Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

AHS Safety Issues

U.S. Department of Transportation
Federal Highway Administration
Publication No. FHWA-RD-95-150
November 1994

PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS

Activity Area N

AHS Safety Issues

Results of Research

Conducted By

Delco Systems Operations

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

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof. This report does not constitute a standard, specification, or regulation.

The United States Government does not endorse products or manufacturers. Trade and manufacturers' names appear in this report only because they are considered essential to the object of the document.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS Activity Area N AHS Safety Issues		5. Report Date 6. Performing Organization Code
7. Author(s) A. Cochran*, F. Ryan**, S. Hayes, M. Halseth, B. Culver, D. Milner**		8. Performing Organization Report No.
9. Performing Organization Name and Address Delco Electronics Corporation Delco Systems Operations 6767 Hollister Avenue Goleta, CA 93117		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFH61-93-C-00194
12. Sponsoring Agency Name and Address IVHS Research Division Federal Highway Administration 6300 Georgetown Pike McLean, Virginia 22101-2296		13. Type of Report and Period Covered Final Report September 1993-November 1994 14. Sponsoring Agency Code

15. Supplementary Notes
Contracting Officer's Technical Representative (COTR) - J. Richard Bishop HSR 10
* Hughes Aircraft Company, San Diego, CA; ** Daniel, Mann, Johnson, and Mendenhall, Phoenix, AZ

16. Abstract

The issues of automated highway system safety are addressed from a system design standpoint. Four general areas of concern: failure prevention in the areas of vehicle subsystems, infrastructure instrumentation, and roadway mechanics; implementation of complex systems in terms of reliability and redundancy; structured methodologies for supporting systems assurance; and collision avoidance in the presence of external disruptions, are discussed. The trade offs involved in maintaining a certain level of safety using the most effective approach are addressed. The implications of system configuration in terms of headway maintenance policy and coordination units are presented. Examples are used to illustrate the relative vulnerability of each representative system deployment to a variety of hazards. Recommendations are made concerning specific systems configurations attributes which have significant impact on system safety requirements.

17. Key Words	18. Distribution Statement
Safety, reliability, maintainability, availability, systems assurance, headway maintenance, coordinated braking, collision avoidance, hazard analysis, external disruptions, malfunction prevention, redundancy, vehicle, instrumental content, roadway	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161

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

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

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

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This analysis — Activity Area N, AHS Safety Issues, addresses the issues of safety from a system design standpoint. The Automated Highway System (AHS) will be required to meet a certain standard of safety, regardless of the system configuration chosen.

The AHS Safety Issues analysis is organized into three general areas of study. The issues and risks involved in implementing AHS in terms of vehicle instrumentation, roadway deployment, and vehicle control and communications dynamics are discussed first. The engineering practices used to ensure safety and reliability as they relate to the introduction of increasing levels of automation are addressed next; system safety assurance is presented as a methodology which may be followed to ensure that appropriate steps are taken to maintain safety at each phase of AHS design, development, deployment, and operation. The final area of analysis encompasses the issues involved with preventing collisions in the presence of sub-optimal operating parameters. This topic discusses the safety of travel on automated highways compared to conventional highways under various adverse conditions.

A primary goal of AHS is increasing the safety of the nation's highways. A general assumption is that by eliminating human error as an element in a large percentage of traffic accidents, the overall safety of vehicle travel will be significantly improved. This assumption may be valid if the AHS operates in isolation, neglecting the effects of all external factors, and if the number of failures due to AHS-specific equipment does not exceed the number due to human error. A first area of study presents an array of factors that can affect the design and development of an AHS which meets the goal of collision-free operation in the absence of malfunctions.

One facet of system configuration addresses the vehicle control implementation and the primary safety issues involved in selection of the system operating mode. Of central concern are the dynamics of platoons as they pertain to safe maintenance of intra-platoon vehicle headways. There are many scenarios in which collisions within a platoon may occur. A control system that can limit the difference in vehicle velocities during collisions to acceptable levels while maximizing traffic throughput will enable platoons that experience low delta velocity collisions to resume operation and drive to the nearest exit after the collision. This approach will prevent the original failure from affecting other AHS platoons. The alternative to forming platoons is to establish conservative vehicle spacings such that either no collisions occur or collisions are limited to single vehicles. This approach is

advantageous in terms of control complexity when compared to the platoon

concept, but the decreased overall throughput may detract from the benefits.

A coordinated braking concept is presented which discusses the longitudinal control parameters that are necessary to provide close vehicle following in conjunction with minimizing intra-platoon collisions in emergency braking modes. A common concept regarding platoons is that rapid deceleration of the lead vehicle will cause collisions in following vehicles due to the delay in brake actuation along the length of the platoon and differences in vehicle deceleration rates. Appropriate communications to the platoon control loop can provide timely control information updates within the platoon and eliminate delays associated with daisy-chained brake actuation. Feedback algorithms in the control loop can also be used to optimize the deceleration rate of the platoon while maintaining constant headways between vehicles within the platoon.

The potential for coordinated braking to eliminate intra-platoon collisions has not been fully explored. Additional quantitative analysis must be performed to identify the ideal platoon size, control loop update rates, and maximum communication delays that will optimize the available throughput of automated lanes while minimizing the risk of collisions during emergency maneuvers. The preliminary findings indicate that separating passenger vehicles and commercial or transit vehicles in platoon configurations will minimize design complexity in terms of ensuring system safety. In addition, it is recommended that some form of communications be used to eliminate braking delays in platoon configurations in order to prevent low differential velocity collisions in close-vehicle-following deceleration maneuvers.

Another aspect of system configuration is the specific roadway implementation. Several options for deployment of automated lanes exist, including conversion of conventional highway right-of-way to AHS use. Some of the safety issues involved with instrumentation of existing roadways include the compatibility of the road surface with high-speed platoon travel, the availability of adequate shoulders, and the need for barriers to prevent collisions with non-AHS vehicles. Deployment of AHS on new alignment may present fewer safety hazards if the facility is dedicated to AHS vehicles. Another safety consideration is the potential hazards introduced by operating passenger cars and commercial and transit vehicles in common automated lanes. The early analysis of infractructure issues concludes that roadway surface friction and its effect on safe travel speeds in high density configurations is a primary consideration in selection of AHS operating modes. The use of barriers is another important factor in the degree of potential safety risks in automated travel.

The ideal AHS scenario will provide collision-free driving under normal operating conditions. Normal conditions are defined for the purposes of this discussion to consist of the absence of equipment failures. A primary focus of this analysis is the interrelationship between system safety and reliability. System reliability is a necessary system requirement that encompasses the consideration of fail-safe design features as well as system cost and maintainability concerns throughout the project's life cycle. The issues concerning reliability of AHS equipment are discussed in terms of vehicle-specific components, infrastructure electronics and communications, and roadway-specific concerns.

Vehicle safety on an automated highway is based on the system implementation and on the design and reliability of the vehicle equipment. The reliability and fault tolerance of the design are dependent on a variety of factors, representing a tradeoff between the equipment cost and the upper bound of technology set by the current state of the art. The issue of equipment cost can be viewed from two angles. The reliability of very inexpensive equipment may be improved econ-omically by increasing redundancy, while the reliability of relatively expensive equipment may be enhanced through improved manufacturing and testing, adding to the overall component cost but providing better reliability gains on a cost/benefit basis.

The relationship between overall system safety and reliability of the vehicle-specific components is a key issue in the division of responsibility for automatic control between the vehicle and the infrastructure.

Detailed statistics are needed that link specific malfunctions with related incidents and demonstrate the principal issues associated with vehicle safety to conclusively identify high-risk failure modes for further analysis. The discussion presented in the detailed analysis presents a set of potential risks and provides a preliminary assessment of the relative importance of each failure mode in terms of hazard reduction and failure prevention. The precursor analysis of vehicle failure modes indicates that the two most critical areas are steering and braking. These functions are integral to the automated control function. Degraded operation of functions such as acceleration or engine timing can be more readily compensated for using redundant functionality. Steering has been determined to be the most difficult function to provide back up, increasing the safety-critical nature of single-point failures.

Safety has been established as one of the primary influencing factors on the success of AHS. Concern for safety permeates every level of the system design, and must be addressed at each stage of study, development, and deployment. The second section of the Safety Analysis

discusses the importance of developing a system safety program that consists of safety-related activities in the planning, design, construction, deployment, and operations phases of AHS projects. The topic includes an overview of hazard analysis methodologies and the stages in the program life where each analysis method is applicable. System safety emphasizes the verification and demonstration of the overall safety of the system as implemented for subsequent long-term operation. Identification of safety as a system-level issue and establishing design practices and standards at the outset of the development phase are important steps toward creating a system that will meet the safety design goals.

Safety is an important concern at the subsystem design level. Safety can be improved by introducing higher levels of subsystem redundancy, but this tends to increase system cost out of proportion to the benefit. Improving component reliability and providing cross-functionality among subsystems may yield higher safety benefits at lower overall cost. AHS can use existing vehicle subsystems such as engine controllers or ABS as models for reliable, cost effective, safe implementation. The effect of the system architecture on the cost of safe system design will be a primary consideration in the flowdown of subsystem functionality.

A related area of study is identifying specific hazards or failure modes that are generic to the system architecture, and consequently apply uniformly to each of the representative system configurations used in this analysis. Categories are assigned to individual hazards in terms of their relative severity. An approach to risk assessment is presented that applies to systems throughout the design life cycle to evaluate a specific system configuration and identify safety-critical areas. Standard system safety program analyses apply to all facets of deployment, including test, maintenance, and support. Each activity of the system development, such as design, production, and operation, should be included in the system assurance plan.

The objective of system safety is eliminating hazards by design. This objective may be achieved by characterizing hazards by severity and probability. A risk assessment procedure that considers primarily hazard severity will generally be sufficient during the early phases of design to minimize risk. Hazards that are not eliminated by design must be analyzed by a risk assessment procedure based on each hazard’s probability and severity category to establish priorities for resolution. The mitigation approach can include acceptance of the risk for non-safety-critical failures with low probabilities of occurrence, while corrective action may be required in safety-critical cases with higher occurrence rates.

The risk assessment methodology is illustrated using typical failure modes in various categories. The preliminary hazard analysis looks at infrastructure risks associated with roadway deployment, the check-in/check-out process, and entry/exit facilities. Another category focuses on vehicle hazard severities in the areas of physical instrumentation and control dynamics. Other areas of analysis present failure modes in communications and operations control at the system level. The preliminary hazard analysis uses a small subset of the potential failure modes to illustrate the first phase of the system risk assessment process. The failure modes which receive the highest degree of severity ranking in this stage of analysis are candidates for more detailed analyses. Failure mode effects and fault tree analyses are next order risk assessment tools that become applicable to these identified risk areas.

Several safety-critical areas are indicated in the preliminary hazard analysis. One of the infrastructure failure modes with high potential for catastrophic consequences is the failure of the barrier method to prevent intrusion of uncontrolled vehicles. Several barrier methods are discussed, including physical barriers, electronic barriers, and enforcement similar to deterrents used in high-occupancy-vehicle facilities. Vehicle mechanical and control breakdowns including tire failure, brake failure, and lateral or longitudinal control failure are identified at the highest level of safety criticality. Each of these failure modes is a candidate for detailed fault tree analysis in the specific system configuration selected for implementation.

A third area of study focuses on identifying disruptions to the AHS by external disruptions — snow or fog, natural disasters such as earthquakes, terrorism or vandalism, operator error, and non-standard roadway conditions due to construction or maintenance. Each event is evaluated in terms of severity of risk. Each disruption is categorized according to the relative severity of a typical occurrence. An occurrence that is considered less severe may cause reduced throughput, for example, without risk of injury or damage. More severe occurrences may require closure of automated lanes. Risk assessment criteria will be applied based on the hazard severity and probability of occurrence to determine the appropriate mitigation strategy.

There is a certain level of risk in traveling on conventional highways associated with such events as floods, earthquakes, and other occurrences. The susceptibility of AHS configuration to risk must be considered to prevent creation of a greater safety risk than that which would be encountered on conventional highways. The design of the AHS must also avoid increasing the cost associated with prevention of environmental effects out of proportion to the benefit attained. Safety can be maintained economically through a range of approaches, including

such measures as rerouting traffic in adverse weather conditions or eliminating certain sites from consideration for AHS deployment.

The study of potential disruptions to AHS operation concludes that automated lanes are typically no more vulnerable to environmental effects than conventional lanes. In certain low visibility or low traction conditions, the AHS can improve performance through appropriate design of operating modes. The primary area in which AHS may be at risk to external forces will be its vulnerability to vandalism and intentional or accidental misuse. The cost and complexity of the AHS can increase dramatically in an effort to prevent catastrophic occurrences caused by entry of uncontrolled vehicles. This is one the key safety considerations which has surfaced repeatedly in the safety analysis of roadway implementation and infractructure electronics.

INTRODUCTION

The degree of mobility exhibited by AHS must be in balance with other values related to social, economic, and environmental issues. The following points must be considered in the design of this highway system:

- Safe and efficient transportation.
- Attainment of community goals and objectives.
- Needs of low mobility and low income groups.
- Overall effects on natural resources, environmental values, public service, aesthetics, and community integrity.
- Deployment based on realistic financial estimates.
- Consideration of impact to maintenance and operation.

The AHS Safety Issues analysis evaluates the aspects of these design considerations as they pertain to safety. The organization of the analysis is presented in the following paragraphs.

The topic of safety encompasses all aspects of system reliability and failure mode effects, as well as hazard detection and mitigation. The present analysis will address issues regarding the prevention of AHS malfunctions and will discuss the impact of reliability, fault tolerance, and redundancy on system safety and design. This effort will discuss the subject of system safety as it is influenced by the AHS operating environment, taking into account a variety of risks associated with external factors. The issues concerning the appropriate actions to take in the event of failures are addressed in Activity E — Malfunction Management and Analysis.

This activity is divided into several topics of discussion. The effort is based on an extensive literature search performed in task 1, encompassing the resources of the contract team. Relevant safety issues gathered from team discussions and experience as well as those raised in the literature are summarized and discussed in task 2. The representative system configurations (RSC's), defined in the Contract Overview report, are used to highlight some of the advantages and disadvantages from a safety standpoint of certain features of the three RSC's. The RSC's are discussed in terms of their unique safety aspects when there is a significant disparity between the RSC's. Where no major differences exist in safety issues among the RSCs, individual configurations are not specifically mentioned in the discussions of risks. The design considerations which result from the analyses of reliability and safety

issues are included in this discussion. The impact to various aspects of design are presented in categories covering vehicle subsystems, roadway implementation, and communications and infrastructure electronics.

A major emphasis of the safety analyses is the identification and evaluation of critical failure modes and hazards. It is important to provide a uniform interpretation of the criticality of failure modes and the severity and probability of hazards. Task 3 will provide an analysis of the expected frequency of occurrence and relative severity of the failures discussed in task 2. Risk assessment criteria will be applied to the identified failures based on their severity rating and probability of occurrence to determine the proper mitigation approach. Acceptance of the risk may be the recommended action for non-safety critical failures with low probabilities of occurrence, while corrective action may be required in safety-critical cases with higher occurrence rates. A detailed discussion of the methodology is included in task 3.

Task 4 provides an overview of hazards identified as potential threats to the safety of AHS. Each hazard is categorized in terms of the degree of impact to normal AHS operation, and methods for mitigating risks associated with the hazards are discussed. The potential for continued safe operation of the AHS is estimated and actions which may be taken to operate safely in adverse conditions are suggested. This task focuses on the aspects of each hazard which are unique to the AHS, providing identification of areas where the AHS may be more or less vulnerable than conventional highways to specific hazards. The categories describing severity and probability of failures in task 3 are used to evaluate hazards in a similar manner. The severity category and probability ranking can be combined to establish an initial risk index, providing a quantitative tool for evaluating risks.

REPRESENTATIVE SYSTEM CONFIGURATIONS

The representative system configurations (RSC's) were generated very early in this Precursor Systems Analyses of AHS program. These RSC's are used throughout the various areas of analysis whenever a diversity of system attributes is required by the analysis at hand. The RSC's identify specific alternatives for twenty AHS attributes within the context of three general RSC groups.

Since the RSC's have such general applicability to these precursor systems analyses, they are documented in the Contract Overview Report.

TECHNICAL DISCUSSION

Task 1. Literature Search

Articles related to AHS safety have been researched in various trade journals and the broad literature search performed for the entire program was also used as a source of material for this analysis. A literature search of the Institute of Traffic Engineers (ITE) bulletin board service for documents related to AHS issues was performed. The resources of DMJM have been utilized in the area of highway design and transit safety, in the form of literature from industry journals and expert input. The PATH database was another source of information regarding recent developments in the area of safety considerations in automated vehicle control. The specific references used to develop the discussions presented here are listed at the end of the document.

Task 2. Identify Safety Issues and Risks

Introduction

One of the primary goals of AHS is increasing the safety of the nation's highways. A general assumption is that by eliminating human error as an element in a large percentage of traffic accidents, the overall safety of vehicle travel will be significantly improved. This assumption may be valid if the AHS operates in isolation, neglecting the effects of all external factors, and if the number of failures due to AHS-specific equipment do not exceed those due to human error. This task will focus on the safety risks of AHS based on the RSC's. The risks will be weighed in terms of the impact of the physical environment and emergency conditions on vehicle and roadway design in each of the RSC's.

A list of topics which impact the development of AHS has been compiled which considers a variety of influences on safe system design. Each of the major subjects is expanded and the implications with respect to the RSC's are discussed in the succeeding paragraphs. The following table provides a preview of the areas of discussion and includes a cursory list of pertinent issues in each category. The primary topics of system configuration and system reliability address the need to integrate safety assurance into the design process at the system level. The secondary subjects address issues and risks which are raised when the liability for malfunctions is placed with the system, and summarize the safety design considerations which affect risk management, feasibility, and user acceptance.

Table 1. Safety Issues and Risks

Primary Topics	Secondary Topics
System Configuration • Vehicle Control • Roadway Implementation System Reliability • Vehicle performance • Failure modes • Communications backbone • Effects of environment on infrastructure electronics	Catastrophic Failure • Injury risk • Multi-vehicle involvement • Public perception Failure Recovery • Reliability assurance • User satisfaction • Coordination of control of vehicles Collision Free Environment • Aspects of natural hazards unique to AHS • Effect of operational hazards unique to AHS Automatic/Manual Interface • Transitions between automatic and manual control • Eliminating risk of collisions preventable by human interaction Comparison With Conventional Highway • Feasibility of implementation • Role of driver and benefits of automation

System Configuration

Two aspects of highway implementation specific to AHS issues will be discussed in this analysis. The first area concerns the impact of the vehicle control solution selected for the AHS. The impact of vehicle spacing, maneuvers, and the level of control and where the vehicle control loop is closed will be discussed in terms of safe system operation. The second area considers physical highway sections which might be appropriate to AHS implementation.

The discussion includes how highway safety is determined, and the facets of highway design which can enhance automated vehicle travel.

Vehicle Control

One of the most important functional parameters of the AHS will be the approach to optimizing traffic density. Several approaches have been evaluated, including platoons of varying sizes, point-following, and coordinated flow management. The key to ensuring the safety of the AHS in any system configuration will be headway maintenance and maneuver management. The lateral/longitudinal control loop, the communications technology, and vehicle actuation devices will all derive their performance specifications from the requirements for the level of service stated in the Operations and Maintenance plan, safe headway maintenance, and vehicle maneuverability.

Studies have determined that differing deceleration rates are a major factor in the relative velocities of vehicles in a collision. Minimizing differences in relative velocities during emergency braking will provide a step toward improving safety over existing highways. One of the most attractive features of the AHS in terms of safety is the benefits of automatic longitudinal and lateral control of vehicle position, and the capability of stabilizing the spacing and relative velocity of vehicles under steady state operation. The maintenance of vehicle headways becomes a safety issue under conditions requiring emergency maneuvers. Some of the design parameters concerned with safe position control are outlined in the following paragraphs.

Vehicle braking ability is a critical safety consideration. Modern vehicles can decelerate in the range of 0.7 to 0.9 g's on dry, high quality pavement. The performance factors degrade as the pavement composition deteriorates, the surface becomes slippery and the vehicle's tires wear down. To address this issue, each roadside management system may be designed to control the desired speed of AHS vehicles. Speed zones can be defined based on type of pavement used. Different pavement compositions produce different coefficients of friction. Maintenance work resulting in an isolated section with a lower coefficient of friction than the rest of the zone may require a reduction in the zone's maximum speed. Under conditions of rain, snow, ice, oil, etc., the zone's maximum speed may also be reduced.

Safe Headway Maintenance

The difference in velocity between two vehicles during a collision plays a key role in determining the severity of the collision. Figures 1 through 4 display the relationships between various operating parameters and collision speed. The figures show worst case braking scenarios in which the vehicles within the platoon brake independently, without coordination. Further discussions will present a framework for coordinated platoon braking with the potential to alleviate intra-platoon collision issues. Failure decelerations and braking performances were chosen to bound current realistic vehicle stopping capabilities. The response times were chosen to bound expected communication and actuator delay times. The initial velocity is the highest operating speed considered in this study.

Figure 1 shows the relationship between collision velocity and vehicle spacing for equal values of lead vehicle deceleration and following vehicle braking with a given response time and initial velocity. Under this scenario, the control system commands each vehicle in a platoon to brake at the same effective rate. For any vehicle spacing, collision speeds of 18 km/h or less can be expected. When all vehicles brake at the same rate, collision velocity is affected by only response time. At an intra-platoon spacing of 1 m, the collision speed is about 16 km/h.

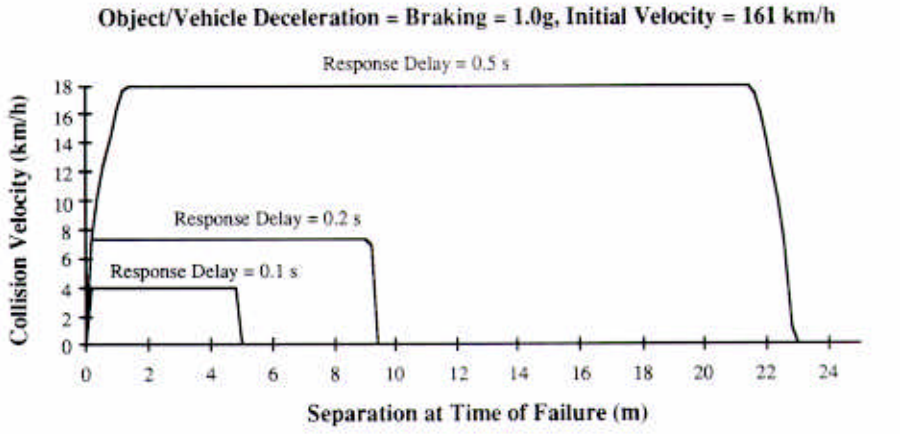

Figure 1. Collision Speed Versus Separation at Time of Failure
Failure Deceleration = 1.0g, Braking = 1.0g

Note that vehicle manufacturers generally require airbags to deploy for frontal impacts beginning at 25 km/h and for frontal angle (30 degree) impacts beginning at 30 km/h. Impacts occurring at less than 18 km/h must rely on the seat belt restraint to prevent injury, since the airbag system is designed so that frontal impacts at these speeds will not deploy the airbag. These figures are based on a collision with a stationary object, which implies that the velocity of the moving vehicle changes to zero instantaneously. Collisions between two vehicles moving in the same direction undergo different dynamics due to the elasticity involved in the transfer of momentum. A collision in which a following vehicle traveling 10 km/h faster rear ends the lead vehicle is not expected to be as severe as a vehicle traveling 10 km/h hitting a brick wall and stopping instantly.

Figure 2 shows the relationship between collision velocity and vehicle spacing for equal values of lead vehicle deceleration and following vehicle braking with varying response delays. The figure indicates the collision speed relative to the vehicle spacing at braking rates which are half those used in figure 1.

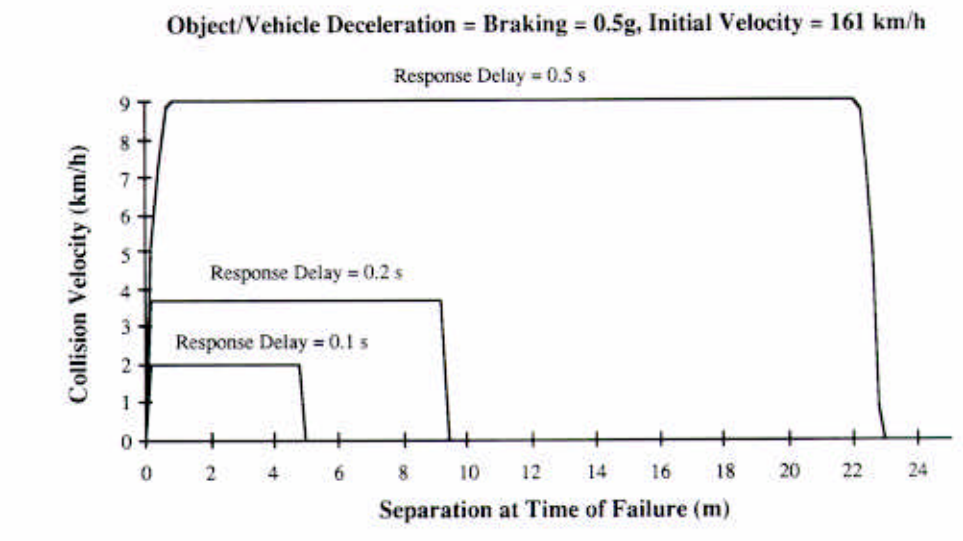

Figure 2. Collision Speed Versus Separation at Time of Failure
Failure Deceleration = 0.5g, Braking = 0.5g

The difference in mass between two colliding objects is also a measure of collision severity. By evaluating the difference in kinetic energy the relative differences in both mass and velocity can be considered. Although the direct effect of kinetic energy on occupant safety is difficult to determine, larger values are clearly undesirable.

It is unreasonable from a safety standpoint to assume that trucks and subcompact cars will be included in the same platoon. Even though control systems can be designed and implemented to ensure complete safety under nominal conditions, failures can occur with the potential to cause intra-platoon collisions. Therefore, designers must specify a maximum allowable mass difference between vehicles in the same platoon.

As an example, a subcompact car such as the Daihatsu Cuore CS has a gross vehicle weight including the driver of 650 kg. The Ford Lincoln Town Car has a gross vehicle weight of 2,430 kg, including passengers and luggage. Table 2 shows the absolute values of the differences in kinetic energy when the Ford (vehicle 1) is the leading vehicle and the Daihatsu (vehicle 2) is the trailing vehicle. Table 3 shows the absolute values of the differences in kinetic energy when the Ford trails the Daihatsu. For all cases, the difference in velocity is held constant at 4 m/s.

Table 2. Kinetic Energy Differences for Daihatsu Following Ford

	mass $_1$ = 2,430 kg mass $_2$ = 650 kg velocity $_1$ = 0 m/s velocity $_2$ = 4 m/s	mass $_1$ = 2,430 kg mass $_2$ = 650 kg velocity $_1$ = 1 m/s velocity $_2$ = 5 m/s	mass $_1$ = 2,430 kg mass $_2$ = 650 kg velocity $_1$ = 3 m/s velocity $_2$ = 7 m/s
|Kinetic Energy $_1$ – Kinetic Energy $_2$| Note: 1 N-m = 1 kg – m^2/s^2	5,200 N-m	6,910 N-m	4,990 N-m

Table 3. Kinetic Energy Differences for Ford Following Daihatsu

	mass $_1$ = 650 kg mass $_2$ = 2,430 kg velocity $_1$ = 0 m/s velocity $_2$ = 4 m/s	mass $_1$ = 650 kg mass $_2$ = 2,430 kg velocity $_1$ = 1 m/s velocity $_2$ = 5 m/s	mass $_1$ = 650 kg mass $_2$ = 2,430 kg velocity $_1$ = 3 m/s velocity $_2$ = 7 m/s
|Kinetic Energy $_1$ – Kinetic Energy $_2$| Note: 1 N-m = 1 kg – m^2/s^2	19,440 N-m	30,050 N-m	56,610 N-m

It is clearly undesirable to allow the Ford to follow the Daihatsu in a platoon as the resulting kinetic energy from a collision can be quite high. Thus, vehicle mass should be included in the list of operating parameters used by the Traffic Operations Center (TOC) to determine platoon members. Based on table 2, it seems reasonable to allow larger vehicles to be placed in the front of a platoon, as collisions from the rear by vehicles the same size or smaller will produce only moderate levels of kinetic energy differences.

Intra-platoon collisions may be avoided by employing coordinated braking. Figure 3 illustrates the dynamics within the platoon when the lead and following vehicle are decelerating at the same rate. The time to collision is relatively long when deceleration and braking rates are equivalent, even at close vehicle spacings. For example, at 1 m spacings, for vehicles decelerating at 1.0 g, and an initial conservative response delay of 100 ms, roughly 1 second will pass before the vehicles impact. Intelligent control algorithms can adjust vehicle braking and possibly acceleration values during this time to maintain adequate headways. Subsequent sections discuss this concept further. When all vehicles brake at the same rate, collision velocity is affected only by response time. To illustrate the safety concept as a function of collision velocity, vehicle manufacturers generally require airbags to deploy for

frontal impacts beginning at 24 km/h and for frontal angle (30 degree) impacts beginning at 35 km/h. Frontal impacts at 14.5 km/h should not deploy the airbag.

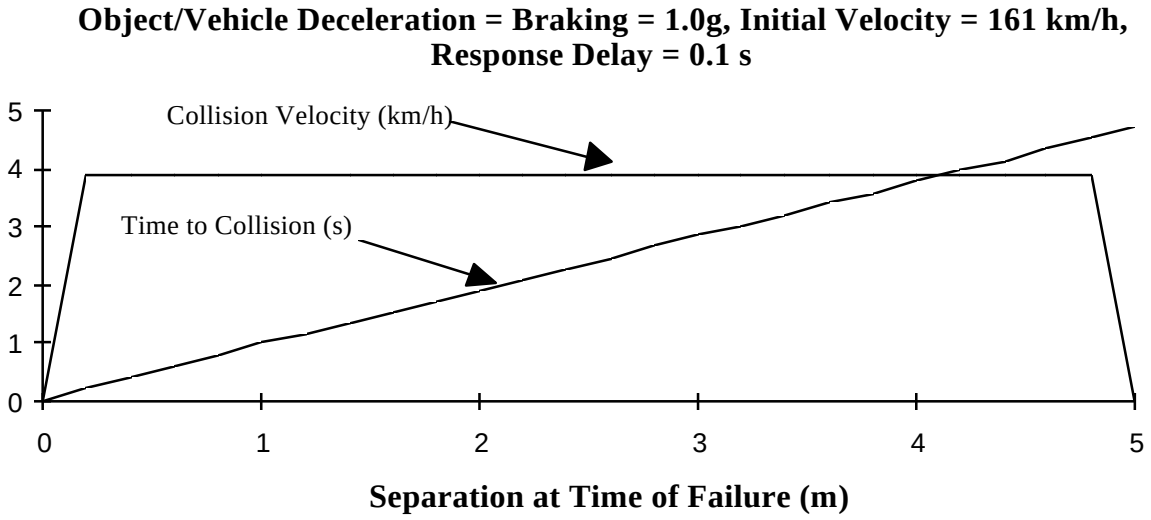

Figure 3. Collision Speed Versus Separation At Time Of Failure
Failure Deceleration = 1.0g, Braking = 1.0g

Intra-platoon collisions may occur in the event of a vehicle or system malfunction; therefore, platoon “buckling” must be considered. Not all vehicle front and rear ends align with each other, and since failure conditions are largely unpredictable and potentially uncontrollable, collisions may result in significant angular differences between vehicle headings. A pitching moment also results during vehicle braking. The vehicle will pitch forward with a greater pitch angle as the braking force and the deceleration of the vehicle increases. This forward pitch will misalign a vehicle’s front bumper with the rear bumper of the preceding vehicle. Collision performance requirements may result in the need for front-rear compatibility within platoons.

The case of a platoon encountering an emergency braking condition on a curve is another example of the potential alignment problem. Furthermore, nonhomogeneous traction (e.g., scattered wet or icy spots) will complicate this issue by creating significantly different operating conditions between vehicles. Control systems can be designed to compensate for unforeseen forces acting on the vehicle; however, intra-platoon collision forces may be strong enough to render the lateral control system ineffective. The point at which the potential exists for vehicles to cross lanes and collide with other vehicles or roadway barriers occurs when the control system cannot keep vehicles in their lanes in an acceptable orientation and at a

controlled speed. This scenario is very detrimental to system safety and must be avoided through detailed specification of headway control algorithms.

Safety issues must be considered from the viewpoint of each vehicle in a platoon. Consider the case of a 20-vehicle platoon, where maximum lead vehicle braking will not stop the platoon from impacting an object with relatively large mass on the roadway. The lead vehicle will suffer a frontal collision with a much greater force than that created if it was acting independently, due to the mass of the 19 trailing vehicles. The last vehicle in the platoon will receive the least amount of damage. This analysis considers the worst case, since some or all of the vehicles in a platoon could change lanes to either avoid a collision or reduce the severity of an unavoidable collision.

Longitudinal control stability is more critical for relatively long platoons. It may be desirable to allow platoon lengths of 15 or 20 to increase traffic throughput. Longitudinal control algorithms are designed to maintain the desired intra-platoon spacing. Errors in spacing must be prevented from propagating down the platoon, which if not addressed could cause the last vehicle to continuously make significant headway corrections. This phenomenon is referred to as the “slinky” effect. Instabilities could lead to intra-platoon collisions, especially between the last few vehicles in a platoon unless averted through effective control algorithm design. Stability must be considered in view of all system nonlinearities which have a potential effect on the control system.

Velocity and acceleration information from the preceding vehicle and the lead vehicle, as well as range and range rate data concerning the preceding vehicle, are integral components of the longitudinal control effort for a given vehicle in a platoon formation. The accuracy of the control algorithm can be improved by incorporating range, range rate and acceleration information from the following vehicle. This constitutes a distributed control system, where a disturbance may affect the entire platoon as opposed to only a few vehicles. This type of control has been shown to decrease the magnitude of peak headway corrections, as well as accelerations among vehicles in steady state operation. Distributed control also has the potential to decrease the risk of intra-platoon collisions, as all vehicles will be actively involved in collision avoidance. The primary consideration in this approach is the effect on platoon stability of single vehicle control failures. Distributed control systems are often less vulnerable to single point failures. Further analysis is required to determine whether this premise holds true in terms of platoon dynamics.

Coordinated Braking

Various problems can occur in an AHS requiring vehicles to perform emergency braking. This discussion concerns two significant safety issues involving platoons. The first is a case where the lead vehicle in a platoon either senses an upcoming hazard requiring braking (all RSC's), or is commanded to brake by the infrastructure (RSC 1) or another platoon (RSC 2). The second case is defined by a vehicle malfunction or other event within a platoon requiring certain vehicles to perform emergency braking. Each of these scenarios has the potential of serious damage to vehicles and injury to their occupants if adequate platoon command and control is not maintained. The first safety concern is used as a framework to introduce a coordinated platoon braking approach. A potential solution to the second issue will draw upon concepts from the coordinated system.

Relatively large response delays and the disparity between deceleration rates can be prevented in the system control design for AHS. Initial brake commands may be issued based on the braking capabilities of the vehicles in the platoon. Differences in deceleration rates between vehicles could be minimized by controlling vehicle brake and throttle systems. Figure 4 depicts a representative control system to accomplish the task of decelerating a platoon while avoiding intraplatoon collisions. This system is applicable to any RSC, as it is independent of locations for measurement and control systems. The critical design parameters involved in a coordinated braking approach are discussed in the following paragraphs.

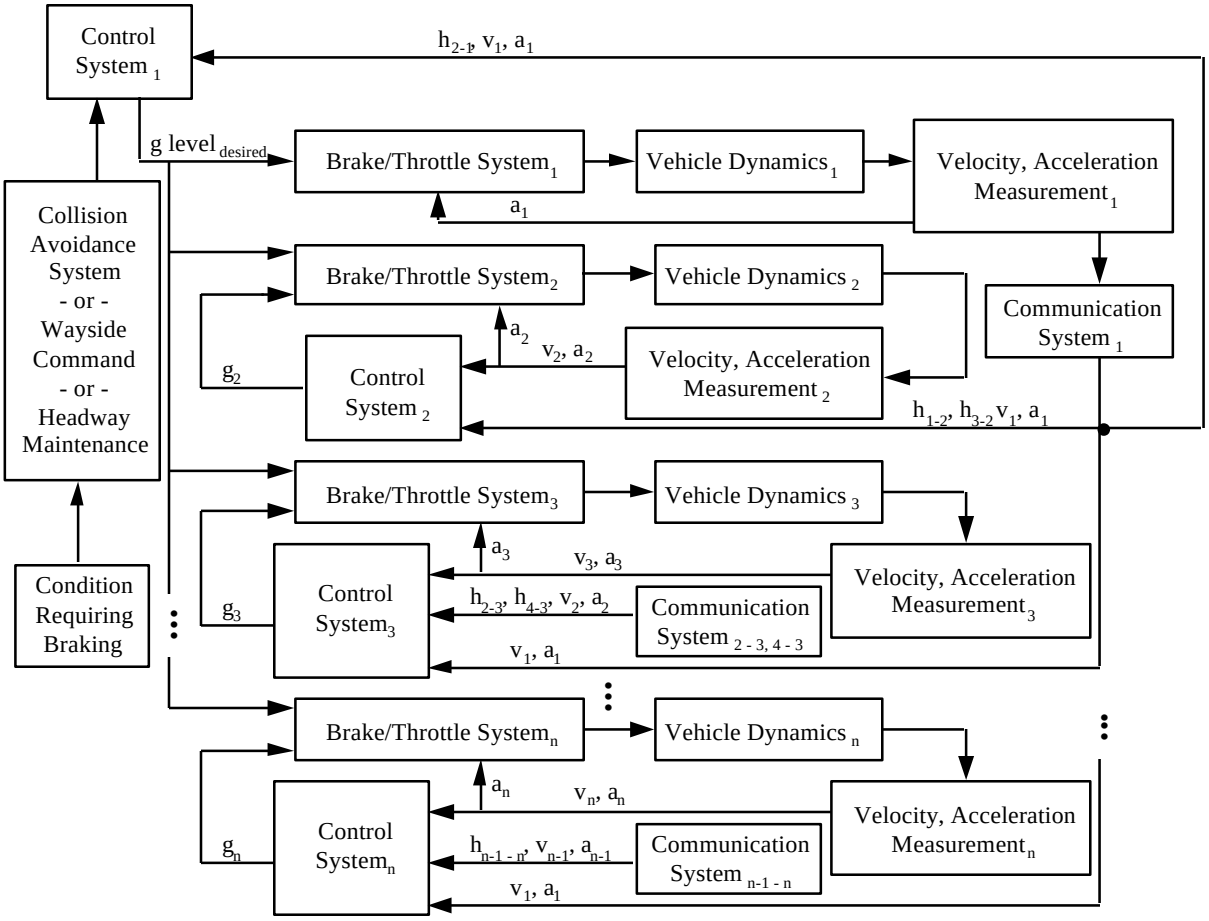

Figure 4. Representative Platoon Braking Control System

In this figure, the platoon consists of (n) vehicles. The lead vehicle initially transmits braking commands in the form of desired deceleration (g) levels to all following vehicles for the purposes of avoiding such obstacles as a foreign object on the road, another AHS vehicle, or a platoon. The following (n–1) vehicles then brake simultaneously. Coordinated braking can be achieved by requiring the lead vehicle to broadcast braking signals to all following vehicles. A more detailed discussion of the approach to communicating the braking commands to the vehicles within the platoon is covered in task 3 of Activity D — Lateral and Longitudinal Control Analysis. Each vehicle tries to attain the desired g level using an internal braking feedback control system which is designed to drive the error between the desired g level and the measured deceleration to zero. Each vehicle must convert the desired g level into a brake signal based on vehicle characteristics, such as weight, tire conditions, brake system, and engine inertia. Compensation for differences in vehicles deceleration rates can be achieved through control algorithms in each vehicle which adjust that vehicle's braking rate. The vehicle control algorithms utilize velocity and acceleration signals from the lead vehicle,

preceding vehicle, on-board measurement systems, and headway information from surrounding vehicles in the platoon as inputs to the feedback system.

This control scheme is designed to decelerate a platoon without causing intra-platoon collisions, and presents a tradeoff. A platoon which encounters an object on the roadway that cannot be avoided via a lane change may be required to revert to emergency control systems. Emergency braking may be employed to command braking actions if the platoon will not be able to safely avoid the object at the time of detection using coordinated braking. The platoon will stop in a shorter distance if all vehicles brake according to their maximum capabilities in an emergency than if it used the coordinated control scheme. This method has the potential to cause intra-platoon collisions, but would minimize the collision velocity between the platoon and the object. The following vehicles in a closely spaced platoon are likely to collide with the lead vehicle in cases where an obstacle is not avoidable in the coordinated braking scheme as well.

A possible solution to this problem is to allow intraplatoon headways to decrease as a function of velocity, to the point where all vehicles are very close together once the platoon has come to a complete stop, which presents a very difficult control problem. Simulations which compare the relative velocities of each vehicle in the platoon upon impact using both braking schemes must be analyzed to determine the safest approach.

Figure 5 depicts this concept by relating collision velocity and vehicle spacing for lead vehicle deceleration of 1.0g, following vehicle braking of 0.5g, varying response times and initial velocity of 161 km/h. Controllers issue braking commands such that the lead vehicle (and thus the platoon) comes to rest in the shortest amount of space for this uncoordinated braking scenario. The assumption is made that the lead vehicle is capable of higher brake performance than the following vehicle to illustrate the worst case. The lower braking value can be considered a minimum allowable to enter the AHS. The larger value is effectively the maximum attainable by any passenger vehicle on an ideal road surface. Relatively high collision velocities exist for practical vehicle spacings when the controller sacrifices intra-platoon collisions for an overall minimum platoon stopping distance.

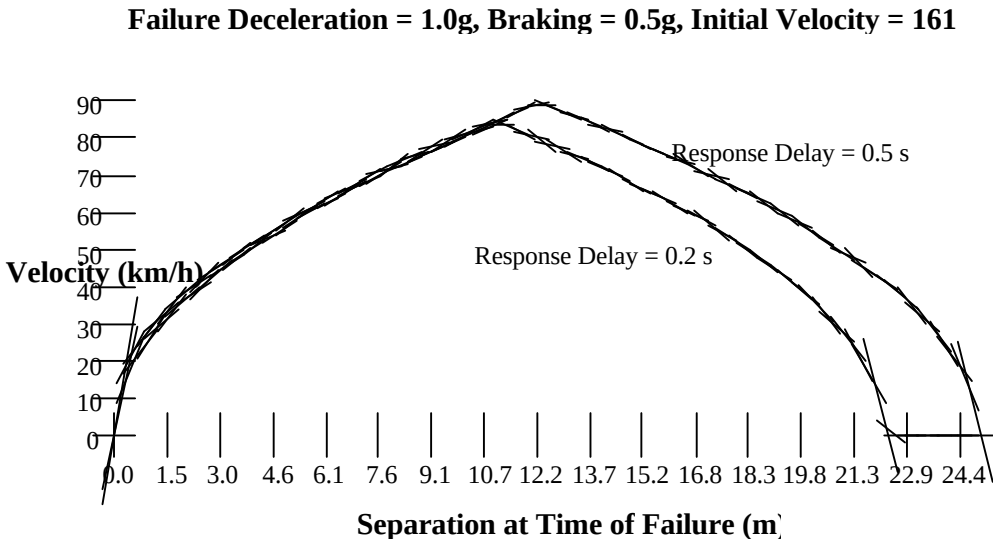

Figure 5. Collision Speed versus Separation at Time of Failure
Failure Deceleration = 1.0g, Braking = 0.5g

Lateral Momentum Transfer During An Intra-platoon Collision

Spacing between vehicles in a platoon may be kept to a very small value in order to avoid momentum transfer during a collision caused by a system failure. H owever, if the energy is transferred in both the longitudinal and lateral directions, then the vehicles involved will be spun about and may in turn impact barriers or vehicles in adjacent lanes. This issue may drive the auto manufacturers to consider vehicle bumpers which are designed to impart very low lateral momentum during a collision. The time interval before the vehicle has swung partially into the next lane is large, because the lateral momentum is never very large under any circumstance in which the vehicles are close together, so there is adequate time for the vehicles in adjacent lanes to adjust their positions and avoid collision. The steering algorithm which avoids lane transfer after a blowout would be more than adequate to prevent lane transfer in this case.

Conclusions

There are many scenarios where collisions within a platoon may occur. A control system capable of limiting collision velocities to acceptable amounts while maximizing traffic throughput will enable platoons experiencing inter-vehicle collisions to resume operation and drive to the nearest exit after the collision. This approach will prevent the original failure from impacting other AHS platoons.

The alternative to forming platoons is to establish conservative vehicle spacings such that either no collisions occur or collisions occur with a minimal impact velocity. This approach is somewhat advantageous in terms of safety and control complexity when compared to the platoon concept, but the decreased overall throughput may detract from the benefits.

Roadway Implementation

The purpose of this section is to identify the various safety aspects that must be addressed in the development of the AHS roadway and their associated risks, and to evaluate highway design issues that will improve congestion levels and improve travel time reliability in adverse weather conditions. The most comprehensive means of gathering statistics, and for ranking the safety of various highway systems, would be the development of an exposure-based accident rate. This rate would be developed after determining the vehicle miles traveled and the vehicle hours traveled on the various portions of highway.

Recent statistics indicate that one person is killed every 11.4 minutes on the nation's highways. The primary roadway information available to the highway engineer when analyzing accidents is either from police reports or computer-processed accident reports. Generally, this information is inadequate for the professional to determine if the condition of the road or its design contribute to the cause of a particular accident. The conclusion is often reached that the accident is caused by driver error, and this is based on incomplete information. Data that would be helpful in making a more comprehensive opinion on the cause of the accident include: the shoulder width, surface conditions, drivability, and shoulder drop-off conditions. This type of information can contribute to an AHS implementation plan which will effectively address the creation of a safer and more efficient highway system.

Accidents on conventional highways are discrete, random events caused by the interaction of highway, driver, and vehicle characteristics. Critical rates of accidents are developed for various classifications of roadways and intersections. A high accident rate is identified as a site where the actual accident rate is higher than the critical rate. Department of transportation budget limitations often force safety improvement projects to be prioritized based on ranking systems. These

systems take into account such factors as accident severity, traffic count, and cost of improvements. This standard of safety analysis may need to be rethought in view of the development of AHS.

The design process for safer highways may be broken down into developing an information system, developing some analysis techniques, implementing countermeasures by installing and evaluating improvements, monitoring the implementation process through a periodic maintenance period, developing a set of policy statements, performing an effort to educate the general public, and developing an assurance program by using enforcement techniques. A particular highway would be given a safety rating by considering its roadway geometrics, its roadside features, and the environment in which the highway is placed. Newly planned systems intended to improve highway safety ratings over conventional lanes would allow the capability at any location to:

- Introduce roadside safety measures.
- Forestall future accidents.
- Develop preventive measures.

Conventional highway design provides “forgiveness” for errors by providing recovery capability where the potential for accident occurrence is recognized. Current statistics show that:

- 45 percent of all deaths occur on curves.
- 34 percent involve crashes on hills.
- 65 percent occur on rural roads.

The installation of a guardrail or the placement of median barriers, the addition of impact attenuators, and the installation of breakaway signposts are currently used to mitigate the likelihood of a serious consequence in specific areas where there is a potential for an accident to occur. The design aspects of AHS lanes will take into consideration the advantages and limitations of automated vehicle control as potential substitutions for these physical barriers.

The highway facility that exhibits the safest characteristics will consider geometry features, road conditions, traffic volumes, weather conditions, and the level of roadside development; while considering the driver’s comfort, awareness, and level of communication with the

automated system. The issues associated with safe roadway designs are discussed in the following text.

Clearance

Horizontal clearance within existing rights-of-way will be important for placement of roadside instrumentation. Clearance is defined as the distance between the edge of the travel way and the closest physical object located along the highway. Current standards for conventional highway design recommend a minimum clearance of 10 meters be provided without requiring the addition of a barrier. The minimum clearance provided to the face of barrier is typically one meter. Retrofit of existing lanes must allow sufficient clearance to accommodate roadside instrumentation to ensure safe maneuverability within the automated lanes.

Consistent clearance on the shoulders is important for driver and passenger comfort and provides a buffer zone to prevent occupant distress due to perceived obstacles such as light standards, signposts, or structures such as bridge abutments and drainage facilities. This may be an important factor in placement of hardware when there is a viable option between the vehicle or the highway. Clearance within existing right-of-ways will also be a factor in the adaptability of a section to dedicated lanes. Barriers between AHS lanes and non-AHS traffic will require space in addition to the lane width. Shoulders may also be required to provide maneuverability within the AHS as well as access for emergency service vehicles. This subject is discussed in detail in Activity H — AHS Roadway Deployment Analysis.

Standard vertical clearances are required to accommodate the full range of vehicle sizes and maintenance equipment. Vertical clearance is defined as the distance between the pavement surface and the bottom of an overhead structure such as a bridge or sign. Federal requirements for conventional highways specify a minimum of 5 meters of vertical clearance. Maneuverability is not an issue when considering the encroachment of AHS instrumentation on vertical clearances, so this aspect is not expected to have a significant impact on the evaluation of retrofit choices from a safety standpoint. An AHS configuration which allows the driver to revert to manual control in certain emergencies may have some effect on the clearance specification. Drivers may be more comfortable driving with standard clearances and will be more likely to make errors while in manual control if the vertical clearance causes stress or reduced visibility.

Typical Section

A significant design factor in safe AHS operation is the surface of the travel lane. Pavement can consist of varying strength and quality, depending on the material used. Rigid concrete provides superior skid resistance when the surface is tyned or scored. Asphalt concrete is a flexible pavement type with a reasonable skid resistance friction factor. The strength of the road surface will be a factor in allowing truck and transit traffic on the travel lane, as well as the equivalent axle loads which can safely be sustained before the life of the pavement is consumed. The skid performance of the pavement surface must be taken into consideration when the maximum safe travel speeds are determined for the AHS vehicles. Pavement characteristics can be incorporated into traffic operations center (TOC) data base information to allow traffic flow to be managed in differing sections of highway.

Differential skid resistance is of great importance to safe AHS operation. Variation in the coefficient of friction due to the presence of water, snow, ice and spilled materials has a more profound impact on the range of skid resistance than the composition of the roadway surface. It is very common during rain showers to have patches of wet pavement interspersed with dry pavement. Areas in shade typically dry more slowly and stay wet longer than adjacent road surfaces. Widespread degradation of system operation may occur to accommodate worst case skid resistance, unless the AHS can detect and adjust for differentials across sections in real time.

The composition of the highway section may also affect the performance of certain candidate RF instrumentation. Reinforced concrete pavement contains steel which may introduce backscatter that has the potential for interfering with accurate radar reflections, for instance.

Evolutionary introduction of AHS equipment in RSC 2 may introduce a greater risk due to variability of the roadway surface. Vehicle-centered control may be implemented on existing highway sections without modification of the roadway. The position control instrumentation onboard the vehicle must be designed to minimize sensitivity to less than desirable physical conditions. Imperfections in surface conditions such as ruts or bumps may influence the onboard guidance components, whereas wayside control schemes may be calibrated to adjust for local variations. Another consideration is the reaction of the system to debris in the roadway. It may be important to develop a vehicle control method which does not respond violently to minor obstructions or defects in the roadway surface.

Access

Several issues are involved in providing access to the automated highway. The first concerns the location of access and egress points. Secondly, there exists the concern of providing a means to transition to the AHS from other highways. Finally, the issue remains of preventing entrance to the AHS by unauthorized vehicles. The impact of each of these issues on safe roadway design is discussed in the following paragraphs.

The design of onramps and offramps must take into consideration the system configuration, which dictates whether the automated lanes are reached via mixed traffic lanes or from dedicated access points. Non-dedicated facilities which require merging and weaving to occur between the onramp and entry to the automated lane will determine the appropriate spacing of onramps and offramps based more closely on conventional criteria. Conventional designs account for a variety of factors including:

- Traffic volume and design speed.
- Type of vehicle control, such as free flow or metered.
- Alignment and gradients.
- Pavement and shoulder widths and cross slopes.

The system configuration may also affect the spacing of onramps and offramps depending on the controlled vehicle spacing and whether platoons are implemented. The primary considerations of dedicated access AHS lanes will be the design speed and traffic volume, in addition to coordination of vehicles in platoon or non-platoon configurations.

RSC 1 and RSC 2 are proposed as dedicated facilities, with a physical separation between conventional travel lanes and automated lanes. Traffic barriers constructed of concrete or beam rail or cable systems may be used to delineate the AHS. There is normally a 1 to 2 meter clear zone between the edge of the travel way and the face of the barrier. Another consideration is the clearance required between a highway and railroad tracks. A 3 meter lateral clearance is typically required between the edge of the travel lane on a highway and the centerline of any railroad track. The clear zone specifications must be considered in the trade-off between alternative highway configurations for each AHS section. RSC 3 is defined as a non-dedicated facility relying on enforcement to prevent unauthorized vehicles on the AHS. The AHS may be identified by markings placed on the pavement, and/or signs to indicate the automated lane. Additional physical obstructions introduced into the roadway by signage

increase the risk of collision and must be considered in the trade-off analyses among potential AHS implementations.

Geometry

A critical feature to the safe design of an AHS facility will be to properly take into consideration the aspect of sight distance. Safe stopping sight distance and safe passing sight distance are of utmost concern and must be taken into consideration in conventional highway design. The design parameters of: horizontal and vertical alignment, lengths of horizontal and vertical curves, the lengths of pavement tapers, transition zones, and the layout and design of interchanges and intersections, must all take into consideration sight distance. It has a definite impact on design and safe operating speed of the facility, and in some conventional highway sections it is supported by signage and marking. Both safe stopping and safe passing are specified in minimum distances and are governed by the design speed, pavement and tire friction factors. The design issues which translate to the AHS include two factors: the “sight distance” of the obstacle detection employed and the coordination of traffic flow.

Sight Distance

The range at which the obstacle detection system can accurately detect intrusions into the automated lanes will determine the sight distance of the AHS vehicle. Sensor sight distance which is greater than human capabilities may allow travel speeds to be increased safely. A maximum range which is less sensitive than human capabilities may require that the travel speeds be decreased to allow for safe stopping distances. Driver perception may be a factor in determining the optimum travel speeds where AHS allows significantly higher speeds in low visibility situations.

Maneuverability

The ability of the AHS to provide communication between vehicles on roadway sections will provide early knowledge of traffic situations ahead of specific vehicles. The transfer of information may occur directly between vehicles or between vehicles and the roadway. Passing and other lane change maneuvers will not rely on sight distance around curves and on hills to the extent that conventional highways do. Vehicles which make maneuvers may be informed of the locations of other vehicles on the roadway in order to perform safe actions without relying on the visibility of those vehicles.

Barriers

Median barriers are used on conventional highways to prevent head-on collisions between opposing lanes of traffic, assist in directing the traffic flow, and provide protection where adequate clearance can not be maintained. The AHS will provide reliable lane-keeping, but median barriers may be desirable as a back-up safety system or to enhance driver perception of safety. Most people may be highly apprehensive of facing oncoming traffic at high speeds in an automated lane without the reassurance of a visual barrier as a minimum. Barriers have other benefits which may enhance safety through relieving stress on the driver. These attributes include improving ride quality by eliminating buffeting due to turbulence at high speed and close lateral spacing and reducing headlight glare from oncoming traffic. Barriers may also be used to prevent unauthorized access, as indicated in RSC 2. Barriers are an effective method for segregating nonAHS vehicles from the AHS lanes, but are implemented at the expense of a wider clearance requirement. Another consideration in the use of barriers is the fact that the barrier itself can be considered a traffic hazard in the event of a malfunction, especially during the merge to and from automated and manual lanes.

Shoulder Availability

Conventional highway designs include shoulders to provide a safety area for disabled vehicles, and as a clear zone available for recovery maneuvers. The shoulder may be either paved or loose gravel. A portion of the shoulder in rural areas may be grass. The shoulder is a relatively flat area and generally conforms to the normal cross-slope of the main paved lanes, but may be slightly steeper or reversed slope in some cases. Shoulder widths are often extended across bridge structures on high capacity facilities; however, normal shoulder widths are not provided on short bridge structures in some instances, especially in older designs. The shoulder in urban areas has often been converted to provide additional travel lanes in an attempt to increase capacity at the expense of safety.

The highway configuration chosen to implement the AHS lanes on existing highway lanes must consider the availability of right-of-way, including shoulders or breakdown lanes. Maneuverability in a dedicated AHS facility will require horizontal clearance in excess of the minimum required for a single travel lane. Access for emergency vehicles, deposition of disabled vehicles, maintenance activities, or emergency lane changes to avoid hazardous obstacles will require shoulders. The shoulder area can be effectively used as an additional travel lane in the absence of incidents. The breakdown lane can be used for AHS travel over

most of its length even if a vehicle is disabled, since the remaining cars can be maneuvered effectively around an obstacle with a known location. This situation may require reduced speeds or traffic throughput, but will allow the performance to degrade gracefully. A disabled vehicle in a single lane dedicated facility, by comparison, would require complete shutdown to prevent collisions.

The composition and geometry of the shoulder in existing highways may affect its usefulness for conversion to AHS breakdown lanes. The compatibility of existing shoulders to AHS requirements may limit the ability of converting to full travel lanes without extensive modification. The lack of shoulders across some bridge structures may not be a serious deterrent to implementing AHS, since the TOC database can factor this information into route guidance provided to the automated vehicles.

Interchanges

The purpose of an interchange is the transferring of traffic. Conventional highway interchanges consider the design speed, the proper transition zones and sight distance, especially with regard to the required weaving sections, and the need for signage for proper guidance through the transition area. Existing interchanges must be evaluated for compatibility with AHS operating speeds and automated traffic flow capabilities. Maximum speeds may be altered for automated lanes, and sign requirements may change when the route guidance is performed automatically. The amount of space designated for lanes on interchanges may also be modified with the assumption that weaving maneuvers will be under control of the system. Other issues related to interchanges are treated extensively in Activity J — AHS Entry/Exit Implementation.

Construction/Maintenance

Detours may be temporarily required to maintain traffic flow during periods of construction or maintenance. The ability to safely negotiate construction zones and detours is related to the system configuration. Lateral control mechanisms which are imbedded in the infrastructure may require extensive modification to maintain lane demarcation during construction periods. Vehicle centered methods are more flexible and can adapt to shifts in automated lane locations more readily. RSC 3 may require lane closures to maintain safe operation. Inadvertent access to an automated lane by unauthorized vehicles will be difficult to prevent if signage is the primary method for indicating the AHS, especially in construction zones.

Additional instrumentation or other temporary measures will add to the level of complexity involved in construction and maintenance plans if required. The additional details necessary to maintain safe automated control can add significantly to costs, both in the physical implementation of detours and in the quality of labor required to execute the plans.

One alternative to instrumenting detours involves relinquishing automatic control through the detour. This solution may be considered when the detour lasts a short period of time, such as for a maintenance procedure, or during periods of light traffic density. Closure of lanes is the safest solution to any maintenance or construction problem, but has the greatest impact to throughput and user acceptance. Each alternative must be evaluated in terms of the cost of maintaining safety during construction and operation.

Signage

Signs are used extensively on conventional highways to control traffic and improve safe operations by providing information regarding interchange and exit locations. Signage will not be required for purposes of navigation and maneuvers in dedicated AHS lanes, but may be used as a method of keeping the driver alert to upcoming events. RSC 3 may require an extensive amount of additional signs as the primary method for identifying the automated lane and its access points. Supports for signs are potential hazards, which is a safety issue in the mixed traffic configuration or any scenario in which the driver can take manual control. Signs installed to demarcate mixed use lanes should conform to the Manual on Uniform Traffic Control Devices (MUTCD) standards for safe location, reflectorization, and lighting.

Vehicle Mix

Traffic mix is another critical item in the design of a highway facility. It deals with percent of various vehicle types, such as passenger cars, trucks, and buses. It is influenced by whether the facility is in an urban or rural setting. It is further influenced by whether or not the design has some unique, critical features related to day or night, or peak or non-peak traffic operations. For the purposes of this analysis, RSC's 1 and 2 will not consider the issue of traffic mix, limiting the discussion to RSC 3.

An effective AHS design must take into consideration the impact of truck and transit vehicles on the roadway construction and safe operation. All but a few isolated situations such as the parkway toll system in the northeast operate with a traffic mix, and in practice the issue of

sharing the road with buses and trucks will exist on the freeways and urban arterials that are candidates for AHS implementation. It is feasible to consider an AHS in which classes of vehicles are segregated by time of day. An example system could schedule truck-only traffic from midnight to four a.m., when the ratio of trucks to other vehicles is high and total volumes are low.

Existing highways which are designed to accommodate heavy, multi-axle vehicles will be compatible with AHS implementation of mixed traffic. The primary implications will be in how the vehicle types are segregated, and whether truck and transit vehicles will be intermixed with passenger cars or limited to a single travel lane. Limiting the heavy vehicles to a single lane will affect the life of the pavement, but is not a safety issue if the roadway was originally designed for truck and transit use.

Environment

The operating capacity will be affected by the environment of the application area. One of the more challenging aspects of designing a system to operate under a variety of environmental effects deals with the dynamic, unpredictable nature of the events. It would be ideal to prevent any negative impact on safety across the full range of environmental conditions; however, this may not be possible based on the cost of mitigating strategies and their relative benefits.

Conditions including dry versus wet or humid weather, fog, snow, unusually warm or cold climate, wind or dust factors, and severe weather such as hurricanes or intense rainfall may affect safe travel. Roadway design which accommodates changing site conditions will require consideration of issues including:

- Varying friction factors of the road surface.
- Temporary reduced horizontal clearance due to snow accumulation.
- Proper functioning of drainage systems.
- Obstruction of vehicle guidance instrumentation.

Snow storms which result in the accumulation of snow requiring plow removal from the travel lanes can cause shoulders or breakdown lanes to be obstructed. The accumulation of snow adjacent to the travel lane can affect the ability to perform emergency maneuvers or safely remove a disabled vehicle from the AHS lane. Snow also has the potential for obscuring such position guidance devices as lane markers for video tracking or magnetic markers for lateral

control. Dense fog or intense rain may have similar negative effects on the vehicle guidance system.

Storm drainage systems are another factor in regions where frequent major rainfall occurs. Current design parameters allow the drainage system to permit up to half a shoulder width to pond storm water on highways. Ponds may accumulate a maximum of 100 mm of water, extending between drainage inlet structures. This type of flooding may be a major consideration in choosing sites for AHS where existing lanes are converted to automated lanes. Maintenance of the drain inlets is required to prevent flooding from encroaching on the travel lane. Drainage improvements to reduce potential ponding may be required in order to use the shoulder in the automated right-of-way. Areas where short duration cloud bursts cause extensive and/or isolated flooding are also an issue. Detection of flooding and implementation of traffic flow control may be preferable to increased drainage capacity in these instances.

Effect on Safe Travel Speed

Geometric design features such as the steepness of grades or sharpness of curves on a proposed AHS section affect the maximum safe travel speed. AASHTO guidelines recommend travel speeds in excess of 75 km/h only in level terrain and where other environmental conditions are favorable. Implementation of AHS lanes intended for high speed travel on existing sections must consider the geometry of the lanes and the maximum design speed to maintain safe levels of traction. An implementation such as RSC 2 which is intended to support high performance vehicles must take the geometry of existing lanes into consideration when evaluating potential locations for compatibility with AHS.

Varying coefficients of friction due to rain, snow, spilled materials, or ice on the road surface may cause the need to reduce travel speeds. This requirement has the potential to affect traffic throughput significantly unless the AHS incorporates the ability to sense and react to variations along different roadway sections. One option for improving the coefficient of friction under adverse weather conditions involves developing pavement designs that minimize environmental effects. One example of this approach is the Connecticut experimentation with open-aggregate asphalt coarse mix. The mix is designed to allow surface water to be drained through the depth of the pavement and eliminate or reduce the amount of surface water that collects on the pavement and runs off.

Terrain

Hilly or mountainous areas with severe grades or curves may affect the ability of the automated vehicle to maintain consistent speeds. This will be a significant factor in mixed traffic, where trucks may require an additional lane to optimize throughput and travel time for cars. This will be a consideration in RSC 3, where commercial vehicles operate in the same lanes with passenger vehicles. The impact of terrain on RSC 1 and 2 may be insignificant, since the automated lanes will not mix commercial and passenger vehicles. Throughput may be affected on winding roads if reduced speeds are required due to the capability of the obstacle detection and headway maintenance functions. This topic is considered primarily an operational issue, and is covered in depth in Activity F — Commercial and Transit AHS Analysis.

Design Risks

Table 4 provides a ranking of the risk factors in terms of the roadway construction, traffic control, and capacity in relation to major highway design issues. Safety design issues are evaluated by assigning a weight corresponding to individual risk factors in each category. The risk associated with retrofit of existing lanes without making physical improvements to the roadway are shown in the first column of the table. The risk figures assume no improvements to pavement or typical section features, and no access control or enhancements to signs. The next column addresses the risk of not providing designated travel lanes, thus allowing mixed flow of AHS and non-AHS vehicles. Thirdly, the dependence of safety on the method used to prevent unregulated vehicles from accessing the AHS facility is evaluated. Finally, the effect of AHS implementation is considered, including the nature of the terrain, average running speeds, and average and peak hourly traffic volume. The risk factor values were assigned by roadway engineers experienced in infrastructure construction and maintenance, taking into consideration the feasibility of various AHS implementation options, including barriers and dedicated entry/exit facilities. The values were generated following several team meetings in which concensus opinion was gathered to provide a numerically weighted measure of the relative difficulty of safe, cost effective design for deployment methods such as retrofit of existing lanes or construction of new lanes.

The design risk factors of horizontal/vertical clearance, access to the AHS, and sight distance are considered a significant risk if not addressed when existing lanes are converted to AHS use. This grouping of high risk issues in the design category indicates that selection of an

AHS site is a primary safety consideration. The risk factors are greater in this area than the issues of allowing manual vehicles access to the AHS lanes, the risk of unauthorized vehicles intruding into AHS lanes, or the choice of system configuration from the aspect of physical highway design.

The traffic control risk factors of construction/maintenance and signage are ranked as significant risks in the category of preventing intrusion to the AHS by unauthorized vehicles. The risk factors of barrier use, shoulder availability, and interchange configuration are also ranked very high in this group. This cluster of high risk factors denotes that these highway implementation features have the greatest impact to safety in this area.

Table 4. Rating of Risk Factors by Design Issue

Risk Factor		Design Issues			
		Retrofit Existing Lanes	**Dedicated AHS Lanes**	**Intrusion of Non-AHS Vehicles**	**System Configuration**
Design	Clearance	10	6	6	8
	Typical Section	6	5	5	5
	Access	10	8	7	8
	Sight Distance	10	5	6	7
Traffic Control	Barriers	6	6	8	6
	Shoulder Availability	6	6	8	6
	Interchanges	6	8	8	8
	Construction/Maintenance	8	3	9	9
	Signage	8	4	10	4
Capacity	Traffic Mix	5	3	10	10
	Environment	4	3	10	8
	Speed	4	4	10	8
	Terrain	4	3	6	6

Scale: 1 = Little or no risk if not addressed
10 = Significant risk if not addressed

The capacity related risk factors of traffic mix, environment, and travel speed also rank high in
the category of intrusion. The relatively low weights assigned in the retrofit column to the capacity risk categories indicates that the decision to convert existing lanes to automated lanes will not have a significant impact on safe capacity levels when compared to the issue of intrusion or system configuration. Similarly, the capacity risk factors are comparatively low

when the issue of dedicated lanes is considered because the system will be in control of all vehicles in the lane and will be capable of adjusting vehicle spacing and speed to compensate for changes in weather conditions and terrain.

System Reliability

One of the important aspects of the AHS Safety activity involves the interrelationship between safety and reliability, and how it should be addressed in the Precursor Systems Analysis as well as the implications that will extend across an AHS project life cycle. System reliability is a necessary system requirement that encompasses the consideration of fail-safe design features and system cost and maintainability concerns throughout the project life cycle. Reliability is defined as the probability that a system will perform satisfactorily for a given period of time when used under stated conditions. AHS system reliability will reflect the ability to operate continuously without collisions under stated operating conditions for a specified length of time.

System assurance analysis is a term commonly used to describe the method used to monitor, define and implement system reliability. The system assurance function is responsible for analyses that identify deficiencies in operations, maintenance, and testing which could affect safety, reliability, and maintainability. It is recommended that an AHS project require implementation of a Systems Assurance Plan (SAP) to ensure development and operation of a safe and cost-effective AHS that provides an acceptable level of service. The SAP should consist of reliability and maintainability activities that occur during the planning, design, construction, startup, and operational phases of the life cycle of the individual AHS projects. The SAP would charge all governing agencies/personnel, consultants, and contractors with the responsibility of ensuring safe, reliable, and cost-effective AHS service to the public. It is further recommended that system reliability criteria and specifications require all governing agencies/personnel, consultants, and contractors to understand reliability specification requirements and that the SAP tasks would:

- Improve operational readiness and level-of-service of the major AHS system elements.
- Reduce item demand for maintenance manpower and logistic support.
- Minimize system reliability and system maintainability impact on overall cost.

The ideal AHS scenario will provide a collision-free driving environment under normal operating conditions. Normal conditions are defined for the purposes of this discussion to

consist of operating the AHS in the absence of equipment failures. The issues concerning reliability of AHS equipment are discussed in terms of vehicle-specific components, infrastructure electronics and communications, and roadway-specific concerns.

Vehicle Subsystems

Vehicle safety on an automated highway is based on the system implementation and upon the design and reliability of the vehicle equipment. The reliability and fault tolerance of the design are dependent on a variety of factors, representing a tradeoff between the equipment cost and the upper bound of technology set by the current state-of-the-art. The issue of equipment cost can be viewed from two angles. The reliability of very inexpensive equipment may be improved economically by increasing redundancy, while the reliability of relatively expensive equipment may be enhanced through improved manufacturing and testing, adding to the overall component cost but providing better reliability gains on a cost/benefit basis.

The relationship between overall system safety and reliability of the vehicle-specific components is a key issue in the division of responsibility for automatic control between the vehicle and the infrastructure. The intrinsic reliability of a vehicle on the AHS might appear to be greater if the majority of the automated equipment were installed as part of the infrastructure; however, the vehicle reliability is actually an integral part of the system safety. The vehicle cost of ensuring operator safety is dependent on the system implementation as well. Upgraded vehicle safety features, such as bumpers designed for various impact strengths and angles or additional body stability can be implemented to compensate for poor position control fault tolerance. This approach may incur higher vehicle costs on an infrastructure-based AHS than an implementation with reliability designed into the infrastructure. The comparable vehicle cost for a vehicle-centered approach may be less if the reliability of the control loop is such that the body can be lighter, or bumper designs simplified.

Reliability of non-AHS specific vehicle equipment is a well known quantity, and periodic maintenance is a primary factor in minimizing the risk of failure. Routine maintenance requirements for AHS certification can eliminate the cause of a great number of current highway breakdowns, such as brake failure and overheating. Check-in procedures which include dynamic testing of critical vehicle parameters such as tire pressure can prevent another large portion of potential failures. Implementation of maintenance and check-in measures may be expected to reduce failure of non-AHS specific equipment to a very rare occurrence on the AHS. Several key areas of vehicle performance are addressed in the

following paragraphs. Each vehicle element is discussed in terms of failure modes, detection methods, and suggested alternatives to ensuring reliable operation.

A considerable body of statistics has been gathered about vehicle accidents on the highway and on city streets; however, the type of information which would be of most use in this analysis is either not available or has not been culled from the existing data. Consider brake failures as an example. Limited information on the number of accidents caused by brake failures on certain highways exists. It is desirable to know exactly how many accidents per kilometer occurred because of a brake failure which took place without any prior warning signal. The statistics generally identify only that brake failure is a cause, and prior knowledge of brake malfunctions is not a known parameter. The number of instances of instantaneous brake failure per kilometer which did not cause a serious accident are also of interest, but is also not an available statistic. These data are of prime importance because the AHS entry criteria can be used to screen vehicles during the check-in process, based on identification of brake system degradation or warning signals associated with brake failure.

Detailed statistics which link causes with events and demonstrate the principal issues and risks associated with vehicle safety are required to avoid speculation in this analysis. The objective of this discussion is to provide an overview of the myriad elements affecting vehicle safety. Many causes of accidents, regardless of their likelihood of occurring, are included in this survey of vehicle failure modes. It may be possible to prevent a percentage of these accident types through screening during check-in. A set of design considerations concerned with preventing risks to AHS safety and their potential impact to vehicle subsystem design is addressed in each failure mode category where applicable.

Steering System

There are two potential types of steering failures. The first type of failure occurs when the steering locks in a single position and the steering system is unable to move the wheels to a different position. A situation in which the vehicle is proceeding in a straight line on a straight highway may be compatible with a simple controlled stop. Other scenarios are more complex, including steering loss during a lane change maneuver, on a curved section of roadway, or during the transition from automatic control. The issue might be more severe if the vehicle consists of a truck and trailer combination, because of the increased risk that exists for the vehicle to overturn on a curve.

The impact of the failure may be reduced through implementation of a fully redundant steering system to eliminate the risk caused by loss of steering control in the event of a single system failure. The steering system in the automated mode is expected to exclude the steering wheel from the control loop. Statistics on the likelihood that the steering system exclusive of the steering wheel would lock up are needed in order to determine the importance of this failure mode.

The steering system function may be accomplished through differential braking of one or two wheels or the use of an alternate steering system. Current vehicle braking systems allow detailed control of different wheels for anti-lock applications and systems are being developed which provide selective braking to enhance stability. Systems which permits braking at one wheel in order to totally control vehicle steering are not planned. Similarly, although four wheel steering systems have been developed, few have reached production because of low consumer interest. Future developments may permit steering system failures to be handled gracefully by allowing the vehicle to be maneuvered out of the AHS using an alternate vehicle control mechanism.

The second type of failure involves the steering actuator becoming unstable, causing the vehicle to wander significantly about its desired path. This failure tends to be gradual in nature, is likely to be detected early, and can be overcome by utilizing an independent controller which would allow the vehicle to be safely removed from the main stream of traffic. An actuator failure is easily mitigated through controller redundancy, a capability which could be incorporated into the system level vehicle design. The primary issues regarding steering system failures are the probability of their occurrence and the degree of potential risk to operator safety. These issues must be weighed to assess the level of reliability which must be specified and designed into this subsystem.

The key to preventing vehicle component failures is early, accurate detection and high system reliability. Failures associated with the fluid in the power steering assembly may be anticipated through early detection of a fluid leak. A very small crack in the fluid system would allow little fluid to escape in 5 seconds. A sensor mechanism capable of measuring and evaluating the steering fluid level at a refresh rate on this order may be more than adequate if it is assumed that the majority of AHS driving time will be spent in steady state, without requiring steering control.

Another great concern is the occurrence of a structural failure. This type of failure has the potential to release all of the fluid at once, or cause an instantaneous break in the axle or king pin of the steering rack. The delay time between occurrence of the failure and impact to the steering system may be less than a second. The safety risk of structural failure is significant because the failure cannot be predicted and therefore screened during the check-in process. The nature of the steering mechanism causes full redundancy of the structural components to be unfeasible, further increasing the safety risk of this failure type.

Alternative steering systems which allow electronic control of vehicle steering rather than mechanical means present an enabling AHS technology. The emergence of electric power steering as an alternative to standard hydraulic power steering will affect the safety concerns to a significant degree. The first system to be marketed will probably be an electronically controlled hydraulic system. This device will simplify the transition from manual to automatic steering that occurs at highway exit and entry. This system will be a major competitor for the automated steering element of AHS, and appears to have passed the research stage at both GM and TRW. The second steering device would operate with an electric motor as the power source, and TRW appears to be reaching the last phase of research on this instrument. When this system becomes available, hydraulic fluid loss will no longer be a concern, and the emphasis will be on fail-safe motor design and on the reliability of the computer controller. The implications of integrating steer-by-wire systems into AHS will be addressed in more detail in Activity L — Vehicle Operational Analysis.

Engine Failure

This is more benign in nature than a steering failure. The failure is likely to be gradual compared to the reaction time constant of the AHS system and the result is likely to be a gradual slowing down of the vehicle which allows the other vehicles near the failure to steer around or brake before an unsafe condition occurs. Impact to the automated power steering by the engine failure creates a major risk, and the time interval between the initiation of failure and the loss of steering is important. Instantaneous engine failure resulting from material fatigue is a serious safety issue, since this type of failure cannot be mitigated through detection and prevention of the incident. Statistical data is needed to evaluate the likelihood of this event.

Gradual engine failure is compatible with early detection, providing sufficient operating margin to allow the vehicle to be maneuvered out of the AHS lane before an unsafe condition

occurs. Two parameters may be used to monitor engine health: oil pressure and temperature. Sudden decrease in engine oil pressure or increase in engine temperature can be used to trigger notification of impending failure to the AHS controller. The lead time between sensing of critical parameters and degradation of engine operation will typically be on the order of several seconds. Current engine designs incorporate oil pressure and temperature sensors, allowing prevention of malfunction on the AHS due to anomalies in these characteristics to be easily implemented.

Drivetrain Failure

Most failures associated with the drivetrain are not major safety risks because of their slow development time and low degree of impact to vehicle maneuverability. An example failure might involve a transmission locked in a low gear during highway entry, requiring the vehicles behind to slow down. The instance of the transmission locking in high gear will require the vehicle to maintain a nominally high speed to avoid engine stall. Either case of drivetrain failure will require an AHS which allows vehicles under automatic control to readily maneuver around a disabled vehicle, and/or the ability to maneuver the disabled vehicle into a breakdown area. The system design can easily include fault tolerance for this type of non-critical failure, providing detection of the condition and coordination between adjacent vehicles to maintain individual vehicle safety.

A more serious malfunction can occur in which the drivetrain becomes completely disengaged, and the vehicle loses propulsion. Collisions due to a major drivetrain failure can be effectively prevented by providing the capability for functional vehicles to maneuver around the disabled vehicle until the vehicle can be removed from the AHS.

Brake Failure

The failure of the vehicle brake system can be catastrophic if there is no advance warning. The most common cause of rapid brake degradation is the loss of master cylinder brake fluid. The loss of master cylinder pressure can be detected by a sensor in the brake line. All modern braking systems have built in redundancy in the brake cylinder design. Two separate inner chambers are contained within the outer master cylinder shell, each chamber couples to one front brake and one diagonally split rear brake. Fluid loss which occurs in one chamber will result in lost braking capability in only half of the braking system. Current brake pressure

sensors detect the pressure difference between the two chambers and provide a warning if one chamber differs significantly from the other.

A failure caused by a fluid leak is partially mitigated by splitting the front and rear brake lines so that one front and one (diagonal) rear brake are operating on each cylinder. Loss of braking power in one set of brakes due to a rapid fluid leak through a break in one line is offset by the availability of the alternate set of brakes, allowing the system to bring the vehicle to a controlled stop. The vehicle would lose all braking power if both cylinders failed at the same time. Reliability analyses of previous fault experience regarding this type of failure is not currently available. The likelihood of both brake lines failing concurrently must be evaluated to determine the necessity for increasing the existing level of redundancy in the system.

Another mode of brake fluid degradation which can be serious is the gradual loss of braking force associated with buildup of water in the line or evaporation of the fluid in both lines simultaneously. Fluid degradation can be caused by a parking brake that is stuck and therefore always partially on, causing both brake lines to overheat. These effects are gradual, and the system can be modified to reduce the associated risk at a finite cost. Monitoring the pressure sensors individually and measuring fluid temperature are both methods of resolving these problems.

Individual hardware failures will result in the loss of braking at one or possibly two wheels but should never result in the loss of all braking. The primary exception to this would be the loss of the master cylinder outer shell as a result of structural damage. One possible response to this risk is the implementation of a secondary electromechanical brake, an option which would be a major addition to vehicle cost. Electromechanical brake systems, which totally eliminate hydraulic fluid and the master cylinder, have been designed with possible application to electric cars. The risk to operator safety of brake failure is a major issue which may justify additional redundancy in performance monitoring and/or braking hardware.

Power Failure

The dynamics of power failures are generally such that the event can be effectively detected and prevented. Existing vehicle systems provide the ability to monitor battery voltage, allowing weak batteries to be detected and screened with relative ease. Vehicles are not currently instrumented to detect a degraded or disabled alternator. The failure of this component does not directly cause a power failure; however, it will eventually cause the

battery voltage to be drained. The sensor which measures battery voltage may be used to detect degradation caused by alternator failure. Both sources of potential power failure can be effectively eliminated from the AHS through the check-in process. Redundancy may be used to increase reliability, one cost effective approach is implementation of a secondary battery.

Instantaneous loss of power will disable all control systems including the engine controller. This may be a very remote possibility, but has serious implications. The risk to operator safety in the event of power failure within the vehicle is significant, because all automated systems may be disabled, such as the steering and braking. Sudden loss of electrical power due to a short or open circuit can not be detected prior to complete failure. This type of failure is not compatible with backup capability through redundancy, since this would require a complete redesign of the vehicle wiring system. Critical systems such as AHS-equipment controllers could be equipped with battery back-up for short term operation. The mobile telephone market has provided the impetus toward compact, lightweight battery technology which may be ideal for this application. The likelihood of instantaneous power failure and the impact to safety of individual subsystem power outages must be balanced with the cost of implementing battery power for fail-safety.

Failure of a Tire

The blowout of a tire on the highway can be catastrophic and result in a more severe incident than loss of brakes because of the possibility that the vehicle will swerve into another lane of traffic. Vehicle crossover may be prevented by isolating each lane with a dividing barrier. Dedicated AHS lanes separated by barriers from the manual transition lanes, such as those proposed in RSC’s 1 and 2, can reduce the number of accidents caused by blowouts. The potential capacity of the system will be degraded due to the additional space that barriers consume. The risk to system safety will still exist at a lower level since gaps in the barrier must be maintained at the entrance and exit points to the automated lane.

Mitigation systems such as tire inflation monitoring or tire pressure management may be more effective approaches to fail-safety. Direct pressure monitoring systems have been designed but have failed to possess the desired reliability or the desired low cost. Processing the wheel speed data required as part of the ABS and deriving variations in wheel rotating radius associated with under inflation has proven to be a more reliable and cost effective method of evaluating tire pressure, and tire pressure monitoring devices based on this methodology have been fully researched and are available for production.

A certain percentage of tire failures are caused by excessive wear, and this source of tire blowouts may be effectively prevented through periodic maintenance requirements. Check-in screening may include verification of correct tire pressure to further decrease the possibility of tire failure on the AHS. A puncture which causes a tire to flatten quickly may be prevented by high-resolution obstacle detection and avoidance techniques. Closely spaced, high-speed platoons may not be compatible with cost effective implementation of this measure. Another option is to provide fail-safety in the form of improved maneuverability in the event of a tire failure.

There are several mitigation systems currently being investigated which could potentially prevent loss of control during tire failure. One option involves refining the lateral control algorithm to produce adequate steering during tire failure to avoid disastrous lane changes. A tire inflation monitoring which allows rapid detection of tire failure could be coupled with rapid adaptive steering to preserve AHS safety. A tire which contains within itself a second tire has been used on race tracks effectively to avoid accidents caused by blowouts. Tire pressure management and monitoring systems have been developed which can provide sufficient air pressure to the tire to allow the vehicle to exit the AHS lane before significant air pressure has been lost. The relative cost in terms of the gains in system safety for each of these alternatives must be evaluated to determine the best approach.

AHS Controller Failure

Two major safety issues are associated with controller failure. The first involves the short time interval between failure and impact to the control system, which is assumed to be a typical cycle time on the order of 50 ms. The second concerns the possibility of concurrent multiple controller failure. The risk of controller failure impacts system safety in a manner similar to the corresponding subsystem it controls. The overall fail-safety of the vehicle systems will be dependent on the reliability of each of the subsystem components.

The issue of controller failure may be addressed in terms of preventing failure through detection and mitigation, or implementing redundancy to provide back up capabilities in the event of failure. Several techniques are available for improving the robustness of the controller design. Controller software may be implemented with built-in-test (BIT) capability, designed to detect most failures during the check-in process, resulting in denial of access to the automated highway. Another method for preventing failure relies on redundant circuitry capable of monitoring functionality and assuming control in the event of malfunction.

Existing systems implement hardware which automatically takes over and notifies the system manager that a circuit failure has occurred. This approach allows the vehicle to be removed gracefully from the AHS without resulting in an incident.

Another reliability issue concerns the data bus architecture used to connect various AHS control subsystems in the vehicle. The data bus and its operating protocol must be capable of preventing data errors. A common technique is to employ an error detection and correction scheme in either the hardware of the bus itself or the software protocol. Prevention of errors on the data bus is an integral factor in improving the control subsystem reliability.

Infrastructure Electronics

The processors, communications devices, and sensors which are located along the roadway are classified as infrastructure electronics. The reliable operation of the infrastructure electronics is critical to the safety of AHS. The extent to which this instrumentation affects the ability of the AHS to provide a safe operating environment is dependent upon the allocation of functions to the infrastructure. In RSC 1 and RSC 3, the control algorithms and the majority of the sensors are located in the infrastructure. Infrastructure based control instrumentation will place a relatively larger burden of ensuring safety with the infrastructure electronics. In RSC 2, most of the safety-critical electronics reside on the vehicle with the infrastructure electronics providing status and other non critical information. Depending on the configuration of the detailed system implementation, there may be some amount of safety-critical infrastructure electronics in RSC 2. The safety of vehicle-based control configurations will be dependent to a much lesser extent on the instrumentation of the roadway.

A major safety issue with infrastructure electronics is the detection of failed equipment at a site and the ability to maintain safe operations in the event of a failure at a single site or even two adjacent sites. Adjacent sites can be spaced at half of the effective range of their sensors, allowing coverage for a failed site in the event of a single point failure. This option may involve running self test diagnostics continuously in the background of processor operations. Coordination with an adjacent site can be initiated if the diagnostics detect a failure, allowing an adjacent site to perform coverage of the area normally covered by the failed site. Degradation of electronics at a site due to a dirty lens or an intermittent component failure is more difficult to detect. One technique available for detecting an intermittent failure requires each site to operate over its entire range, thus providing multiple measurements for each vehicle. The duplicate measurements are analyzed in an arbitration process. The sites are

assumed to be operating correctly if all of the measurements are the same from each sensor covering a specific area. One set of measurements which appears out of range with respect to the others indicates a potential malfunction, allowing that site to be flagged as requiring service.

Another safety issue concerns the maintenance cycle for infrastructure electronics. It is anticipated that the infrastructure electronics will be very reliable, with subsystems developed using best commercial practice having failure rates on the order of fewer than one in 500,000 hours. System failure rates are dependent on the number of subsystem elements. The scope of the AHS will impact system reliability as the quantity of instrumentation increases. It is inevitable that amongst the multitude of sites , periodic failures of the electronics will occur. Maintenance crews must be available to quickly replace failed electronics. The effect on system safety of infrastructure components must be evaluated to determine the control architecture which will be most reliable from the system level. Periodic maintenance of the infrastructure electronics may also be required. This could include swapping out the equipment for bench testing at the repair depot, or running diagnostics in the field. Sensors may have to be periodically cleaned or replaced, especially if dirt or debris on the sensor causes loss of sensitivity.

The loss of power to a section of the Automated Highway could have a catastrophic effect on the AHS. Measures must be taken to insure that the loss of power does not affect the performance of the infrastructure electronics. One option available to prevent loss of functionality during a power failure is through implementation of uninterruptable power supplies (UPS) at each safety-critical site. The UPS has the ability to provide power to equipment for a period of time after loss of line power. Enough time can be provided by the UPS to allow the AHS operation to be gracefully terminated. Alternately, a second source of power could be provided to each site. A second power source, such as battery-back-up or secondary generator, must be sufficiently isolated from the primary power source so that there is a high probability that one power source will remain active upon loss of the other source.

Communications System

A properly functioning communications system is critical to the performance of AHS. Loss or impairment of communications between the vehicle and another vehicle or with the roadside is a serious issue because it is an integral part of the position control loop. The reliability and testability of the communications system depends on development of a built-in test (BIT)

function. This function will both detect and isolate faults within the system, providing an important feature in averting failures.

The major issues concern accurate detection of communications loss, and the ability of the control systems to operate without external information. Platoon based RSC's are highly susceptible to communications failures due to the close vehicle spacing and high update rates required to support the control algorithms. The prevention of communications system failure can be accomplished through effective fault tolerance and high system reliability. The BIT function of the system must be able to detect system degradation prior to loss of communications. The timing of the fault detection must be designed to allow the affected vehicles to be maneuvered to a safe position within the constraints of the position control system.

The reliability of the AHS communications system will be dependent on two primary factors, the robustness of the link design, and the fault tolerance of the system hardware. The link design must consider many aspects of the communications environment, including the number of users, the quantity of data, allowable error rates, and security of the data package. Aspects regarding hardware reliability include the mean-time-between-failure (MTBF) of individual components, complexity of the system, and redundancy. Each of these topics are addressed in terms of the impact to AHS safety and feasibility of implementation.

Link Reliability

Mobile communications systems are subject to several sources of interference which have the potential to cause degradation of the communications link. Noise due to interfering transmitters is commonly referred to as radio-frequency interference (RFI). RFI is a significant design consideration in areas where the receiving antenna is subject to a high-density transmitter environment, such as mobile communications in a large city. The AHS must support high densities of vehicles with concurrent transmission demands, obviating the need for detailed analysis of the communications system diversity requirements. Access protocols such as code-, time-, or frequency-division multiple access are effective in supporting large numbers of users within the same band. Multiple access technology is currently being implemented in the cellular telephone market.

Another source of interference is multiple transmission paths, which result from reflections off other vehicles, bridges and similar objects. Multipath can cause reduction in received

signal strength when the phases of multiple signals combine destructively at the receiver. Spread spectrum modulation is a well known scheme for combating the effects of multipath through correlation techniques.

Signal degradation can also occur because of random attenuation changes within the transmission medium. The signal perturbations caused by fading can result in drop-outs in the received signal, generating errors in the received data. Coding schemes can be implemented to detect errors in the data stream, and error correcting codes or data block retransmission can be implemented to recover data lost in a fade. The best approach to error recovery depends on the characteristics of the channel and the length of the fades. Mobile communications channels tend to experience relatively long fades, which are more compatible with retransmission of lost data. The overhead associated with error correction coding is most compatible with shorter length errors.

The robust communications link for the AHS environment will include a multiple access protocol capable of supporting large numbers of users in a confined area. Interference caused by multiple signal paths must be accounted for in the modulation scheme. The detrimental effect of these reliability factors can be effectively mitigated using spread spectrum modulation techniques, combining the advantages of good multipath performance and inherent code diversity. Finally, fading must be addressed through message format and coding techniques.

Another issue concerning reliable communications is the variability of the propagation environment. The AHS may include segments passing through urban, suburban, or rural areas. The terrain may include hills, curves, bridges, or tunnels. The technology used to communicate between the roadway and the vehicle must be evaluated in terms of the operating frequency and line-of-sight (LOS) propagation characteristics. The literature contains studies of radio wave propagation in tunnels and in adverse terrain which can be used to evaluate candidate frequencies for critical operating parameters. [1]

Fail-Safe Electronics

The primary factors of interest in evaluating the reliability of the communications hardware include the mean-time-between-failure (MTBF) of the system resulting in system shutdown, and the overall communications system availability. Availability is an attribute that reflects the probability that the communications link will be ready to perform a necessary function at a

single instant or over a stated period of time. MTBF of the system is the inverse of the failure rate of the system. The rate at which a hypothetical communication system can be expected to shutdown is one occurrence in 10 years for a corresponding MTBF of 87,600 hours, for example. Using the component values for MTBF, the overall system MTBF may be estimated using the method given in MIL-HDBK-217F. The general mathematical expression for system failure rate is:

£system = Ni × (£comp × Q)i summed over the value i = 1 to n (1)

where

£system = Total system failure rate (failures/10**6 hours)

£comp = Failure rate for the i^{th} component (failures/10**6 hours)

Q = Quality factor

Ni = Quantity of the i^{th} component

n = Number of different component categories in the equipment

The system MTBF is directly related to the number of components in the system, and the failure rate of the system is greater than the least reliable component in the system. A more complex system design incorporating many components will have a higher failure rate than a more highly integrated system using comparable component MTBF's.

The system availability is derived from the MTBF using the equation:

A_i = MTBF/(MTBF + MTTR) (2)

where

MTTR is the system mean time to repair.

System availability for communications systems with comparable safety and reliability standards are 0.9994 for the BART train control communications system, and 0.9996 for the CAATS air traffic control communications system. Availability figures approaching unity are achievable using redundant transmit/receive (T/R) hardware. The vehicle-roadside system can be designed in a manner which allows on-line standby units to take over while failed units are replaced or repaired along the roadside. This capability can be accomplished through effective placement of the roadside units without requiring full redundancy of every unit. Vehicle T/R unit reliability requirements will require a different approach to optimizing MTBF since full redundancy in the vehicle may not be a cost effective option.

Detection of communications hardware failures is a capability which can be readily incorporated into the system design. Two standard methods are available for performing dynamic testing. One approach includes a pre-defined test pattern in the message protocol which is periodically transmitted by each user in the system. Failure to correctly receive the test pattern by any of the receivers is reported in a status message, which is also periodically transmitted by each user. This type of testing will use a portion of the bandwidth which would otherwise be available for transmission of data. As the number of users in the system increases, the system bandwidth used for test messages increases as the number of transmissions increases. The advantage of this technique is that it can be used to recognize both hardware problems and other conditions that cause data to be received in error, such as low signal strength, multipath and noise. The technique is very effective but must be considered as part of the top level communications design in order to allocate sufficient bandwidth for the anticipated quantity of users.

Another common self test technique is referred to as loopback test. In a loopback test, a transmitted message will be fed directly from the unit transmitter to the receiver. A comparison can be made between the original transmitted message and the loopback reception. Any change in the data will indicate a problem in the communications hardware. The advantage of a loopback is that no RF bandwidth is consumed. This is done at the expense of additional loopback hardware.

A properly functioning communications system is critical to the performance of AHS. The reliability and testability of the communications system depends on development of a built in test function. This function will both detect and isolate faults within the system. Loopback testing is often used for fault isolation by looping the signal back at various points in the system. When combined with a self test of the processing hardware within the communications system, a complete fault isolation test can be performed. Self test capabilities in addition to design for reliability are key parameters in the communications system design.

Catastrophic Failure

The occurrence of catastrophic failure is a significant issue in AHS implementation because of the potential risk of user injury. A catastrophic failure is defined for the purpose of this discussion to be any event affecting the AHS which causes a collision and interrupts normal AHS operation. Non-catastrophic failures are events which are managed through fault tolerance or redundancy and do not cause a collision, although these failures may cause degradation of service. The category of catastrophic failure within the AHS goes beyond fail-safety of individual control systems such as vehicle acceleration or maneuvering. Catastrophic failure can encompass scenarios ranging from infrastructure destruction by natural disaster to loss of critical vehicle communications capabilities due to vandalism of the system.

Platoon-based RSC's may have the highest potential injury rate resulting from catastrophic failure due to the clustering of vehicles. The term "brick-wall" is commonly used in highway literature, and the interpretation used for this discussion is presented here. A brick-wall failure occurs when an obstacle appears instantaneously in the path of moving vehicles. A non-brick-wall failure occurs when the obstacle is moving in the same direction as the flow of traffic, but may be decelerating at a rapid rate or may be out of control of the system.

A situation in which a brick-wall failure occurs may cause all of the vehicles in the platoon to be involved in the collision. Allowing brick-wall stopping distances between every vehicle will minimize the number of vehicles involved in collisions. From this standpoint, the large platoons of RSC 2 are most susceptible to multi-vehicle collisions, followed by the smaller platoons of RSC 1. RSC 3 has the best possibility for avoiding multiple car collisions by virtue of the space/time slot control definition of vehicle spacing. Providing conservative stopping distances between each vehicle will severely curtail potential capacity to ensure maximum safety in vehicle spacing.

The brick-wall failure is not a probable occurrence in a realistic assessment, but is considered for the worst case. The AHS vehicle control algorithms will prevent a majority of the collisions due to non-brick-wall failures. Emergency braking and lane changes can be utilized to prevent involvement of multiple vehicles in a collision which may be unavoidable by the lead vehicle. Failures which cause accidents limited to a small number of vehicles will not result in a catastrophic failure which shuts down the affected section of the AHS.

Catastrophic failure is an issue which can impact public perception of AHS safety. Assuming that accident rates are improved to the level that air travel has achieved, the airliner crash syndrome may apply to AHS. While air travel is statistically safer than automobile travel, media attention to multi-fatality accidents promotes a sense of apprehension in many potential fliers. The same phenomenon is likely to occur with platoon based configurations of AHS where accidents may be rare, but involve 15 to 20 vehicles when they occur.

Failure Recovery

A catastrophic failure, system malfunction, or external hazard may result in the complete shut-down of a portion of the AHS. The system design must include a contingency plan for bringing the system back into normal operation following a failure which may leave significant numbers of vehicles on the highway. This issue may be addressed in one of two ways. The failure response strategy may include the disposition of vehicles in its failure mode resolution, and provide a process for safely removing all vehicles from the AHS. The alternative is to resume movement of vehicles once the malfunction is corrected. The second method involves several safety implications.

The resumption of vehicle control following a system failure when the vehicles are left on the automated lanes carries the problem of verifying the continuing reliability of the vehicles remaining in the system. The failure which caused the system to shut down may result in damage to vehicles resulting in a potential safety risk. The system may be required to clear all existing vehicles from the roadway and require them to proceed through the check-in process before continuing travel. The impact of this option on user satisfaction is likely to be very negative.

Assuming that the vehicle is capable of sufficiently reliable self-tests following shut-down, the system could restart operation with vehicles in place on the roadway. All vehicles would require assignment into platoons or space/time slots for coordination of control. This would require significant processing capability and must be completed prior to allowing lane changes or entry/exit maneuvers via automated control. Activity E — Malfunction Management and Analysis, will provide alternate scenarios and address these issues in more detail.

Collision-Free Environment

The safety of AHS can be evaluated independently only if the AHS is designed in such a way that AHS vehicles are completely isolated. Overall safety will be affected by the extent to which external forces are capable of interfering with vehicles in the system. Accidents may be caused by unauthorized vehicles entering the AHS lane, or by debris from accidents occurring in non-AHS lanes. The design of AHS may address these issues through prevention and/or mitigation.

Another concern is the possibility for AHS-compatible vehicles to enter the system with an unapproved trailer or load. A primary safety issue is concerned with the risk of an object falling from a vehicle onto the automated lane. Establishing regulations regarding exterior cargo and the use of visual inspections to reduce the possibility that some part of the car itself will fall off may be the best method for preventing this type of occurrence. Vehicles with unapproved loads can then be denied access to the AHS through the check-in process. An object which falls directly into the path of an AHS vehicle can pose a serious problem in a platoon configuration, especially if the object lands in the middle of a platoon. Vehicle-vehicle spacing on the order of one meter or less will not allow maneuverability if the object falls backward from a leading vehicle into the path of the vehicle directly behind. There may be no method for avoiding collision before the platoon can be brought to a controlled stop or moved to another lane.

Dedicated AHS entry/exit facilities such as those specified in RSC's 1 and 2 will minimize the potential for impact by non-AHS vehicles. The addition of physical barriers between the AHS lanes and adjacent lanes will also contribute to enhanced safety by preventing non-AHS vehicles from intruding on the AHS lanes accidentally or intentionally, and can reduce the likelihood of debris entering the AHS lane. RSC 3 is the most susceptible to non-AHS elements, and its safety standards may be achieved through detection and avoidance of the hazards. The reliance on obstacle detection and hazard avoidance for preventing collisions with foreign objects will place additional requirements on the spacing of vehicles to maintain safe distances between vehicles for emergency maneuvers.

Automatic/Manual Interface

The human element in the safety equation has both positive and negative effects. Estimates based on accident report data indicate that improper driving is a factor in over 85 percent of all accidents. The delay between the perception of a hazard and braking has been found to be the dominant influence in collision statistics. AHS has the potential to be a mitigating influence on these types of accidents by controlling braking, maneuvering, and acceleration of the vehicle in the AHS lanes. Several considerations remain regarding the fail-safety of automated control.

The first issue concerns the risk of introducing accidents that are preventable by human interaction in the manual driving mode. The human field of view and the benefit of driving experience allow a driver to anticipate and avoid many potential collisions. The AHS design must be capable of detecting and avoiding unplanned intrusions into the travel lane. These requirements place significant demands on various elements of the automated control system.

The transition between manual control and automatic control and the corresponding transition back to manual control is another source of safety risks. The potential for human error exists if vehicles are allowed to enter or exit the AHS under manual control and the transition is made within the AHS lane. Similarly, if the vehicle is under AHS control in the non-AHS lane during a merge maneuver for entry or exit, then the AHS is susceptible to human error occurring among the vehicles operating manually in the non-AHS lane. A primary factor in the risk associated with the transition period is the length of time required to convert from manual to automatic control. The risk will decrease as the time decreases, implying that shorter transition periods are relatively safer than long transition processes. One option to minimizing these risks is to dedicate entry/exit facilities to eliminate the possibility of error caused by vehicles under manual control.

The transition from manual to automatic control and back may be more safely accomplished in a dedicated facility such as RSC’s 1 and 2. The vehicle and driver must clear an entry plaza prior to accessing the AHS in these configurations. The transition to automatic control may be accomplished at the conclusion of the check-in process in isolation from manually controlled vehicles. Exit from the AHS may be accomplished in a similar manner by requiring vehicles to pass through a transition facility where control may be reverted to the driver in an area separate from the AHS travel lanes. RSC 3 does not support dedicated facilities for the check-in and check-out process, which results in a greater safety risk during transition.

Related issues include releasing the vehicle to manual control and assuring driver qualifications for assuming control; releasing the vehicle at less than manual spacing from the preceding vehicle; or releasing the vehicle at an unsafe relative speed to adjacent vehicles. These safety considerations are all possible precursors of high delta velocity collisions. The recommended configuration must prevent these scenarios to ensure optimum safety.

The driver may attempt to regain manual control of a vehicle in a sudden desire to exit the AHS, or in a panic situation if a hazard is perceived. The large risk to the safety of AHS this action presents must be addressed, and methods to prevent unnecessary and unsafe transitions to manual control must be considered. Manual override of automated control while traveling at high speeds at close spacing is considered an unacceptable option in terms of safety. Implementation of full automatic control may require disconnection of mechanical steering and braking functions to prevent operator intervention.

The safety implications of the manual/automatic interface encompass the operator interaction with the automated system. Recent task force efforts have produced guidelines on man-machine interaction and traffic safety. The surveys indicate that the primary issue involves the usability of the operator interface. An effective man-machine interface must be capable of effectively monitoring driver performance to evaluate AHS-compatibility and must provide a safe workload level during AHS transition and operation.

Comparison with Conventional Highways

One of the deciding factors in the feasibility of the AHS will be the expected safety in relation to conventional highways. In order to justify the expense and logistics required to implement AHS, it must provide a measure of improvement in safety in comparison with existing freeways. RSC’s 1 and 2 may provide significant improvements by requiring separate facilities for passenger cars and commercial vehicles.

Studies have determined that differing deceleration rates are a major factor in the relative velocities of vehicles in a collision. Eliminating differences in braking rates and reducing reaction times can effectively minimize collision impact velocities during emergency braking. Automated control of braking and evasive maneuvers may provide a significant factor toward improving safety over existing highways

Current freeway operations are subject to great variability in driving styles, including inconsistent driving speeds and disparate driver reactions to hazardous conditions such as fog or construction zones. One of the most attractive features of the AHS in terms of safety is derived from the benefits of automatic longitudinal and lateral control of the vehicle position. The ability to stabilize the spacing and relative velocity of vehicles under steady state operation will contribute a large portion of potential safety improvements.

Task 3. Risk Assessment

This task is concerned with identifying specific hazards or failure modes which are generic to the system architecture, and consequently are applicable uniformly to each of the RSC's. The effort involves assigning categories to the hazards in terms of their relative severity. A standard methodology is presented which is based on MIL-STD-882C, a Department of Defense document which summarizes system assurance requirements for military contracts. Subsequent system designs may use a similar approach throughout the design life cycle to evaluate a specific system configuration and identify safety critical areas.

Standard system safety program analyses apply to all facets of deployment, including test, maintenance, and support. Each activity of the system development such as design, production, and operation should be included in the system assurance plan. The guidelines set forth in the system safety standard may be tailored according to the specific application. A program of the magnitude of AHS may find a large proportion of the system assurance requirements applicable, while subcontracts within the development cycle may be subject to a modified subset.

System safety is a term which refers to a system-level approach to the elimination or mitigation of hazards. Design criteria oriented towards hazard reduction are developed and applied. System safety methodology provides a proactive approach to eliminating hazards by design. The design objectives may be achieved by characterizing hazards by severity and probability. A risk assessment procedure which considers primarily hazard severity will generally be sufficient during the early phases of design to minimize risk. Hazards which are not eliminated by design must be analyzed by a risk assessment procedure based on the hazard probability in addition to the severity category to establish priorities for resolution. The mitigation approach can include acceptance of the risk for non-safety critical failures with low probabilities of occurrence, while corrective action may be required in safety-critical cases with higher occurrence rates.

Functional Hazard Analysis

The system architecture will determine the failure conditions that must be addressed in a functional hazard analysis. This step in the process of standard categories of hazard severity and criticality of failure modes are described in the following sections.

Hazard Severity

Hazard severity categories are defined to provide a qualitative measure of the worst credible vehicle collision(s) resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure, or malfunction as follows:

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

The risk assessment of the hazard should also include a probability of occurrence. Assigning a quantitative probability to a potential hazard is usually not possible early in the design or planning process. A qualitative hazard probability can be derived from research, analysis and evaluation of historical safety data from similar systems.[2]

Hazard Probability

The hazard probability is the probability that a hazard will occur during the planned life of the system. Hazard probability may be expressed in quantitative or qualitative terms. An example of a hazard probability ranking system is:

Description	Level	With Specific Individual Item	Within a Platoon or Inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in life of item	Unlikely but can reasonably occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

Criticality Categories

Criticality categories are defined to provide a qualitative measure of the potential consequences of a failure, for use in performing a Failure Mode Effects and Criticality Analysis (FMECA), as follows:

- Category 1 — Failure which may result in system shutdown or loss of life.
- Category 2 — Failure which may result in a delay or personal injury.
- Category 3 — Failure which may result in excessive unscheduled maintenance.
- Category 4 — Failure which may result in non-disabling loss of assembly function.

The general approach to system safety analysis establishes a hazard severity category (I through IV) and hazard probability ranking (A through E) for each identified hazard. The two rankings are combined into an Initial Risk Index, reflecting a combined severity and probability ranking which indicates the relative risk to system safety of the group of hazards under evaluation. Risk assessment criteria will be applied to the identified hazards based on their severity and probability of occurrence to determine the acceptance of the risk or the need for corrective action to further reduce the risk.

The hazard rankings are usually developed using historical data bases. Hazard severities and frequencies of occurrence can be adapted from transit data or comparable air traffic systems

during initial development of the system assurance program. Typical values which have been established in the past have been on the order of one failure in one million hours attributed to human error, or one failure in one billion hours due to an equipment failure. The goal in establishing guidelines in the development phase will be to minimize fatalities and system disruptions during the transition to full deployment.

Hazards which are identified as unacceptable or risks identified as undesirable may be analyzed with Fault Tree Analysis or comparable network analyses to determine effectiveness of corrective action. Fault tree analysis is tailored to exhaustively identifying a specific set of faults, environmental conditions, and failure modes that contribute to a single top event. The goal is to reduce unacceptable and undesirable risk to a specified level before design acceptance. Use of safety analyses and methodologies to identify hazards early in the design phase enables implementation of effective hazard mitigation techniques. The long term objective is the elimination and control of hazards to make the RSC chosen for detailed design as safe, reliable, and maintainable as possible.

Applicable Modes

System safety analyses can provide risk assessment and corrective action that applies under three AHS modes of operation:

- Normal — A condition where the AHS is functioning correctly according to the intended design and operating parameters.
- Abnormal — A condition or environment where the AHS is operating under faults or malfunctions that are not critical or catastrophic but degrade level of service and/or possibly increase risk exposure. Abnormal conditions may require departure from standard operating procedure and implementation of failure management and failure recovery to continue the level of service. Alternate operating procedures may be used to provide an equivalent level of safety in lieu of failed equipment, such as relying on a backup system for a failed automated feature.
- Emergency — A condition which causes immediate danger to property or lives. The condition may be a failure within the system such as a loss of lateral control, or external to the system in the form of a bomb threat or fire inside or outside the vehicle.

A comprehensive system safety analysis will address each of these modes of operation to ensure all levels of risk are understood and accounted for on the design. Many of the implications of operating under the three modes are addressed in Activity E — Malfunction Management and Analysis. The subjects of safety issues and risks and malfunction have been separated for this analysis, but are both integral parts of the process of system assurance in program design and development.

Preliminary Hazard Analysis

The Precursor Systems Analysis has been focused on identifying top level issues and risks, and highlighting areas of concern for future analyses. The representative system configurations outlined for this study were chosen to provide a very wide overview of enabling technologies for AHS. They have been combined in a manner which allows both ends of the spectrum and a point in the middle to be explored. Infrastructure centered platoon control (RSC 1) is at one extreme, vehicle based platoon control (RSC 2) is at the other, with time-slot control (RSC 3) presenting a mix of vehicle and infrastructure control elements. It is not possible to select a single optimum RSC from this set, but the implementation approaches can be used to highlight strengths and weaknesses of the broad array of options.

A detailed hazard analysis is highly implementation specific, and for this reason fault tree analysis has not been applied at this stage. The system functional decomposition discussed in the Contract Overview Report has been used as the basis for presenting an example functional hazard analysis. The failure conditions identified in table 5 are not intended to be exhaustive, but are used to demonstrate the methodology. The detailed design phase would begin with a functional hazard analysis (FHA), followed by a Failure Mode and Criticality Analysis (FMECA) on failure modes identified as Category I and II in the FHA. Frequencies of occurrence can also be assigned at this phase. Hazard probabilities are implementation specific in addition to being sensitive to deployment scenario, and have not been addressed in the preliminary example. The following paragraphs describe some of the reasoning that is used in assigning the hazard categories to typical failure conditions in each safety component area.

Table 5. Risk Assessment Criteria

Safety Component	Hazard Category	Failure Condition
Infrastructure:		
Roadway	I	1. Bridge collapse
	I	2. Loss of barrier integrity
	III	3. Degraded road surface
Check In/Out	I	1. Admit uncontrollable vehicle
	I	2. Allow intoxicated driver manual control
Entry/Exit	I	1. Lose barrier control
	IV	2. Overflow depot capacity
Vehicle:		
Mechanics		
• Structure	I	1. Tire failure
	I	2. Spill load
• Propulsion	I	1. Lose braking capability
	I	2. Lose steering capability
	IV	3. Lose acceleration capability
Control		
• Headway Maintenance	I	1. Lose longitudinal control
	III	2. Degraded control accuracy
• Lane Change	I	1. Lose lateral control
	II	2. Degraded control accuracy
• Emergency Maneuvers	I	1. Lose lateral or longitudinal control
Communications:		
Vehicle Position	I	1. Lose data link
	I	2. Long fade in high delta g maneuver
Coordination	I	1. Lose control of platoon members
	III	2. Lose inter-platoon information
Priority Messages	I	1. Miss transfer opportunity
	I	2. Severe data corruption
Operations Control:		
System Shutdown/Recovery	I	1. Insufficient residual power
	IV	2. Uncontrolled vehicles remain in AHS lane during start
Throughput Management	I	1. Platoon not notified of lane obstruction
	IV	2. Excessive queue length develops

Infrastructure

Roadway

Bridge collapse is a straightforward example of a failure with the potential to cause multiple deaths in the worst case. Loss of barrier integrity can cause a range of effects, including having negligible impact on system operation, but must be identified as potentially catastrophic because of the risk that unauthorized vehicles could enter the automated lane and cause collisions. Degraded road conditions such as ruts or potholes are considered to have at most the potential for causing minor damage if the control algorithms cannot compensate for irregularities causing low delta velocity collisions.

Check In/Out

The hazard caused by inadvertently allowing an unqualified vehicle entrance to the AHS has the potential to be catastrophic. Vehicles admitted erroneously could include vehicles with substandard instrumentation or hazardous cargo. Errors in the checkout process which transfer manual control to an incapacitated driver are considered Category I. The system must be designed carefully to avoid the possibility of injury or death caused by manual drivers under the influence.

Entry/Exit

Barrier control is a failure condition with implications similar to barrier integrity. Unauthorized vehicles may be capable of accessing the automated lanes and causing major collisions. The overflow of depot space will cause a negligible hazard, since the worst case solution might be to continue automatically guiding the vehicle which must be parked to the next depot along the highway.

Vehicle Mechanics

Structure

Most structural failures have the potential to cause fatal accidents. The system design must account for a wide variety of potential failures including tire blowouts and spilled loads. A situation which can present an obstacle in the path of a vehicle within a tightly spaced platoon has the potential for causing collisions and consequent injuries or death. Inter-platoon spacing

can be designed to prevent this type of hazard, but obstacles in the path of non-lead vehicles are a much more difficult problem.

Propulsion

The majority of failures which cause the vehicle to lose maneuverability have the potential to become catastrophic, such as loss of steering or braking. Loss of acceleration is considered a negligible hazard at worst, since adjacent vehicles can maneuver to avoid the disabled vehicle, and it can be brought to a stop safely.

Vehicle Control

Headway Maintenance

The complete loss of longitudinal control is placed in Category I, since the worst case result could be high delta velocity collision. A degradation in control accuracy might result in increased spacing between vehicles or reduced speeds if close following cannot be maintained. This failure might result in a low delta velocity collision before increased spacing can be put into effect, and is placed in Category III.

Lane Change

Complete loss of lateral control also has the potential of becoming catastrophic, since the vehicle could leave the automated lane or intrude on another lane and cause a major collision. Degraded lateral control accuracy is considered more serious than longitudinal control because of the greater risk of injury in non-straight line collisions. Glancing collisions which impact a vehicle traveling at high speeds can cause more damage due to the angle of impact.

Emergency Maneuvers

Loss of either lateral or longitudinal control will affect the ability to perform emergency maneuvers in the same manner that lane change and headway maintenance capabilities are affected.

Communications

Vehicle Position

The loss of the communication link which provides the control algorithm information to the vehicle can be catastrophic. One of the most critical situations occurs during transfer to automatic control and merging with the automated traffic. Interruption of the flow of position control information either due to a hardware failure or drop out in signal strength are both Category I since errors or missing control data can allow collisions to occur at high velocities.

Coordination

Communications may be used to provide coordination within the platoon of acceleration and deceleration. The ability to maintain constant headway between vehicles, especially in close following mode, will require close coordination of the control information within a platoon. Loss of control information may cause a following vehicle to collide with a lead vehicle in an emergency braking maneuver, which is considered Category I. Information required to allow adjacent platoons to maneuver is not as time critical, and the onboard systems should be able to allow platoons to stop or change lanes with marginal system impact in the event of a failure.

Priority Messages

Priority messages may be used to transfer time critical information. Missing a single message or suffering severe errors in the data is considered Category I. Timely, accurate information will be required to ensure safe operation during emergency maneuvers.

Operations Control

System Shutdown/Recovery

A catastrophic condition can occur if sufficient residual power is not available to support vehicle control loop functions in the event of a system shutdown. The system must be capable of providing continuous control data until all vehicles have been brought to a stop or transferred safely to manual control. The risk of starting the system with vehicle under manual control in the automated lanes must also be avoided. This situation can be managed by

preventing access to the AHS until lanes have been cleared. This may create a large throughput risk, but has negligible safety impact.

Throughput Management

The regional supervisory function may be responsible for providing notification of hazardous materials or other obstructions to vehicles traveling in the automated lanes. Failure to provide timely notification can be catastrophic, especially in close following modes. Inadequate system wide coordination of access control can have the effect of decreased throughput in the system, either by increasing the travel time as densities increase, or causing excessive delays at check-in as capacity is regulated. This will have a major impact on system efficiency, but will have negligible risk to safety.

Task 4. Identify Potential Disruptions And Discuss Alternate Actions

Introduction

This task will focus on identifying disruptions to the AHS by agents not within the control of the AHS itself. The disruptions have been categorized and are presented in table 6. The characteristics of each event will be discussed in terms of the severity of the safety risk presented. Each disruptive influence will be qualified as either a soft or hard hazard and the rationale will be presented. Risk assessment criteria will be applied based on the hazard severity and probability of occurrence to determine the appropriate mitigation strategy.

Hazard Classification

The AHS will be subject to situations classified as soft or hard hazards. Soft hazards are defined as situations in which the optimum operating conditions of the AHS are reduced. The AHS may adjust the capacity, travel speed, or route of vehicles, providing continuous system operation with limited degradation. Hard hazards are those which cause a portion of the AHS to cease operation. The hazards summarized in the table above will be categorized as soft or hard in terms of their potential impact to the AHS operating environment.

Table 6. Disruptions to AHS

Category	Typical Classification	Vulnerability with Respect to Conventional
Weather Conditions		
Rain	Soft	Less
Snow/Sleet	Soft	Less
Ice	Soft	No Change
Lightning	Soft	More
Wind	Soft	Less
Fog	Soft	Less
Environment		
Electromagnetic	Soft	More
Contaminants	Soft	More
Corrosion	Soft	More
Altitude	Soft	More
Natural Disasters		
Avalanche/Mudslide	Hard	No Change
Flood	Hard	No Change
Fire	Hard	No Change
Earthquake	Hard	No Change
Volcanic	Hard	No Change
Tornado/Hurricane	Hard	No Change
Human Subversion		
Terrorism — Fire/Explosives	Hard	More
Vandalism	Soft	More
Operator/Non-AHS		
Unauthorized merge	Soft	N/A
Accident debris	Soft	No Change
Hazardous Materials	Hard	Less
Roadway Conditions		
Scheduled closures	Soft	Less
Minor repairs	Soft	Less
Emergency repairs	Hard	Less

Weather Conditions

Hazardous situations resulting from most weather conditions will be soft in nature. The AHS will generally require reduction in travel speeds or capacity to allow additional safety margins when rain, snow, or ice affects the traction of the roadway surface. Snow may also obscure lane markers used for lateral control, which can be a soft or hard hazard depending on the impact to safe operation. Loss of a certain percentage of lateral control points results in degraded operation, which may be addressed through reduced speeds or increased spacing. Obstruction of guidance markers preventing reliable or accurate control of the vehicles will cause a hard hazard to occur, resulting in complete shutdown of the AHS in that area. Wind may affect the lateral control of vehicles, and this factor must be taken into consideration when control algorithms are designed. Lightening has the potential to cause catastrophic failures of infrastructure electronic subsystems, making it a cause of hard failure of the AHS. Proper design of safety critical subsystems must take the lightening hazard into account in their design for fault tolerance.

Fog may be considered as soft, hard or not a hazard depending on the sensing scheme developed for lateral and longitudinal guidance. Infrared ranging will be susceptible to fog and a soft hazard will develop if vehicle headways must be adjusted. Video sensors used for lateral control inputs are also subject to degradation due to fog. Loss of lateral control or severe degradation of vehicle-vehicle ranging may cause a hard hazard if the foggy portion of the AHS is not capable of safe operation. Fog will not affect system operation at all in configurations which use non-optics based lateral and longitudinal sensing such as magnetics or radar. Radar systems currently exist at millimeter wave frequencies which demonstrate reliable performance under weather conditions including fog, mist, or rain. The majority of weather conditions will cause graceful degradation of ideal AHS operation as a worst case result. Lightning has the greatest potential for causing a catastrophic failure and should be accounted for in the system design for fail-safety.

Environmental

The external environment may produce hazards to AHS-specific equipment in the form of electromagnetic interference, contaminants, corrosion, or effects of high altitude. Electromagnetic hazards include sensor interaction, interference and voltage drops, or power disruptions. Sensor interaction may interfere with vehicle sensing and affect safe position control. Electromagnetic interference may be caused by car phones, microwave relay towers,

power substations, and radio transmissions. Voltage drops or disruption of power service may be the result of electrical storms, construction, temperature effects, and animals. RSC 2 may be less sensitive to these effects due to its vehicle-centered nature. A form of auxiliary power and lightning arrestors may be required to prevent a hard hazard or minimize a soft hazard.

Contaminants may include dust, sand, or gravel. Immersion and splash can affect infrastructure electronics through corrosion or contamination of internal components. Similar effects are caused by exposure to fine dust and sand, especially in desert areas. Changes in altitude can cause reduction in heat transfer efficiency, increased mechanical stress on electronic packages, and reduction of high-voltage breakdown characteristics. Impact to AHS operation resulting from the majority of environmental hazards can be prevented through proper design and test of components and subsystems.

Natural Disasters

Several categories of natural disasters have the potential to be classified as hard hazards. It is not clear whether obstacle detection technologies are capable of detecting avalanches and floods which obstruct the AHS roadway. The commonly used method is reflective RF energy, which may have reduced effectiveness on objects consisting of water, such as several feet of flood water or a snowslide obstructing the road. The best method for prevention of catastrophic failure for these types of disasters may be prediction and rerouting of vehicle traffic. Minor flooding of a few inches of water or less may be treated the same as heavy rain conditions, with a soft hazard causing severely reduced speeds without causing complete shutdown of the roadway. The AHS may be capable of safely controlling cars under minor flood conditions. Drivers tend to travel in severe weather conditions in spite of advisories, and the AHS may provide a significantly safer alternative to manual control in minor flood conditions.

Wildfires may be classified as soft or hard hazards, depending on the location and extent of the burn. Soft hazard conditions may be classified as those in which smoke obscures visibility, but flames are not in the immediate vicinity. The AHS may provide significantly enhanced operation over manual control in this scenario, since lateral and longitudinal control will not depend on driver visibility. This assumption will be negated if the sensing technology is optical, however, as discussed in the preceding paragraph concerning fog. The AHS will also provide an advantage in reducing driver variability due to apprehension or curiosity under soft hazard conditions associated with traveling past a wildfire area.

Fires which actually threaten the AHS roadway must be considered a hard hazard, and detection of approaching flames through advisories or other methods is a design concern. Vehicle traffic can be detoured to alternate routes, resulting in complete closure of affected sections of the AHS.

Earthquakes may be classified into soft or hard hazards, depending on the magnitude and epi-center. The most prudent approach may be to provide sensing at the Traffic Operations Center (TOC) level and to cease operation when any earthquake is detected. Normal operations can resume when accurate seismic data is verified. An alternative might be to only require shutdown if the magnitude is greater than a certain limit. This approach would establish the need for sensing devices at the TOCs capable of determining the severity of the earthquake within moments.

The potential impact of rock or mudslides are similar to avalanches. The severity of the hazard is dependent on the extent to which the AHS is affected. Detection of rock may be more straightforward than mud. Mud may spread to a uniform level, making radar detection difficult. Detection by sensors in the pavement may be required. Eyewitnesses are another potential source of identifying obstacles, but the time lag is not acceptable in most cases.

The majority of volcanic disturbances are rare and are not usually a surprise. Advisories may be the best method for detection of potential volcanic interference with AHS operation. The statistically small possibility of this type of disaster interrupting service may determine that the most cost effective approach will be to cease operation in the area where volcanic eruptions are imminent.

Human Subversion

Damage to the AHS caused by terrorism such as bombs will usually result in a hard hazard. The extent of the immediate damage may not require shutdown of the highway, but the risk of related occurrences must be ruled out before normal operations are resumed. Vandalism may cause soft or hard hazards in the short term, but is typically limited to isolated cases, and may not prompt the AHS to cease operations. The classification of the hazard in cases of vandalism will be determined by the extent of the initial damage.

Operator/Non-AHS

A major hazard can be introduced by an inexperienced operator attempting to negotiate the AHS. The risk involves the complexity of operator actions required during AHS travel. The interface must be designed to minimize the work load of the driver and avoid requiring additional training and possible special licensing for AHS operation. High levels of operator involvement in a heavily congested urban arterial during a rush-hour period has the potential for introducing a significant hazard through human error. Inclement weather could further compound the situation.

Foreign or vacation travelers may be unfamiliar with AHS travel and facility locations. This is a special area of concern in terms of safety. AHS can provide distinct advantages to these drivers in terms of route guidance and eliminating human errors such as using the wrong side of the road. The risk of inadvertent entry to the AHS with an unqualified vehicle is present when drivers unfamiliar with the facility attempt to gain access. The instructions provided to the driver during check-in must be unambiguous to a wide range of potential users, and signs used to indicate AHS facilities must be designed with international symbols.

The unauthorized entrance of a manually controlled vehicle onto the AHS is potentially a hard hazard. The impact of unapproved vehicles depends on the hazard containment plan implementation. One possibility might be gradually slowing the entire AHS to a complete halt when an uncleared vehicle is detected. This approach will produce a hard hazard by definition since service suffers total degradation until the vehicle is removed. The possibility of a collision is not eliminated, since the AHS has no control over the maneuvers the manually controlled vehicle might make during the shutdown process. Another option might be to continue operation at reduced speeds and increasing all vehicle headways using conservative criteria, providing the maximum safety margin for unpredictable lane changes by the rogue vehicle. This approach will result in a soft hazard in that the AHS will continue to operate but at significantly reduced capacity. This approach carries similar risks as the first, although cars in motion have the advantage of maneuverability in the event that the manually operated vehicle continues to operate within the AHS. One far-fetched approach might be to dispatch a helicopter to remove the offender from the AHS using a hook or magnet. This idea may be discussed in terms of removing disabled vehicles as well.

Accident debris from adjacent non-AHS lanes is most likely to cause a soft hazard. The obstacle detection mechanism should include the capability to identify foreign objects entering the roadway and initiate the process of collision avoidance. The AHS may deny access to the affected lanes until the hazard is clear, or it may reduce speeds and coordinate lane change maneuvers to avoid the debris. Both of these options produce a soft hazard in which the AHS continues to operate at a reduced level.

Hazardous material spills have the potential to cause temporary shutdown of the AHS until the spill is cleaned up. Caustic spills also have the potential to affect the roadway surface condition, causing soft hazards in the long term by requiring resurfacing.

Roadway Conditions

The highway configuration selected for AHS implementation will be a factor in determining the potential safety hazards. Deploying the AHS within existing lanes will introduce the risk of hazards due to non-compatible highway elements. AHS safety requirements for horizontal and vertical curvature must provide the minimum sight distance for the sensor technology chosen, and take into account driver comfort on the typical section traveling at 100 km/h. Horizontal or vertical clearances to an obstructions must be considered to allow for emergency maneuvers, and provision for designating travel lanes for AHS must be allowed.

The following mitigation steps can be considered in an effort to maintain safe AHS operation on existing highway facilities:

- Reducing the design speed.
- Adding traffic barriers.
- Providing additional guidance signs.

A deteriorated pavement that includes ruts and uneven surface conditions would significantly impact the safety aspects of the system. This could have a negative impact on the proper operation and efficiency of the AHS because of the automated control loop response to the variations in the roadway surface. This hazard is most significant for the vehicle centered control proposed for RSC 2. Driver comfort and safety may both be compromised if jerky operation occurs due to large rapid changes in braking or steering caused by uneven road surfaces.

The mitigation effort would include a comprehensive reconstruction of the highway system, prior to initiating the AHS. Aggressive preventive maintenance would also be required to ensure consistent road surface quality. Digitized photographic information could be implemented to assist in producing a “conditions” survey of the highway facility. A document similar to GIS (photo logging) could be used as an infrastructure record keeping tool, including documenting any improvements made.

Routine maintenance functions will generally cause soft failures. This type of maintenance activity can be scheduled in advance and the traffic management facility can adjust traffic flow requirements accordingly. The result may be reduced capacities and/or vehicle speeds in the construction area. The degradation of AHS service may still offer significant improvements over existing freeways under extensive maintenance or expansion. A major cause of vehicle slowing and bunching around highway construction is the alteration of normal travel lanes, with lane change maneuvers and lane reductions often required. The AHS may allow traffic to flow smoothly at reduced capacity or speed without the stop and go slowing common to typical construction zones.

Emergency repairs may cause hard or soft hazards, depending on the type of repair necessary. The considerations are similar to those for scheduled repair with the exception of detection of the problem and delays involved in addressing the problem.

Safe operation under hazardous conditions will rely on traffic control devices. These devices provide information, warnings, and guidance to affected vehicles. The devices used in the implementation of AHS may differ from those used currently on conventional highways, but the purpose will continue to serve the needs of obtaining attention to the hazard, providing clear, concise messages, ensuring the respect of the users, and timely availability. Devices used to relay hazard condition information must consider the roadway design, physical placement, maintenance requirements, and conformance to standards.

Emergency Service

Utilization of the AHS by emergency vehicles may present a soft hazard resulting in reduced system capacity or travel speeds. RSC’s which incorporate dedicated lanes are most susceptible to disruption of normal traffic flow. RSC’s with limited access such as infrequently spaced entry/exit facilities may introduce unacceptable delays in emergency service response to disabled vehicles or drivers in need of medical attention.

CONCLUSIONS

A stated goal in the development the AHS concept is collision free operation in the absence of malfunctions. Overall safety will also be affected by the extent to which external forces are capable of interfering with vehicles in the system. Operation of the AHS in conjunction with conventional travel lanes or in areas that are vulnerable to intrusion will create the potential for collisions with non-AHS vehicles. Accidents may be caused by unauthorized vehicles entering the AHS lane, by debris from accidents occurring in non-AHS lanes, or animals or pedestrians entering the roadway. A collision free environment can not be guaranteed unless all types of intrusions can be prevented, and there will remain a certain degree of risk which must be managed.

The role of the driver in the AHS is the center of debate in terms of safety. The human field of view and the benefit of experience allow a driver to anticipate and avoid many potential collisions in conventional driving. The AHS design must be capable of detecting and avoiding unplanned intrusions into the travel lane. A balance must be achieved between automated control and operator intervention. The spacing and grouping of vehicles has a great impact on the complexity of the problem. The potential for error in close following mode may be greater than the benefit of allowing the driver to intervene in a perceived emergency. One option which may be considered is allowing the lead vehicle in a platoon to retain some degree of manual control. This issue is one of the most pressing in terms of maintaining system safety, especially with respect to implementing platoons. The capability to prevent collisions is removed from system control if the operator is allowed to interrupt automated control at any time.

A major safety consideration involves the risk of collision during the transition between automated and manual control. The potential for human error exists if vehicles are allowed to enter or exit the AHS under manual control and the transition to automated control is made within the AHS lane. Similarly, if the vehicle is under AHS control in the non-AHS lane during a merge maneuver for entry or exit, then the AHS vehicle is susceptible to human error occurring among the vehicles operating manually in the non-AHS lane. One option to minimizing these risks is to dedicate entry/exit facilities to eliminate the risk of collisions in transition lanes caused by vehicles under manual control. A related issue in a configuration which allows the transition to take place in lanes with mixed flow is the assignment of liability in the event of a collision.

The degree of risk in terms of injury or destruction may be dependent on the system configuration. The failure of a critical function or a disruption such as a power failure in a close-following platoon has the potential to cause multiple collisions and/or injuries. The statistical probability of this type of event must be extremely small, placing high reliability requirements on the system. An important goal will be to maintain user confidence in the safety of the system, especially in the early stages of deployment. An analogy may be drawn with the airline industry, where accidents are very rare but can be catastrophic when they occur and often cause multiple deaths, adversely affecting public perception. This type of accident receives greater publicity in proportion to the number of lives lost than a comparable number of traffic accidents in the same time period. The system must be brought on line in a way which minimizes the risk of collision-inducing failures, allowing a safety track record to be established which will promote user confidence. This may be accomplished by evolutionary introduction of increasing levels of automation and deployment of a platoon configuration after automated control of individual vehicles has been widely accepted.

Classical safety analyses promote safe stopping distances between vehicles which allow a vehicle to stop without a collision when a “brick wall” failure occurs in the preceding vehicle. This stopping distance is greater than the current following distance commonly used on congested freeways. An AHS which requires large headways will sacrifice throughput. Alternative studies show that platoons with tightly spaced groups of vehicles with “brick wall” stopping distances between platoons can be safe, because in emergency maneuvers the vehicles traveling close together will be traveling at nearly the same speed and energy transfer between them in the event of a collision will be very small. The problem occurs when an intrusion to the AHS occurs, such as an unauthorized vehicle cutting into the safe gap, or an animal entering the roadway. These situations will cause a collision if the obstacle is closer to the lead vehicle than the safe stopping distance. The platoon of vehicles will be at a greater risk for multiple injuries than single vehicles spaced at the standard safe stopping distance.

The ability to safely maneuver incapacitated vehicles out of the flow of traffic will require instrumentation to support longitudinal and lateral control outside of the automated lane. A system configuration which places all of the functionality for latitudinal and longitudinal control within the vehicle will not be constrained to operation within an instrumented lane. Lateral and longitudinal control which depends on interaction with the roadway will require instrumentation in any travelway in which control must be maintained. One option is to implement a two lane AHS in which both lanes are used for travel, or configured as a travel lane with a breakdown lane or shoulder. One lane can be used by the traffic operations

management to allow malfunctioning vehicles to be parked while oncoming traffic is maneuvered into the second lane and back as necessary. A concern with a single dedicated lane with barriers on each side is how much horizontal clearance is necessary to maneuver safely around incidents within the automated corridor.

Lanes dedicated to automated control introduce the concern over how to safely limit access. Barriers between the automated lane and manual lanes decrease the likelihood of intrusion into the AHS by unauthorized vehicles, animate obstacles, or debris. Allowing manually controlled vehicles to operate in the same lanes as system controlled vehicles makes it more difficult to design a collision free system. The AHS must be responsible for controlling all vehicles within the system; in mixed mode traffic, there is additional work load added by accounting for unpredictable movements of manually controlled vehicles.

There is a certain level of risk in traveling on conventional highways associated with such events as floods, earthquakes, and other natural occurrences. Evaluating the safety of the AHS must consider the vulnerability of the system to this type of occurrence. The susceptibility of the system configuration to natural disasters must be considered to prevent creation of a greater safety risk than that encountered on conventional highways in the event of these occurrences. The design of the AHS must also avoid increasing the cost associated with prevention of environmental effects out of proportion to the benefit attained. Safety can be maintained economically through a range of approaches, including such measures as rerouting traffic in adverse weather conditions or eliminating certain sites from consideration for AHS deployment.

The impact of system safety at the subsystem design level is another important concern. Safety can be improved by introducing higher levels of subsystem redundancy but this tends to increase the system cost out of proportion to the benefit. Improved component reliability and providing cross functionality among subsystems may provide higher safety benefits at lower overall cost to the system. AHS systems can use existing vehicle subsystems such as engine controllers or ABS as models for reliable, cost effective, safe implementation. The effect of the system architecture on the cost of safe system design will be a primary consideration in the flow down of subsystem functionality.

Safety has been established as one of the primary influencing factors on the success of AHS. It is an area of concern that permeates every level of the system design, and must be addressed at each stage of study, development and deployment. It is recommended that system safety be

addressed as an integral part of subsequent contracts. A System Safety Program can be implemented which consists of safety related activities in the planning, design, construction, deployment, and operations phases of AHS projects. A primary goal of the safety plan is the elimination or mitigation of failures through design criteria which indicate areas of concern. System safety emphasizes the verification and demonstration of the overall safety of the system as implemented for subsequent long term operation. Identification of safety as a systems level issue and establishing design practices and standards at the outset of the development phase are important steps toward creating a system that will meet the safety design goals.

GLOSSARY

Availability — An attribute that reflects the readiness of the system to perform its intended function when called upon at a stated instant of time or over a stated period of time. It is usually expressed as the probability that the system will be available when required, or as a proportion of total time that the system is available for use. The availability of an item, system element, or system is a function of its reliability and maintainability.

Braking Distance — The distance required to stop the vehicle from the instant brake application begins. AASHTO, 1990, pp. 118.

Horizontal Clearance — The measured distance between the edge of the roadway and the closest face of the physical object located along the highway. The objects include lighting, signposts, landscaping, and structures.

Maintainability — The probability that a device will be restored to its specified functional operation within a given time period when a maintenance action is performed in accordance with specified procedures. The defined proability can be converted to equivalent component repair rates or Mean-Time-to-Repair (MTTR) values.

MTBF — Mean-Time-Between-Failure, see Reliability

MTTR — Mean-Time-to-Repair, see Maintainability

Reliability — The probability that the system or subsystem will perform satisfactorily for a given period of time when used under stated conditions. The probabilistic definition is converted to an equipment attribute by converting probabilities to equivalent component failure rates or Mean-Time-Between-Failure (MTBF) values.

RMA — Reliability, Maintainability, Availability. Three related system assurance activities which define the attributes of a system in these areas.

Safe Passing Sight Distance — Based on the length of unoccupied lane needed to safely complete normal passing maneuvers. AASHTO, 1990, pp. 128.

Safe Stopping Sight Distance — The sum of two distances; the distance traversed by the vehicle from the instant the driver sights an object necessitating a stop to the instant the brakes are applied, and the distance required to stop the vehicle from the instant brake application begins. AASHTO, 1990, pp. 118.

Sight Distance — The length of roadway ahead which is visible to the driver. Sight distance is usually discussed for (1) distances required for stopping applicable to highways; (2) distances required for the passing of overtaken vehicles only on two lane highways; and (3) special conditions related to sight distances at intersections to minimize risk of collisions of vehicles. AASHTO, 1990, pp. 117–118, 126–127, 135–136.

System Safety — A system level approach for the elimination or mitigation of hazards, through design criteria oriented towards hazard reduction.

Systems Assurance — A system-level approach to establish and maintain an efficient RMA program to support a cost-effective achievement of overall program objectives.

Vertical Clearance — The measured distance between the pavement surface and the bottom dimension of an overhead structure. AASHTO, 1990, pp. ?.

REFERENCES

1. Benzair, B., H. Smith, and J.R. Norbury, “Tree Attenuation Measurements at 1-4 GHz for Mobile Radio Systems”, IEEE Transactions on Antennas and Propagation, Vol. AP-35, No. 5, May 19872.

2. Pendleton, O.J., Systemwide Methodology for Evaluating Highway Safety Studies, FHWA-RD-92-049, 1992, Texas Transportation Institute.

BIBLIOGRAPHY

1. Balke, K.N. and G.L. Ullman, “Method for Selecting Among Alternative Incident Detection Strategies”, 1232-12, 1993, Texas Transportation Institute.

2. Beason, W.L., “Development of an End Treatment for a Low-Profile Concrete Barrier”, 1949-2, 1992, Texas Transportation Institute.

3. Brackett, R.Q., “Evaluating Texas Traffic Safety Programs: A Manual for Assessing Program Effectiveness: Final Report”, 1992, Texas Transportation Institute.

4. Brackett, R.Q. and O.J. Pendleton, “Safety Impact of the 65 MPH Speed Limit”, 1991, Texas Transportation Institute.

5. Buth, C.E. and T.J. Hirsch, “Improved End Treatment for Metal Beam Guardrail”, 189-1F, 1977, Texas Transportation Institute.

6. Chang, E.C. C.J. Messer, and S. Wang, “Development of Freeway Ramp Control Evaluation System”, Paper No. 940666, 1994, Texas Transportation Institute.

7. Chang, E.C. and S. Wang, “Improved Freeway Incident Detection Using Fuzzy Set Theory”, Paper No. 940603, 1994, Texas Transportation Institute.

8. Crouse, M.R., “1991 Tabulation of Accidents in the State of Texas”, TARE-91, 1992, Texas Transportation Institute.

9. Effenberger, M.J. and H.E. Ross Jr., “Report on the Static and Dynamic Testing of Franklin’s U-Post and EZE-Erect Connection”, 1977, Texas Transportation Institute.

10. Hirsch, T.J., “Analytical Evaluation of Texas Bridge Rails to Contain Buses and Tracks”, 230-2, 1978, Texas Transportation Institute.

11. Hirsch, T.J., J.J. Panak, and C.E. Buth, “Tubular W-Beam Bridge Rail”, 230-1, 1978, Texas Transportation Institute.

12.Ivey, D.L., K.K. Mak, H.D. Cooner, and M.A. Marek, “Safety in Construction Zones Where Pavement Edges and Dropoffs Exist”, Paper No. 870523, 1991, Texas Transportation Institute.

13.Ivey, D.L., L.I. Griffin III, J.R. Lock, and D.L. Bullard Jr., “Texas Skid Initiated Accident Reduction Program”, 910-1f, 1992, Texas Transportation Institute.

14.Ivey, D.L. and L.I. Griffin III, “Safety Improvements for Low Volume Rural Roads”, 1130-2F, 1992, Texas Transportation Institute.

15.Jella, R.K., S.R. Sunkari, W.L. Gisler, N.J. Rowan, and C.J. Messer, “Space Management: An Application of Dynamic Lane Assignment”, 1232-18, 1993, Texas Transportation Institute.

16.Kohutek, T.L. and H.E. Ross Jr., “Safety Treatment of Roadside Culverts on Low-Volume Roads”, 225-1, 1978, Texas Transportation Institute.

17.Krammes, R.A. and G.O. Lopez, “Updated Capacity Values for Short-Term Freeway Work Zone Lane Closures”, Paper No. 940725, 1994, Texas Transportation Institute.

18.Mak, K.K., J.G. Viner, and L.I. Griffin III, “Assessment of Existing General Purpose Data Bases for Highway Safety Analysis”, Paper No. 870232, 1991, Texas Transportation Institute.

19.Marquis, E.L., “New Concepts for Traffic Barrier Systems”, FHWA-RD-79-65, 1977, Texas Transportation Institute.

20.McCasland, W.R., “Use of Freeway Shoulders to Increase Capacity”, 210-2, 1978, Texas Transportation Institute.

21.Morhig, G.A ., H.E. Ross Jr., and K. Walker, “Full-Scale Crash Tests of Aluminum Signposts”, 3683-1F, 1978, Texas Transportation Institute.

22.Newton, T.M., “Vehicular Crash Test of a “Palomar” Glass Fiber Reinforced Plastic Pole for Road Lighting”, RF 3965-1,1979, Texas Transportation Institute.

23.Olson, R.M ., N.E. Walton, G.D. Weaver, and T.J. Hirsch, “Highway Safety Design: Course Notes”, 1978, Texas Transportation Institute.

24.Pezoldt, V.J. and R.Q. Brackett, “Impact of Radar Detectors on Highway Traffic Safety”, DOT HS 807 518, 1991, Texas Transportation Institute.

25.Ross Jr., H.E. and D.G. Smith, “Impact Behavior of Roadside Barriers on Nonlevel Terrain-Crash Test Study”, 3659-1, 1979, Texas Transportation Institute.

26.Ross Jr., H.E., J.L. Buffington, G.D. Weaver, and D.L., Schafer, “State of the Practice in Supports for Small Highway Signs”, Interim Report, 1977, Texas Transportation Institute.

27.Ross Jr., H.E. and K. Walker, “Static and Dynamic Testing of Franklin Steel Signposts”, 3636-1f, 1978, Texas Transportation Institute.

28.Ross Jr., H.E. and K.C. Walker, “Impact Behavior of Thin-Walled Steel Tube Signposts and Delineator Post”, 264-1F, 1978, Texas Transportation Institute.

29.Samuelson, G.R., “Full-Scale Crash Test of Kaiser 50-foot Luminaire Support with Cast Aluminum Base”, 1978, Texas Transportation Institute.

30.Sparks, D.W. and R.J. Flowers, “Highway Safety Improvements: An Evaluation of Title II Countermeasures in the State of Texas”, TARE-04, 1979, Texas Transportation Institute.

31.Thompson, B.A., “Evaluation of Safety Results as Part of the Motorist Survey on Houston Mobility and Transportation Information”, 1992, Texas Transportation Institute.

32.Ullman, G.L., C.L. Dudek, and K.N. Balke, “Effect of Freeway Corridor Attributes Upon Motorist Diverson Responses to Travel-Time Information”, Paper No. 940313, 1994, Texas Transportation Institute.

33.Walker, K.C. and H.E. Ross Jr., “Full-Scale Crash Tests of “Telespar” Sign Supports”, 3775-1F, 1978, Texas Transportation Institute.

34.Womack, K.N., “1991 Survey of Front Seat Occupant Restraint Use in Eighteen Texas Cities”, 1992, Texas Transportation Institute.

35.Womack, K.N., “1992 Survey of Child Restraint Use in Fourteen Texas Cities”, 1992, Texas Transportation Institute.

36.AHS Precursor Systems Analysis, Activity D Report, Task 3, Delco Systems Operation, 1994.

37.“Have Automobile Weight Reductions Increased Highway Fatalities?” Report to Congressional Requesters — October 1991. US GAO, GAO/PEMD-92-1.

38.Motor Vehicle Safety. “Selected Rulemakings by the National Highway Traffic Administration”, Fact Sheet for Congressional Requesters — January 1989. US GAO, GAO/RCED-89-11FS

39.“Trends in Highway Fatalities 1975–87”, Report to the Chairman, Subcommittee on Investigations and Oversight, Committee on Public Works and Transportation, House of Representatives — March 1990. US GAO, GAO/PEMD-90-10.