



# **National Automated Highway System Consortium Technical Feasibility Demonstration Safety Plan**

for the

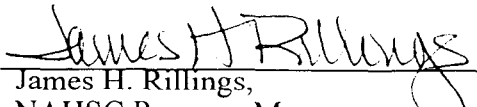
**Automated Highway System  
System Definition Phase  
Cooperative Agreement Number:  
DTFH61-94-X-00001  
Amendment 1**

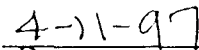
**April 7, 1997**

**Prepared by:**

**National Automated Highway System Consortium  
3001 West Big Beaver Road, Suite 500  
Troy, Michigan 48084**

**Approval:**

  
James H. Rillings,  
NAHSC Program Manager

  
Date



## Distribution

Name	Organization	Responsibilities
Bob Battersby	CALTRANS	Safety/Certification Team I-15 Corridor Safety Engineer
John West	CALTRANS	PMOC Chair, Safety Board Chair
Todd Jochem	CMU	Safety/Certification Team Development Engineer for Control Transition, Maintenance Certification
Phil Koopman	CMU	Safety/Certification Team Software Engineer
Michael Leshner	Eaton VORAD	Safety/Certification Team Vehicle Engineer for Truck Certification
Robert Neff	Eaton VORAD Technologies	Safety/Certification Team Vehicle Engineer for Truck Certification
George Clancy	General Motors	Safety/Certification Team Vehicle Engineer for Platoon, Multi-Platform Free Agent and Maintenance Certification
Mike Atkinson	General Motors	GM Proving Grounds, Safety Board Member
Damon Delorenzis	Honda	Safety/Certification Team Vehicle Engineer for Control Transition and Alternative Technologies Certification
Chris Barnes	Houston Metro Transit Authority	Development Engineer for Transit Buses in Multi-Platform Free Agent
Bill Kennedy	Lockheed Martin	Safety/Certification Team Development Engineer for Truck and Alternative Technologies
Joe Meyer	Lockheed Martin	Safety/Certification Team Co-Chair, Safety Engineer
Patrick Langley	Lockheed Martin	Alternate Safety/Certification Team Demonstration Integration Engineer
Patrick McKenzie	Lockheed Martin	System Integration Lead, Safety/Certification Team Demonstration Integration Engineer
Bill Stevens	NAHSC Program Office	Technical Director, Safety/Certification Team Software Engineer, Safety Board Member
James H. Rillings	NAHSC Program Office	NAHSC Program Manager, Safety Board Co-Chair
Ron Colgin	NAHSC Program Office	Vehicle Integration, Safety/Certification Team Chair, Safety Board Member
Terry Quinlan	NAHSC Program Office	NAHSC Demonstration Task Lead, Safety Board Member
Tommy Viner	NAHSC Program Office	Alternate Safety/Certification Team Demonstration Integration Engineer
Umit Ozguner	Ohio State University	Safety/Certification Team Vehicle Engineer for Alternative Technologies Certification
Andrew Segal	PATH	Safety/Certification Team Software Engineer
Wei-Bin Zhang	PATH	Safety/Certification Team Development Engineer Evolutionary and Multi-Platform Free Agent Certification
Michael Wolterman	Toyota	Safety/Certification Team Vehicle Engineer for Evolutionary Certification
Riley Garrett	Transportation Research Center	Safety Board Member





## National Automated Highway System Consortium

Suite 500 • 3001 W. Big Beaver Road • Troy, Michigan 48084

Phone: (810) 816-3400

Fax: (810) 649-9569

**Date:** 11 April 1997

**To:** See Distribution

**From:** Tommy Viner, Demonstration System Integration, NAHSC Program Office

**Subject:** NAHSC Technical Feasibility Demonstration Applicable Documents

**Enclosures:**

1. NAHSC Technical Feasibility Demonstration Safety Plan, dated 7 April 1997
2. NAHSC Technical Feasibility Demonstration Specification, dated 7 April 1997
3. NAHSC Technical Feasibility Demonstration Test/Certification Plan, dated 7 April 1997
4. NAHSC Technical Feasibility Demonstration Performance and Safety Certification

Procedure, dated 7 April 1997, with Appendices:

- Appendix 1 - Platoon Scenario
- Appendix 2 - Multi-Platform Free Agent Scenario
- Appendix 3 - Maintenance Scenario
- Appendix 4 - Evolutionary Scenario
- Appendix 5 - Control Transition Scenario
- Appendix 6 - Alternative Technology Scenario
- Appendix 7 - Truck Scenario

Enclosures 1 through 4 provide the safety, functional and performance requirements and procedures established for the conduct of the NAHSC Technical Feasibility Demonstration safety certification. These documents are provided for your reference and guidance during the certification and demonstration activities.

If you have questions related to any of the enclosures, please contact Tommy Viner at (810) 816-3405 or e-mail [vinert@nahs.org](mailto:vinert@nahs.org).

File#: 9700522



# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **SAFETY PLAN**

Draft Plan provided via Purchase Order RG6-437408

January 31, 1997

P.A. Reynolds

and

D.J. Funke

Calspan Final Report No. 8420-1

Updated by the NAHSC Consortium Safety Review Team

March 31, 1997





# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

## TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
1	SCOPE AND INTRODUCTION .....	1
2	ORGANIZATION AND IMPLEMENTATION .....	1
3	REQUIREMENTS.....	7
3.1	National Requirements .....	7
3.2	State and Local Requirements .....	7
3.3	Definitions .....	7
3.4	General Consortium Consideration .....	7
3.4.1	Demonstration Characteristics.....	7
3.4.2	Demonstration Reliability .....	10
3.5	Safety Requirements.....	13
3.5.1	Fault/Hazard Mitigation Form.....	13
3.5.2	Hazard List .....	15-16
3.5.3	Hazard Analysis.....	17
3.5.4	Requirements for Gaps Between Vehicles .....	17
3.5.5	Operational Safety Procedures .....	18
3.5.6	Driver Qualifications and Training Plans.....	19
3.5.7	Incident Management .....	21
3.6	Vehicle Certification Requirements .....	21
3.7	Mini-Demo Requirements .....	22
3.7.1	On-Site Demonstration.....	23
3.7.2	Off-Site Demonstration .....	23
4	DOCUMENTATION .....	23
5	SCHEDULE.....	24

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

## TABLE OF CONTENTS (Continued)

<u>Section</u>		<u>Page</u>
6	ISSUES AND RECOMMENDATIONS .....	27
6.1	No - Collision Gaps .....	27
6.2	Passenger Briefings and Waivers .....	27
6.3	Passenger Restraints .....	27
6.4	EMI From Manual Lanes .....	27
6.5	Software Loading .....	28
6.6	Mode Transition .....	28
7	REFERENCES .....	28
Appendix		
A	VEHICLE FAULT AND HAZARD CHECKLIST .....	A-1
B	FORMULAS FOR DETERMINING POTENTIAL COLLISIONS OF VEHICLE IN TRAIL.....	B-1

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

## LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
2-1	DEMO ORGANIZATION SAFETY INTERFACE .....	2
2-2	DEMO SAFETY ORGANIZATION .....	3
5-1	SAFETY PLAN IMPLEMENTATION SCHEDULE .....	25
5-2	SAFETY TASK FLOW .....	26

## LIST OF TABLES

<u>Table</u>		<u>Page</u>
3-1	OTHER DEMONSTRATION PLANS WITH SAFETY RELEVANCE.....	8-9
3-2	FAILURE PROBABILITY DEFINITIONS .....	11
3-3	AHS VEHICLE COMPONENTS RELIABILITY PROJECTIONS .....	12
3-4	PROJECTED GENERIC AUTOMATED VEHICLE SINGLE FAILURE RATE	12
3-5	HAZARD MITIGATION FORM.....	14
3-6	MINI-DEMONSTRATION SAFETY APPLICATION .....	22



# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **1. SCOPE AND INTRODUCTION**

This Safety Plan covers the I-15 live vehicle demonstrations and the activities involving moving vehicle demonstration at the Exhibition Center test area or nearby public roads. It does not cover activities at the Exhibit Hall and security measures at any of the sites. It also does not cover transportation of test vehicles to or from the Demonstration. The Plan includes procedures for implementation including the vehicle/scenario certification procedure and is designed to be executed in the short time available to the target August '97 demonstration.

The Plan provides checklists of vehicle/scenario faults and hazards based on general Calspan experience with automated flight and ground vehicles and study of AHS Safety, Malfunction Management, Incident Management, Entry/Exit, Vehicle Operations, Roadway Operations, and other tasks as part of the AHS Precursor Studies. The Plan calls for identification and mitigation of faults and hazards specific to the demo vehicles and scenario designs for the Demonstration requiring that the checklists be adopted and expanded to suit.

The Plan recognizes that the vehicles are experimental and are largely complete as this document is finalized, making safety requirements specifying redundancy, independent safety monitoring sensors, special monitoring software, etc. impossible to provide within budget and time available. Therefore the emphasis is on failure mitigation by limiting authority and by manual takeover.

## **2. ORGANIZATION AND IMPLEMENTATION**

Safety activities will be accomplished by a Safety Review Team (referred to as "the Team") and a Safety Board (referred to as "the Board. Figures 2-1 and 2-2 illustrate how the safety activities fit with the other demonstration activities and the division of the safety task into areas of responsibility.

The Team and Board are formed by the System Integration Lead with the approval and recommendations of the Demo Lead, NAHSC Technical Director and NAHSC Program Manager. The recommended size for the Team is six to eight, roughly one person for each area of responsibility shown on Figure 2-2.

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

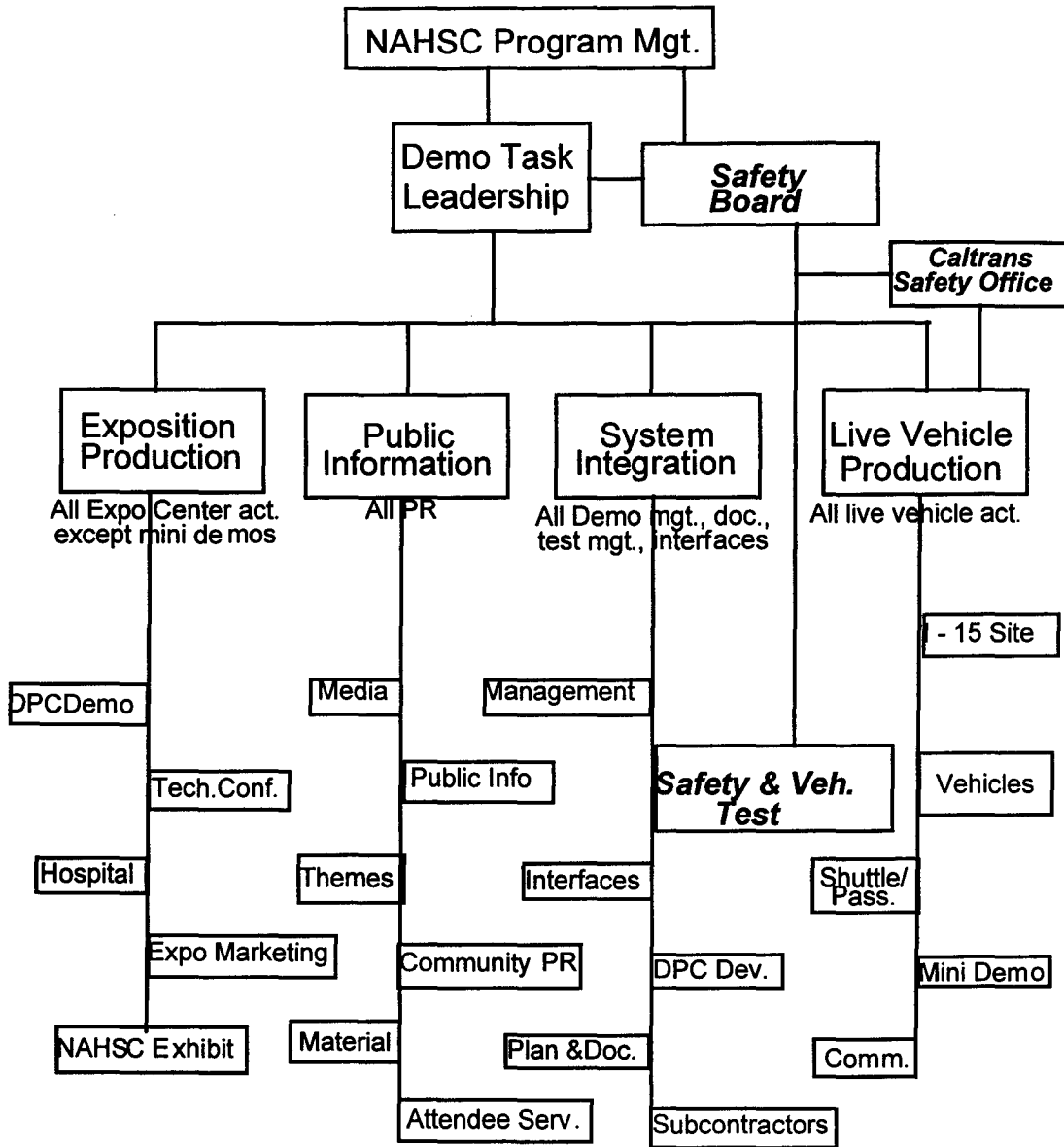


Figure 2-1 Demo Organization Safety Interface

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

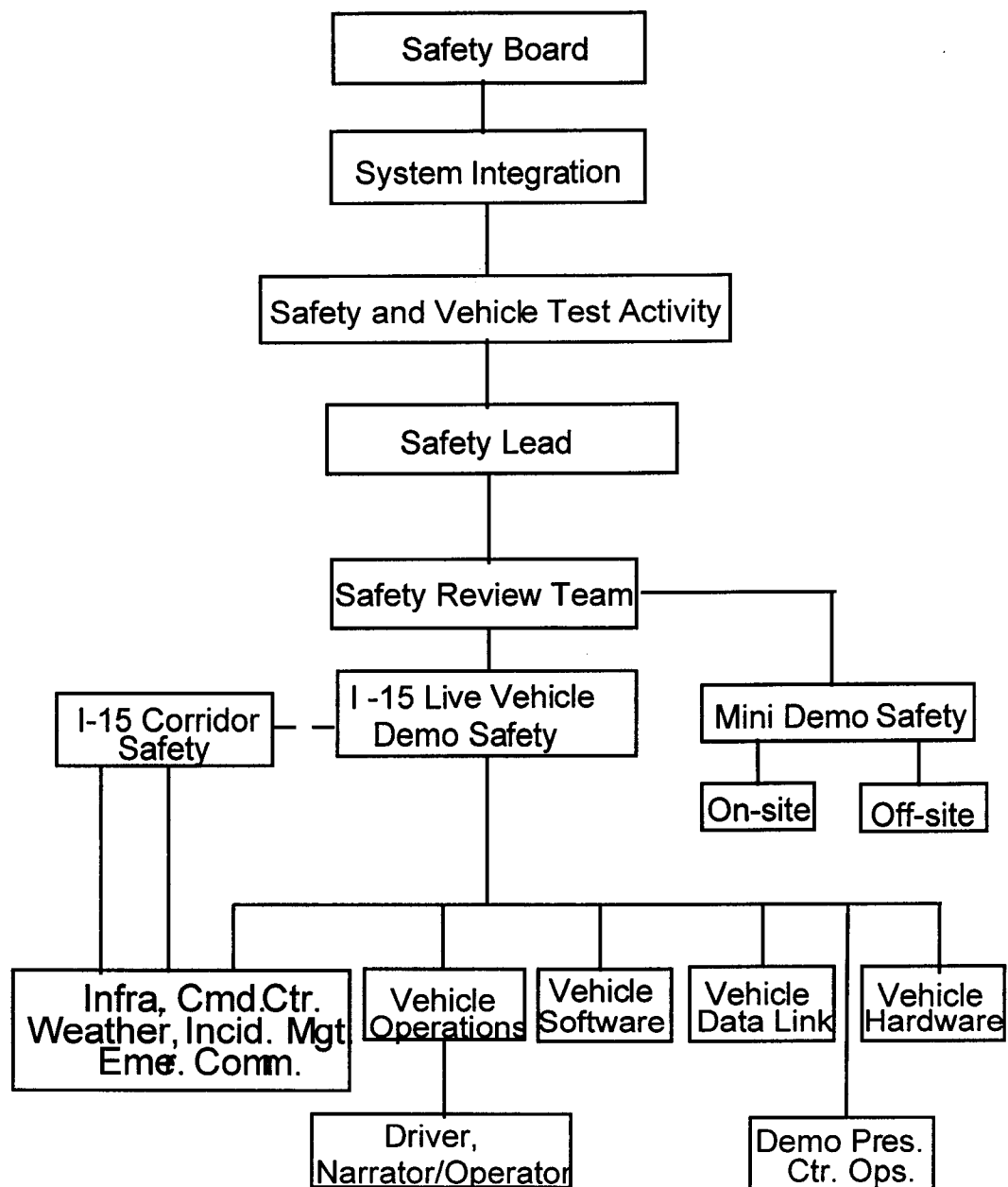


Figure 2-2 Demo Safety Organization

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

Members of the Team are drawn from System Integration and Live Vehicle Production or elsewhere in the Core membership. They qualify as "Domain Experts". Some have ground and/or flight vehicle automation in their backgrounds with experimental or prototype hardware experience. One member of the Team will serve as the Safety Team Chair.

Membership will include both regular and rotational members. This group will also serve a dual role as the Certification Test Team overseeing pre-certification and certification activity. Members include:

<u>Name</u>	<u>Organization</u>	<u>Responsibilities</u>
Ron Colgin	NAHSC P.O.	Safety/Certification Team Chair, Vehicle Integration Engineer
Joe Meyer	LMC	Safety/Certification Team Co-Chair, Safety Integration Engineer
Pat McKenzie	LMC	Demonstration Integration Engineer
Phil Coopman	CMU	Software Engineer
Andrew Segal	PATH	Software Engineer
Bill Stevens	NAHSC P.O.	Software Engineer
Bob Battersby	CALTRANS	I-15 Corridor Safety Engineer
George Clancy	GM	Vehicle Engineer for Platoon, Multi-Platform Free Agent and Maintenance Certification
Damon Delorenzis	Honda	Vehicle Engineer for Control Transition and Alternative Technology Certification
Michael Wolterman	Toyota	Vehicle Engineer for Evolutionary Certification
Michael Leshner	Eaton VORAD	Vehicle Engineer for Truck Certification
Bill Kennedy	LMC	Development Engineer for Truck and Alternative Technology Certification
Wei-Bin Zhang	PATH	Development Engineer Evolutionary and Multi-Platform Free Agent Certification
Todd Jochem	CMU	Development Engineer for Control Transition, Maintenance and Platoon Certification
Tommy Viner	NAHSC P.O.	Alternate Demonstration Integration Engineer



# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

Responsible for the day-to-day contact with the Demo Team for all Safety related issues. This team will be responsible for finalizing and implementing the Demo '97 Safety Plan and associated certification procedures. It will finalize the Safety requirements and ensure their inclusion in vehicle certification procedures. The team will ensure proper staffing of safety related positions for Demo execution. This group will also develop recommended "pass / fail" criteria for each step in the certification process and provide that criteria to the Safety Board for their approval. This team will distribute the hazard questionnaires and facilitate the return of said material with appropriate vehicle developers. A subset of the Safety Review Team will be present at all pre-certification and certification runs executed by vehicle scenarios. Each subset group will report findings to the rest of the Safety Review Team and summaries will be provided to both the Safety Board and the Demo Team at large. The Safety Review Team Chair will coordinate and present appropriate briefings to the Safety Board at their monthly meetings.

The Safety Review Team will hold teleconferences regularly beginning in April 1997 and meet face-to-face once a month (may want to hold just prior to each Demo Team meeting to try to cut down on travel expenses). All regular members of the Review Team should participate in the weekly Safety Review Team teleconferences with rotational members "taking turns". All regular members of the review team will participate in as many pre-certification and certification runs as possible. As the team Chair, Ron will be responsible for coordinating the participation of the rotational members in pre-certification and certification activities. Rotational members may wish to delegate their participation in a given certification event to another member of their team should they not be available. Replacement would be coordinated well in advance with Ron. (NOTE: No rotational member will be allowed to participate as a part of the review team for their own scenario.)

After certification, the Team collects further information during Dry Runs and Dress Rehearsals in the form of Configuration Control and failure report documentation.

The Demonstration Safety Board is the principle adjudication body regarding Safety issues for Demo '97. Their primary responsibility will be to ensure that all reasonable efforts have been made to ensure the safety of participants and attendees at all Demo '97 events (dry runs, dress rehearsals, the demo itself). They will accomplish this by meeting on a regular basis (exact dates TBD) to review safety materials (safety questionnaires, hazard mitigation forms, safety requirements, pre-certification test results, and certification test results) and to receive

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

safety requirements, pre-certification test results, and certification test results) and to receive safety briefings related to those materials. In cases of significant safety concern, selected members of the Safety Board may choose to exercise a "hands on" approach to working the issue. The Safety Board will report it's findings to the PMC and make the final decisions on live vehicle participation with the advice and counsel of the PMC. If the PMC disagrees with a Safety Board recommendation, it could appeal to the PSB.

The Board members should have served on other safety boards on programs involving early testing of experimental, person-rated ground or flight vehicles. Preferably these persons will have automotive experience. At least one Board member should come from outside the Consortium membership. Membership criteria and selection will be finalized by the Safety Board Chair, John West. Tentative membership includes:

John West (PMOC Chair)	- Safety Board Chair
Jim Rillings (NAHSC Program Manger)	- Safety Board Co-Chair
Bill Stevens ( Technical Director)	- Member
Terry Quinlan (NAHSC Demo Task Lead)	- Member
Ron Colgin (Safety Review Team Chair)	- Member
Mike Atkinson (GM Proving Grounds)	- Member
Riley Garrett (Transportation Research Center)	- Member
Others as determined by the Board Chair	

The Board will meet approximately once a month during the period from March through June 1997. At those meetings, decisions regarding safety issues (such as "can the Houston Metro buses carry passengers without having seat belts?") will be made for subsequent presentation to the PMC. Decisions regarding live vehicle scenarios will also be made by the Board (scenario passed pre-certification, scenario failed pre-certification ... must redo, scenario passed certification, scenario is cleared for Demo '97 participation, etc.). The Board will probably need to meet twice in July (just prior to dress rehearsals and a few days after the last dress rehearsal). The Board may also decide it needs to be "on call" in early August and throughout the Demo in the event an unforeseen safety issue arises.

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **3. REQUIREMENTS**

### **3.1 NATIONAL REQUIREMENTS**

The NAHSC Collaborative Agreement does not specifically call out Governmental or industry safety requirements as applicable. However, the Safety Review Team should use these requirements as a guide where practical.

### **3.2 STATE AND LOCAL REQUIREMENTS**

The Caltrans I-15 Testing Safety Procedures (Ref. 5) are required.

If a vehicle is to be operated on public roads (other than the I-15 HOV test track), it will be required to have valid registration. All individual live demonstration vehicles including live mini-demo vehicles must be covered by liability insurance provided by the vehicle owners.

There are no known local safety requirements.

### **3.3 DEFINITIONS (Refs. 6 and 7)**

**Fault** - Physical defect, imperfection or flaw in hardware or software (can be latent).

**Error** - Unintended or incorrect physical or logical state of a subsystem element; the result of a fault.

**Failure** - Incorrect performance of subsystem element(s); the result of an error.

**Hazard** - an existing or potential condition that can result in a mishap.

Not all faults produce errors and not all errors produce failures. A failure can create a hazard if it happens at the wrong time or place. A hard-over failure is one that causes the subsystem output to move to its maximum possible value at maximum possible rate.

In the fault/hazard analysis required by this plan, our interest centers on those faults/hazards that could result in critical or catastrophic mishaps if not mitigated.

**Catastrophic** - loss of life or severe injury

**Critical** - moderate injury and/or property damage

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

Marginal - minor injury, failure to achieve Demo goal(s).

Negligible - no significant impact on Demo goal(s).

## 3.4 GENERAL CONSIDERATIONS

### 3.4.1 Demonstration Characteristics

Since I-15 activity involves fully automated vehicles at freeway speeds and closer than normal spacing, the activity must be undertaken with more than the normal caution. Orchestrating multiple-vehicle scenarios, sometimes simultaneously, involves coordination of many separate people and activities from many different organizations. Timing and control are important to a smooth, fast-paced and entertaining presentation and to a safe demonstration. Table 3-1 is a list of other demonstration planning documents that are relevant to the Safety Plan. The Safety Review Team will be familiar with the provision of these plans, particularly as indicated in the "Relevance" column.

**Table 3-1**  
**OTHER DEMONSTRATION PLANS WITH SAFETY RELEVANCE**

Paragraph in Demonstration Planning Document	Relevance
Entire report	Defines content of all plans.
6.6 Development	Should mention Fault/Hazard Process in preparation.
6.9 Communications	Baseline for defining procedures for loss of communication.
6.12 Operations	Baseline for defining procedures in the event of operational failures
6.10 Live Demo Procedures	Defines contingency operational procedures and go/no-go criterion.
6.2 Traffic Mitigation	Minimizes probability of incident in manual lanes.
6.1 Risk Mitigation	Overlaps with Fault/Hazard process in dealing with technical risks.
6.4 Test/Validation	Describes details of pre-certification , certification dry-run and dress rehearsal tests.
6.5 EMC/EMI Control	Describes analysis and tests specifically designed to prove EMC and EMI immunity in the actual I-15 environment.

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

Table 3-1 (Cont.)

## OTHER DEMONSTRATION PLANS WITH SAFETY RELEVANCE

Paragraph in Demonstration Planning Document	Relevance
6.17 Maintenance and Repair	Includes required Configuration Control of hardware and software.
6.13 Security	Includes precautions against deliberate disruptive or damaging activity at the I-15 site
6.15 Contingency	Cover contingencies not mentioned in other plans.

In accomplishing these plans the System Integration and Vehicle Production activities have close contact with the eight vehicle/scenario participants, three of which are led by Core Consortium members and five led by Associate members. (One Core member has joined together with one Associate member to stage a combined scenario). Much of the vehicle fault/hazard process will be accomplished by the organizations with Safety Review Team responsibility. The participants will provide the Safety Review Team with their top-level vehicle designs and enough analysis and test information to satisfy safety concerns as documented in the Fault/Hazard Mitigation forms and in this document.

The Safety Review Team and the Safety Board will be aware that many of the vehicle automated subsystems are proof-of-feasibility, non-redundant elements with low hours of unit and integrated testing. Software verification and validation testing may not be as complete as that of a pre-production prototype and fault tolerance may not be fully demonstrated. Demonstration safety is to be provided by trained test drivers with many hours of experience in the demo vehicles, executing scenarios with detailed scripts, capable of safely dealing with worst-case, hard-over failures of the major control subsystems. The effect of these failures will be minimized by limiting the authority of the automated mode compared with the manual mode of each critical subsystem - throttle, steering and braking.

The Safety Review Team also needs to be aware that safety as perceived by the passengers will also be very important. The scenario should not require maneuvers, timing or driver actions which are more urgent than a non-stressful freeway ride. The vehicle performance should be as smooth and comfortable as possible. Rough or erratic and possibly non-repeatable

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

performance would be reasons for insufficient perceived safety even though real safety criteria are satisfied.

## 3.4.2 Demonstration Reliability

This section provides a numerical framework for estimating the reliability of the demonstration preparation activity on I-15 and the probability of running four days of demonstration without critical sub-system failures. Hazard analysis questionnaires prepared by vehicle developers will be followed up by high level fault tree analysis for each of the potential hazards which fall into the “critical” or “catastrophic” range. Actual application of this analysis by the Safety Review Team would treat the specific vehicles and their equipment and will specifically address questions like, “What is the probability of conducting all I-15 runs without a steering failure?” Assuming that the experimental nature of these vehicles will result in “some” failures, the next significant question to consider is, “Assuming you do have a steering actuation failure, how is the operator made aware of the failure and is he/she capable of safely taking over control of the vehicle?”. Finally, from a “perceived safety” perspective, how many failures over the course of Demo week would the Consortium deem “acceptable” and how will the certification team test for this “robustness”?

In Table 3-2 are listed failure probability definitions to be used in the Fault/Hazard Mitigation Form and the implied mean time between failure (MTBF) of the subject component.

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

**Table 3-2**  
**FAILURE PROBABILITY DEFINITIONS**

Definition of Failure Probabilities based on Demo Lifetime	Single Vehicle MTBF (hours)		Probability of at least one failure in Lifetime
	Lifetime of 200 hrs.	Lifetime of 1300 hrs.	
• Frequent - Likely to occur frequently	44	286	.99
• Probable - Will likely occur several times	87	565	.90
• Likely - Equal chance of occurring as not occurring	289	1,879	.50
• Remote - Unlikely, but possible	1,898	12,337	.10
• Improbable - So unlikely that it may be assumed it will not happen	19,900	129,350	.01

The assumed lifetimes for this table are 200 and 1300 vehicle-hours on the basis of the planned I-15 activity. The lifetime defined for Safety Plan purposes is the total vehicle-hours with passengers which is the sum of planned dress rehearsal and actual demonstration vehicle-hours. At the present time this is estimated at 200 vehicle-hours.

Based on data on disabling vehicle failure (failures causing stoppage) frequency for the Toronto 401 and the San Francisco Bay Bridge, the mechanical/electrical failure rate for the vehicle populations in those localities is about 450 per million vehicle hours (Ref. 8).

To estimate projected AHS vehicle reliability we looked at failure data of similar components available primarily from Government sources and put components together to make systems. The basic data is summarized in Table 3-3, and an estimate for an entire demo vehicle with no redundancy, based on this data, is given in Table 3-4.

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

**Table 3-3**  
**AHS VEHICLE COMPONENTS RELIABILITY PROJECTIONS**

	Failures per Million Hours
1. Longitudinal Sensing	14 to 135
2. Lateral Sensing	6 to 135
3. Computer Processing	7 to 22
4. Longitudinal Control	78 to 134
5. Lateral Control	58 to 72
6. Communications	40 to 94
7. Status and Operations	22 to 292
8. Malfunction Management	<u>53 to 213</u>
TOTAL	278 to 1,097

**Table 3-4**  
**PROJECTED GENERIC AUTOMATED VEHICLE SINGLE FAILURE RATE**

Subsystem	Failures per Million Vehicle Hours (FPMH)
Basic Vehicle	411 to 490
Speed and Gap Control - Items 1, 3, 4	99 to 304
Lane Control - Items 2, 3, 5	71 to 229
Status and Operations - Item 7	22 to 292
Vehicle Data Link - Item 6	40 to 94

$$\begin{aligned} \text{Total FPMH} &= 643 \text{ to } 1409 \\ \text{MTBF} &= 1555 \text{ to } 710 \quad \left( \text{MTBF} = \frac{10^6}{\text{FPMH}} \right) \end{aligned}$$

Using the exponential probability distribution, the probability of experiencing at least one failure in time  $t$ , is  $e^{-t/\text{MTBF}}$ . If all vehicles in a given activity had the same failure rate using the above assumptions, then the probability of having at least one failure in 200 vehicle-hours is .12 to .25.

Assuming the numerical analysis presented above is flawed (after all, it is based on data which may or may not accurately reflect the components being used in Demonstration '97), we must utilize the fault tree analysis method combined with a rigorous certification process to get better "failure probability" numbers for each live vehicle scenario. Requirements need to be included in the Demonstration Specification which address "robustness" of major vehicle systems along with requirements which assure the safe transition to manual control should failures occur. The experimental systems may not be as reliable as in Table 3-4. They could end



# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

up being more reliable. Since the data we have to work with is limited, it is best to assume that the probability of a failure to critical subsystems is "Likely" (see Table 3-2). Therefore a major focus of the safety plan is to ensure that if a failure is experienced, the vehicle design and operational procedures will provide the required safety.

## **3.5 SAFETY REQUIREMENTS**

Safety requirements which will be included in all vehicle certification procedures are documented in the NAHSC Technical Feasibility Demonstration Requirements Specification.

### **3.5.1 Fault/Hazard Mitigation Form**

A form similar to the one shown as Table 3-5 shall be used to document the faults and hazards which are initially classified as catastrophic or critical. Lower-level fault/hazards can be documented if the resources are available.



# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

**Table 3-5  
Fault/Hazard Mitigation Form**

**Title of Fault/Hazard :** \_\_\_\_\_

**Description:** \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

**Submitted by :** \_\_\_\_\_

<u>Demo Element</u>
<input type="checkbox"/> DPC
<input type="checkbox"/> Infra., Cmd. Ctr., Weather Incident Mgt., Emer. Comm.
<input type="checkbox"/> Veh. Software
<input type="checkbox"/> Veh. Data Link
<input type="checkbox"/> Veh. Hardware
<input type="checkbox"/> Veh. Operations

<u>Scenario</u>
<input type="checkbox"/> Multiplatform Free Agent
<input type="checkbox"/> Platoon
<input type="checkbox"/> Maintenance
<input type="checkbox"/> Truck
<input type="checkbox"/> Control Transition
<input type="checkbox"/> Radar Reflective
<input type="checkbox"/> Evolutionary

<b>Hazard Assessment</b>	
<b>Estimated Probability in 200 Veh. Hrs. (Dress Rehearsals, and Demo )</b>	<input type="checkbox"/> A. Frequent (>.99) <input type="checkbox"/> B. Probable (.90 to .99) <input type="checkbox"/> C. Likely (.1 to .9) <input type="checkbox"/> D. Remote (.01 to .10) <input type="checkbox"/> E. Improbable (<.01)
<b>Seriousness of Consequences</b>	<input type="checkbox"/> I. Catastrophic <input type="checkbox"/> II. Critical <input type="checkbox"/> III. Marginal <input type="checkbox"/> IV. Negligible
<b>Mitigation</b>	<b>Description</b>
<b>Assessment after Mitigation</b>	<input type="checkbox"/> A. Frequent <input type="checkbox"/> B. Probable <input type="checkbox"/> C. Likely <input type="checkbox"/> D. Remote <input type="checkbox"/> E. Improbable
<b>Remarks</b>	
<b>Status</b>	<input type="checkbox"/> Open <input type="checkbox"/> Closed
<b>Reviewed by</b>	



# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **3.5.2 Hazard List**

A hazard list will be produced as a first step in defining safety precautions. Hazards will be identified and listed for:

- The operations involved in each scenario
- The operations involved in coordinating among scenarios
- All possible environmental conditions
- The operations for supporting the demo in general
- Procedures for manual takeover following failures

The hazard list will consider timing errors, communication errors, communication failures, vehicle failures, and so forth. Several examples are given on the next page:

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

Hazard	Mitigation Approach
<b>Scenario-Specific Hazards</b> <b>Multiplatform Free Agent Scenario (CMU):</b> <ul style="list-style-type: none"> <li>- Front vehicle avoids obstacle too late for second vehicle to acquire and avoid (obstacle hit, or severe maneuver attempted by driver causes skid, etc.)</li> <li>- Emergency vehicle in wrong lane, lane change maneuver creates accident</li> <li>- Lane change at wrong time creating accident with other vehicle</li> <li>- Lateral control is erratic when buses are side by side.</li> </ul> <b>Platoon (PATH):</b> <ul style="list-style-type: none"> <li>- Inter-vehicle data-link lost.</li> <li>- Driver intervenes in vehicle braking beyond 0.3 gs</li> </ul> <b>Maintenance (Caltrans; IDV, DRV):</b> <ul style="list-style-type: none"> <li>- IDV instrumentation indicates unscripted faulty magnet</li> <li>- DRV fails to locate designated debris</li> </ul> <b>Heavy Commercial Vehicle (Eaton/Vorad):</b> <ul style="list-style-type: none"> <li>- Sensor fails to acquire stopped vehicle target</li> </ul> <b>Control Transition (Honda):</b> <ul style="list-style-type: none"> <li>- Change in lateral control sensor disengages lateral control</li> </ul> <b>Radar Reflective Technology (OSU):</b> <ul style="list-style-type: none"> <li>- Passing vehicle starts to return to right lane before proper gap has been established</li> </ul> <b>Evolutionary (Toyota):</b> <ul style="list-style-type: none"> <li>- Passing vehicle timing is in error and blocks right lane automated vehicle from avoiding obstacle.</li> </ul>	<ul style="list-style-type: none"> <li>- Set following distance to avoid problem</li> <li>- Verify during vehicle/scenario certification</li> <li>- Obstacle is lightweight, not dangerous threat</li> <li>- Operational procedure to avoid lane confusion</li> <li>- Vehicle certification, operational procedure, scenario monitoring</li> <li>- Vehicle certification</li> <li>- Operational procedures</li> <li>- Operational procedures, driver training</li> <li>- Vehicle maintenance</li> <li>- DRV driver surveys larger section of lane</li> <li>- Minimize time when buses are side by side</li> <li>- Procedure specifies manual braking to start at given roadside marker</li> <li>- Procedure to re-engage lateral control after control error is corrected</li> <li>- Driver intervenes and prevents lane change until safe</li> <li>- Procedure allows margin for error. Requires achieving desired speed at a pavement marker and gap</li> </ul>
<b>Inter-Scenario Hazards</b> <ul style="list-style-type: none"> <li>- Failure or speed variance in one scenario creates unsafe headway</li> <li>- Failure of inter-demo coordination</li> </ul>	<ul style="list-style-type: none"> <li>- Operational procedure, staff training</li> <li>- Operational procedure, staff training</li> </ul>
<b>Environmental Hazards:</b> <ul style="list-style-type: none"> <li>- Communication interference</li> <li>- Weather (rain, fog, wind gusts)</li> <li>- Accident spill-over (from public lanes)</li> <li>- Unintended obstacle</li> <li>- Low sun angle, glare</li> </ul>	<ul style="list-style-type: none"> <li>- Vehicle cert./verification, operational procedure</li> <li>- Vehicle cert./verification, operational procedure</li> <li>- Jersey barriers, operational procedure</li> <li>- Jersey barriers, demo monitoring, operational procedure</li> </ul>
<b>General Demonstration Operational Hazards:</b> <ul style="list-style-type: none"> <li>- Camera or monitor failure prevents demo monitoring</li> <li>- Distraction impact on manual lanes</li> </ul>	<ul style="list-style-type: none"> <li>- Operational procedure</li> <li>- Operational procedure (e.g., minimize use of flashing lights)</li> </ul>
<b>Failure Mode Mitigation Hazards:</b> <ul style="list-style-type: none"> <li>- Failure mode causes hand-off to driver under unsafe conditions</li> <li>- Obstacle is hit into manual lanes</li> </ul>	<ul style="list-style-type: none"> <li>- Operational procedures, vehicle certification</li> <li>- Jersey barriers</li> </ul>

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **3.5.3 Hazard Analysis**

Each hazard identified on the hazard list will be analyzed using the Fault/Hazard Mitigation Form (Table 3-5). The analysis will define the hazard in terms of: description, causal factors, and possible mishaps, probability of occurrence, and seriousness of consequences. It will also be used to define mitigation strategies and requirements for hazard tracking and verification. The Safety Board will review all hazard analyses to ensure that adequate safeguards are planned.

## **3.5.4 Requirements for Gaps Between Vehicles**

The minimum gaps between vehicles will be stated in the scenario scripts. Operationally, these are controlled by the software while under automated longitudinal control and by the driver while under manual control. Safe gap depends on detection time, vehicle decelerations, and speed. Detection time depends on how the failure is detected and on how the trailing vehicle knows about the failure. Hazard analysis by the individual vehicle development teams will lead to spacing requirements that are unique to the given scenario. These requirements are to be verified, for the most part, utilizing the “analysis” test method whereby the vehicle developers will submit documentation which describes why the spacing selected is “safe”. An example of one method for doing spacing analysis is included as Appendix B of this document. Analysis provided by vehicle developers will be reviewed by the Safety Review Team and if deemed acceptable, will go forward to the Safety Board for final approval. This analysis will be combined with a rigorous certification process to verify the satisfaction of the “spacing” requirement.

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

## 3.5.5 Operational Safety Procedures

Based on the above analyses, Operational test procedures will be defined for integration within the appropriate test planning documents (e.g., the 1997 Demo Plan, etc.). These procedures will focus specifically on safety matters and will include: (1) tests and/or checks to be conducted at the beginning of each demo day to ensure that all safety critical equipment and functions are working properly; (2) procedures to be implemented within the demo control process to ensure that potential hazards are avoided; (3) procedures to be implemented under anticipated and unanticipated failure and/or hazard conditions (e.g., weather conditions); (4) communications protocols to communicate safety-critical information among demo participants; and (5) emergency procedures for implementation in safety critical situations.

The major required safety procedures are identified below:

- A procedure for verifying at the beginning of each demo day that all safety critical vehicle components (e.g., lateral and longitudinal control components, control logic, communication equipment) are working properly.
- A procedure for ensuring that all safety conditions are met before each scenario is allowed to enter onto the I-15 course, and before automated driving is permitted. This procedure will ensure that: all vehicles in the scenario are ready and operating properly; all communication channels are available and working properly; the scenario to be run is the proper scenario in the plan sequence; that obstacles are absent from the route or properly placed for the scenario starting; and the vehicle occupants are ready to go. If obstacles are to be placed or removed during the scenario (after it is underway), the procedures will ensure that the obstacle placer is in position to properly place or remove the obstacle, is aware of the proper obstacle placement/condition for the scenario and is not exposed to automated traffic.
- A procedure for ensuring that the Command Center is made aware of all major state changes for each scenario, and for tracking these states. State changes will include: scenario ready to start; scenario starting; major scenario events starting/ending; vehicles reaching passenger loading/unloading point.



# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

All operational safety procedures will be defined in the Operations Plan and the Live Demo Procedures Plan and implemented to ensure safety of all dress rehearsals and demo runs. They will also be applied during dry runs. During the dry runs the safety procedures will serve to ensure safety, but will also be verified and fine-tuned to ensure they are efficient and effective for providing safeguards against mishaps.

Because Demonstration '97 will involve new technology implemented with experimental equipment, careful definition and implementation of safety procedures will serve a critical role for ensuring safety.

## **3.5.6 Driver Qualifications and Training Plans**

Based on the hazard analyses and operational test procedures, training plans will be made for ensuring that demo staff are adequately prepared for safe demo conduct and for implementing all defined safety procedures. This will include training for all drivers, vehicle communicators, Command Center operators, operators at the North and South Yards, and all support staff (e.g., obstacle placers, incident response team, etc.)

Drivers will need experience in safe, high-speed maneuvering of vehicle in close quarters. They will have demonstrated skill in rapidly exercising good judgment in handling contingencies similar to some of those arising in race car driving. They also will have previous experience in integrated testing of experimental vehicles. Previous testing experience is probably more important since extreme racing-type maneuvering should not be required under any circumstances, but executing the proper procedure following a failure could very well be necessary. The logical candidates would be the drivers involved in the vehicle's development with the most time in the vehicle at highway speeds. Driver backups will be needed.

The major training objectives are identified below:

- All demo staff must understand relative responsibilities for implementing emergency safety procedures and the conditions under which they should be used. These procedures will be defined based on the operational hazard analysis to be accomplished during the implementation of this safety plan.
- Demo staff must be able to implement all emergency procedures including associated communication actions.

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

- Vehicle drivers must be familiar with and skilled in the operation of the vehicle(s) they will be “driving” including the operation and monitoring of all automated vehicle control systems and in the implementation of emergency procedures (e.g., re-taking manual control). They should also have sufficient hands-on experience operating the vehicle(s) so that they are able to readily recognize uncharacteristic vehicle performance that could lead to failure conditions.
- Vehicle drivers must be practiced in re-taking vehicle control following a hard-over steering failure and a hard-over throttle failure.
- Command Center operators must understand and be able to implement procedures for monitoring scenario progress and be able to recognize failure and/or hazardous situations (e.g., correlate voice reports and video monitors to ensure safe spacing between scenarios, verify correct obstacle status/location).
- The vehicle communicators must understand and use proper protocol to convey messages that are brief and unmistakable.
- Obstacle placers must be fully familiar with all aspects of the scenarios in which they will be participating and particularly obstacle placement/removal and associated communication requirements. This will include participating in sufficient dry runs prior to actual live-demo operation to ensure error-free operation.

The Vehicle Production Safety Officer must understand all procedures and protocols for communication and coordination among scenario participants throughout all scenarios, and be able to communicate with the Command Center as necessary to convey safety concerns and to obtain needed safety and scenario status information. This person must be sufficiently familiar with scenario and daily plans to be able to recognize error conditions and potentially hazardous conditions.

The training will be accomplished by the organizations participating in the demo in conjunction with the System Integration activity. It will consist of written material, briefings, remote site vehicle testing, demo site dry runs and dress rehearsals.

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **3.5.7 Incident Management**

Caltrans will provide incident management plans to include requirements for fire fighting, emergency medical response, and vehicle/debris removal. These plans will define conditions under which events in the manual lanes will affect activity in the HOV lanes.

## **3.6 VEHICLE CERTIFICATION PROCEDURE**

Vehicle certification will depend, at this stage, on existing design information and analysis and testing that has already been done or can be done in the months of February and March by the vehicle suppliers. The required certification procedures, produced by the Certification / Safety Review Team and reviewed with all vehicle developers should include the following:

1. Review vehicle top-level design and detailed design as necessary to understand how critical control systems can fail.
2. Review documentation such as hazard analyses, high level fault tree analysis, hazard mitigation actions, and test results to determine likelihood of critical failure.
3. Observe (or review results of) the required hard-over tests.
4. Run certification tests to include the following:
  - manual control
  - check-in tests
  - engagement
  - acceleration to scenario speed
  - lane change if applicable
  - obstacle detection and avoidance if applicable
  - maximum acceleration at scenario speed
  - maximum automated deceleration
  - automated acceleration to scenario speed
  - exposure to repeatable EMI from roadside and overpass
  - EMC with vehicle communication

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

- normal disengagement at scenario speed
  - re-engagement at scenario speed
  - disengagement by manual braking action
5. Examine vehicle configuration control procedures for hardware and software.
  6. Safety Review Team submits a summary of findings to the Safety Board.
  7. The Safety Board provides approval to dry run.
  8. Conduct individual and vehicle-following runs on the I-15 Demo lanes.
  9. Conduct dry runs of demonstration scenarios.
  10. Safety Board approval (in consultation with the PMC) to demonstrate the vehicle in scenario as tested.

## 3.7 MINI-DEMONSTRATIONS

Providers are required to provide safety information as specified in Table 3-6. General safety requirements stated below.

**Table 3-6**  
**MINI-DEMONSTRATION SAFETY APPLICATION\***

On-site information required (for vehicles that will not be demonstrated on public roads)

1. Description of vehicle, systems to be demonstrated, scenario to be demonstrated, requirement for personnel inside the protective perimeter.
2. Brief description of failure modes and procedures following failure.
3. System maturity, development history, and testing history.

Off-site information required (for vehicles that will be demonstrated on public roads)

1. Same as on-site plus testing history on public roads in the vehicle demonstrated.

---

\* Required if system manipulates vehicle controls.

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

4/07/97

## **3.7.1 On-Site Demonstration**

A barrier-protected area will be provided at Miramar College for dynamic vehicle demonstrations. This area will be contained within an existing five-acre paved parking lot. Vehicles and operations will meet the following requirements:

1. Spectators will be kept outside the barrier when vehicles are operated.  
(They will be easily able to view the action).
2. Vehicle speeds must be appropriate for a parking lot.
3. Demonstrations will be sequential rather than simultaneous and will involve only single vehicles or two vehicles with one operated manually by test personnel.
4. There must be at least one way for the driver and one independent way for test personnel to quickly cause transition to the manual mode.

## **3.7.2 Off-site Demonstrations**

On-road demonstrations are also permitted for vehicles that have met common highway-operational prototype safety criteria and have been tested successfully in public road operation. Passengers for these demonstrations will be loaded and unloaded at the Exposition Center. On-road demonstration vehicles must be properly licensed and equipped to operate on California roads. These demonstrations will be preferably conducted on non-residential roads. If automated systems which directly control vehicle motion are not involved in the particular demonstration, the feature may be demonstrated off-site, as long as it has a valid license, without meeting further safety requirements. Demonstrations that involve automated vehicle control, must have successfully demonstrated safe operation on public roads. An example of an acceptable off-site vehicle control system demonstration is an Intelligent Cruise Control system that has many hundreds of hours of public road testing with pre-production hardware that has been thoroughly tested for failure characteristics.

## **4.0 DOCUMENTATION**

The following documentation is planned:

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

1. Fault/Hazard Mitigation Forms - single sheets as in Table 3-5 describing mitigation of the major faults and hazards for each vehicle and scenario. These are to be prepared by the Safety Review Team, the vehicle/scenario participants, and all other interested parties.
2. Safety Assessment Report - a summary of the hazard analysis results and the vehicle certification documentation prepared by the Safety Review Team for the Safety Board.
3. Vehicle/Scenario Certification Applications - a collection of all documents furnished by the vehicle providers as evidence that the vehicle and the scenario are safe to demonstrate on I-15. This package will include the results of all certification runs.
4. Mini-Demo Application - to include information as in Table 3-6 to apply for either parking lot or on-road demonstration.
5. Software Change Notices - logs of software changes and re-testing to be maintained by each participant from the time of vehicle certification.
6. Maintenance and Repair Logs - logs of hardware removals and replacements, inspections and repairs to be maintained by each participant after vehicle certification.
7. Dry-Run and Dress Rehearsal Failure Log - log of failures while operating on I-15 from the time of vehicle/scenario certification to the start of demonstrations.

## **5. SCHEDULE**

Figure 5.1 shows the schedule for the Safety Plan implementation. Figure 5.2 shows how each scheduled task flows from one to another. The task flow has been laid out to provide sufficient time for adequate thoroughness, aggressive enough to permit completion within the tight demo schedule. The tasks build from initial analyses and draft plans to definition of final procedures and implementation of defined safety precautions. Safety reviews are scheduled at key points to facilitate review of safety plans and coordination with other parallel demo planning efforts.

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

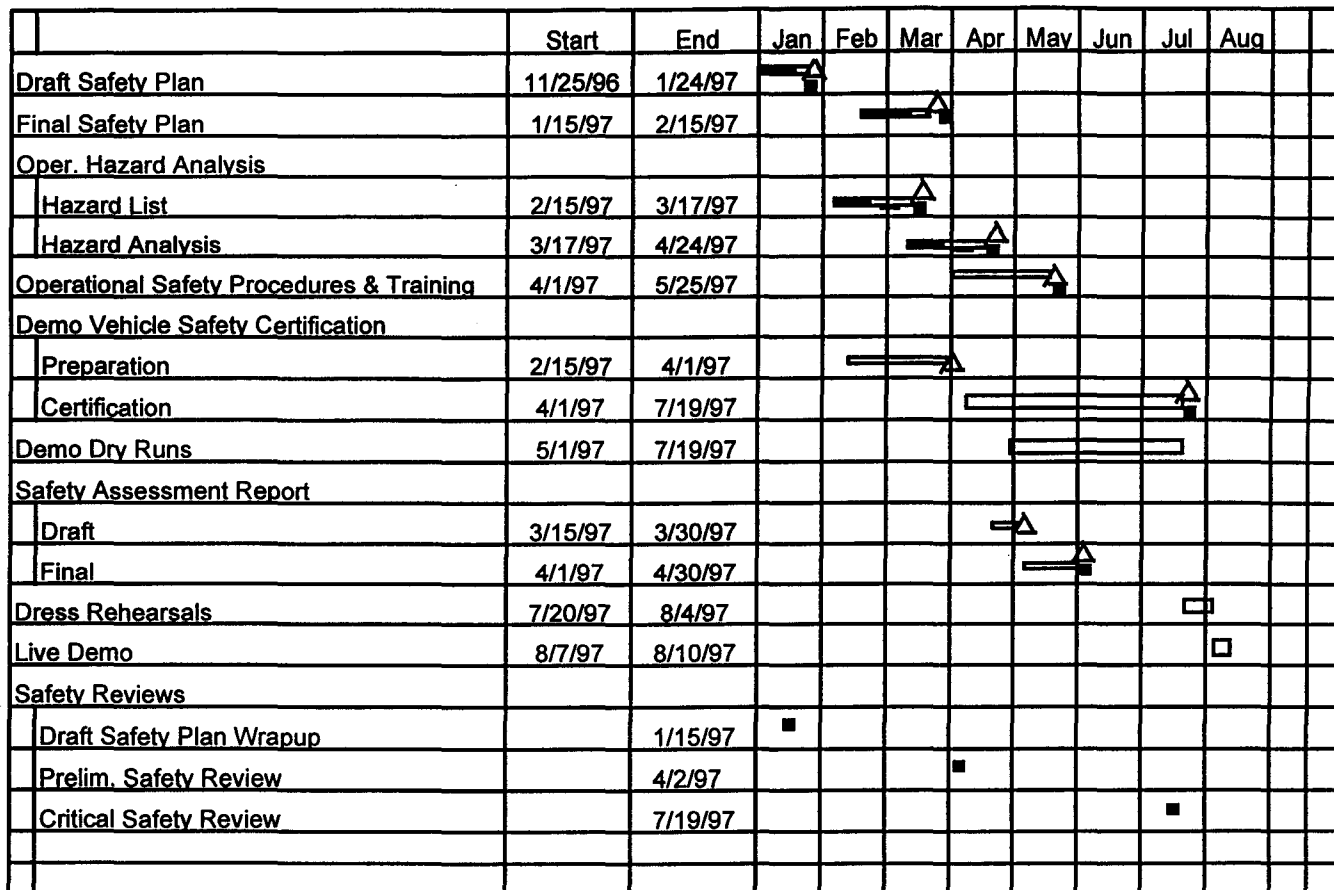


Figure 5-1 SAFETY PLAN IMPLEMENTATION SCHEDULE

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

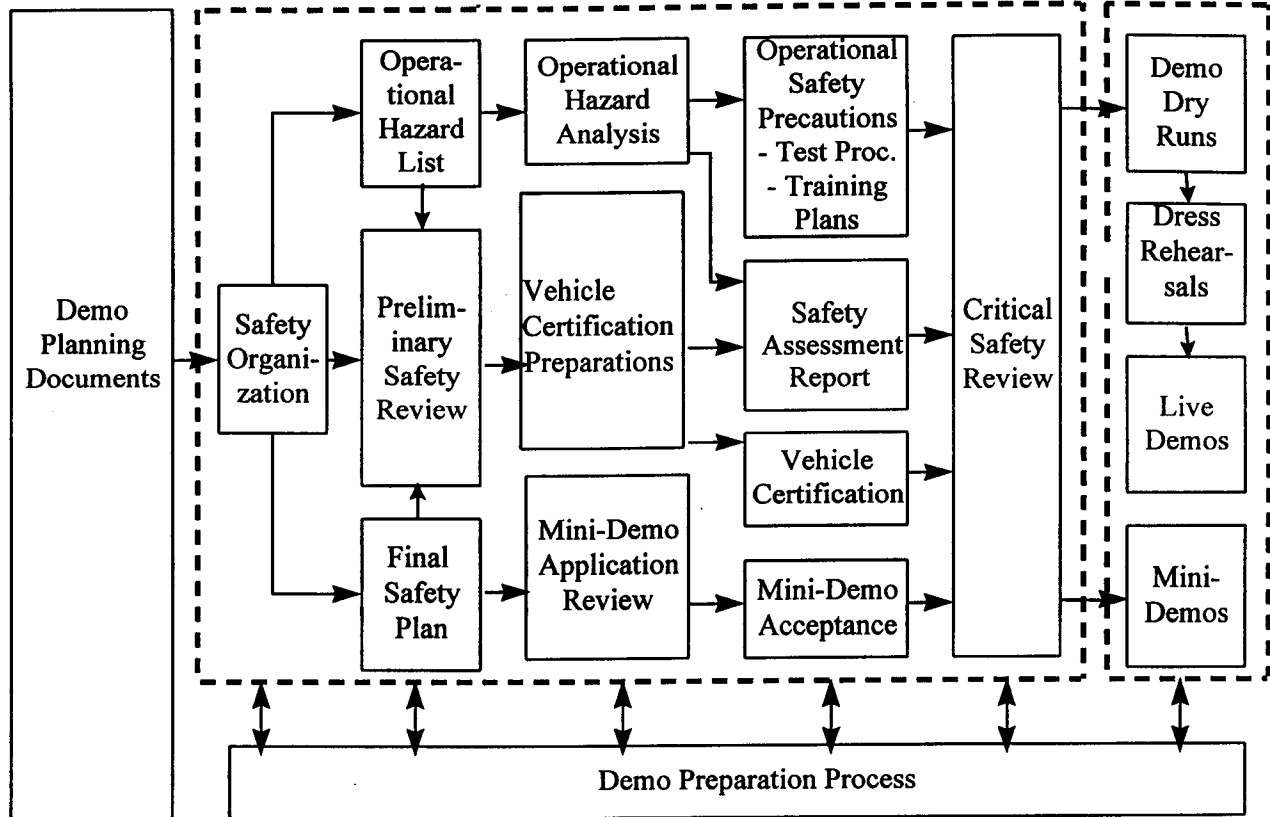


Figure 5-2 SAFETY TASK FLOW



# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **6. ISSUES AND RECOMMENDATIONS**

### **6.1 NO-COLLISION GAPS**

Will all single failures be fully mitigated i.e. no collision is predicted? According to available data, safe full manual braking such as would be necessary in the event of an unplanned obstacle requires a gap of 25 to 30 meters at 60 mph.

This safety plan recommends this minimum spacing for all but the platoon scenario which is designed to demonstrate the feasibility of smaller gaps. Here the "unplanned obstacle" criterion can be relaxed but full automated deceleration or acceleration should result in no-collision.

### **6.2 PASSENGER BRIEFINGS AND WAIVERS**

It is imperative that all passengers understand the risks of riding in experimental vehicles and be required to sign an informed consent document. It can be done as a routine part of registration and the briefing prior to each run.

### **6.3 PASSENGER RESTRAINTS**

All vehicles in Demonstration '97 must be equipped with appropriate safety gear as mandated by law. This means passenger vehicles and trucks must have seat belts and shoulder harnesses. Automated transit vehicles will not be required to "force fit" seat belts in vehicles not designed to incorporate them but will implement appropriate measures to ensure the safety of their passengers.

### **6.4 EMI FROM MANUAL LANES**

This Plan recommends that potential interference from EMI be tested. The safety organization should then determine and apply appropriate safety measures as needed. These cases should include the airborne radar from nearby Miramar NAS, high-powered truck CB broadcast and commercial radar/IR scramblers.

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **6.5 SOFTWARE LOADING**

The recommendation is that all volatile and/or non-volatile memory be checked with a checksum. If possible, other components such as A/D's, D/A's should be checked with a simple built-in test (BIT).

## **6.6 MODE TRANSITION**

Since manual mode reversion is a major safety measure for this activity, the recommendation is that driver-activated transition be software-independent and that computer-activated transition software be specially protected against unintended changes. Such software should be tested frequently using BIT. Transition to manual control should be accompanied by an audio tone as well as an independent light to ensure that the driver will take control immediately. It should also be very improbable that the automated mode become engaged without driver action.

## **7.0 REFERENCES**

1. NTSA Order 700-1, November 4, 1981, "Protection of the Rights and Welfare of Human Subjects in NHTSA-Sponsored Experiments.
2. 45 CFR Subtitle A (10-1-93 Edition) Department of Health and Human Services; "Part 46 - Protection of Human Subjects".
3. 49 CFR Subtitle B (10-1-93 Edition), Chapter V NHTSA, "Part 571 Federal Motor Vehicle Safety Standards"
4. SAE Standards Vol. 3, Sections 28-34, 36.
5. "Caltrans Procedures and Guidelines for Research of the I-15 Reversible HOV Lanes," copy transmitted to the authors, January 1997.
6. Delco System Operations, "Precursor Systems Analyses of Automated Highway Systems, Activity Area L, Vehicle Operational Analysis," November 1994, page 42.
7. Military Standard; "System Safety Program Requirements," MIL-STD-882B March 1984.
8. Calspan SRL Corporation, Precursor Systems Analyses of Automated Highway Systems, Activity E, Malfunction Management and Analysis," November 1994.
9. Calspan SRL Corporation, "Precursor Systems Analyses of Automated Highway Systems, Activity Area J, Entry/Exit Implementation," November 1994.

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

## Appendix A VEHICLE FAULT AND HAZARD CHECKLIST

### 1. Passenger Compartment

- mounting of passenger-compartment equipment has strength inadequate to withstand collision inertia loads
- automation equipment can be easily hit or disturbed by passengers
- equipment inside the passenger compartment is unmounted or unrestrained

### 2. New or Modified Controllers, Switchology, Lights, Indicators

- becomes inoperable due to internal failure, external foreign objects or dirt
- feel or tactile cue controller malfunctions
- controller interferes with access to critical controls
- driver unable to reach system-disengage device easily and quickly
- driver unable to see lights, displays, lighted buttons or indicators due to sunlight, temporary line of sight blockage, etc.
- controls, lights, etc. difficult to properly interpret or can be used improperly

### 3. Primary Automated Control Systems - Throttle, Brakes, Steering, Transmission, Other

In the following components:

#### a) all single failures mitigated by:

- automatic detection and action
- driver detection and action
- automatic detection and driver action
- detection by maintenance action and failure shown to cause no significant hazard for the time it remains undetected.

#### b) all EMC/EMI hazards mitigated

Subsystem List

#### 1) Sensors

- linear position, rate, acceleration
- angular position, rate, acceleration
- position relative to lanes
- position relative to other vehicles
- other sensors affecting control laws

#### 2) sensor analog signal processors

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

- 3) sensor A/D conversion
- 4) data link from other vehicles
- 5) data or discrete signals from the infrastructure
- 6) digital processing hardware, software, algorithms, etc.
- 7) actuator command D/A conversion
- 8) actuator command analog data processors
- 9) actuator subsystems
- 10) actuator monitoring
- 11) mode switching units
- 12) mode switching commands
- 13) mode switching monitoring

## 4. Mode Switching

System must avoid failures associated with mode switching such as:

- not able to transition from automated to manual
- manual mode engaged but automated mode not disengaged
- mode switching causes hazardous transients
  - normal manual engagements and disengagements
  - automatic disengagements with and without preceding driver input or override

## 5. Cooling

- computer or other heat-sensitive subsystems cooling inadequate
- cooling provisions fail

## 6. Hydraulic Subsystem

- leak in automation equipment causes loss of basic vehicle function
- pressure shock fatigue causes leak or rupture
- increased hydraulic load causes source malfunction
- source malfunction causes both automated and basic vehicle failures simultaneously

## 7. Electrical Subsystems

- failure of any non-standard power source causes multiple simultaneous automation system faults.
- failure of any non-standard power source interferes with manual control or transition from automated to manual control
- power source failure causes hazard to vehicle occupants

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

- high voltage not adequately protected
- short in power distribution causes smoke or fire hazard

## 8. Warnings, Alarms, or Procedures

- no single failure should prevent critical visual or audio annunciations unless that failure is otherwise immediately obvious to the driver.
- no single event or failure shall prevent the driver from executing the primary and the backup takeover procedure, short of driver incapacitation.

## 9. Software

- top-down design not accomplished or not revealed ( may restrict last minute software modifications)
- unit testing not adequately documented
- system testing not adequately documented
- software failures (data link problems, infinite loop, improper branching, frame overrun, division by zero, etc.) not mitigated by techniques such as:
  - watchdog timer
  - stale data check
  - check sums
  - parity checks
  - value reasonableness checks
  - output value limits
  - output rate limits
  - error correcting codes
- version control inadequate

## 10. Wiring and Circuitry

- chafing hazard
- wires exposed to flexing or external damage
- power grounding biasing signal
- circuit cards vibrate
- wires not properly attached to connectors
- high humidity causes circuit card malfunction
- high local temperatures cause circuit problems
- short causes loss of signal

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

## **11. Data Link**

- Frame time or data latency too long for gap proposed
- Data transmitted inadequate for gap proposed
- Handshaking protocol inadequate
- Drop-out protocol causes automation disengagement
- Link controller versus passive role as link terminal
- Vehicle position in string and addressing protocol

### **Added Questions for Vehicle Developers**

- 1) **Passenger Compartment**  
no additional items
- 2) **New or Modified Controllers, Switchology, Lights, Indicators**
  - What happens to feel of steering wheel, brakes, and throttle after system engagement and what produces the change? After disengagement?
  - Can driver see and/or feel control action? Can driver overpower system?
  - Can driver superimpose his/her inputs on the system inputs without system disengagement?
  - How is manual disengagement caused?
  - Where should driver place hands when system is engaged?
- 3) **Primary Automated Control System**
  - Have any system components been produced in quantity and have known reliability?
  - What data words and discretes are on the vehicle data link at what frame rate?
  - What happens on the data link on manual takeover or disengagement?
  - Can data link errors cause hard-overs?
  - What is data link range? Can dropouts cause hard-overs?
- 4) **Mode Switching**
  - Does mode switching require software? How is that software integrity assured?
  - Do mode switching analog component failures always result in return to the normal manual control?
- 5) **Cooling**
  - Cooling from an external source required when vehicle is at the dock in ambient temperature above some limiting value?

# **NAHSC 1997 DEMONSTRATION SAFETY PLAN**

**4/07/97**

- At what ambient temperature is vehicle air conditioning inadequate to cool both occupants and computers?
- 7) Hydraulic Subsystem
  - no additional items
- 8) Warnings, Alarms and Procedure
  - no additional items
- 9) Software
  - Have end-to-end time delays been tested?
  - What is a top-level time line for real time execution during system engagement?  
Is the data link synchronized with the control law processor? Are A/D's and D/A's synchronized with that processor?
  - How is the frame rate and can it be changed?
  - Can control laws be changed while the system is engaged? While vehicle is under manual operation?
  - Can test input files be executed inadvertently?
- 10) Wiring and Circuitry
  - no additional items
- 11) Data Link
  - Can the data link faults cause braking hard-overs?
  - Do all vehicles at close head-ways receive and process data from all other vehicles simultaneously or within one processor frame?





# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

## Appendix B

### POTENTIAL FORMULAS FOR DETERMINING COLLISIONS OF VEHICLES IN TRAIL

Actual time histories of the initiation of a braking or a throttle hard-over must be examined, along with the typical data link behavior, to enter simple collision analysis. Knowing equivalent constant and equal decelerations  $D$  with time lag  $\tau$ , the minimum gap to avoid any collisions or to avoid a second collision at a given speed  $V$  can be estimated. Equal-deceleration cases are important since this control action mimics the automated behavior in a non-failure condition. Unequal decelerations are analyzed in Ref. 9. The formula for no-collision gap is given below.

Table B-1 indicates the formulas relating collision relative velocity and time of collision to gap, deceleration, time delay and speed for vehicles in trail. These formulas apply to situations where all vehicles have the same deceleration and where all trailing vehicles start decelerating at the same time but  $\tau$  seconds after the first vehicle involved starts decelerating.

For the situation where vehicles have unequal decelerations, the gap to avoid collision is

$$s = \left( (D_1 - D_2) V^2 / 2D_1 D_2 \right) + V\tau$$

where  $s$  = gap between vehicles

$D_1$  = equivalent constant deceleration of the vehicle ahead

$D_2$  = equivalent constant deceleration of the vehicle behind

$V$  = initial common speed of vehicles

$\tau$  = time delay between the leading and following vehicle deceleration

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

**Table B-1**  
**SINGLE COLLISION CRITERIA**  
**FOR EQUAL DECELERATION OF**  
**TWO OR MORE VEHICLES WITH  $V \geq D\tau$**

Case	Range of Gap	Time of Collision	$\Delta V$	First Collision	Gap to Avoid Between Veh. 3 and Veh. 2
Collision before Veh. 2 starts to decelerate	$0 < s \leq D\tau^2/2$	$t_c = (2S/D)^{1/2}$	$(2Ds)^{1/2}$	Inelastic	$s > D\tau^2(2k+1-(4k+1)^{1/2})/4k^2$ where $k = 5D\tau / 8V$
				Elastic	Cannot avoid for $V > D\tau$ For $V = D\tau$ can avoid with $s = D\tau^2/2$
Collision after Veh. 2 starts to decelerate but before Veh. 1 stops	$\frac{D\tau^2}{2} < s \leq \tau V - D\frac{\tau^2}{2}$	$\tau_c = (s/D\tau) + \tau/2$	$D\tau$	Inelastic	$s > (V\tau/3) + D\tau^2/12$
				Elastic	$s > V\tau/2$
Collision after Veh. 1 stops	$\tau V - \frac{D\tau^2}{2} < s \leq \tau V$	$\tau_c = (V/D + \tau) - (2(V\tau - s)/D)^{1/2}$	$(2D(\tau V - s))^{1/2}$	Inelastic	No second collision
				Elastic	No second collision

# NAHSC 1997 DEMONSTRATION SAFETY PLAN

4/07/97

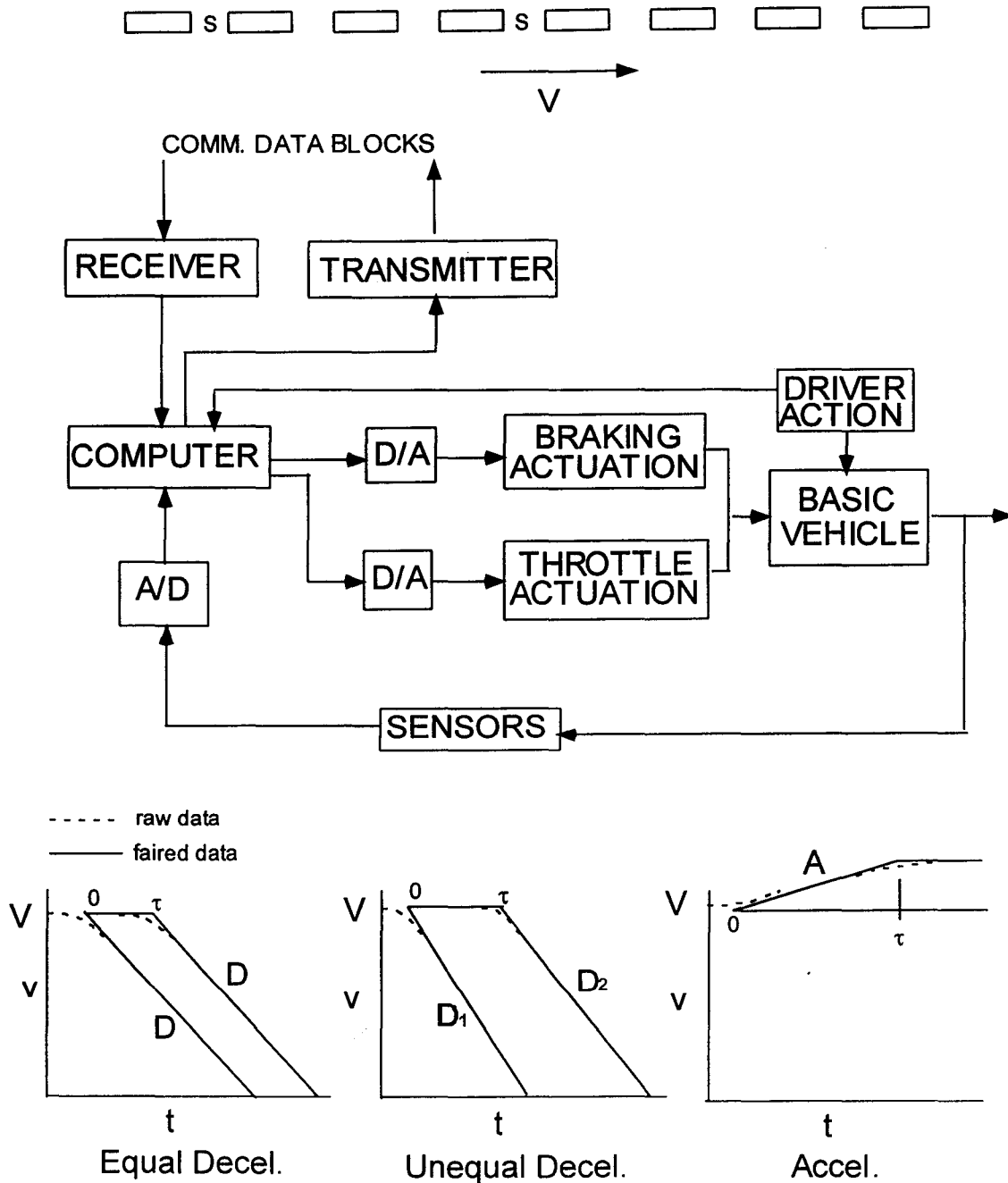


Figure B-1 GENERAL BLOCK DIAGRAM AND TIME HISTORIES FOR CLOSE HEADWAY SAFETY ANALYSIS

