Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

AHS Malfunction and Safety Analysis

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-95-123
November 1994

FOREWORD

This report was a product of the Federal Highway Administration's Automated Highway System (AHS) Precursor Systems Analyses (PSA) studies. The AHS Program is part of the larger Department of Transportation (DOT) Intelligent Transportation Systems (ITS) Program and is a multi-year, multi-phase effort to develop the next major upgrade of our nation's vehicle-highway system.

The PSA studies were part of an initial Analysis Phase of the AHS Program and were initiated to identify the high level issues and risks associated with automated highway systems. Fifteen interdisciplinary contractor teams were selected to conduct these studies. The studies were structured around the following 16 activity areas:

(A) Urban and Rural AHS Comparison, (B) Automated Check-In, (C) Automated Check-Out, (D) Lateral and Longitudinal Control Analysis, (E) Malfunction Management and Analysis, (F) Commercial and Transit AHS Analysis, (G) Comparable Systems Analysis, (H) AHS Roadway Deployment Analysis, (I) Impact of AHS on Surrounding Non-AHS Roadways, (J) AHS Entry/Exit Implementation, (K) AHS Roadway Operational Analysis, (L) Vehicle Operational Analysis, (M) Alternative Propulsion Systems Impact, (N) AHS Safety Issues, (O) Institutional and Societal Aspects, and (P) Preliminary Cost/Benefit Factors Analysis.

To provide diverse perspectives, each of these 16 activity areas was studied by at least three of the contractor teams. Also, two of the contractor teams studied all 16 activity areas to provide a synergistic approach to their analyses. The combination of the individual activity studies and additional study topics resulted in a total of 69 studies. Individual reports, such as this one, have been prepared for each of these studies. In addition, each of the eight contractor teams that studied more than one activity area produced a report that summarized all their findings.

Lyle Saxton
Director, Office of Safety and Traffic Operations Research
and Development

NOTICE

Technical Report Documentation Page

1. Report No. FHWA-TS-95- Volume V	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS Final Report Vol. V, Malfunction Management and Safety Analysis		5. Report Date November 1994 6. Performing Organization Code
7. Author(s) Calspan Corporation – Joseph A. Elias, Program Manager		8. Performing Organization Report No. 8281-1
9. Performing Organization Name and Address Calspan Corporation Advanced Technology Center P.O. Box 400 Buffalo, New York 14225		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFH61-93-C-00192
12. Sponsoring Agency Name and Address Turner-Fairbank Highway Research Center Federal Highway Administration 6300 Georgetown Pike, HSR-10 McLean, Virginia 22101		13. Type of Report and Period Covered Final Report Sept. 9, 1993 – October 30, 1994 14. Sponsoring Agency Code
15. Supplementary Notes Contracting Officer's Technical Representative (COTR) – J. Richard Bishop		

16. Abstract

The program described by this eight-volume report, a resource materials document type, identified the issues and risks associated with the potential design, development, and operation of an Automated Highway System (AHS), a highway system that utilizes limited access roadways and provides "hands off" driving. The AHS effort was conducted by a team formed and directed by the Calspan Advanced Technology Center. Primary Team members included Calspan, Parsons Brinckerhoff, Dunn Engineering Associates, and Princeton University. Supporting members of the team were BMW, New York State Thruway Authority, New York State Department of Transportation, Massachusetts Department of Transportation, the New Jersey Department of Transportation, Boston Research, Vitro Corporation, and Michael P. Walsh of Walsh Associates.

Calspan provided overall management and integration of the program and had lead responsibility for 5 of the 17 tasks. Parsons Brinckerhoff provided transportation planning and engineering expertise and had lead responsibility for 5 tasks. Dunn Engineering provided traffic engineering expertise and had lead responsibility on 2 tasks. Princeton supported the areas of transportation planning and automated control.

The 17 task reports (A through P plus Representative Systems Configurations) are organized into 8 volumes. This volume describes AHS malfunction management and safety analysis. It covers Malfunction Management and Analysis (Task E), supervised by Philip A. Reynolds of Calspan and supported by Keith Giordano of Calspan and H. Grady Lee of Vitro Corporation; and analysis of AHS Safety Issues (Task N), supervised by Linda O. Parada of Calspan and supported by Mary M. Lloyd, also of Calspan.

17. Key Words Automated Highway Systems Intelligent Vehicle Highway System Intelligent Transportation Systems	18. Distribution Statement No restrictions. This document is available to the public through the National Technical Information Services, Springfield, Virginia 22161.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 402	22. Price

Form DOT F 1700.7 (8-72)Reproduction of completed page authorized

(PF V2.1, 6/30/92)

TABLE OF CONTENTS

VOLUME V — AHS MALFUNCTION MANAGEMENT AND SAFETY ANALYSIS

CHAPTER 1: MALFUNCTION MANAGEMENT AND ANALYSIS (TASK E)

List of Tables

List of Figures

VOLUME V — AHS MALFUNCTION MANAGEMENT AND SAFETY ANALYSIS

CHAPTER 1: MALFUNCTION MANAGEMENT AND ANALYSIS (TASK E)

1.0 EXECUTIVE SUMMARY

1.1 INTRODUCTION

This analysis area examines the role of malfunctions in the reliability of an AHS. Although various safety judgments are needed in this chapter, safety is primarily addressed in Chapter 2. Malfunctions can occur in any of the five physical components -- the vehicle, the roadway, the driver, the payload and the environment. We concentrate on the vehicle since the other four components, for a variety of reasons, are less important to malfunction management at this stage of AHS development. Of the 21 functions considered at the vehicle operations mini-conference, we consider primarily the three normal cruising functions -- gap regulation, lane tracking, and space regulation.

1.2 TASK OBJECTIVE

The task objective was to define, in the most inclusive way possible, the physical subsystems of an AHS, then consider what design precepts might be applied to achieve reliability goals. From these precepts and present-day achievable failure rates for comparable systems, we seek a conclusion regarding achievable AHS vehicle failure rates. We also desire an analysis framework which can be used by future researchers to obtain specific results for various specific physical designs and protocols.

1.3 TECHNICAL APPROACH

Today's vehicles pull to a freeway shoulder because of malfunctions at the rate of one per 1,000 veh-hrs. This figure is justified by examining three highway data sources and by vehicle manufacturer's and fleet operators' data. Many of these failures are avoidable by better maintenance, inspections, onboard monitoring and operating procedures. The result of this study is the conjecture that the AHS basic vehicle failure rate could be improved by a factor of two or one per 2000 veh-hrs.

Create an AHS vehicle automation system reliability budget of one per 2000 veh-hrs. This results in a total vehicle failure rate of one per 1000 hours or the same as today's vehicles. If we can achieve this level of automation reliability, the public should accept the reliability of these vehicles as it does today's manual vehicles. The key questions are: 1) Can we achieve this level of reliability, 2) are the initial and lifetime maintenance costs acceptable for this reliability, 3) can we design AHSs that provide safe failure modes when failures occur.

Data from Government and industry sources were obtained from publications and telephone conversations' A table of MTBFs (Mean Time Between Failure) for twelve generic components was constructed. Six of these are components located in each vehicle.

Strawman protocols are proposed and analyzed to yield composite AHS reliability numbers. Other designs are suggested to get a feel for the range of failure probabilities obtained. It is shown that the roadside reliability would play a minor role simply based on the number of vehicle-borne components versus the roadside components

1.4 CONCLUSIONS

1. User data and analysis show that an automation failure rate of one per 2000 veh. hrs. is feasible.

2. The full answer to the cost question, both acquisition and lifetime maintenance, must remain uncertain until specific designs are considered, but we are optimistic.

3. The key issues in the approach to the question of safety are the use of redundancy in vehicle equipment, and the use of a breakdown lane, entry/exit protocol, and handling communication failures. Our study suggests design approaches to deal with these issues.

4. Barriers in the I2 scenario would reduce the probability of vehicles and other objects from moving into the AHS lane from the manual lanes. The ability of an automated vehicle to cope with such objects is problematical, making consideration of barrier use part of this malfunction management.

5. Driver role in malfunction management remains a controversy. We examined two driver roles-one where the driver is continually alert to the vehicle's behavior and progress throughout the trip and one where the driver can turn attention to unrelated activities but can expeditiously tend to systems alerts and advisories. These two roles both find application depending on the proximity of manually-operated vehicles as dictated by RSC definition.

1.5 RECOMMENDATIONS

1. Preliminary subsystem design studies should be performed and integrated into an overall system design containing life cycle cost/reliability tradeoffs.
2. Redundant subsystems should be considered to obtain reliability goals with the following design questions addressed.

   a) Use of dissimilar technologies as part of the redundancy
   b) Failure detection availability
   c) Failure identification technique
   d) Transition without dynamic disturbance
   e) Common mode failures

3. The driver role in malfunction management should be studied in simulations and field tests.

4. A target basic vehicle locomotion MTBF should be established by standards organizations and vehicle manufacturers.

5. Further study is needed to resolve the issues of
   a) continuous breakdown lane
   b) malfunctions during access and egress functions

c) management of communication failures

6. Realistic affordable methods for managing the problem posed by an object in the lane must be developed. This study should consider the role of barriers in the AHS designs placing an automated lane contiguous to those used by manual traffic.

7. A related study should address the legal implications of enforcing traffic laws addressing obstruction of AHS traffic. Such violators should be easily detectable and therefore easy to fine or at least bring to trial. The delay caused in the AHS lane is, in worst case, equivalent to stopping three or more lanes of today's congested manual traffic. There appears to be no method short of a physical gate or severe legal consequence to prevent intended or negligent obstruction.

2.0 INTRODUCTION

2.1 DESCRIPTION

This task employed RSC definitions, data gathering and analysis to create a framework for posing AHS reliability questions and eventually answering those questions. We concentrated on events immediately after a malfunction to minimize the effects on vehicle occupants, vehicle damage and system performance but system design, preventative maintenance and integrity monitoring. The roadside incident management task of clearing vehicles, giving medical attention and restarting flow if stopped were not examined here but is part of Volume III, Chapter 3. Also, the safety issues are treated in detail in Chapter 2. Enforcement issues are covered in Volume III Chapter 3 and Volume VIII Chapter 1.

2.2 PURPOSE

Our objective is to examine the reliability/cost tradeoff primarily as cost is reflected in MTBF of each subsystem and the number of redundant subsystems. Many researchers have concluded that the AHS enabling technologies are presently available. But are they affordable and mature enough to produce a practical system? The approach in this Chapter is directed at answering this question.

2.3 OVERALL APPROACH

A five-step approach was used.

1. Describe a generic AHS in terms of physical subsystems or categorization.

2. Concentrating on the vehicle itself, determine its present locomotion reliability.

3. Project what might be accomplished to increase this reliability so that automation subsystems can be added without a large decrease in overall reliability.

4. Obtain MTBF estimates for the vehicle automation subsystems based on present-day performance.

5. Propose and evaluate single-failure strategies to obtain a feel for the issues involved in matching today's manual vehicle reliability.

2.4 GUIDING ASSUMPTIONS

1. We assume that vehicle exposure time is the dominant factor in interpreting failure data. This assumption equates expected numbers of failures when the samples have the same vehicle-hours. By using vehicle-hours rather than vehicle-miles, an MTBF for the basic vehicle can be directly combined with MTBFs for automation components.

2. For the time period important to AHS development (we could say the next generation), AHS vehicles will have two control modes for normal operation-manual and automated. This is not to preclude fully automated trips. However, we are assuming there will be away to fully control the vehicle velocity and direction by continuous human inputs and this mode will be used in normal vehicle operation.

3. During normal operation, there will be designated regions where transition between modes should occur. If it does not occur, there is a malfunction. There will also be regions where transition should not occur. If it does occur there is a malfunction.

4. For this task there will be a driver in the vehicle.

3.0 RESEARCH ACTIVITY

3.1 AHS COMPONENT DESCRIPTION

We have organized malfunction management about physical entities arranged in an hierarchical fashion. Later we discuss failures in these entities. By extending a manual freeway system description we obtain the block diagram in Figure 1-1. The five major components are each further described in Figures 1-2 through Figures 1-6. These major components are meant to be all-inclusive but a minimum number, that is necessary and sufficient. One might assert that payload is not necessary, but there is always a reason for the trip even if it is just to get out of the house and the driver frequently serves as the only passenger. Also, quite critical malfunctions can occur that involve the payload.

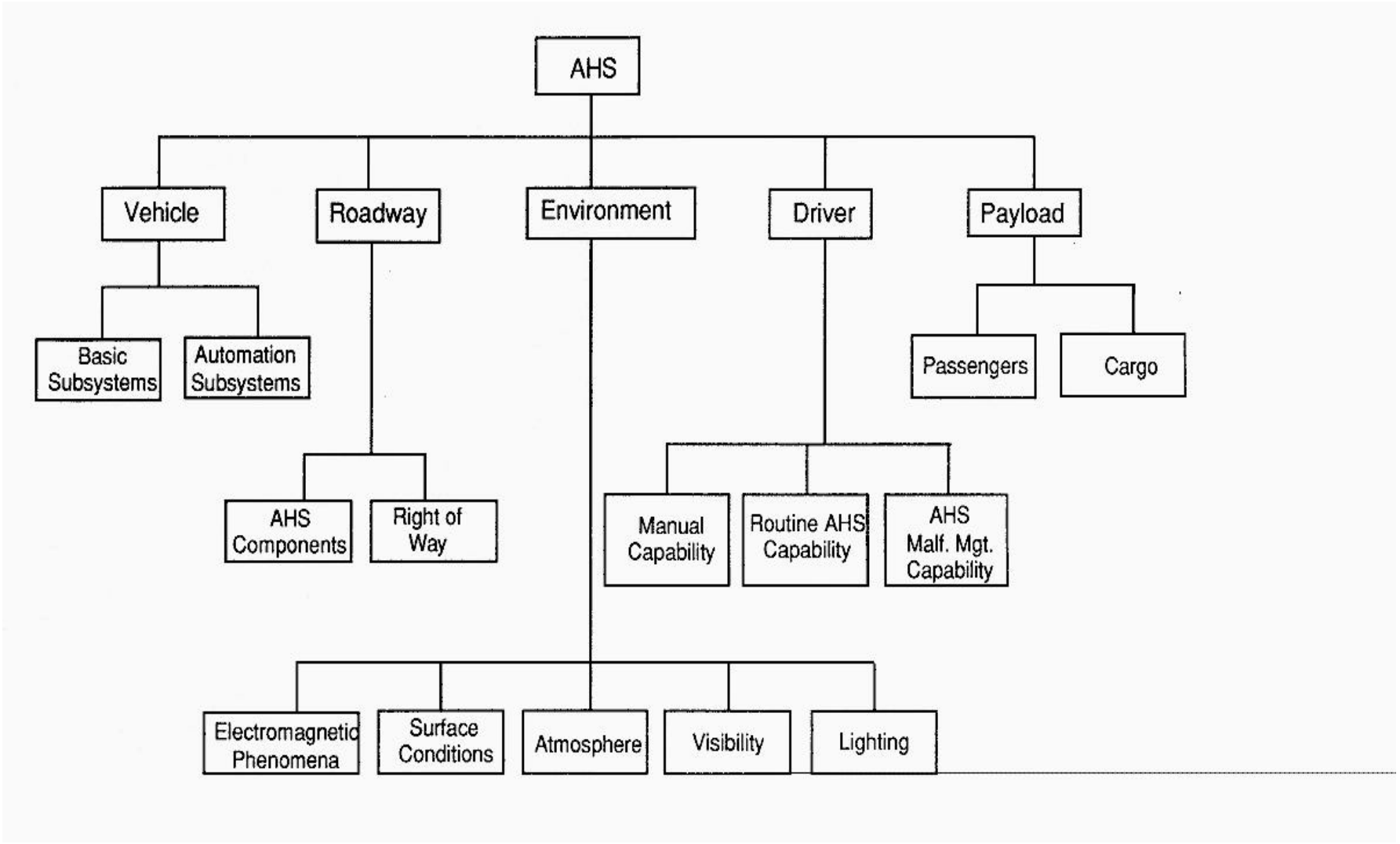

FIGURE 1-1 AHS PHYSICAL COMPONENTS

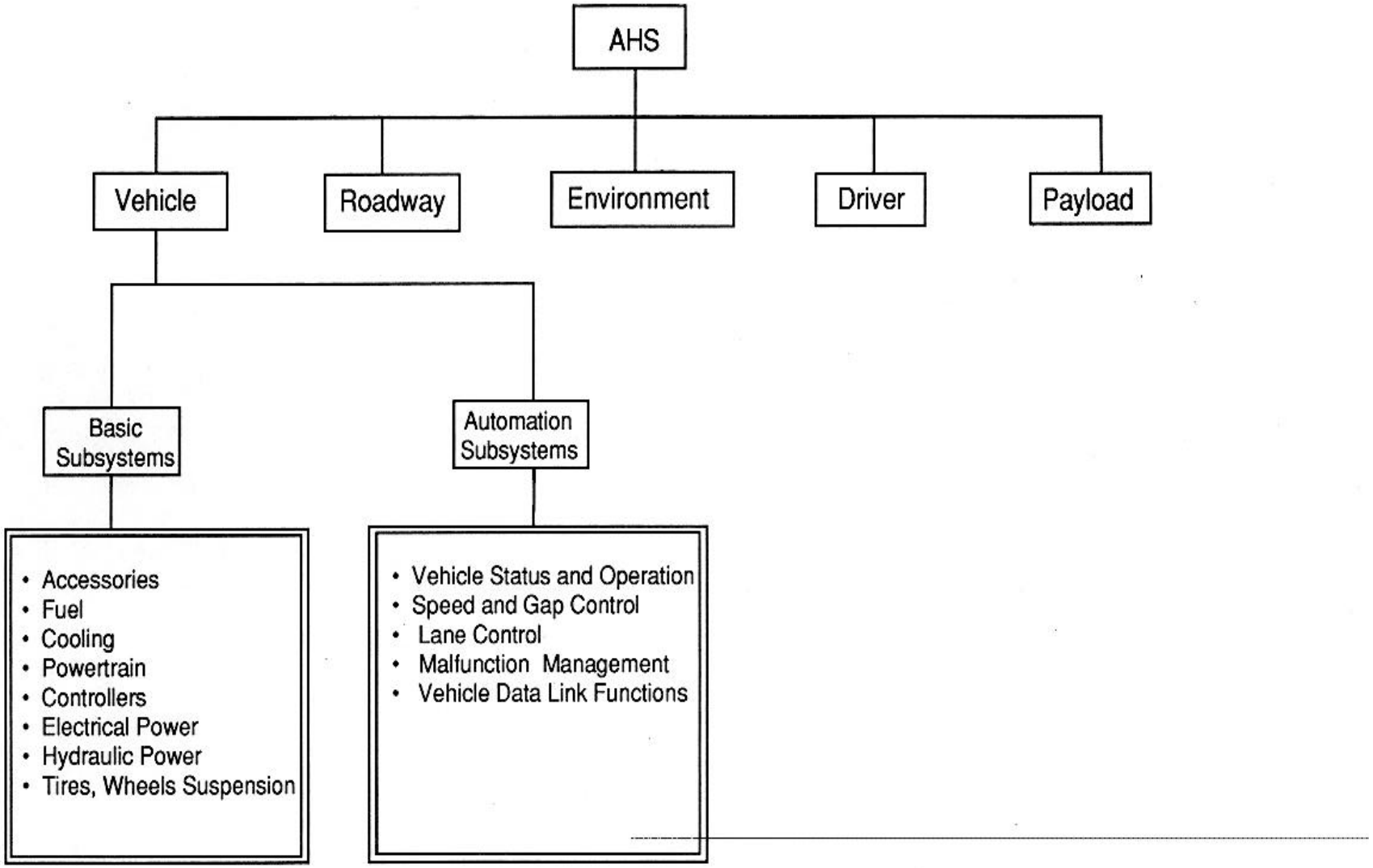

FIGURE 1-2 VEHICLE SYSTEMS

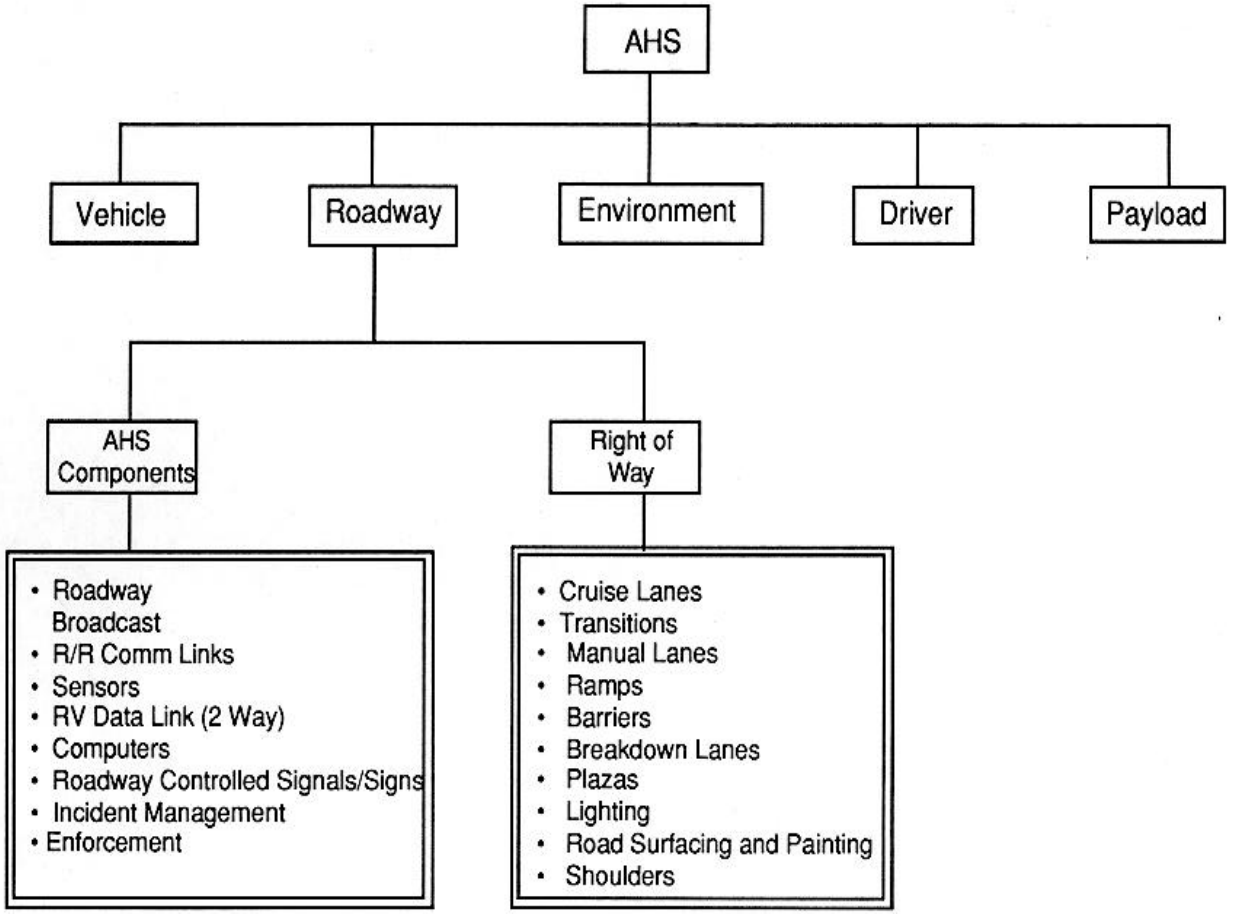

FIGURE 1-3 ROADWAY COMPONENTS

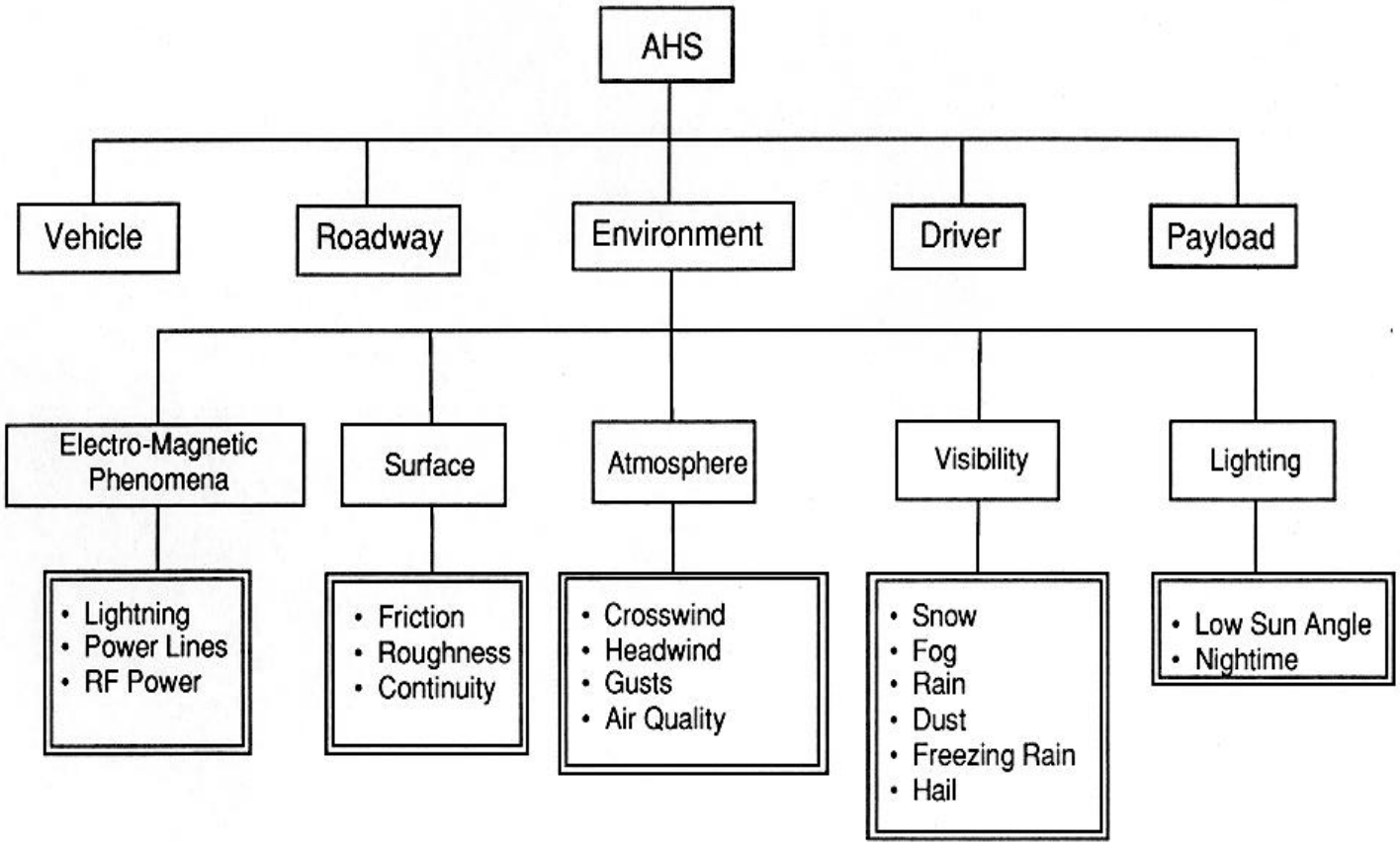

FIGURE 1-4 ENVIRONMENTAL FACTORS

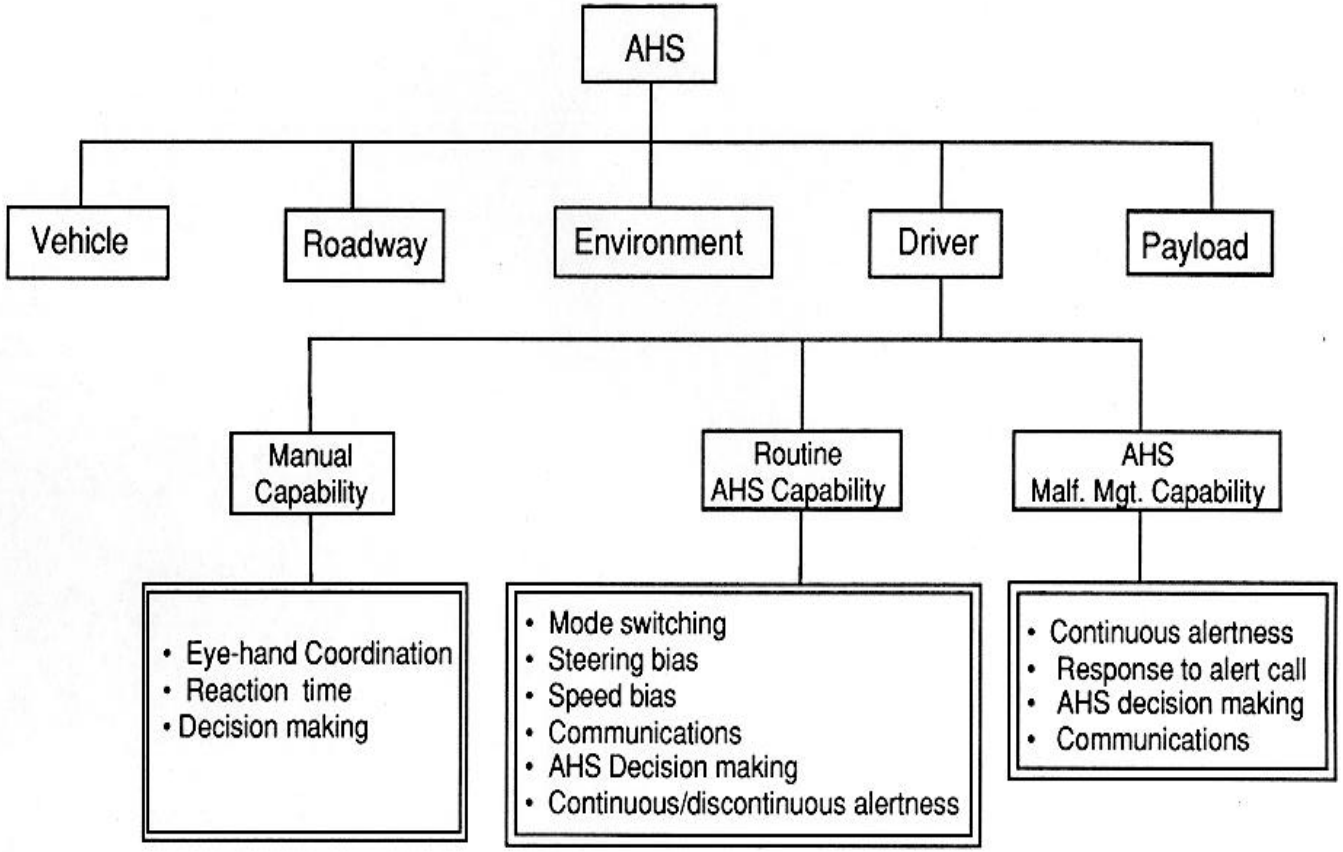

FIGURE 1-5 DRIVER CAPABILITIES

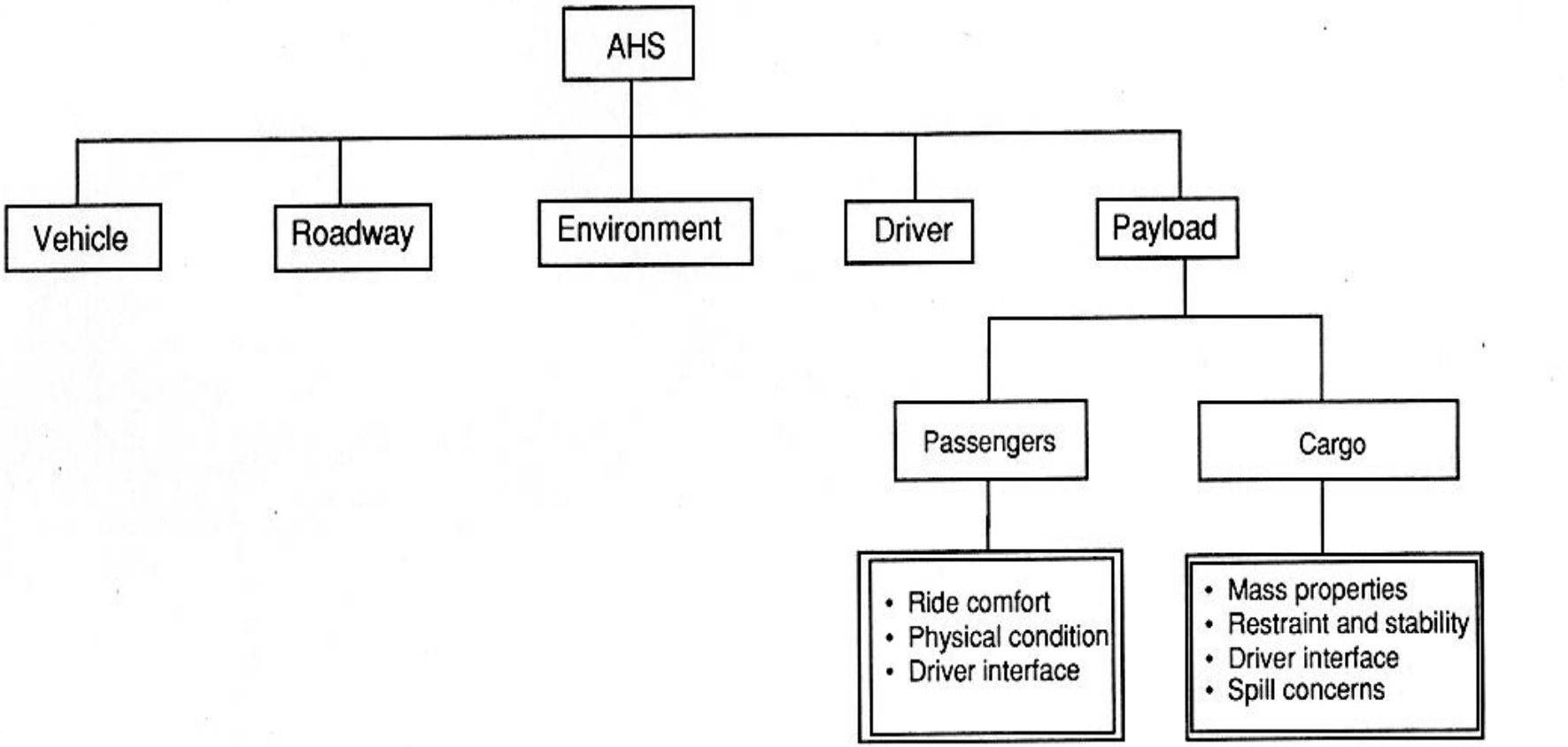

FIGURE 1-6 PAYLOAD FACTORS

Is the driver necessary in AHS? The driverless concept is permitted. However as discussed later, this method of moving payload involves extensive infrastructure and/or a very mature level of malfunction management that would allow such vehicles on existing freeways.

The environment is a necessary factor unless we are enclosed as in a tunnel and covered freeways would be expensive. However even tunnels have environmental problems such as air quality and flooding.

The five components, in addition to being physical entities we can easily differentiate, are historically treated separately in legal matters. The individual owner (and the manufacturer) are responsible for the vehicle. The public sector (or the private owner) is responsible for the roadway. The driver is responsible for operating the vehicle and, in the AHS for the driver role as defined. Malfunctions due to the environment are "an act of God". Payload problems are legally assignable depending on responsibility.

Further definition of subcomponents for vehicle, roadway and driver is a straightforward division into basic manual system items and items needed for AHS operation. The environment and payload division is again along physical lines.

3.1.1 Vehicle

We have assigned function to the component lists for the vehicle (Figure 1-2). The basic vehicle subsystem functions are well known. The following definitions are offered for the vehicle AHS subsystems:

Speed and Gap Control -- Subsystem consists of sensors interface electronics and wiring, computers, actuation electronics, mechanical interconnection and actuators. It provides speed control in response to command and gap control in response to command. It could use sensors maneuvering gaps to vehicles in adjoining lanes to provide correct computer response to vehicle movements in adjoining lanes. For example, the computer should be able to distinguish between the vehicle ahead suddenly decelerating and a vehicle entering the lane to occupy a space provided by the gap control.

Lane Control -- Subsystem consists of elements like the speed and gap control. It provides lateral positioning in the lane (normally vehicle centerline tracks lane centerline) and response to lane change command.

Vehicle Status and Operation -- Subsystem consists of the driver's controls, displays, computer interfaces and computer necessary to operate the vehicle just before, during, and just after automated mode engagement.

Malfunction Management -- Subsystem consists of elements like the status and operations subsystem plus the sensors necessary to detect and identify failures within the vehicle. For example, this subsystem might provide the capability to correctly manage failures of a dual device.

Vehicle Data Link Functions -- Subsystem consists of one or more transceivers, computer interfaces, and computers to exchange data with other vehicles and the roadway. The VV link data is assumed to be used to help protect gap by transmitting deceleration and deceleration command. It also could be used to

transmit the vehicle intention to change the number of empty spaces ahead held by the gap controller and intention to change lanes. The RV link data allows control of the speed and spacing of blocks of vehicles (C2) or the number of empty spaces ahead and lane change of individual vehicles (C3).

3.1.2 Roadway

The roadway AHS components (Figure 1-3 have the following definitions: Roadway broadcast - an audio message or in-vehicle graphics display message to all vehicles in a sector.

RR Data Link -- A data link among roadside computers and sensors which can be implemented by cable or fiber optics as well as microwave or radio.

Sensors -- Surveillance TV cameras, counters, surface friction sensors precipitation sensors, GPS receivers, laser timers, beacons, etc.

RV Data Link -- A two-way data link between each vehicle and the roadway used for ATMS control of automated vehicles, in group and/or as individuals. If this link is used for each vehicle's gap control, we assume that gap control sensing is still available in each vehicle as a redundant capability and as the primary control on rural freeways.

Computers -- Probably operated by ATMS and designed to handle a sophisticated network with a large data base and parallel satellite computer network with suitable redundancy.

Roadway -- Controlled Signals/Signs -- roadside electronic signs, lights, beacons, gates, etc.

3.1.3 Driver

The three driver functions named here (Figure-5) involve overlapping capabilities. Since we are interested in what happens when various driver failures occur we would like to define gradation of capability. The lowest demand on the driver is potentially the driver role assumed for routine AHS operation. A stronger interaction is visualized for malfunction management. The strongest interaction is in the manual portions before automatic mode engagement, and after normal and abnormal disengagement.

3.1.4 Payload

Payload (Figure 1-6) is defined by the reason for the trip, but if we are talking about the family vehicle rather than a commercial vehicle, the term "payload" is strange. Malfunctions of the payload are even more unfamiliar. However, there are some important considerations. Vehicle mass influences what is safe space around the vehicle. Therefore the cargo weight is important in a fundamental way. Items carried externally become a critical hazard should they not be restrained properly, fall off, and become an "object in the lane"- perhaps the most troublesome malfunction for automation to handle. Passengers, including the driver, have definite and rather low limits to the abruptness and level of accel/decel, level of steady side acceleration and turn rate, and they generally would not tolerate small limit cycles, noisy behavior _of the lane and gap tracking, and other sources of poor ride qualities.

3.1.5 Environment

Figure 1-4 lists environmental factors separated by the physical phenomena involved as they might affect various parts of the AHS. Electro-magnetic phenomena would influence data links and electrical data paths within the vehicle. Road surface condition would determine speed, steering, braking and ride qualities. Crosswind gusts might become the most important design criterion for lane control. Sensor usability is a factor throughout. Driver visibility is a factor near the egress point and for unplanned manual mode use. Lighting is separately considered because the physical phenomenon involved is sunlight rather than weather although the relevance is visibility.

3.2 AHS NON-VEHICLE COMPONENT MALFUNCTIONS

Considering fault trees that might be constructed from Figure 1-1 and its extensions becomes a highly complex task. We have studied the vehicle failures in some detail. To bound the study, we have not pursued the other elements to add to the failure rate data base. Several reasons beyond this general one are given in the following sections.

3.2.1 Roadway AHS Components

Roadway AHS failure rate due to component failures should be low. Within a given sector, which we later take as thirty miles to obtain some numerical results, many thousands of vehicles could pass in a day. Yet this sector might be equipped and managed with relatively few, relatively reliable roadside components. Our study of a C3 system - the most elaborate roadway requirement- indicates numbers like one hundred per mile. Then for thirty miles we have 72,000 component-hours per day of components with 20,000 hour MTBFs as opposed to 72,000* vehicle-hours per day with 1000-hour MTBF per vehicle. It would also be possible to sustain several roadway component failures and remain fully functional.

---

* Assume an average 3000 vph flow in an eastbound lane over 24 hours. Assume an average speed of 60 mph. Then for a thirty-mile sector, total vehicle hours is 36,000. Double this for two directions.

3.2.2 Roadway Right of Way

Roadway right of way problems except for objects in the lane are largely covered elsewhere. These are environmental problems (discussed below), traffic problems (part of ATMS), maintenance (part of the Roadway Operations task) and incident management (also part of the Roadway Operations task).

An object in the lane poses a challenge. The object can be anything: a paper bag, smashed bottle, muffler, tire tread, tarp, damaged vehicle from an adjoining manual lane, deer, cow, etc. We currently do not have fully automatic technology that can cope with the range of threat that exists on today's freeways. Not only would the sensor(s) have to detect all manner of materials and detect them at distances up to 200 feet or so, the computer would have to decide what evasive action to take, if any, __and then signal the control systems to respond appropriately. One correct action might be to do nothing since the consequences of hitting are less than the jolt to everyone in the vehicle caused by abruptly steering to another lane.

Better that we concentrate on preventative measures such as fences, barriers, and maintenance vehicles that can pick up objects without disrupting flow. We need

rules about acceptable ways to carry and restrain external cargo and to maintain exhaust systems and tires.

If we give the driver a steering mode that allows bias of lane tracking position, the driver, with continuous malfunctions monitoring attention, could be on the lookout for obstacles and could avoid a large number after judging what the object is and whether it is worthwhile to avoid. But this defeats the potential driver task relief benefit.

When we think about our own experience and take a sample of the drivers around us, we soon realize that the probability of encountering an object in the lane we would not care to hit is fairly high - perhaps of the order of ten per year or one per 40 vehicle-hours.

On a dedicated AHS lane with a barrier separating manual and automated vehicles, the chances of an object should be less, since the manual vehicles, which are not inspected as vigorously and therefore would drop parts more readily, would be prevented from hitting objects into the AHS lane. Manual lane accidents would not send disabled vehicles into the dense AHS stream.

3.2.3 Environmental Factors

Environmental factors could almost not be classed as malfunctions. They are part of normal operations since AHS operation must continue in all weather. The control design must cope with low surface friction. The safe lane density as a function of speed must vary to allow for increased stopping distance. The malfunction aspect appears when we consider ice on bridges, low sun angle blinds a TV camera sensing lane markings, extra large side gusts during a thunderstorm saturate the lateral control, lightning strike nearby knocks out a roadside computer, etc.

Although these matters are important, they were not judged of the highest priority for a precursor study. The influence of decreased surface friction on lane capacity is treated in the entry/exit chapter as a matter for normal operation.

3.2.4 Driver Malfunctions

Driver capabilities and how they might vary across drivers and throughout an AHS trip are the subject of extensive research outside the precursor studies. The possibility of incapability to resume manual driving is considered in the checkout task. The check-in task also mentions a test of the driver. We assume that driver incapacity to resume manual driving would result in an automated parking maneuver to a position out of the AHS lane. Demand on the driver to perform normal duties while automated or even perform malfunction management might be low enough to make __the incapacity rate quite low. The latter is not true if, as we will examine later, the driver is required to take over manually if there is a single failure of dual lane control or gap control.

The number of driver mistakes can be minimized by thoughtful human engineering. Other research efforts are addressing this subject for AHS. We urge that the following precepts be considered by AHS designers:

1. Use similarity with the manual mode operation.

2. Use maneuvers that are similar to smooth manual maneuvers of a non-aggressive driver.

3. Use simple procedures with few steps.

4. Present few choices and allow plenty of time to decide what to do.

5. Design controls, switches, buttons etc. that can be verified and operated without looking at them.

6. Integrate information before presentation.

7. Have large displays that are easy to read in all lighting conditions.

8. Minimize driver mental workload by minimizing the number of messages to be processed.

9. Use system feedback questioning unusual actions such as a request to take over manually.

10. Make the driver responsible for system engagement or well informed of progress toward engagement.

11. Make sure all maneuvers are complete and the vehicle is at constant speed in the transition lane before disengagement and give adequate notice before automatically disengaging. It might be advisable to give the driver opportunity to disengage manually prior to the system dropoff point.

The effect of driver mistakes can be minimized by a forgiving design. Interlocks that nullify the effect of inappropriate button presses or switch actions should be used. Engaging too soon or too late and disengaging too soon or too late, if the driver has responsibility for the functions or can preempt them, should not cause dangerous conditions. They should mean little more than the driver might miss that opportunity to ingress or egress the AHS lane and must go on to the next opportunity or go around an auxiliary lane to try again (I3 entrance).

3.2.5 Payload Problems

Payload difficulties should be quite infrequent provided special attention is given to how cargo is loaded and constrained. Passenger tolerance of a control problem that is not disabling but simply annoying could be handled by taking the next _exit.

3.3 SOFTWARE SAFETY ANALYSIS

The Software Safety subtask did not deal with specific reliability numbers. Rather, it was directed at:

a. Identification of system hazards that could affect the software,
b. Development of a systematic approach to system and software safety, and
c. A safe, efficient approach to communications.

At this early stage of system development little is known about the eventual design of the system. Because little is known, identification of system hazards must rely on past experience with similar systems. The AHS system, regardless of the final design, will have interfaces, operate in a realtime environment and communicate, similar to Department of Defense (DOD) command control systems that exist today.

During the concept stage of system development, it is paramount that the __foundation for the project safety effort be established. This foundation must include a system safety program plan that describes how the safety effort will be executed. As the AHS project develops and more is learned about the system design and its hazards, it may be necessary to modify the plan.

No matter what the final design of the AHS system, safe and efficient communications will be critical to successful deployment. The communications design must be efficient enough to process critical and non-critical messages from the highway infrastructure and from other AHS-equipped vehicles and ensure that only messages from valid sources are processed. The final design must demonstrate that the software has the capability to react faster and with greater precision than human operators when system malfunctions or external events pose imminent danger.

Each of the above analysis areas will be discussed in detail below.

3.3.1 Identification of System/Software Hazards

Software is no different than any other component of the AHS System. Software should be a part of the system hazard analysis as well as a subsystem hazard analysis specifically called a software hazard analysis. When this study was conducted little was known about the actual design of the system, and consequently, most of the software behavior and interfaces to the rest of the system had to be derived from systems of like design. The AHS System will operate in a real-time environment, issue commands, process commands, operate in an unpredictable environment, and expose humans to risk, much like current DOD Command and Control Systems do today. Two DOD systems were analyzed in this study, the Aegis System and the __Cruise Missile Weapon System. Both systems make extensive use of software in commanding and controlling hazardous operations. These systems also rely heavily on data from various system components to make decisions that affect the whole system. The Aegis system also relies on inputs from other identical systems, and from other systems that perform like it, but are not identical, to make decisions affecting it. The AHS System will be exposed to most of the same software hazards that affect DOD Command and Control Systems or any other real-time decision making system that uses software.

The AHS software must be capable of making decisions regarding AHS component health, when to reduce or increase speed, when to brake, its position on the highway, when to enter AHS control, when to exit AHS control, and probably many __more as the AHS design matures. When making these decisions the individual AHS software must rely on the accuracy and timeliness of the data from sensors and from other AHS systems. Vehicle speed and roadway position are examples of critical signals internal to each AHS Vehicle. Signals advising of emergencies and requesting a change of position are examples of critical signals external to the AHS vehicle.

Table 1-1 is a software fault hazard analysis for the AHS. The RSC I2C2 system configuration was chosen to perform the analysis. I2C2 was chosen because it represents a sophisticated system and will operate on a conventional highway in a dedicated lane. If this type of configuration is chosen it will present safety challenges due to the mix of conventional and AHS vehicles.

TABLE 1-1 Software Fault Hazard Analysis

Hazard	Cause	Effect
Erroneous dtat from the data link	Vehicle System acts upon latent data, data from oncoming AHS vehicle, or data from AHS vehicle behind it	Processing of erroneous data could cause impact with other vehicles; slow or stop traffic in AHS lane
Data link overload	Vehicle data link component receives messages at such a rate that an emergency message is missed	Possible impact with leading vehicle, slow or stop AHS traffic
AHS vehicle software processes an erroneously low speed sensor output	Speed sensor outputs valid but inaocurately low vehicle speed to the system causing the software to command the vehicle to accelerate to match a commanded speed	Possible impact with leading vehicle
AHS vehicle software processes an erroneously low speed sensor output	Speed sensor outputs valid but inaccurately low vehicle speed to the system causing the software not to commend vehicle deceleratlon for upcoming curve	Vehicle leaves AHS roadway
AHS vehicle software processes an erroneously high speed sensor output	Speed sensor outputs valid but inaccurately high vehicle speed to the system causing the software to command the vehicle to slow to match a commanded speed	Possible impact with trailing vehicle; slow or stop AHS traffic
AHS vehicle software processes an erroneously large headway sensor output	Headway sensor outputs valid, but inaccurately large vehicle headway value to the system causing the software to command the vehicle accelerate to maintain, proper headway	Possible impact with leading vehicle

Table 1-1. Software Fault Hazard Analysis (continued)

Hazard	Cause	Effect
AHS vehicle software processes an erroneously small headway sensor output	Headway sensor outputs valid, but inaccurately large vehicle headway value to the system causing the software to command the vehicle slow to maintain proper headway	Possible impact with trailing vehicle; slow or stop AHS traffic , ,
Inadvedent output from AHS vehicle software to the speed control hardware	A software error causes an acceleration command to the speed control hardware	Inadvertent AHS vehicle acceleration could cause impact with the lead vehicle
Inadvedent output from AHS vehicle software to the speed control hardware	A software error causes a deceleratlon command to the speed control hardware	Inadvertent AHS vehicle deceleration could cause impact with trailing vehicle or cause trailing traffic to slow or stop
Inadvertent output from AHS vehicle software to the braking control hardware	A software error causes a "commence braking" commend to the braking system	ff the braking system is commanded to commence braking inadvertently, the AHS vehicle could be impacted by a trailing vehicle or cause AHS traffic to stop or slow
Inadvertent output from AHS vehicle software to the braking control hardware	A software error causes a "cease braking" command to the braking system	If the braking system is commanded to cease braking the AHS vehicle could impact the lead vehicle or leave the roadway on a curve
Software execution after vehicle impact	Inadvertent commands after impact	AHS vehicle impact could cause erratic software behavior and result in erratic vehicle behavior
Software ceases execution	"Dead code" is executed	Possible collision with lead or trailing vehicle; slow or halt AHS traffic
Automatic and operator inputs confuse software	Operator demands vehicle control at worst possible time	Possible collision with lead or trailing vehicle; slow or halt AHS traffic
Data overload causes indication of upcoming curve to be lost	Software is receiving too much data for processing capacity	Vehicle leaves AHS roadway

3.3.2 Systematic Approach to System Safety

A comprehensive and effective safety program for the AHS should begin at this early stage of system development. A Safety Policy document should be written to define the role of safety with respect to other organizational goals and provide guidance in deciding what actions should be taken in specific situations. The safety policy should state the goals of the AHS safety program; procedures for reporting problems in working with the policy; and a clear statement of responsibilities, authority, accountability, and scope of activities. Prior to

completion of the Safety Policy document, policy decisions will need to be made that will have a direct effect on the safety of the AHS System. Policies regarding the development of the AHS vehicle system and the AHS highway system and the role that the Department of Transportation and other government agencies will play in the AHS system development must be made as early as possible in the current stage of system development.

The development scenario that would be the simplest and lowest cost from the safety standpoint, is one that would have the DOT or other government agency select a single developer for development of the vehicle and highway components or multiple contractors to build different components of the system and a contractor to integrate the components. In this scenario, the government would have the tightest control over design decisions that would affect the safety of the AHS vehicle and highway components. This scenario may not produce the most cost effective system or be the most desirable for DOT.

Another development scenario that could be employed is one that would have DOT or other government agency assume the regulatory role. The regulators would develop design, manufacturing, and verification requirements for the vehicle and highway system as well as construction requirements for the highway system. This scenario would allow vehicle manufactures and highway builders the latitude to choose AHS component developers that complement their particular highway or vehicle. In this scenario, the safety costs would be higher due to verification of safety requirements at multiple manufacturers, but would probably be offset by lower system cost due to competition.

Regardless of how the AHS is developed, safety policies and goals must be in place as soon as possible. A System Safety Working Group should be established to begin defining the AHS safety policy and begin work on the AHS System Safety Plan. The AHS System Safety Working Group should be made up of representatives from each agency and each contractor and be the focal point for interfaces between the DOT and AHS contractors and subcontractors. Members of the working group would be responsible for making input for their respective organizations on system safety issues and policy as well as reporting the status of unresolved issues to their respective organizations. One of the first tasks of this group would be to develop software and system safety requirements from a software fault hazard analysis (see the previous table), from other system hazard analyses conducted, and from future system and software hazards analyses as the design matures.

If DOT assumes the role of regulatory agency, the establishment of an Automated Highway System Safety Review Board would help to assure that AHS safety requirements are incorporated in each AHS component by periodically reviewing system development throughout the life-cycle. This review should include any software associated with component development. This board would review the component developer's system and software safety analyses and test programs and would be independent of any AHS developers.

At this stage of AHS development, the foundation for project safety should be established. The most important part of this foundation is the System Safety Program Plan. The System Safety Program Plan will describe the system safety objectives and how they will be achieved. It will provide a regulatory agency, contracting agency, or manager with a baseline document to be used to evaluate compliance and progress. Subsystem safety plans should be included in the System Safety Program Plan.

The System Safety Program Plan should include at a minimum; sections describing: (a) the System Safety Organization; (b) the System Safety Program Schedule; (c) System Safety

Criteria; (d) Safety Data requirements; (e) Hazard Analysis types, Documentation Requirements and when to apply; (f) Verification Requirements; (g) Audit requirements; (h) Emergency and Contingency Procedures, (I) Configuration Control Procedures; (j) Safety Training Requirements; (k) Hazard and Incident Reporting and Investigation Procedures; and (I) System and Software Safety Requirements.

The System Safety Program Plan should be a living document and plans should be made to review and update it at the beginning of each new system life-cycle phase. The review and update should take into consideration changes in AHS design and safety policy.

3.3.3 Safe and Efficient AHS Communications Study

In order for the AHS to operate smoothly and safely, AHS vehicles must have the capability to pass pertinent data among themselves and pass and receive information from the roadway. A key factor to the success of the AHS will be a safe and efficient communications design. In this study, the RSC I2C2 system configuration was used. It was also assumed that communication between cars and between cars and the roadway was necessary. In the study, vehicles were assumed to be traveling in platoons of five vehicles. The study scenario also assumed that the vehicles were making decisions regarding vehicle spacing, speed, and handling entry into existing platoons or starting new ones. In emergency situations it was assumed that the roadway component could override speed, spacing, entry, as well as intended exit.

As apart of this study, a search was made for like systems that rely heavily on communications to complete their mission. A DOD communications system was studied. In the DOD system ships, planes, and ground forces participate in a communications link and are provided information from other participants to help their defensive posture or to complete their assigned mission. The units participating in the communications link are assigned unique identifiers and decode only messages addressed to them or emergency messages with unique identifiers. These systems operate in a hazardous, real-time environment, rely on a radio communications system, and must rely on accurate and timely information from other participants to complete their mission. The AHS must operate in a similar real-time environment and must rely on information from other participants to remain safe and successfully meet its mission.

One obvious hazard associated with AHS communications is sending emergency messages to vehicles that do not need it. Sending emergency stop messages to vehicles traveling in the opposite direction on an AHS roadway or to vehicles ahead of the emergency situation would only add to the havoc. In the AHS scenario described earlier, vehicles could be assigned unique identifiers upon entering the AHS lane, the roadway stations could be assigned unique identifiers, and when created, platoons could be assigned unique identifiers. The roadway station identifiers would remain static. The vehicle and platoon identifiers could be assigned when the vehicle enters the AHS system and when a platoon is created. Messages sent within a platoon could be addressed to all platoon participants or to individual vehicles within the platoon. The roadway could communicate with platoons and individual vehicles using the platoon and vehicle identifiers. Unique roadway identifiers combined with the position of an emergency would prevent vehicles
traveling in the opposite direction or ahead of the emergency from acting on the commands issued as a result of the emergency.

Using this scenario, each platoon should have a leader and platoons should have the capability to communicate with each other to combine or split platoons. Platoon leaders would

communicate with platoon members to provide speed and spacing information, to command spacing to allow a new vehicle to enter, to request destination information, and to request any other data necessary to keep the platoon moving and safe. The roadway could request certain platoons to split or join together, to maintain a specific headway or speed, to require platoons to maintain a certain speed and headway within the platoon. Certain messages such as requests to join a platoon and emergency messages could have unique identifiers and would be decoded by all vehicles that would be effected. This communications scheme is based on the design of DOD communications systems.

A study by the Texas Transportation Institute of the Texas A&M University System (Communications In Intelligent Vehicle Highway Systems--Part I) indicates that the scheme described above could possibly be implemented in the AHS. The Texas Transportation Institute study investigated the viability of using radio communications between individual vehicles and a highway station. This study concluded that radio transmission was viable, but a problem existed with the bandwidth necessary to communicate with all vehicles within range of the highway station. The study indicated that the optimum method of communicating to vehicles from the highway station was to divide the vehicles into groups.

Based upon lessons learned from the DOD communications systems and the information provided in the Texas Transportation Institute study, an AHS communications scheme similar to the one described above is possible. Studies must be made to determine system data rate requirements and the types of data that is necessary to transmit over the data link. A rapid prototype of this type of data communications system would allow experimentation with various designs, data rates, and communications protocols to determine a design that would satisfy AHS data communications needs.

3.3.4 Summary

At this early stage of AHS development, software hazards analysis can only be conducted using lessons learned and comparison to existing systems methods. Using rapid prototyping to model various designs could help, but may not be cost effective.

Development of a System Safety Program Plan that includes software would be very beneficial at this time and is strongly recommended. The plan should define criteria for developing a safe system as well as safe software. The plan should define safety and performance requirements that must be met to field a safe Automated Highway System and specify the types of hazard analyses that should be conducted at each stage of systems development. The plan should define the roles of the government as well as the developers and define the process for safety approval of the system and components including the software.

The communications component of the Automated Highway System is critical to safe system operation. Rapid prototyping of the communications component at this time would help to arrive at a safe design, that would support the desired vehicle per hour rates of the AHS.

3.4 VEHICLE COMPONENT MALFUNCTIONS

3.4.1 Basic Vehicle Malfunctions

3.4.1.1 Present Basic Vehicle Reliability

Several sources of data were used in support of this study. This includes case

studies of the San Francisco Bay Area Bridge (MacCalden, 1984) and Highway 401 near Toronto (Reiss, 1991). The New York State Thruway Authority (NYS Police 1994) also provided data on vehicle reliability and several sources of information were used in evaluation of basic vehicle reliability. This included reports and databases maintained by the ARMY Tank Command for the CUCV (modified four-wheel drive vehicle) and BMW data fore recent model run (U.S. Army 1992 and BMW, 1994).

Data such as this are available from various agencies throughout the world. However, they are not gathered according to a consistent specification. To help reduce that variability we assumed the average number of incidents is proportional to the vehicle hours of exposure. Thus a vehicle-hour traveled at 30 mph would have the same incident rate as a vehicle-hour traveled at 60 mph. This is not appropriate for tires, but certainly applies to an AHS throttle actuator that has no wear or breakdown associated with how fast it is moving over the road. Thus we make a generalization here, but one that makes sense for ma of the basic vehicle components of the existing data sets and a-11 of the AHS vehicle components we will add to the vehicle.

Vehicle average speed does enter the exposure equation for a given length of AHS lane since the faster the vehicles move through the region, the lower the vehicle-hours for each vehicle. In two of the three data sources we have been obliged to assume an average speed to convert vehicle-miles to vehicle-hours, since the average speed was not given. The most reliable assumption here 1530 mph for the San Francisco Bay Bridge. Assuming 60 mph for the Toronto data might be questioned by virtue of the region including rush-hour urban traffic. (The NYS Thruway data specified an average speed of 61.9 mph).

Another very important matter of interpretation is how the data was gathered and what was the definition of "incident". In all three data sources, we can be confident that a stopped vehicle was involved. Were all stopped vehicles counted? In the Toronto and Bay Bridge data, we can be fairly sure that most stopped vehicles were counted. In the NYS Thruway data we have police reports on vehicles stopped at the side of the road. When accident calls are added to these reports the result is compatible with the other two data sources.

The Toronto, Bay Bridge and NYS Thruway data showed good concurrence on vehicle incident data of approximately 1,000 hours MTBF. The Toronto study indicated a failure rate of 877 hours MTBF (19 failures per million miles at an estimated 60 mph), the Bay Bridge study indicates a1042 hour MTBF (40 failures per day over a 5 mile section at an assumed speed of 30 mph and a daily volume of 250,000 vehicles), and the NYS Thruway data indicated a913 hour MTBF (111,254 incidents in 6.3 billion miles of road travel for 1993 at a speed 0f62 mph). The close agreement among these different sources lends confidence in 1,000 hour MTBF estimate as abase for AHS estimates.

The reported statistics included flats, overheats, mechanical failures, electrical failures, out of gas, and accidents. A comparison of category failure rates (Table 1-2) for the Bay Bridge and Toronto data shows reasonable correlation in the fault categories provided. A breakout of the NYS Thruway data to this level is not available. Table 1-3 distributes the overall FPMH (Failures Per Million Hours) among the failure categories using the Toronto failure categories. As can be seen, about 440 FPMH are expected for mechanical and electrical failures.

An attempt to approach the vehicle reliability question from manufacturer or operator databases ended in variable result quality. Many assumptions were involved, the major one being the criticality of the failures. The highway incident data has the advantage of directness. The highway databases are huge and vehicle condition appropriately mixed. The criticality is

defined because the vehicle has definitely been disabled to even appear in the failure list. None of these things are true for the failure data from the other sources. The CUCV database 15931,000 miles on 157 vehicles over three years. The average vehicle speed is unknown but assumed low because the vehicles are used off-road. The failures are mission failures defined to include failures discovered during a pro-mission inspection. The BMW database is 85,500,000 miles on 4500 vehicles, all in the (estimated) first 19,000 miles of usage. The average speed was assumed to be 30 mph.

Table 1-2. Frequency of Vehicle DIsabling Malfunctions

	Toronto 4011.	San Francisco Bay Bridge[2]
Overheat	.08	.08'*
Out of Gas	.07	.18
Flat Tim	.18	.09
Mechanical/Electrical*	.36	.51
Accident	.15	.03
Other	.16	.11
Total	1.00	1.00

1. Source: Reiss, 1991
2. Source: MacCalden, Jr. 1984
* Includes abandoned vehicles
** Subtracted from an overall mechanical/electrical total of .59

Table 1-3. Disabling FPMH Estimates For Basic Vehicle

	Toronto 401	SF Bay Bridge	NYS Thruway
Overheat	91	77	
Out of Gas	80	173	
Flat Tim	205	86	no breakdown
MechanicaVElectfical	411	490	available
Accident	171	29	
Other	180	106	
Total FPMH	1140	960	1,095
MTBF (hrs.)	877	1042	913

on 157 vehicles over three years. The average vehicle speed is unknown but assumed low because the vehicles are used off-road. The failures are mission failures defined to include failures discovered dudng a pre-mission inspection. The BMW database is 85,500,000 miles on 4500 vehicles, all in the (estimated) first 19,000 miles of usage. The average speed was assumed to be 30 mph.

The breakdown is given in Table 1-4 with Calspan researcher judgment used to separate disabling failures (failures that would stop the vehicle). The results should compare with 411 FPMH and 490 FPMH from Table 1-3 for mechanical and electrical failures, but they are lower (289 FPMH* and 121 FPMH). However, at least the results are not an order of magnitude different from the highway data.

---

*The CVCV result can be forced to equal the BMW result if a speed of 2.4 mph is assumed and all failures judged to be disabling.

Table 1-4. Mechanical/Electrical FPMH for Basic Vehicle

	CUCV Database	BMW Database	
	All Failures	All Failures	Disabling Failures
Axles	1.2	0	0
Brakes	4.8	4.9	4.9
Cooling	0	9.5	9.5
Electrical	144.4	275.0	74.0
Engine	16.9	62.8	14.0
Fuel	89.1	88.5	4.9
Steering	12.0	12.6	0
Transmission	7.2	23.9	13.3
Wheels/Suspension	7.2	0	0
Total	288.8*	478.0	120.6

*This is failures per 10^6 miles. Average speed unknown.

Two other data points are worth mentioning. The first is the basic vehicle reliability for an electric vehicle postulated in Elias, 1977. This vehicle was estimated to have an FPMH of 961 divided into 564 for the basic vehicle and 397 for the automatic control and the radar (AHS components). The other is the Year 2000 reliability goal for automotive electronics of .01 ppm (part failures per million parts) cumulative at five years or 50,000 miles, equivalent to 1,800 ignition-on hours stated in Zanoni, 1993. This reference also states that, according to a Prometheus project forecast, the automobile of 1995 will have about 100 sensors, 80 actuators, 45 motors, 5 displays, 4 imagers and 1000 integrated circuits. Each of the electronics components might have 100 subcomponents. Of course, not all these components would be vital to the locomotion of this 1995 vehicle. If they were, and each had a failure rate of only an FPMH of 5.6 x10*(-6), they would contribute only an FPMH of about .5 to the basic vehicle total of 478-a worthy goal.

3.3.1.2 Future Basic Vehicle Reliability

If we presume an AHS vehicle with at least today's breakdown frequency, we will avoid an unfortunate public perception, i.e., when it works it is great but it is always in the shop or the automated mode is frequently unable to pass check-in. Of course, there is no way to guarantee such success. We are intending to add components to the machine. Conventional analysis would predict a lower reliability. However, the Toronto data indicates a large component of what we might term "avoidable" failures. In Table 1-2 the overheat, out of gas and flat tire categories account for 33 percent of the total. Accidents account for 15 percent more. We cannot eliminate all of these failures but vehicle improvements will certainly help and automating driver functions will reduce the accident rate. Automatic monitoring and more frequent routine inspections will also help. These improvements will also lower the number of mechanical/electrical failures. Since "other" is unknown, we leave that percentage unchallenged, but roadside passenger relief stops, etc., would be eliminated in the AHS.

Based on these factors we take the position that roughly 50 percent of today's basic vehicle stoppages can be eliminated in the AHS vehicle of the future. This leaves a budget of 50% for automation components to achieve an overall AHS vehicle reliability equal to today's

vehicle. But do we have a reasonable chance of fitting into this budget? Out of an FMPH of 1000, the automated mode must account for no more than 500.

3.4.2 Automation Subsystem Reliability

An analysis of similar subsystems and components currently in use or under development is presented in Appendix A. This work covers fifteen items, nine of which would be found in every vehicle. The nine reliability budgets are listed in Table 1-5. The total FMPH is 500 to fit the budget, with the data of Appendix A as justification. The other six are roadway components, which were mentioned earlier and will not be studied further in this section.

The probability of the kth subsystem avoiding failure in a given exposure time T is given by :

Table 1-5. AHS Vehicle Subsystem Reliability Projections

Subsystem	Toronto 401"
1. Longitudinal sensing	50
2. Lateral sensing	50
3. Computer processing	20
4. Longitudinal control	80
5. Lateral control	60
6. Communications	50
7. Status and Operations	50
8. Malfunction Monitoring	140
TOTAL	500

$$a(k)=e^{*-T/MTBF} = e^{*-T(FPMH\ 10^{-6})} \qquad (1\text{-}1)$$

For example, if a gap control system with J channels but only I necessary for the operation described and no possibility of a common mode failure, the formula becomes

$$a = SUM\ e^{*=-iT/MTBF}\ (1 - e^{*-T/MTBF})^{*J-i}\ (J!/i!(J-i)! \qquad (1\text{-}2)$$

For example, if we have dual gap control and operation is possible with one channel inoperative, then J = 2, I = 1 and

$$a= (.86)\ (.14)\ (2)+(.86)^2= .98$$

3.4.3 Vehicle Design and Malfunction Management

3.4.3.1 Subsystem Reliability and Cost

Using combinations of the items in Table 1-5, we can look at the failure rates of the subsystems of Figure 1-2 (see Table 1-6). Note that four subsystems - speed and gap control, lane control, status and operations, and malfunction management - each have their own digital processor (see Appendix A). The design could use one processor for all four subsystems but this would introduce common mode failures. A highly redundant processor (triple or quad) could make such failures very remote and perhaps be more cost effective.

To introduce the cost factor, assume that an optimistic cost is five percent of total vehicle cost and a pessimistic cost is twenty-five percent. Assume the acquisition cost of a fully dual system is twice these numbers and a fully triple system is three times. (Judging by the increased numbers of failures in the redundant systems, the life cycle cost will also increase.) This places a fully dual system between ten and fifty percent of total vehicle cost. The fully triple systems are optimistically within reach but pessimistically out of the question. An interesting compromise is listed in the last column of Table 1-6. The cost is more like the single system cost but redundancy is used where it can help the most in reducing failures to the breakdown lane and __failures causing lane blockage.

3.4.3.2 Single Failure Management

Table 1-7 lists assumed safety procedures and associated frequency of occurrence per million vehicle miles. The driver is assumed passive in the sense that the procedures do not require driver action. We will impose the ground rule that single-channel operation of either speed/gap or lane control will be disallowed.

Speed and Gap Control -- In a non redundant system, fail-soft design would allow the vehicle to coast or brake to a stop. Since lane control would still be functional, the vehicle could be parked in a breakdown lane. In actual system with fail-operate capability provided by some clever means, the automatic system could proceed to the next exit on the single system left. However, this would violate our ground rule of no simplex control operation, so the operative lane control would place the vehicle in the breakdown lane. In a triplex systems, voting could be used to decide which channel is faulty and continued dual operation would be permitted to complete the trip. The vehicle might also be permitted to pass check-in on another AHS to complete the trip.

Table 1-6. Subsystem AHS Vehicle Reliability

Subs;ystem	AHS Item Numbers	AHS Items Not Redundant FPMH	Dual Redundant FPMH	Triple Redundant FPMH	Not Redundant Except as Noted FPMH
Speed and Gap Control	1,3 and 4	150	300	450	300 Dual
Lane Control	2, 3 and 5	130	260	390	390 Triple
Status and Operations	7	50	100	150	50
Malfunction Management	8	140	280	420	140
W Data Link (C1)	6	50	100	150	50
RV Data Link (C2, C3)	6	50	100	150	50
Basic Vehicle	Sec. 3.3.1,2	500	500	500	500
Total AHS Vehicle		1070	1640	2210	1480

Table 1-7. Single Failure AHS Vehicle Reliability - Passive Driver

	Not Redundant I=J=I		Dual Redundant I=J=2		Triple Redundant I=J=3	
Subsystem	**FPMH**	**Procedure**	**FPMH**	**Procedure**	**FPMH**	**Procedure**
Speed and Gap Control	150*	Lane Blockage or Breakdown Lane	300	Breakdown Lane	450	Complete Trip
Lane Control	130'	Lane Blockage	260	Breakdown Lane	390	Complete Trip
Status and Ops	50	Next Exit	100	Next Exit	150	Complete Trip
Malfunction Manaaement	140	Next Exit	280	Next Exit	420	Complete Trip
W Data Link (C1)	50	Next Exit**	100	Next Exit	150	Complete Trip
RV Data Link (C2, C3)	50	Next Exit	100	Next Exit	150	Complete Trip
Basic Vehicle	500	Breakdown Lane	500	Breakdown Lane	500	Breakdown Lane
Total, lane blockaae	130		0		0	
Total, breakdown lane	650		1060		500	

Lane Control -- with no redundancy and no driver intervention assumed, many, if not most, single failures would result in lane blockage at best and fatalities at worst. Dual systems could possibly allow the vehicle to make it safely to the breakdown lane. Operation to the next exit seems ill-advised since, unlike loss of speed/gap control, there probably is no reasonable procedure without steering control. Besides, we would be violating our ground rule.

*This operation would be disallowed by the single-channel ground rule.
**At no-comm. gap

A triplex system could be permitted to finish the trip but subsequent check-in would be disallowed.

Status and Operations -- For emergency operations, the vehicle should be permitted to make it to the next exit without driver displays and with only one of two systems working.

Malfunction Management -- A second failure might go undetected but it seems reasonable to avoid more breakdown lane incidents by allowing operation to the exit on an emergency basis.

VV Data Link -- Failure can be managed by lengthening the gap to one safe without data from the vehicle ahead and proceeding to the next exit. The impact on vehicle density is negligible.

RV Data Link -- Since traffic control could be vital in peak periods, any vehicle not receiving should probably not continue beyond the exit. If operation is C3, it could drop to C1 and complete the trip provided that C3 is designed with C1 as a backup.

Basic Vehicle -- Loss of locomotion, which is the fault assumed in the figure of 500 FMPH, forces the vehicle to the breakdown lane.

Table 1-8 presents data and assumptions with an active driver role. The driver is active in the sense that driver manual takeover can be used to improve safety following single failures of actual system. This is particularly true of gap and steering

Table 1-8. SIngle Failure AHS Vehicle Reliability - Active Driver

	Not Redundant		**Dual Redundant**		**TrIple Redundant**	
Sub-system	**FPMH**	**Procedure**	**FPMH**	**Procedure**	**FPMH**	**Procedure**
Speed and lap Control	150'	Lane Blockage or Breakdown Lane	300	Next Exit At Manual Gap	450	Complete Trip
Lane Control	130'	Lane Blockage	260	Next Exit at **Steerable** Gap	390	Complete Trip
Status and 3ps.	50	Next Exit	100	Next Exit	150	Complete Trip
Mal. Mgt.	140	Next Exit	280	Next Exit	420	Complete Trip
VV Data Link [C1)	50	Next Exit at No Comm Gap	100	Next Exit	150	Complete Trip
RV Data Unk IC2,C3)	50	Next Exit	100	Next Exit	150	Complete Trip
Basic Vehicle	500	Breakdown Lane	500	Breakdown Lane	500	Breakdown Lane
Total, lane blockage	130		0		0	
Total, break down lane	650		500		500	

*This operation would be disallowed by the single-channel rule.

systems where the manual system as a backup is safer than actual automatic system operating with a single failure. The driver has time to mentally prepare for takeover since the automatic system is still operating. The driver proceeds with the appropriate gap size for manual driving at the AHS speed.

3.5 ADDITIONAL COMMENTS

1. If a breakdown lane is not present, we estimate 500 to 750 lane-blocking incidences per million vehicle miles. On a thirty-mile AHS carrying 6000 vph over twelve hours at 60 mph, the expected number of lane blocking incidences is 18 to 27 mostly due to basic vehicle failures. The price paid for a breakdown lane is well justified on this basis alone.

2. With actual steering system and an active driver, the failures to the breakdown lane can be minimized while keeping the system cost down.

3, The Toronto incident data in Table 1-3 totals 1,140 FPMH. This vehicle stoppage data is also identified as resulting in 13 percent lane blockages (Melee, 1991). The lane blockage then occurs at the rate of about 148 FPMH in today's manual traffic which compares with 130 FPMH for the worst case AHS result in Tables 1-7 and 1-8. Of course, the AHS lane blockage is much worse in terms of traffic delay if the lane is carrying as much as 6000 vph or more when the incident occurs.

4. Roadway failures on a thirty-mile AHS with 100 components per mile each with 50 FPMH would expect 3.6 failures per day whereas the vehicle failure rate of 1480 in Table 1-6 and a 24 hour average two-way flow of 6000 vph at 60 mph would expect 106 failures per day. We would presume the roadway portion could be designed so that any single _failure would be of no consequence to the overall system effectiveness and the comparatively small number would indicate that the vehicle reliability should receive major emphasis in future AHS research.

5. If our intuitive notion of the frequency in today's driving (one in 40 hours) with which we encounter threatening objects in the lane is correct, this "failure" is much more prevalent than any of the others we have studied. Reduction in frequency provided by fences and barriers should be considered. Regulations controlling restraint of loads should be considered. More frequent vehicle inspection and higher standards can be required.

6. If a single control failure in a dual, fail-operational system happens during egress, the maneuver would just continue to completion. If it happens during ingress we have three options:

   a) Continue to breakdown lane, if available in the region.
   b) Remain in the cruise lane until a breakdown lane is available.
   c) Return to the transition lane if conditions permit.

–

If the driver is active, the vehicle could complete the egress maneuver automatically and be taken over manually when the driver is ready or the

egress transition region ends.

Failure of the VV link that is creating space for entry would result, in worst case, no ingress allowed. Failure of the WV link in the entering vehicle would result in no ingress unless the maneuver was almost complete. At this point the maneuver would be completed and the malfunction handled as if it had occurred during cruise.

7. Loss of the vehicle end of communication links used for traffic control should not cause wide-scale problems. However, if they are used for individual vehicle speed and gap control as in C3 or for gap and/or lane position regulation, they must be adequately redundant.

8. Note that the vehicle with a dual automation system and an active driver role has roughly half the expected breakdown lane use (500 FPMH) of the standard freeway of today carrying the same volume (1000 FPMH). However, the total failure rate, most of which is managed by taking the next exit, would be sixty percent higher (1640 FPMH) than present breakdown lane use, according to this analysis.

9. The questions of safe following distance and safe lane width are at the heart of AHS design and application because they determine the practical capacity of a lane and of a right-of-way width. Following distance is determined by many factors. Under dry pavement conditions, two major factors are failures of the vehicle ahead and longitudinal transients during lane changes. Assumptions concerning what failures of the vehicle ahead will be imposed on AHS design, what braking system and communication time delays exist, and what collision policy will be followed determine what is judged sufficiently safe. The subject is treated extensively in Volume IV, Chapter 4. Chapter 2 of this volume recommends 10 mph as a criterion for maximum collision relative velocity. How this velocity is derived from crash data is important when comparing the criterion with others (see Volume IV). If the vehicle ahead has hit another vehicle, barrier or damaging obstacle in the fans and is decelerating at higher levels than are possible with braking, the vehicle behind will collide with it and, depending on gap length, multiple collisions can happen. This malfunction can be managed by choosing a suitable minimum gap policy.

10. Steering system failures at the rate of 130 FPMH for a single channel system would imply an average 2.1 million failure per year if the entire present day freeway VMT (.973. 10*12 vehicle-miles on interstates and principal arteries at 60 mph) were automated. If the system is dual and fail-operate, the rate for complete steering failure drops to 274!

4.0 CONCLUSIONS AND RECOMMENDATIONS

4 .1 CONCLUSIONS

1. Data and analysis show that AHS vehicle failure rates of 1100 to 1800 per million vehicle hours are feasible.

2. The full answer to the cost question, both acquisition and lifetime maintenance, must remain uncertain until specific designs are considered.

3. The key issues in the approach to the question of safety are the use of redundancy in vehicle equipment, and the use of a breakdown lane, entry/exit protocol, and handling communication failures. Our study suggests design approaches to deal with these issues.

4. Barriers in the I2 scenario would reduce the probability of vehicles and other objects from moving into the AHS lane from the manual lanes. The ability of an automated vehicle to cope with such objects is problematical, making consideration of barrier use part of this malfunction management.

5. Driver role in malfunction management remains a controversy. We examined two driver roles-one where the driver is continually alert to the vehicle's behavior and progress throughout the trip and one where the driver can turn attention to unrelated activities but can expeditiously tend to systems alerts and advisories. These two roles both find application depending on the proximity of manually-operated vehicles as dictated by RSC definition and whether manual driving in the AHS lane can be permitted during an emergency.

Issues and Risks are summarized in Table 1-9.

Table 1-9. Malfunction Management Issues and Risks

#	Issue Description	Comments	RSC Impact	Discussed
1	Is factor of two improvement projected for the basic vehicle reliability reasonable?	A basic vehicle locomotion MTBF target should be substantiated by vehicle manufacturers and standards groups.	All	3.4.1
2	Can a AHS vehicle com-ponent budget of 2000 MTBF for crftical failures be achieved?	Data and analysis presented in this chapter suggest that the 2000 MTBF is achievable.	All	3.4.2
3	Can AHS vehicle component cost for an overall 2000 MTBF critical failure rate be affordable?	Specific designs must be considered. Two important factors are redundancy used and driver role.	All	3.4.3
4	Would the public initially tolerate a less reliable vehicle if it were safe?	Refer to comparable systems for histories of growing pains.	All	3.5, Item 8

Table 1-9. - Malfunction Management issues and Risks (Cont.)

#	Issue Description	Comments	RSC Impact	Discussed
5	How do we keep objects out of an AHS lane that shares a roadbed with manual lanes?	In I2 we can consider a fence or barrier. In I1 Several measures ar possible but none fully satisfactory	I1, I1	3.2.2
6	In an emergency, can the driver be allowed to assume control and proceed manually with the appropriate headway?	If so, the number of vehicles to be cleared from the breakdown lane can be reduced.	I2, I3	3.4.3.1
7	Do we introduce a psychological problem in a machine operated in a manual niode as part of every normal trip with no means to select that niode in an emeroency?	It seems inadvisable not to provide some means of escaping computer control short of switching off the key (N there is one),	All	2.4, 3.4.3.2
8	Can we afford not to have a breakdown lane?	Data and analysis points to 18 expected lane-blocking incidents on a typical AHS 30-mile lane sector in a 12-hour period d there is no breakdown lane.	I2, I3	3.5, Item 1
9	Can manual interlopers be discouraged through legal penaftles?	There appears to be no practical way to physically prevent manual vehicles from entering the AHS lane.	I2	4.2, Item 7
10	Is the driverless vehicle a serious concept?	Must consider required infrastructure and a highly mature malfunction management	I3	3.1, 3.1.3, 3.2.2
11	What about vehicle occupant medical emergencies or a vehicle fine?	A breakdown lane seems necessary to cope with these malfunctions.	I2, I3	3.1
12	Will breakdown lane use increase over today's manual system?	Under conditions of no single-channel operations allowed and a passive driver role, the answer could be yes.	I2, I3	3.5, Items 2 and 8
13	What safety gap design conditions will the public tolerate?	Must we counter the typical perception that AHS close gaps are unsafe by publicizing our safety crfteria? Will the media assure that this happens anyhow?	All	3.5, Item 9

4.2 RECOMMENDATIONS

1. Preliminary subsystem design studies should be performed and integrated into an overall system design containing life cycle cost/reliability tradeoffs

2. Redundant subsystems should be considered to obtain reliability goalswith the following design questions addressed.

    a) Use of dissimilar technologies as part of the redundancy
    b) Failure detection availability
    c) Failure identification technique
    d) Transition without dynamic disturbance
    e) Common mode failures

3. The driver role in malfunction management should be studied in simulations and field tests.

4. A target basic vehicle locomotion MTBF should be established by standards organizations and vehicle manufacturers.

5. Further study is needed to resolve the issues of

    a) a continuous breakdown lane
    b) malfunctions during access and egress functions
    c) management of communication failures

6. Realistic affordable methods for managing the problem posed by an object in the lane must be developed. This study should consider the role of barriers in the AHS designs placing an automated lane contiguous to those used by manual traffic.

7. A related study should address the legal implications of enforcing traffic laws addressing obstruction of AHS traffic. Such violators should be easily detectable and therefore easy to fine or at least bring to trial. The delay caused in the AHS lane is, in worst case, equivalent to stopping three or more lanes of today's congested manual traffic. There appears to be no method short of a physical gate or severe legal consequence to prevent intended or negligent obstruction.

APPENDIX A: AHS COMPONENT AND SUBSYSTEM RELIABILITY DATA AND ANALYSIS

This appendix develops and documents reliability estimates for AHS roadway/vehicle systems.

1.0 COMPONENT DATA

Table A-1 is a list of failure rtes for components similar to AHS vehicle and roadway components. Data sources referenced include NPRD-91 (Nonelectronic Parts Reliability Data 1991 - Reliability Analysis Center), EERD-2 (Electronic Equipment Reliability Data-1986-Reliability Analysis Center), GIDEP (Government - Industry Data Exchange Program, an on-line database for failure rate data and engineering reports) and vendor data from Motorola on their trunk radio repeaters and computer boards.

Table A-1. Automation Component Failure Rates

Component	FPMH	MTBF	Source	Time Period
accelerometer	703.4Z9	1,422	GIDEP 156925	82
accelerometer	1631.684	613	GIDEP 156925	82
accelerometer	24.833	40,269	NPRD-91	
actuator	44.500	22,472	NPRD-91	
antenna	6.658	150,188	NPRD-91	
camera	503.000	1,988	NPRD-91	
camera,tv motion	135.000	7,407	NPRD-91	
compass-magnetic	834.498	1,198	GIDEP 156925	82
computer-diaftal	1668.768	599	GIDEP 156925	82
computer-dinital	1668.768	599	GIDEP 156925	82
computer-diaital	2309.468	433	GIDEP 157273	87-89
computer-display console	510.000	1,961	GIDEP 16626	90-91
computer-nionitor	292.158	3,423	GIDEP 157114	81-84
computer-processor	21.642	46,206	GIDEP 156816	78-80
computer -68040 brd	6.8256	146,507	Motorola MVMEI 67/DS	93
crt	4.412	226,649	NPRD-91	
display-heads up	3200.000	313	GIDEP 156921	78-80
electrical motor, DC	18.130	55,157	NPRD-91	
gyro	115.400	8,666	NPRD-91	
laser	49.350	20,263	NPRD-91	
motor DC fractional hp	18.13	55,157	NPRD-91	
optical encoder	20.000	50,000	NPRD-91	
PUMP	47.450	21,075	NPRD-91	
Radio repeater (trunk)	20.28	49,310	Motorola	94
radio-trans/rec	1785.714	560	GIDEP 156838	76-77
radio-transmitter	2008.032	498	GIDEP 156838	76-77
radio trans/rec #173	47.6	21,008	EERD-2	85
sensor	3.134	319,101	NPRD-91	
sensor, acceleration	174,190	5,741	NPRD-91	
sensor, angle of attack	50.000	20,000	NPRD-91	

Table A-1. Automation Component Failure Rates (Cont.)

Component	FPMH	MTBF	Source	Time Period
sensor, temperature	0.107	9,354,537	NPRD-91	
sensor, thermocouple	0.010	98,039,216	NPRD-91	
sensor, torque	79.998	12,500	NPRD 91	
transceiver	1245.600	803	NPRD-91	
transducer	52.940	18,889	NPRD-91	
valve	8.290	120,627	NPRD-91	
valve, check	0.372	2,68,285	NPRD-91	
valve, servo	113.960	71,633	NPRD-91	

2.0 SUBSYSTEM REPRESENTATIONS AND RELIABILITY ESTIMATES

2.1 Longitudinal Sensor Systems -- several options exist for longitudinal sensing as described in Task D summary analysis on lateral and longitudinal control. From the table below, we choose for general calculation, 21000 hours MTBF. The high failure rate for vision system reflects 805 technology for vision and should quickly come up to 21000 as this is an active area of development. The 14 FPMH for processors comes from the Motorola MVME167/D spec sheet for their 68040 based processor but has been derated by half to reflect software problems which are typically about half of all computer system failures.

Subsystem Type	Components	Component FPMH	Subsystem MTBF
GPS receiver	radio	48	21000
RADAR	trans/rcv processor	49 14	15886
Vision System	TV camera processor	135 14	6729
Radio	tmscvr	48	21000

2.2 Lateral Sensor Systems -- several options exist for lateral sensing as described in Task D summary analysis on lateral and longitudinal control. Summarized in the table below, a conservative estimate for general calculation is 21000 hours MTBF.

Table A-3. Lateral Sensor Systems

Subsystem Type	Components	Component FPMH	Subsystem MTBF
GPS	radio	48	21000
Vision	camera processor	135 14	6727
Magnetostatic/ Electrostatic	7p ickup coils(2)	6	161290

2.3 Vehicle processors -- As described above, the Motorola MVME167 number adjusted for software of 73000 hours MTBF will be used. This processor should have sufficient power to perform lateral and longitudinal processing and control except for RADAR and Vision systems which will most likely require separate processors to meet the computational needs.

2.4 Longitudinal control -- Subsystem is composed of a brake actuator (44.5 FPMH), a brake valve (13.9 FPMH) and an accelerator stepper motor (18.13 FPMH) yielding 13066 hours MTBF for the subsystem.

2.5 Lateral control -- This subsystem could be composed of a actuator (44.5 FPMH) and a valve (13.96 FPMH) yielding 17105 hours MTBF.

2.6 Vehicle/vehicle communication -- This is a radio transceiver that can deliver 21000 hours MTBF. Communication is an area where great progress has been made over the last decade in digital conversion and modulization of functions yielding great improvements in reliability and cost reduction. The reliability should be much better than this by deployment.

2.7 Vehicle/roadway communications -- The same reliability will be assumed hear as for item 2.6 although the technology might be quite different.

2.8 Status and Operations -- Composed of a computer display, a head-up display and appropriate input devices. A budget of 21,000 hours is established, although the data of Table A-1 would indicate the number was more like 210 in the early 19805.

2.9 Malfunction Monitoring -- Composed of various temperature, pressure, force and position sensors, signal taps and a computer with analog interface hardware. A budget of 7100 hours is chosen.

2.10 Roadway broadcast -- Implemented by radio transceiver as in 2.6 above.

2.11 RR communication -- This adds a repeater to pass messages between roadside communication and central control. Motorola supplied numbers for their Trunk Radio repeater of 49300 hours MTBF.

2.12 Roadway sensors -- These sensors detect roadway environmental conditions for temperature, humidity, etc. and can be used with within system redundancy to obtain very high reliability. For calculation purposes we have included three sensors at 3.1 FPMH each for a total of 9.3 FPMH (108,000 hours MTBF).

2.13 RV communication -- Typical radio transceiver at 21,000 hours MTBF.

2.14 Roadway computer -- This function is more complex than the vehicle control function and a factor of three has been assessed to account for the increased throughput and software yielding 24,000 hours MTBF.

2.15 Roadway signs -- These are variable message signs consisting of a display, driver circuit, power supply and communication function and should easily obtain figures of 20,000 hours MTBF and can be used in redundant configurations.

Table A-4 summarizes the failure rate data used in items 2.1 — 2.12.

Table A-4. Vehicle Subsystem Reliability

Subsystem #	Subsystem Name	MTSF (hours)
1	longitudinal sensor	21000
2	lateral sensor	21000
3	vehicle processor	73000
4	lonaftudinal control	13000
5	lateral corftrol	17000
6	vehicle communication	21000
7	status and operations	21000
8	maffunction nionftorina	7100
9	roadway broadcast	21000
10	RR comniunication	49300
11	roadw;ay sensors	108000
12	RV communication	21000
13	roadway computer	20000
14	roadway signs	20000

REFERENCES

BMW data documented in internal memoranda, January 1994.

Elias, J., et al, "Practicality of AHS; Volume II, Technical Design Considerations," FHWA-RD-79-40, November 1977.

MacCalden, M.S., Jr."A Traffic Management System for the San Francisco-Oakland Bay Bridge; Institute of Transportation Engineers Journal; May 1984.

New York State Police; telephone conversations documented in internal memoranda, January 1994.

Reiss, R.A., and Dunn, W.M., Jr., "Freeway Incident Management Handbook," FHWA-SA-91-056, July 1991.

U.S. Army Automotive Command, Sample Data Collection Program, Logistics Management Analysis; "Summary for the Commercial Utilities Cargo Vehicle; 5 Sept. 1989-31 July 1990 (Report TA-9009) and 1 August 1990-31 July 1992 (Report TAC-3201).

Zanoni, E. and Pavan, P.; "Improving the Reliability and Safety of Automotive _ _Electronics;" IEEE Micro; February 1993.

BIBLIOGRAPHY

Department of Defense Standard 2167A

Military Standard 8828

Military Standard 882C

Military Standard "Software Development and Documentation" (MIL-Std-SOD)

D. Bullock and C. Hendrickson "Development of Software Standards for Advanced Transportation Control Systems. Final Report. Volume 1. A Model for Roadway Traffic Control Software" California University, Irvine Institute of Transportation Studies Corporation.

P. Fancher, L. Kostyniuk, D. Massie, R. Ervin, and K. Gilbert "Potential Safety Applications of Advanced Technology" Michigan University, Ann Arbor Transportation Research Institute.

C.N. Georghiades, S. Patarasen, E. Soljanin, H. Jardak, and H.M. Wills "Communications In Intelligent Vehicle Highway Systems--Part I" Texas Transportation Institute, The Texas A&M University System College Station, Texas 77843.

C.N. Georghiades, E. Soljanin, K. Chang, R. Valid!, L.C. Matias"Commun,cations in Intelligent Vehicle Highway Systems--Part II" Texas Transportation Institute, The Texas A&M University System College Station, Texas

77843.

M.S. Jaffe, N.G. Leveson, M.P.E. Heimdahl, and B.E. Melhart "Software Requirements Analysis for Real-Time Process-Contra! Systems IEEE Trans. Software Eng., March 91, pp 241-258.

N.G. Leveson and P.R. Harvey, "Analyzing Software Safety," IEEE Trans. Software Eng., Sept 1983, pp 569-579.

N.G. Leveson, "Software Safety: What, Why, and How," ACM Comput. Surveys, Vol. 18, No. 2, pp. 125-l64,June 1986.