommended for several hazards, mainly environmental.	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	Manually override is used as a control provision for several hazards. Security and Training were not addressed.	Manually override is used as a control provision for several hazards. Security and Training were not addressed.	
Maintenance of Safe Headway	Covered in other hazards	Covered in other hazards	

4.3 IDENTIFICATION/RESOLUTION OF ADDITIONAL GRUMMAN HAZARDS

Exhibit 4-2 summarizes the Grumman Team response to other safety-related requirements identified in their original statement-of-work which were not specifically covered by the Baseline Hazards and additional hazards identified by Grumman.

4.4 EMERGENCY RESPONSE

4.4.1 Vehicle Emergency Evacuation Overall Strategy

The Grumman evacuation strategy requires passengers to remain on-board the Maglev vehicles 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 or minimizes the probability of life-endangering hazardous situations.

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-track guideway center spine girder which forms a horizontal platform surface 3 to 4 meters wide, shown in Exhibit 4-3. 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 Maglev 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 two power-operated sliding doors 0.81 meters (32") wide, one on each side of the module, for normal entry/exit and emergency egress. Large module windows (4/5 m x 9/5 meter) are provided, some of which will be able to be "popped out" for use as additional emergency exits.

One meter separates the vehicle floor from the spine girder top emergency egress platform, evident from Exhibit 4-3, and a suitably deployable short ladder or folding stairs will be required to assist passengers during egress. This is not addressed in the SCD.

EXHIBIT 4-2
Grumman
Additional Hazards

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Weather Conditions and Constraints	Hazard subdivided into eleven hazards: Trains Operate In Extremely High or Low Temperatures (7.1) results in potential unsafe operation. (Class I) Control provisions include designing safety critical substation, and on-board equipment in "fail-safe" manner relative to temperature related failures.	**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 -29°C (-20°F). **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 49°C (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. (Class 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.	**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.	
	Train Operates In Ice Conditions (7.3) resulting in undesired contact with guideway or train leaves guideway. (Class I) Control provisions include operating at reduced spped 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.	PHA and design plans do not address ice build-up on aerodynamic surfaces of train.

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Weather Conditions and Constraints (continued)	Train Operates In Side Wind Conditions (7.4) resulting in undesired contact with guideway or train leaves guideway. (Class 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.	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. (Class 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 Class I Catastrophic event.
	Train Operates In Rain Conditions (7.6) resulting in safe braking capability reduced. (Class 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.	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. (Class 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.	3.2.3.2.4 p. 3-394 The Grummen 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

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Weather Conditions and Constraints (continued)	Train Operates In Low/Poor Visibility (7.8) resulting in possible collision with another train or object. (Class I) Control provisions include designing system operation to be automatic including automatic detection of objects on guideway.	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.	
		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.
	Train Operates In Lightning Conditions (7.9) resulting in possible electrocution of passenger/crew. (Class I) Control provisions include providing adequate lighting protection via structural design and special provisions.	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.	
		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. (Class II) Control provisions include limiting noise to acceptable levels via aerodynamic design and insulation.	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.

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Weather Conditions and Constraints (continued)	Train Generates High Noise Levels Externally (7.13) resulting in injury to maintenance personnel and others in stations and in vicinity. (Class 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.	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.	
Electro-magnetic interference/ Compatibility (EMI/EMC) and Magnetic Radiation	Hazard was subdivided into two hazards: Train Operates in Vicinity of External Electromagnetic Fields (7.10) resulting in possible unsafe operation of equipment and possible biological effects on humans. (Class 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.	3.2.3.4.3 p.3-415 Since the EMS type Maglev system is very similiar 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 thje magnetic field to the passenger or the external environment.	

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Electro-magnetic interference/ Compatibility (EMI/EMC) and Magnetic Radiation (continued)	System Vehicle/Guideway/Wayside Components Generate EMF (7.11) resulting in possible unsafe operation of equipment and possible biological effects on humans. (Class 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	**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. **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.	

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Electro-magnetic interference/ Compatibility (EMI/EMC) (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 similiar 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.	
Trespassers On Guideway (8.1)	Potential hazard could result in injury/death to personnel on guideway and/or passengers. Control provisions include preventing unauthorized guideway access instations and along row.		

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Vehicle	Identified thirty-one hazards associated with the vehicle, however, most have been covered under other baseline hazards. The remaining twelve are listed: 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. 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. 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. Control provisions include designing on-board computer/control equipment in "fail-safe" manner - emergency braking should result.	Hazard is defined as a Class III Marginal event, therefore, design plan was not verified. Hazard is defined as a Class III Marginal event, therefore, design plan was not verified. **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. Ther is no detailed discussion or description of the batteries in the SCD.

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Vehicle (continued)	Passengers Exposed to High Voltage (5.5) resulting in possible passenger injury. Controling provision includes routing and containing wires in manner to prevent passenger contact/access.	**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.
	Loss of or Reduced Tilt Capability On Curves (5.7) resulting in possible passenger injury. Control provisions include designing tilt control circuit in "fail-safe" manner; use highly reliable components.	**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 failsafe operation. **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.

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Vehicle (continued)	Excessive Tilt Produced On Curves Or Straight Sections (5.8) resulting in possible passenger injury. Control provisions include making highly reliable and employing stop mechanism to prevent excessive tilt.	Same as Hazard 5.7	
	Train Stops On Curve (5.9) resulting in possible passenger injury Control provisions include deactivating tilt if stopped on curves - make mechanism highly reliable.	Same as Hazard 5.7	
	Loss of Structural Integrity Between Upper Vehicle and Bogie (5.10) resulting in possible severe injury/death. Control provisions include designing in highly reliable manner with redundancy.	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.	
	Doors Close On Passenger When Entering/Departing Vehicle (5.18) resulting in possible injury. Control provisions include employing dorr sensors to detect presence in doorway; employing proper timing and use proper door closing force.	Hazard is defined as a Class III Marginal event, therefore, the design plan was not verified.	
	Vehicle Hits Small Flying Object (5.23) resulting in possible crew/passenger injury. 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.	3.2.1.3 p. 3-145 Glazing and nose compartment materials must meet, at a minimum, the requirments 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 snall 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.	

EXHIBIT 4-2 (Continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANAYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Vehicle (continued)	Vehicle Hits Large Flying Object (5.24) resulting in injury/death to crew or passengers. Control provsions include using very high quality glazed window for train front ends and using other impact resistant materials. Front/Rear End Collision Occurs With Another Train (5.25-5.26) resulting in possible injury/death due to structural seat problems. Control provisions include designing redundancy into control system and seats and connecting hardware to resist structural damage in collisions. Vehicle Leaves Guideway While Negotiating Curves (5.31) resulting in death/injury. Control provisions include designing train/guideway interface with high reliability/integrity.	Same as Hazard 5.23 **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. **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.	

EXHIBIT 4-3
Grumman Proposed Vehicle Emergency Egress Means

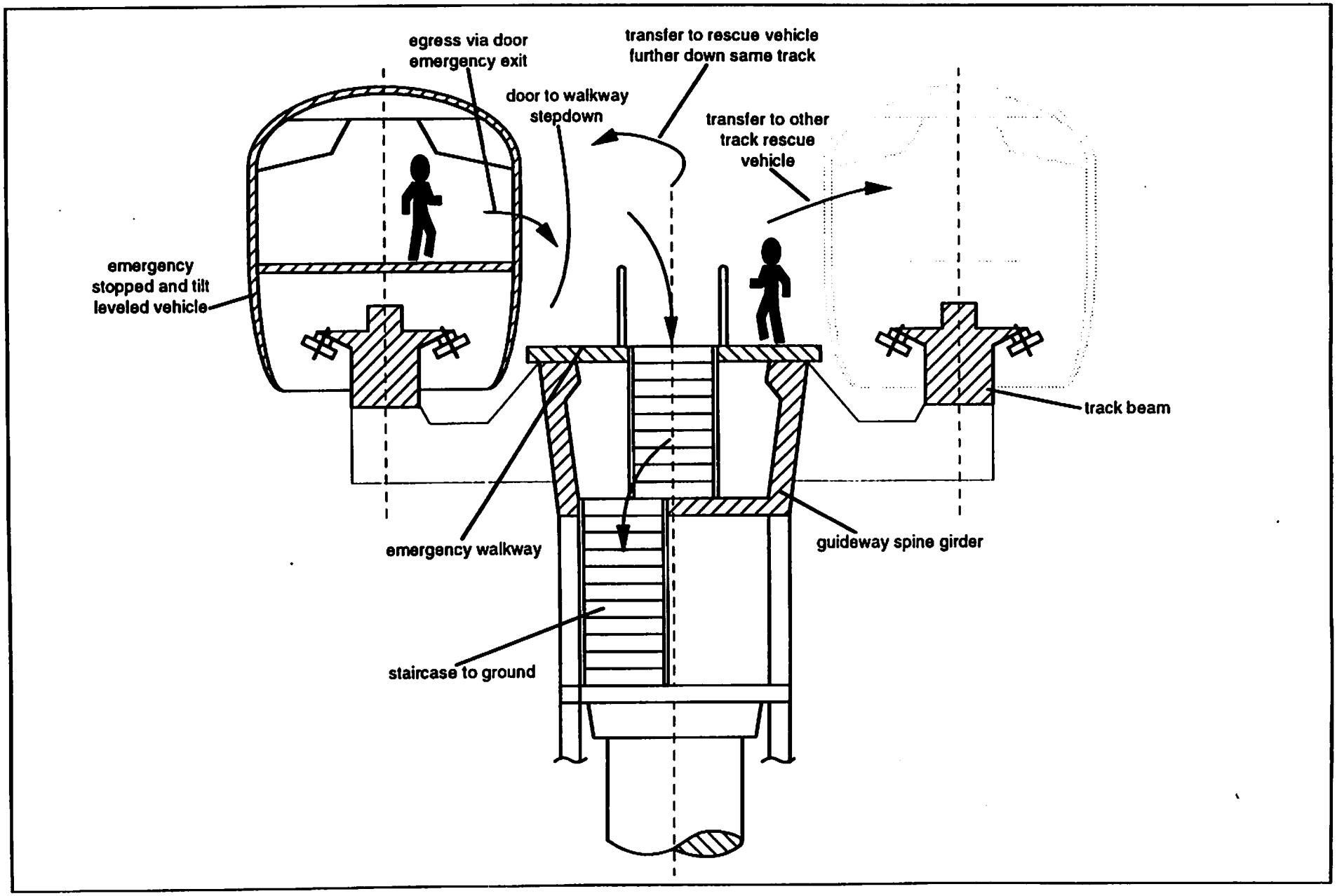
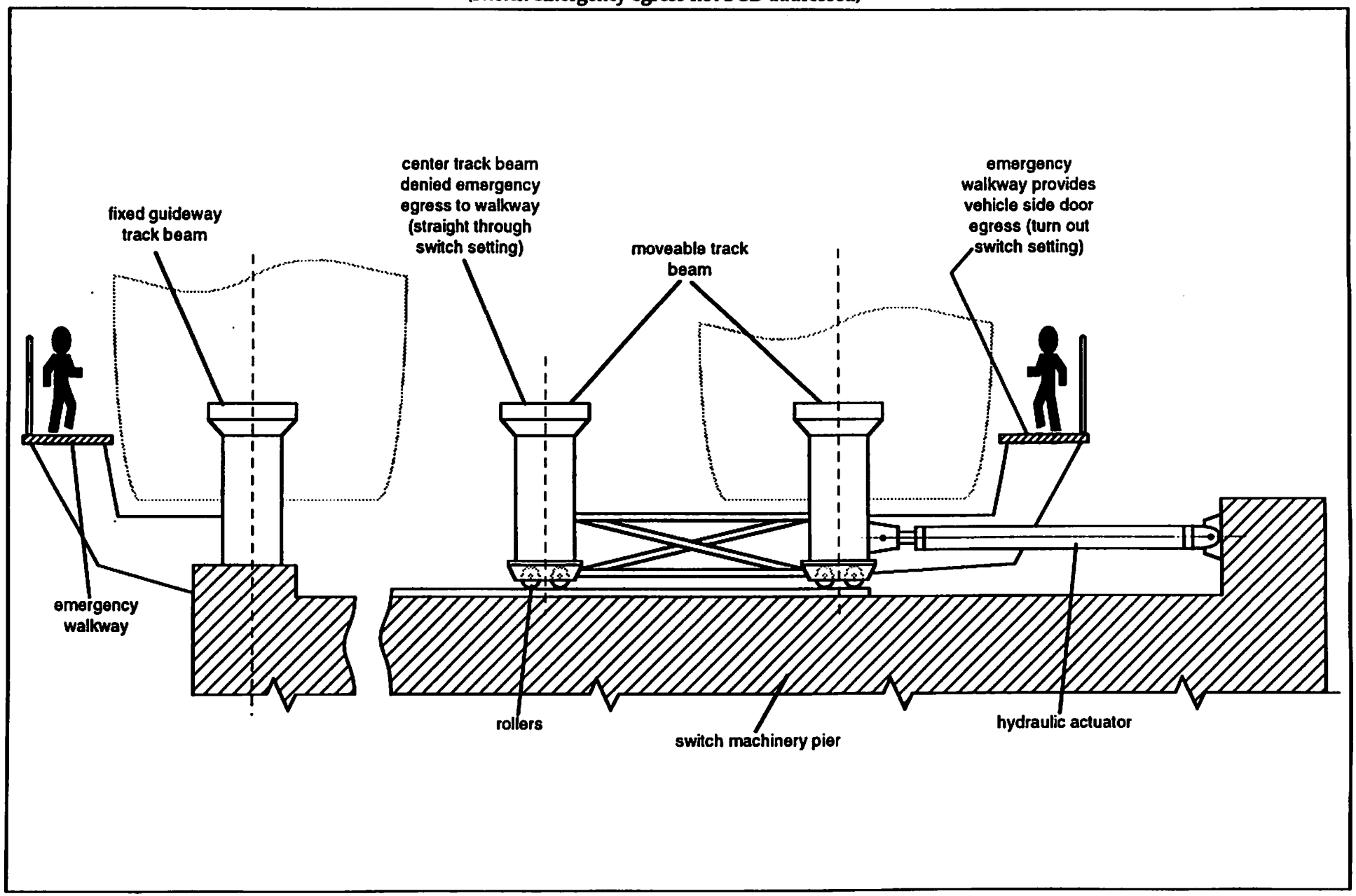


EXHIBIT 4-4
Possible Application Of Grumman Emergency Egress Means To Proposed Lateral Switch Design Concept
(switch emergency egress not SCD addressed)



4.4.2 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 Exhibit 4-4. Instead, the individual-track beams of the switch are supported on pier cross-beam members located at 15 meter 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 (GR SCD 3.2.2.4). 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 Exhibit 4-4.

Although not addressed in the SCD report, emergency egress walkways can 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 Exhibit 4-4. Vehicle clearance considerations are evident from the switch planview shown in Figure 3.2.2-30 of the Grumman SCD.

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.

4.4.3 Vehicle Emergency Evacuation Within Superelevated Track Guideway Curve Zones

The proposed vehicle's hydraulic active tilting system can tilt the vehicle up to 9 degrees from horizontal; and, the guideway track beam superelevation angle may be up to 15 degrees from horizontal (GR SCD 3.2.1.5). Thus, vehicles with operative tilting systems that are stopped on a superelevated track segment can be leveled to within 6 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.

4.4.4 Vehicle Cabin/Crew Compartment Layout and Equipment 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 38" pitch with 22" aisle width specified - - GR SCD Figure 3.2.1-71). 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 adequate for a Maglev vehicle where the risk of rapid fire spreading and/or explosion is lower than the risks associated with aircraft. The Grumman Maglev vehicle complies with aircraft evacuation requirements.

Four 0.8 meter 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 access, as shown in Exhibit 4-4. 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.

4.4.5 Emergency Response Information Communication Means

During emergency situations, communication between vehicles and system central control occurs using vehicle-to-wayside ultra high frequency 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 (GR SCD 3.2.3.1).

The SCD clearly identifies the need for extremely high reliability of the communications link between the vehicles and the wayside regional centers. The SCD states clearly 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 (GR SCD 3.2.3.1.5).

A potentially serious problem is the baseline system ultra-high-frequency (UHF) radio transmission multipath interference problem. This results from the radio waves being reflected off terrain or other ground objects, and will be minimized by continually comparing signal quality among a number of wayside transceivers distributed along the guideway length at nominal 2 km 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 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 is adequate for use in emergency conditions to control the train and to provide subsequent evacuation instructions to passengers.

Grumman suggest having an on-board attendant on the baseline 100-passenger vehicle to provide for passenger needs and supervision (GR SCD 3.2.1.13.6) 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. Presumably, any emergency response-related information will be transmitted to the vehicle attendant, who in-turn, will notify the passengers via the on-board public address system.

4.4.6 Provision for Emergency On-Board Power Supply

The predicted vehicle electrical power demand of about 170 kW requires an on-board lead-acid battery power supply which weighs approximately 6000 lbs (i.e., about 4.5% of the estimated loaded baseline vehicle weight). (GR SCD 3.2.1.7) 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 (GR SCD 3.2.1.2) is unavailable because the train traveling at speeds less than 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 needs to be addressed.

4.4.7 Advantages of SCD Proposed Emergency Response Vehicle Evacuation Means

Emergency evacuation from a stopped vehicle onto the guideway walkway will be available over the entire guideway length, except along one particular track branch of the switch design and through superelevated curves for a vehicle with 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 "safe location" will be available:

- Via a staircase to ground level
- From the walkway onto a Maglev 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, and thus costs for providing for emergency evacuation are limited to constructing egress staircases from the walkway to ground at spaced intervals.

4.4.8 Disadvantages of SCD Proposed Emergency Response Vehicle Evacuation Means

Emergency evacuation from a stopped vehicle with an inoperational vehicle cabin tilting system onto the guideway spine girder top walkway will be difficult through highly superelevated guideway curves. These conditions will make evacuation difficult for disabled and/or 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.

5.0 SAFETY REVIEW OF SCD - BECHTEL

This chapter contains a review of the Bechtel system safety program, their hazard analyses and related issues, and their proposed emergency response strategy.

5.1 OVERVIEW OF SCD SYSTEM SAFETY APPROACH - BECHTEL

The Bechtel Team safety approach during SCD is stated to be one of:

- Identifying the classification to be used for hazards in the maglev system
- Assigning an allowable total probability value to the hazard classification
- Identifying specific potential hazards associated with maglev rapid transit
- Developing design approaches which mitigate the hazard or reduce its probability to an acceptable level.

The Bechtel Team philosophy for dealing with hazards is basically that which is espoused by MIL-STD-882B. Specifically, they claim the following design techniques have been employed:

- Fault Avoidance - Elimination of or limiting the probability of the fault occurring.
- Fail Safe - If fault occurs, system reverts to a known, safe state.
- Fail Degraded - If fault occurs, system reverts to degraded or restricted operating mode.
- Fail Operational - First fault has no operational effect, second fault is fail safe or degraded.
- Fail Operational Squared - No operational effect for more than one fault.

5.1.1 Organizational Structure

No discussion of the Bechtel safety organizational structure used for the SCD effort is provided. A statement is made that the Bechtel Team approach to safety has been to implement a plan which emphasizes designing to mitigate or minimize the probability of hazards. They state that safety plans which detail specific analyses to be used for certification, and reporting requirements will be developed and reported during later program phases. These plans will implement formal MIL-STD-882 type safety programs. They provide a table of MIL-STD-882B tasks by program phase showing when they propose to apply each task.

5.1.2 Safety Process

Hazard severity categories were adapted and expanded from MIL-STD-882B, and an allowable probability was assigned to each category. No quantitative analysis of any design features was provided, however. Their primary effort was to conduct a preliminary system hazard analysis.

Bechtel has identified 25 generic hazards which they used to assess the suitability of various design approaches considered for their baseline design. These hazards were ranked for severity against a scale of eight severity levels that was created by expanding the four levels given in MIL-STD-882B. Eight levels are too many to be workable or meaningful, and are not needed for design guidance. It is sometimes difficult to decide which of two categories on a scale of four to use for a specific event. It will be even more difficult and arbitrary on a scale of eight, and the choice will have no significant impact on the design. This problem is illustrated by the assignment of the same allowable hazard probability to more than one level of hazard severity category.

Eighteen of the 25 identified hazards cover the baseline hazards specified in the statement-of-work except for manual operation, security, training and passenger evacuation, which are considered procedural hazards that Bechtel says will be developed during later phases of the maglev program. However, these topics are addressed to a limited extent in Part E of the Bechtel SCD. The baseline hazards and the eighteen Bechtel hazards are reconciled and discussed in Section 5.2.3. They also identified seven hazards that were not included in the baseline hazards in the statement-of-work. These are discussed in Section 5.3.

High-level, almost generic, design techniques are listed against each of the 25 hazards that are to be "employed to minimize the hazard probability." Many of the listed techniques, however, are intended to mitigate the hazard's effect, but have no influence on its probability of occurring. For example, for the hazard of "Fire aboard vehicle," a design technique recommendation is "Fully automated detection and suppression systems designed into vehicle", but nothing is said about probability requirement for detection and suppression failure.

As mentioned above, each of the 25 identified hazards were assigned to a severity category with an allowable probability. No analyses have been provided at this time which indicate whether the Bechtel baseline design can achieve the assigned levels.

5.1.3 Schedule

Bechtel provides a table of the MIL-STD-882B tasks assigned to various program phases. The allocation of the tasks is appropriate except for Safety Assessment (See 5.4 below). They propose to submit the formal Safety Program Plan, which will include detail task scheduling, during the Conceptual Development Phase.

5.2 RESOLUTION OF BASELINE HAZARDS

Exhibit 5-1 summarizes the Bechtel Team response to the Baseline Hazards identified in the statement-of-work. Eighteen of the 25 hazards identified by Bechtel cover the baseline hazards except for manual operation, security and training, and passenger evacuation and rescue, which are considered procedural hazards that they say will be developed during later phases of the maglev program.

The table correlates the Bechtel hazards identified in their PHA with the applicable baseline hazards. There is overlap in several cases. The hazard severity level identified for each Bechtel hazard is based on their selection from MIL-STD-882B *without applying the expanded categories used by Bechtel.* This was done so that comparisons with severity levels applied to similar hazards by the other SCD contractors could be made more easily.

The table also summarizes some of the hazard mitigating features identified in the design discussion sections of the Bechtel SCD report. Generally, there is no conflict between the design described and the results of the PHA. However many high-level, almost generic, design techniques offered as solutions for hazards in the PHA were not discussed in the subsystem design descriptions.

Several other issues are noted in the table. Specifically, sources of power for some emergency equipment that could be needed in the presence of a power failure are not explained. The specific corrective actions that are assigned to the automated zone controllers are not explained. There is some confusion as to whether Bechtel is or is not proposing to build some sections of the guideway at grade level. Limited information is provided on fire prevention techniques. There are conflicting ambiguous statements in different sections of the report regarding whether onboard manual controls are provided for emergency movement of vehicles.

5.3 RESOLUTION OF ADDITIONAL HAZARDS

Exhibit 5-2 summarizes the Bechtel Team response to other safety-related requirements identified in their original statement-of-work which were not specifically covered by the Baseline Hazards. Also included in the Exhibit are additional hazards identified by Bechtel. While most of these were addressed in the proposed baseline design, there was little or no coverage in the Safety Assurance Plan and no specific hazards were identified in the PHA. EMI/EMC hazards and design issues were not addressed.

EXHIBIT 5-1
Bechtel
Baseline Hazards

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of System Power	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 Section A3.6: Back-up batteries for emergency power. Primarily for hotel functions. LEVITATION Section 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. Section C1.6.1: Air bearings can provide zero speed lift at any place on the guideway so vehicle can be towed. Section C6.9: Air bearings are backed up by hydraulic actuators that can lift the vehicle for takeoff. PROPULSION Section A4.1: Design allows vehicle to move in either direction along guideway in case of power failure on the other guideway. Section A4.3: Back-up batteries used to assure dynamic braking remains available in the event of total power failure. Section 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. Section A4.7: Safe headway automatically maintained if system failures cause reduced speed. Battery back-up proposed for regions where transmission line failures are common.	Section C1.10.1: Not clear what electrical power source is used for fire protection system. Section C1.12.3: Not clear what power source is used to deploy aerodynamic brake or drag chute.

EXHIBIT 5-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of System Power (continued)		Section 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. Section A4.4: Special mounting scheme used to allow quick replacement of port and starboard motor windings. Section 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. Section C1.11: Program of daily maintenance, quarterly inspections, and periodic system overhauls for vehicles is proposed.	
Loss of Control System and/or Communication System	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 contract or derailment , a Category I event. Preventive measures rely on controllers and sensors.	Section A6.1: The communication and control systems for each direction of travel share common facilities, but are functionally independent. Section 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. Section A6.5: Adjacent zone controllers can maintain system integrity at reduced speed if central control is unavailable. Section A6.6: Central control can operate for zone and station controllers in the event of their failure. Section C4.2.2: Any communicated data error results in corrective action by controllers.	Section 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. Section A6.7: Multiple breaks in fiber optic cables could disable system. No discussion on this effect.

EXHIBIT 5-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Levitation or Guidance and Levitation/ Guidance/ Magnet Failure	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.	Section A4.3: Each vehicle has two independent inverters driving port and starboard motors. If a motor system fails the other will provide enough thrust for full speed operation which supports normal levitation. Section C1.6.1: Air bearing can be used for lift at low or zero speed anywhere on the guideway. Section 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. Section C1.6.8: Lateral guidance wheels used to stabilize vehicle when air bearings are in use. Section 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. Section C1.2.5: The emergency tow vehicles will provide air supply for air bearings when required.	Section C1.5.1 states that on-board power can be used for air compressors for air bearings. In Section 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.

EXHIBIT 5-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Loss of Guideway Integrity	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 (but see issue), 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.	Section 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. Section A7.1: Automated test vehicles to make daily inspection trips to ascertain guideway condition. Section 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. Section 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.	Section A5.1: Inconsistency in discussion about whether guideway will be built at grade in some areas.

EXHIBIT 5-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Guideway Obstruction	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. Section 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. Section 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. Section A5.4: Each inverter station has a preferred stopping area where vehicles can make unscheduled stops in relative safety. Section A5.5: Internal combustion powered vehicles used to tow disabled trains to safe area. Section A2.4: Safe headway distance established by required vehicle stopping distance. Section C1.2.4: Effect of small object impacts mitigated by placing baggage and equipment compartments between front of vehicle and passenger/crew compartment. Section C4.2.2: Guideway sensors will monitor and transmit data on the integrity of the guideway. This includes foreign obstacles and intruders.	

EXHIBIT 5-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Fire	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.	Section 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. Section 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. Tanks are located in vehicle to minimize chance of puncture in a collision. Section C1.13.5: Type A aircraft doors used on both sides of vehicle, front and back. Section 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.
Evacuation and Rescue	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 accompanying separate emergency response and evacuation analysis.	
Operation Restrictions	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.	

EXHIBIT 5-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Manual Override, Security and Training	Not addressed	Section 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. Section 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. Section E3.2.3: Controlled access security alarms used at station guideway and other system facilities. Section 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.
Maintenance of Safe Headway	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.	Section 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. Section 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. Section A2.4: Safe headway limit established by conservative vehicle stopping distance values. Section A2.7: During peak capacity periods, vehicles speeds will be reduced to allow shorter safe headway. Section A4.7: Safe headway automatically maintained if system failures cause reduced vehicle speeds.	Section 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.

EXHIBIT 5-1 (Continued)

BASELINE HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Magnetic Radiation	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 sue 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.	Section 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. Section B4.1: Upper and lower rows of magnets on vehicle create a filed 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.

EXHIBIT 5-2
Bechtel
Additional Hazards

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Additional Hazards Identified by Bechtel	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.
	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.	
	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.	
	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.
	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.
	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.	
	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.	

EXHIBIT 5-2 (continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Climatic/ Weather Related	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 in Table 8-A. Section 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. Section C1.7.7: Cabin pressurization prevents dirt, dust, smoke, and other unwanted contaminates from entering cabin. Section 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. Section 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. Section 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.	Section C1.9.5: SCD efforts to lighten vehicle were so successful that the center of gravity moved significantly higher. This aggravated the side wind stability problem. This deficiency is not addressed in the baseline design, but will be in later phase.

EXHIBIT 5-2 (continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Noise and Vibration	Not addressed.	Noise control for stations and other fixed facilities was not addressed. Section C1.13.3: Aerodynamic flow over the vehicle is a major noise source. Cabin noise is mitigated by use of insulation in the floor and walls. Vehicle vibration is another noise source. Floor and wall panels are thick enough to avoid significant vibration. Section H2.1: To reduce aerodynamic drag noise, vehicle height is reduced by an integrated suspension design. The box beam girder design leads to less aerodynamic drag than a channel guideway, but there is less noise shielding with no channel. In noise sensitive areas Bechtel suggests using noise barriers attached to the lower edge of the guideway to absorb and reflect sound. Bechtel uses largest possible single vehicle rather than multiple car trains to eliminate noise sources from the junction between cars. Cover plates are used on guideway covers to eliminate tonal noise. At speeds above 100 m/s the noise power increases as the sixth power of speed. Thus a small speed reduction results in a substantial noise reduction. Bechtel suggests operating at reduced speeds late at night and early in the morning. Further, they claim that because the Bechtel EDS design is so highly efficient at low speed, a low speed can allow the maglev to operate quietly in places where trains and buses are forbidden.	

EXHIBIT 5-2 (continued)

ADDITIONAL HAZARDS	ADDRESSED IN SCD		ISSUES
	PRELIMINARY HAZARD ANALYSIS	CONCEPT DESIGN PLAN FOR MITIGATING HAZARDS	
Tunnels	Not addressed.	No specific discussion on safety hazards of passing through tunnel. General recognition that proper design required to avoid hazards. Section 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%.	

5.4 EMERGENCY RESPONSE

5.4.1 Vehicle Emergency Evacuation Overall Strategy

The emergency evacuation strategy presented in this SCD suggests that passengers will remain on-board the vehicle at all times except for the potentially life-endangering situations identified as category I hazards (BE SCD 4.2, Section J, Vol. II). 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
- A back-up inflatable chute or slide

Controlled Vehicle Coasting to "Safe Stopping" Site

The Bechtel-proposed preferred means of vehicle emergency evacuation (Exhibit 5-3) 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 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 Exhibit 5-4. The SCD specifies aircraft Type-A doors (1.05m x 1.85m) for the Maglev vehicles (BE SCD 1.13.5 and Figure C1-58, Section C, Vol. 1, Book 2); these doors have up to 104 passengers per minute (BE SCD Figure C1-59, Section C, Vol. 1, Book 2).

The emergency platform can be used to transfer passengers/crew to a Maglev "rescue vehicle" on either track of the dual-track guideway, shown in Exhibit 5-4. 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 (BE SCD Figure C1-60, Section C, Vol. 1, Book 2). 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 (BE SCD 4.8, Section A, Vol. 1, Book 1). 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 (BE SCD 1.12.3 and 1.12.4, Section C, Vol. 1, Book 2) will not be used for coasting to a "safe stopping" site because of their relative uncontrollability.

EXHIBIT 5-3

Bechtel Proposed Vehicle Emergency Egress Means

Option A: Preferred "Safe Stopping Zone" Egress Option

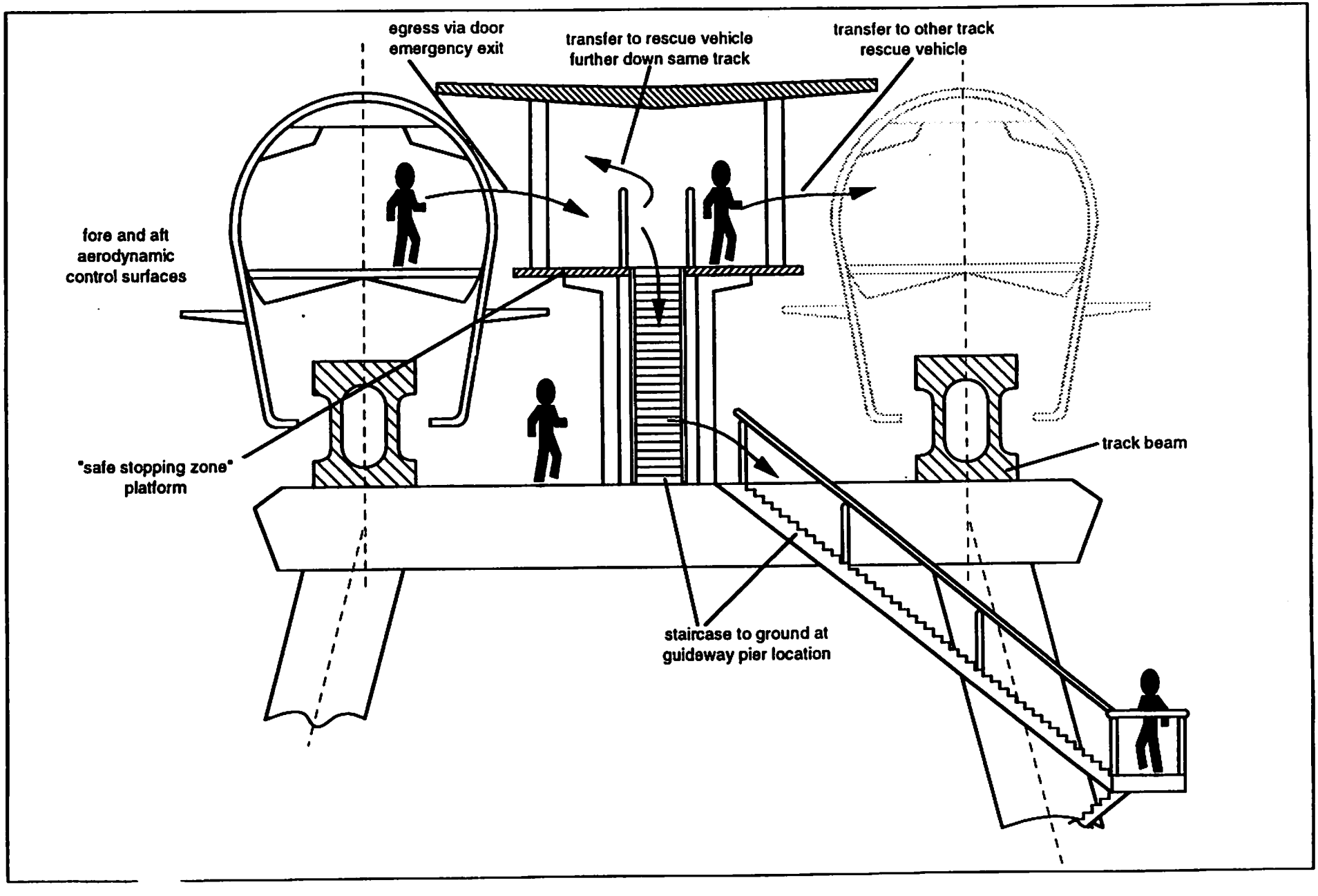
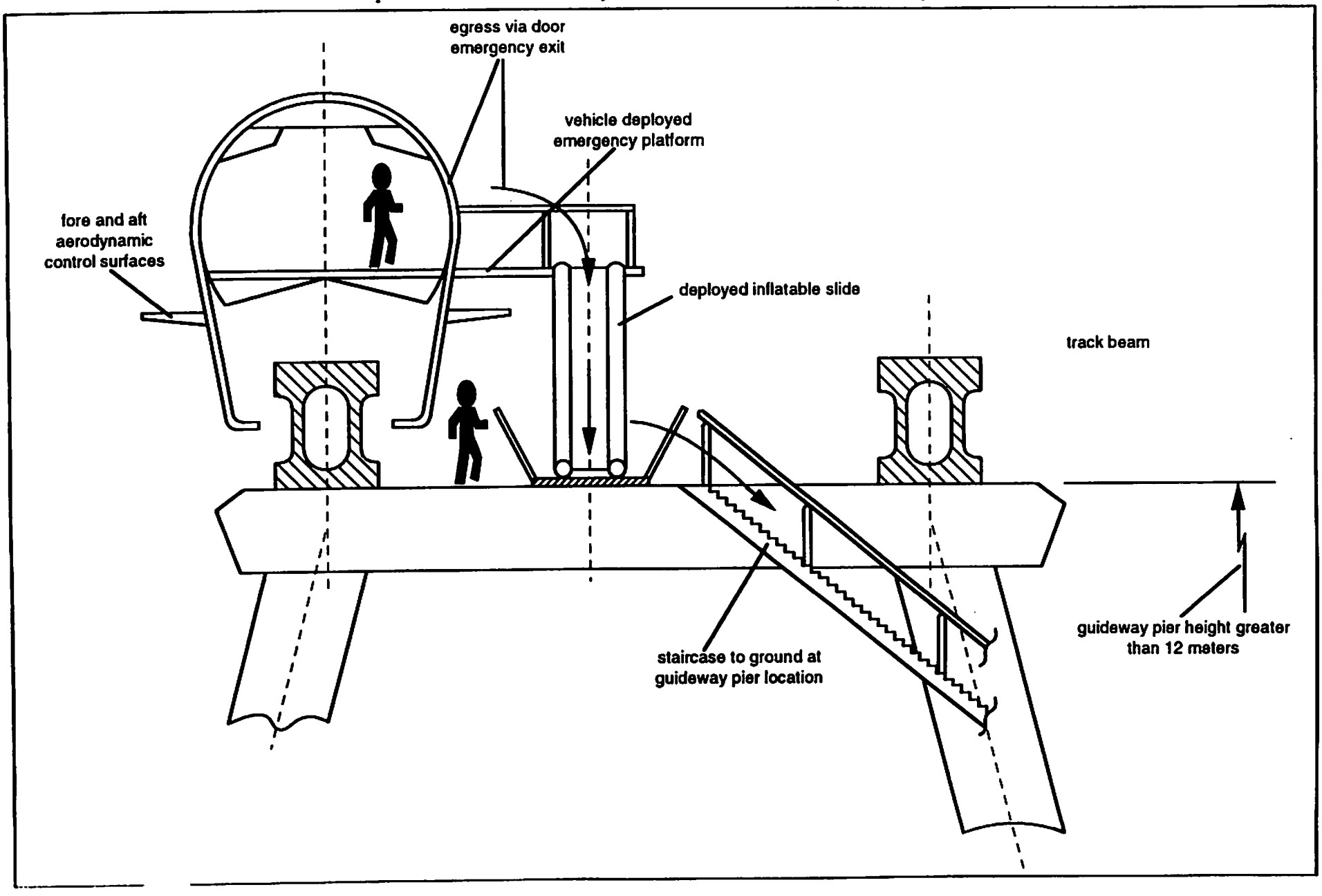


EXHIBIT 5-4

Bechtel Proposed Vehicle Emergency Egress Means

Option B1: Vehicle Doorway Inflatable Slide/Guideway Walkway



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 with the guideway power conditioning substations spaced at 4 km 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. Bechtel claims that a vehicle will coast to a stop in about 6 km from an initial speed of 80 m/s without dynamic braking and can be stopped in about 2 km with maximum dynamic braking (BE SCD 5.4, Section A, Vol. 1, Book 1). 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 (BE SCD 1.12.2, Section C, Vol. 1, Book 2) 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.

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 provide 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 advocated by Transrapid in their Maglev system and requires maintaining a vehicle "safe hover" condition while decelerating the vehicle to a "safe stopping" site. "Safe hovering" 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 loss of the primary magnetic suspension system relative to other emergencies which require safe stopping and vehicle evacuation.

The "safe hovering" condition for Bechtel is comparable to that of the Transrapid system. Thus, acceptance of the "safe stopping" site concept for the Transrapid Maglev system by the transportation regulatory community can be considered a precedent for acceptance of the concept for the Bechtel Maglev system. Loss of the Transrapid vehicle active feedback controlled electromagnetic 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 the suspension system is no longer acceptable for public transportation. This has resulted in Transrapid Maglev system reliance 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 systems, 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 (BE SCD 4.3, Section D, Volume II).

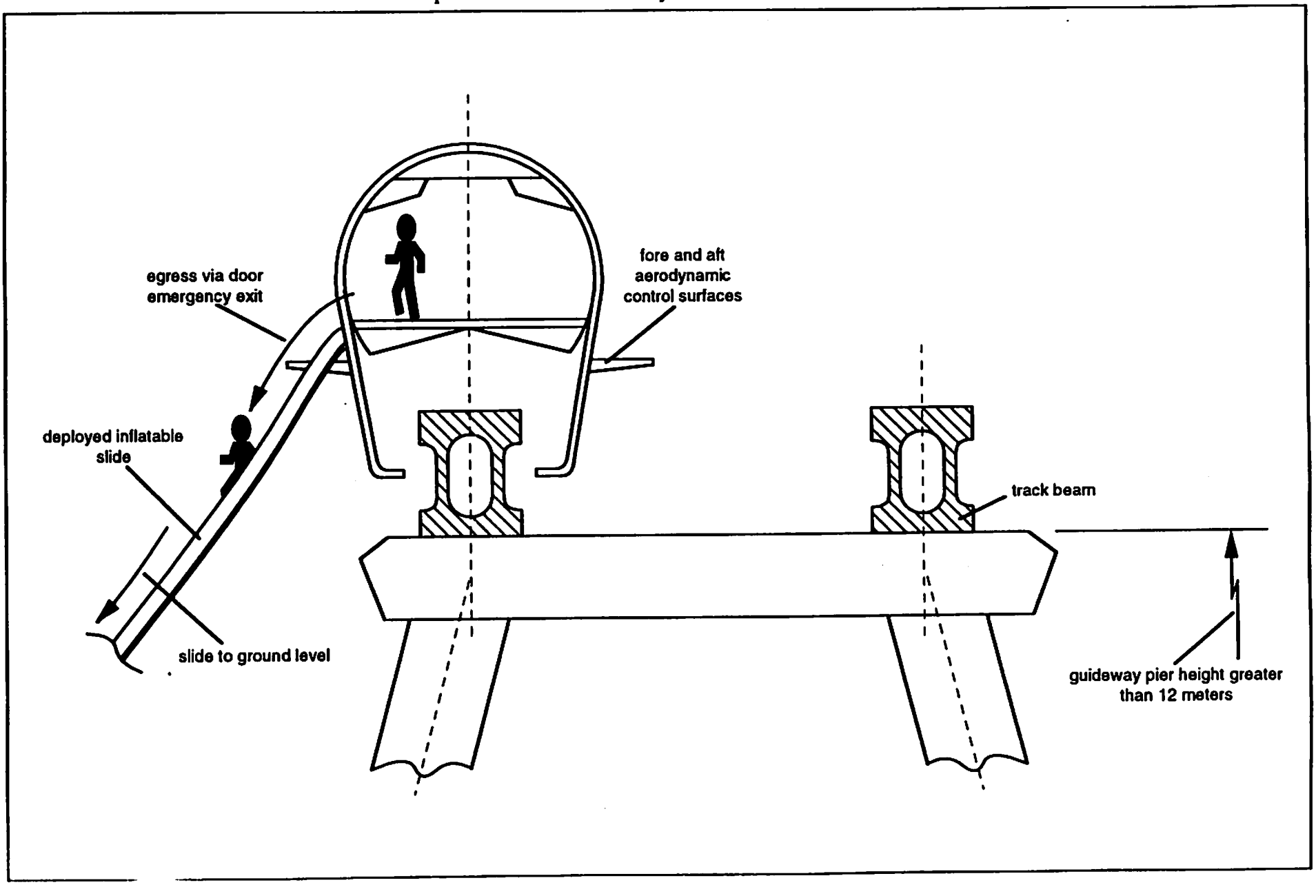
The probability of superconducting magnet quenching can be made extremely low by appropriate magnet design practice such as the practice reflected by the Bechtel SCD baseline magnet design having a winding current density of only 24% of the critical current as to provide for a conservative operational quenching safety margin of 4 (BE SCD 3.1, Section C, Vol. I, Book 2). State-of-the-art lightweight magnet dewars can be designed to exhibit exceptionally high reliability in being a structural rather than a power active component. 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.

Inflatable Chute or Slide Vehicle Egress

The 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 (reference Exhibit 5-5). Passengers and crew egress directly to ground level when the elevated guideway height does not exceed 12 meters, shown in Exhibit 5-4 (BE SCD 1.13.10, Section C, Vol. 1, Book 2).

In emergency evacuation situations where the guideway height exceeds 12 meters or where 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, shown in Exhibit 5-4 (taken from SCD Figure C1-62, Section C, Vol. 1, Book 2). A stairway to ground will be provided at intervals along the walkway, shown in Exhibit 5-5.

EXHIBIT 5-5
Bechtel Proposed Vehicle Emergency Egress Means
Option B2: Vehicle Doorway Inflatable Slide To Ground



5.4.2 Vehicle Emergency Evacuation Within Guideway Switch Zones

The proposed system baseline guideway switch is comprised 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. (BE SCD 5.3, Section A, Vol. I, Book 1).

Two additional alternative guideway mechanically passive switch design concepts are discussed. (BE SCD 4.1 and 4.2, Section D, Vol. II). The first mechanically passive switch design concept (BE SCD 4.1.4, Section D, Vol. II) incorporates auxiliary guidewalls located outside of the guideway boxbeam. This boxbeam is narrowed to a point, then split and progressively widened over the length of the switch to form two turn-off track branches (BE SCD D4-1, Section D, Vol. II). Guidance coils are embedded in the guidewalls and "frog windings" are embedded in the switch guideway floor between the guidewalls and the boxbeams. Suspension levitation/guidance ladders are provided on both sides of the switch boxbeam and inside of the guidewalls.

The preferred implementation of this switch uses passive guidance coils embedded in the guidewalls and boxbeam upstream of the switch point. These coils are interconnected to form null flux loops in two-pair sets. Electrically connecting and disconnecting these null flux loop sets will electrodynamically "steer" a vehicle towards one of the switch branches (BE SCD 4.1.5, Section D, Vol. II).

An alternate implementation of this switch uses active guidance coils embedded in the guidewalls and boxbeam and active "frog coils" embedded in the switch floor between the guidewalls and the boxbeam, all upstream of the switch point. Selectively activating one of two switch coil combinations will electrodynamically "steer" a vehicle towards one of the switch branches (BE SCD 4.1.6, Section D, Vol. II).

The second mechanically passive switch design (BE SCD 4.2, Section D, Vol. II) incorporates auxiliary switch walls located outside of the guideway boxbeam. Suspension levitation/guidance ladders are provided on both sides of the switch boxbeam and on the inside of the switch walls. Vehicle levitation and guidance can be transferred from the boxbeam ladders to the switch wall ladders by hydraulic actuated lateral outward displacement of the vehicle superconducting magnets. These magnets are suspended on swing arm linkages while the vehicle is traversing an upstream extended length of straight switch section. Upon entering the lift-off switch section, the outside switch walls begin to curve upwards, then swing away to one side when there is sufficient vertical clearance for vehicles to pass underneath—this forms the switch turn-out branch.

The most significant differences between the three designs lies in the switching motions. Vehicle motion through the turn-off branch for this switch design will be three dimensional while the corresponding motion through the first passive and baseline switch designs will be two dimensional. All three SCD documented switch design concepts are compatible with the "safe stopping" site emergency evacuation option because these sites will not be located at track switching zones on the guideway.

The baseline switch concept will be compatible with the inflatable slide emergency evacuation options shown in Exhibits 5-4 and 5-5, 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 meters. For straight-through and turn-out branch switch beam settings, switch elevations less than 12 meters 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.

The first of the two mechanically passive switch concepts will be compatible with the inflatable slide emergency evacuation options shown in Exhibits 5-4 and 5-5. Walkways can be placed along the outside of the guidewalls of this switch section that are accessible from the vehicle deployed inflatable slides for switch elevations exceeding 12 meters. Switch elevations less than 12 meters should have adequate switch structure and moveable magnet pod clearance to deploy inflatable slides on one side of the vehicle stopped in straight-through and turn-out switch branches.

The second of the two mechanically passive switch concepts is incompatible with the inflatable slide emergency evacuation options because of inaccessibility caused by the three-dimensional switch structure. It does not appear possible to place walkways along the straight-through and the turn-out branches on some portions of the switch section with elevations greater than 12 meters. Also, not enough clearance exists around the three-dimensional switch structure for deployment of inflatable slides for some portions of the switch length less than 12 meters high.

5.4.3 Vehicle Emergency Evacuation Within Superelevated Track Guideway Curve Zones

For the proposed vehicle, both the hydraulically actuated active cabin tilting and the guideway beam superelevation angles can each be up to 15 degrees (BE SCD 3.4, Section A, Vol. I, Book 1). Accordingly, any vehicle which is stopped on a superelevated track in an emergency should be capable of being 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 or elderly passengers. Emergency egress via vehicle deployable slides onto a guideway-attached walkway, shown for a level vehicle in Exhibit 5-5, cannot be considered because the slide may be misaligned with the walkway enough to jeopardize safe egression.

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 arises with stowage of the deployable slide below each door -- there is no mention of this in the SCD.

5.4.4 Adequacy of Vehicle Cabin/Crew Compartment Layout and Equipment 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 31" pitch with 23.4" aisle width specified on the Baseline Vehicle Specification Sheet of Vol. I, Book 2). Such practice should allow compliance with emergency evacuation standards which call for evacuation of a vehicle within 90 seconds of an emergency stop.

This emergency evacuation duration is considered adequate for a Maglev vehicle where the risk of rapid fire spreading and/or explosion in Maglev vehicles is lower than the risks for aircraft where large quantities of liquid fuel are typically on-board. In this regard, aircraft requirements (BE SCD 1.10.1, Section C, Vol. I, Book 2) for fire protection are specified.

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 (BE SCD 1.2.1, Section C, Vol. I, Book 2).

Four 1.0 meter 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-either for "safe stopping" site platform access or for escape slide deployment, shown in Exhibits 5-3, 5-4, and 5-5. 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, although a Boeing 747 aircraft cabin has 10 exit doors only 50% may be used in the FAA demonstration to evacuate a maximum of 500 passengers and crew. This is equivalent to 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 meters (30 ft) is easily satisfied by the proposed Maglev vehicle cabin layout.

5.4.5 Adequacy of Emergency Response Information Communication Means

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 (BE SCD 6.3/6.7, Sec A, Vol. I, Book 1).

A number of vehicle-to-guideway communication and/or data links are specified in the SCD. (BE SCD 4.3.4, Section C, Vol. I, Book 2). 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 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 and off of 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 (BE SCD 1.13.6, Section C, Vol. I, Book 2). This is consistent with 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 offer 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.

5.4.6 Provision for Emergency On-Board Power Supply

The SCD specifies an on-board fibered NiCad battery emergency power system which is completely independent of the on-board dual fuel cell normal power supply (BE SCD 1.5.3, Section C, Vol. I, Book 2). The emergency power supply is capacity-rated to supply power for emergency lighting, communications and emergency-only dc motors to operate the cabin normal ventilation fans for approximately one hour.

The vehicle hydraulic supply system, is required to operate the cabin tilting actuators and incorporates three accumulators (BE SCD 1.4.1, Sect. C, Vol. I, Book 2). 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 normally 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 uses air tanks sized to power these pads for at least one landing or take-off with the system air compressor inoperative (BE SCD 1.8, Section C, Vol. I, Book 2). 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.

5.4.7 Advantages of SCD Proposed Emergency Response Vehicle Evacuation Means

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 by 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, except the vehicle operating and system failure mode combinations noted in Subsection 5.4.8 below.

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.

5.4.8 Disadvantages of SCD Proposed Emergency Response Vehicle Evacuation Means

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 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.

The capital cost of a guideway mounted walkway required for vehicle emergency evacuation using deployable slides when guideway heights exceed 12 meters, is significant (estimated as about $1,000,000/mile in the BE SCD page C1-218, 1.13.10, Vol. I, Book 2, or about 11% of the cost of the dual guideway structure without the attachments).

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 when there is a power outage and not enough other vehicles are decelerating to provide sufficient regenerative power to provide some coast-extending thrust 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.

Evacuation using vehicle deployable slides when the guideway height exceeds 12 meters will be difficult on highly superelevated guideway curves when the vehicle cabin tilting system is inoperative.

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.

6.0 SUMMARY

The summary is under development and will reflect the outcome of the briefing held on January 7, 1993.