Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Malfunction Management and Analysis

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-95-141
November 1994

PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS

Activity Area E

Malfunction Management and Analysis

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

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 E Malfunction Management and Analysis		5. Report Date 6. Performing Organization Code
7. Author(s) T. Green, A. Cochran*, S. O'Brien**		8. Performing Organization Report No.
9. Performing Organization Name and Address Delco Electronics Corporation Delco Systems Operations 6767 Hollister Avenue Goleta, CA 93117-3000		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

Malfunctions of the AHS vehicle, wayside electronics, roadway, and driver sub-systems along with possible methods of detecting the malfunctions are identified. Possible strategies to manage the malfunctions are proposed. Measures of effectiveness by which the strategies may be evaluated are defined. A method of using the measures of effectiveness is shown and based on this method, conclusions are drawn as to the effectiveness of the strategies. Issues related to management of AHS malfunctions are identified.

17. Key Words	18. Distribution Statement
Malfunctions, factors, strategies, detection techniques, management strategies, measures of effectiveness, Automated Highway Systems	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)

Section **Page**

TABLE OF CONTENTS
(CONTINUED)

TABLE OF CONTENTS
(CONTINUED)

Section **Page**

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Malfunction Management and Analysis Activity E is devoted to an investigation of the necessary reactions of the Automated Highway System (AHS) subsystems to failures or degraded performance of the AHS functions. Proactive measures to prevent malfunctions are often included in the traditional definition of malfunction management but, for the purposes of this investigation, these proactive measures have been declared as the province of Activity N — AHS Safety Issues, and are addressed only incidentally in the Activity E analysis.

The investigation is organized in a rather simple fashion into five tasks which are described in the following paragraphs:

Identify the Malfunctions

The AHS is partitioned into four subsystems and the malfunctions of each subsystem are identified. The subsystems are: Vehicle, Wayside Electronics, Roadway, and operator. The vehicle malfunctions are further divided into malfunctions of standard vehicle functions and malfunctions of AHS-specific functions. Lists of malfunctions for each of the subsystems are found in tables 1 through 4. An initial categorization of the malfunctions according to timeliness of action needed to assure safety or performance is also done.

Define Malfunction Detection Techniques

Management of malfunctions depends not only upon knowing the malfunctions that may occur, but also upon knowing when a malfunction has occurred. That is, there must be a method of detecting each malfunction — recognizing that a malfunction has occurred and identifying the malfunction. In task 2 methods and technologies for detecting each malfunction are discussed. These methods include those that have long been available, those that have been newly introduced, and those that are being investigated for future application.

Define Malfunction Management Strategies

Each management strategy defined consists of two parts — a set of immediate actions by each of the AHS subsystems and some actions to recover from the end result of the immediate actions. Analysis of possible immediate actions that can be invoked by the AHS subsystems to isolate or

remove malfunctions in the safest, least disruptive way has shown that these immediate actions can be organized into five sets which cover all of the malfunctions identified in task 1. Specific actions by the vehicle, wayside, and operator are defined in each set.

The end results of each of the sets of immediate actions may require some further action to bring the AHS back to full operation. The necessary recovery actions for each of the end results are also defined in task 3.

Define Measures of Effectiveness

Measures of Effectiveness (MOE) by which the management strategies can be judged are defined in the areas of safety, performance, and market penetration sensitivity and are ranked by importance within each category. A list of these measures of effectiveness, along with a short description of each, is shown in table 11.

Evaluate the Management Strategies

To aid in the evaluation of the management strategies, a numerical rating was assigned to each of the MOE's within each category. A severity scale was also devised for each MOE and a numerical value assigned to each point on the scale. A method of scoring the effectiveness of each strategy was devised and it is shown how to apply this method by computing a score in the areas of safety and performance for each management strategy. The scores thus computed can be used to evaluate alternate strategies for a given malfunction and to identify which malfunctions are difficult to manage and where attention to prevention must be placed.

Results

While the above tasks were being pursued, conclusions were reached and issues that require further investigation surfaced. These conclusions and issues are noted as follows:

- There is a limited number of malfunctions identified — 19 general vehicle malfunctions, 28 AHS-specific vehicle malfunctions, 15 wayside electronics malfunctions, and 9 roadway malfunctions. (See task 1.)
- Operator malfunctions identified are limited to being unprepared to accept control at checkout time. (See task 1.)

- There exist detection methods for each identified malfunction. Current research is being performed to improve malfunction detection capability. (See task 2.)
- Practicality and cost-effectiveness of applying the identified malfunction detection methods to AHS needs to be examined. (See task 2.)
- The cost-effectiveness and necessity of automating the detection of roadway malfunctions (pavements, bridges, and barriers) must be determined. (See task 2.)
- Malfunction management strategies can be organized into a small number of sets of immediate actions and actions to restore the AHS to full operation. All of the malfunctions identified can be covered by one or more of these sets of actions. Most malfunctions can be effectively managed (i.e., managed with little impact on safety and performance). (See task 3.)
- Malfunctions that lead to a loss of lateral control are difficult to manage since an adequate backup for lateral control has not been identified. Further investigation of this subject must be pursued. (See task 5.)
- The next most difficult malfunctions to manage are those associated with brake failures, tire failures, and failures of roadway pavements, barriers, and bridges.
- Malfunctions that are difficult to manage for safe operation also are difficult to manage for maintenance of performance. Malfunctions that can be managed for safe operation but require closing of AHS lanes, or even an entire section, also have a large impact on performance.
- The role of the operator as a malfunction detector needs exploration. (See task 2.)
- It appears that the operator has very little role in malfunction management, not being capable of providing backup to the automatic control systems. Further investigation of the limits of operator capabilities should be carried out. (See task 3 and 5.)

INTRODUCTION

The goal of Malfunction Management and Analysis is to determine those responses to a malfunction in any part of the AHS that must be performed by the major subsystems of AHS in order that safety of AHS users will be maximized and disruption to AHS operation minimized, with safety considerations always paramount. The malfunctions considered in this activity are those detected after the automatic check-in procedure has been successfully completed and the vehicle has been accepted by and is under control of the AHS.

The major subsystems of AHS involved in the malfunction management strategies are:

- The vehicles which are equipped to operate on AHS lanes, have been explicitly allowed to enter the system, and are being driven on the AHS lanes.
- The operators of the vehicles which are being driven on the AHS lanes, in particular the operator of a vehicle in which a malfunction has been detected.
- The roadway infrastructure of the AHS, which includes the pavements, bridges, drainage systems, and barriers which are part of the AHS, and any personnel required for the operation and repair or replacement of these items.
- The electronic infrastructure of the AHS, which includes the electronic equipment needed for operation of the AHS exclusive of the vehicle electronic equipment. This includes computers, communication equipment, sensors, and the power necessary for the operation of the AHS and any personnel required for the operation and repair or replacement of these items.

The goal of determining proper responses to AHS malfunctions will be reached in two steps. The first step will be to lay a foundation for the malfunction management strategies by identifying the potential malfunctions and determining how these malfunctions can be detected. The importance of this first step is that without the knowledge of what the malfunctions are there can be no strategy laid, and without detection there can be no implementation of the strategy.

Once the malfunctions are known, the second step, which consists of devising and evaluating the management strategies, can proceed. The devising of management strategies will also be conducted in two steps reflecting the objective of the Malfunction Management activity — 1) determine immediate actions by each of the AHS subsystems which will isolate and/or

remove the malfunction, and 2) determine longer term actions in response to the end-results of the immediate actions, which allow recovery from these end-results in such a way that minimal disruption to the AHS occurs and safe operation can continue. A secondary goal in the devising of management strategies is to determine a concise set of strategies which will manage the many malfunctions identified at the beginning of the process. This will be done by organizing the malfunctions into groups which can be managed by common immediate actions and by mapping these groups of immediate actions onto a few sets of longer term recovery actions. The process is illustrated in figure 1.

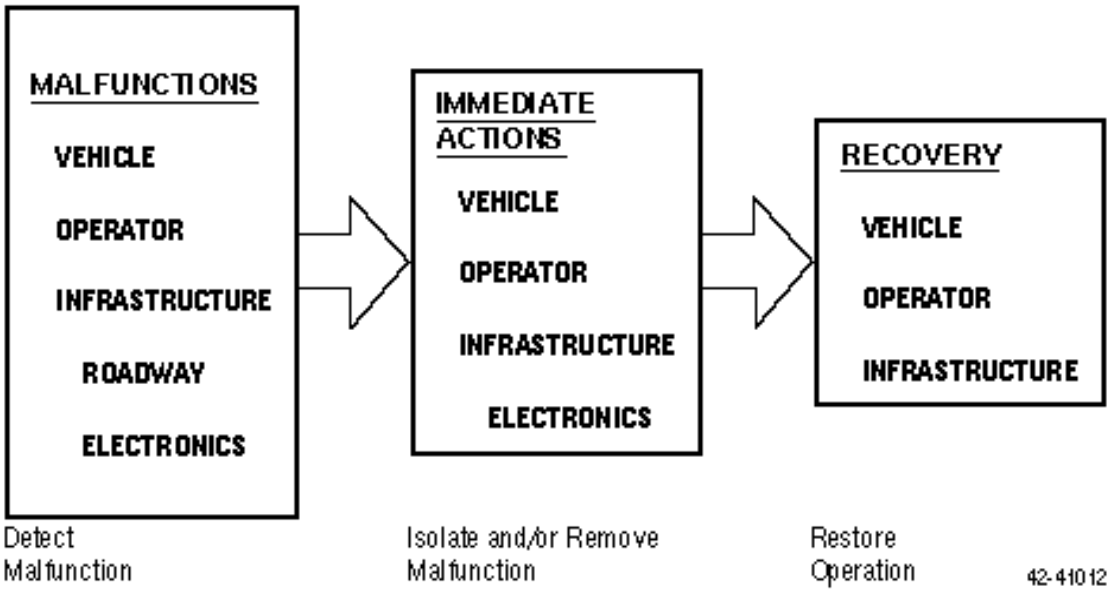

Figure 1. Malfunction Management Process

The end of the process consists of evaluating both the immediate actions and longer term actions of the strategies for adherence to the stated goal of safety and minimal disruption of the operation of the AHS. A set of Measures of Effectiveness will be designed by which an objective comparison of competing management strategies for a specific malfunction can be made. The Measures of Effectiveness will also allow comparison of strategies for different malfunctions as a help in identifying malfunctions which are difficult to manage and thus need greater attention for prevention.

It must be noted that this activity will not include a number of what traditionally are called malfunction management strategies. These are the strategies that are preventative in nature, e.g., component or computational redundancy, periodic inspections, and incident recording and evaluation. The prevention of malfunctions is covered in Activity N — AHS Safety

Issues, while the management of malfunctions that occur regardless of what preventative measures have been taken is covered in this activity.

REPRESENTATIVE SYSTEM CONFIGURATIONS

The representative system configurations (RSC's) were generated very early in this Precursor Systems Analyses of the 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 OF EACH TASK

Task 1. Define and Categorize Malfunctions

A malfunction is defined as any event which degrades or has the potential to degrade the operation of the AHS, and includes the failure or impending failure of equipment belonging to any of the major subsystems of the AHS from whatever cause. This task catalogues the various malfunctions that will affect the operation of the AHS. These malfunctions are categorized as:

- Vehicle malfunctions.
- Operator-related malfunctions.
- Roadway infrastructure malfunctions.
- Nonroadway infrastructure malfunctions.
- Intrusion of non-AHS vehicles and objects.

The malfunctions identified in this task will further be categorized according to the following degrees of severity:

- Warning — not currently a threat. This is an indication that the system detects a potential problem.
- Serious — action required. This is an indication of a malfunction that must be responded to within a certain time period.
- Critical — immediate action required. This category of malfunction must be responded to immediately.

The assignment of malfunctions to one of these categories is based on the perception of the speed with which the AHS must react to the malfunction in order to prevent a large impact to either the safety or performance of the system.

Vehicle Malfunctions

A malfunction of a vehicle on an AHS roadway, whether one that causes a complete stoppage of the vehicle or results in degraded performance of the vehicle, has the potential of significant local disruption to the AHS. These malfunctions are separated into two categories: 1) general malfunctions of vehicle equipment not specifically required for AHS operation, and 2) malfunctions

of vehicle equipment specific to AHS operation. A summary of these malfunctions appears in tables 1 and 2.

Table 1. General Vehicle Malfunctions

Category	System or Element	Malfunction
Critical	Brakes	Full On, Full Off needed for control
	Engine	Inoperable, not running
	Fuel Flow	Full Off, no fuel flow
	Steering	Stuck in place Unstable, no control
	Tire	Blown/wheel falls off
	Transmission	Inoperable, no power transfer
Serious	Brakes	Full Off not needed for control
	Engine	Operable degraded
	Fuel Flow	Full On, throttle stuck or unstable
	Steering	Operable degraded
	Tire	Very low pressure
	Transmission	Operable degraded
Warning	Brakes	Detects pre-fail condition
	Engine	Detects pre-fail condition
	Fuel Flow	Detects pre-fail condition, Low fuel level
	Steering	Detects pre-fail condition
	Tire	Low pressure
	Transmission	Detects pre-fail condition

Table 2. AHS-Specific Vehicle Malfunctions

Category	System or Element	Malfunction	RSC
Critical	Collision Avoidance	Failure	3
	Communication, Vehicle to Roadside	Failure/Major degradation	1,3
	Communication, Vehicle to Vehicle	Failure/Major degradation	2
	Lateral Control Computer	Failure, redundancy exhausted	2,3
	Lateral Measurement	Steering angle, lateral position sensor failures	2,3
	Longitudinal Control Computer	Failure, redundancy exhausted	2,3
	Longitudinal Measurement	Position sensing failure	2,3
	Power Failure	Total loss of electrical power	All
Serious	Collision Avoidance	Failure, critical if obstruction exists	1
	Communication, Vehicle to Roadside	Failure/Major degradation	2
	Communication, Vehicle to Vehicle	Degraded, usable	2
	Display/Keyboard	Failure	All
	Lateral Control Computer	Failure, Fault tolerant	2,3
	Lateral Measurement	Rate and acceleration sensor failure	2,3
	Longitudinal Control Computer	Failure, Fault tolerant	2,3
	Longitudinal Measurement	Velocity, acceleration sensor failure	2,3
	Position/Navigation	Receiver failure	2,3
	Power Failure	Failure of alternator or battery	All
Warning	Collision Avoidance	Detects pre-fail condition	1,3
	Communication, Vehicle to Roadside	Detects pre-fail condition	All
	Communication, Vehicle to Vehicle	Detects pre-fail condition	2
	Display/Keyboard	Detects pre-fail condition	All
	Lateral Control Computer	Detects pre-fail condition	2,3
	Lateral Measurement	Detects pre-fail condition	2,3
	Longitudinal Control Computer	Detects pre-fail condition	2,3
	Longitudinal Measurement	Detects pre-fail condition	2,3
	Position/Navigation	Reception degradation Detects pre-fail condition	2,3
	Power Failure	Detects pre-fail condition	All

General Vehicle Malfunctions

This category of vehicle malfunction is that referred to in the preceding paragraph as applying to all vehicles whether or not intended for AHS operation. The malfunctions belonging to this category affect all RSC's.

Engine Malfunctions

Engine malfunctions will be considered in three classifications: 1) complete failure resulting in a shut down of the engine — this will be classified as a critical malfunction because of the potential blockage of the AHS highway and degrading effect on steering and braking capability, 2) degraded performance in which the engine is still performing but not within the safety/ operational parameters required for the AHS — this will be classified as a serious malfunction because of the potential impact on vehicles in the immediate vicinity, and 3) the engine performance is within required parameters but an indication of an impending failure has been received — this is classified as a warning malfunction as there is no immediate impact on the AHS.

Transmission Malfunctions

A transmission malfunction will have many of the same effects as an engine malfunction, except that the braking and steering functions are not likely to be affected. The malfunctions considered are those in which the transmission a) is incapable of transmitting power to the drive wheels — a critical malfunction, b) is operational but not within AHS requirements — a serious malfunction, or c) a predicted impending failure exists — a warning. These malfunctions are rated the same as the engine malfunctions for the same reasons.

Brake Malfunctions

Braking malfunctions considered will be a) complete loss of braking when the brakes are needed immediately for longitudinal control — this is considered as a critical malfunction, b) complete loss of braking when the brakes are not needed immediately for longitudinal control — this is considered to be a serious malfunction, c) brakes failed full on — this is considered to be a critical malfunction, d) degraded braking outside the limits allowed by AHS requirements — also a serious malfunction, and e) impending brake failure is detected — which is a warning malfunction.

Steering Malfunctions

The types of steering malfunctions are 1) the steering locks in position and is not able to be moved — a critical malfunction, 2) the steering is unstable, not controllable to the requirements of the AHS — also a critical malfunction, 3) the steering is operable but degraded — a serious malfunction, and 4) a notice of impending failure is received — a warning malfunction.

Tire Malfunctions

Tire malfunctions are 1) the tire has blown — which is a critical malfunction, 2) the wheel has fallen off — which is also a critical malfunction, 3) low tire pressure has been detected — this could be categorized as serious if the pressure were deemed to be so low as to affect control or to jeopardize the near future safety of the tire, or merely as a warning.

Fuel Flow Malfunctions

Malfunctions associated with the fuel flow are: 1) throttle is full off/no fuel flow/fuel supply is exhausted — this is a critical malfunction akin to engine failure, 2) the throttle is full on or otherwise not controllable within requirements — this is a serious malfunction, though full throttle braking systems are designed to stop a vehicle and thus control exists, and 3) low fuel is detected — or an impending failure is detected, this is a warning malfunction.

AHS-specific Vehicle Malfunctions

AHS-required functionality indicates the use of certain vehicle subsystems. This category refers to malfunctions in those vehicle subsystems. Not all of the subsystems or functions addressed here are required in all of the RSC's, but all are required in one or more of RSC's. The indication of which subsystem or function is required in which RSC is noted in table 2. For a definition of the RSC's see the Contract Overview Report submitted by Delco Systems Operations.

Vehicle-to-Roadside Communication Malfunctions

A complete failure of communication or degradation of communication below acceptable levels is deemed to be a critical malfunction in RSC 1 as all control commands emanate from the roadside, it is also a critical malfunction for RSC 3 as required longitudinal position data are received from the roadside as well as lane change and emergency maneuver notices. For

RSC 2 this malfunction could be critical if the failure is with the platoon lead vehicle as spacing, lane change, and emergency maneuver notices are sent to the lead vehicle for communication to the rest of the platoon. This malfunction will be classified as serious for a non-lead vehicle in the platoon for RSC 2 as presumably vehicle-to-roadside communication will be or can be routed through the lead vehicle and the vehicle with the communications failure may not soon be a lead vehicle. A malfunction which renders communication degraded but usable is a serious malfunction in all RSC's. Detection of an impending communication failure will be classed as a warning.

Vehicle-to-Vehicle Communication Malfunctions

Malfunctions here are an issue for RSC 2 only. Complete failure or degradation of transceiver performance below a level needed for AHS operation is classed as a critical malfunction as this function is required to derive and communicate headway spacing (both inter- and intra-platoon), platoon speed, and platoon maneuver notices. Malfunctions resulting in degraded but usable communications are classed as serious. Detection of impending transceiver failure is classed as a warning.

Lateral Measurement Malfunctions

The failure of steering angle sensing, and lateral position sensing (magnetometers for RSC 2, visual lane sensors for RSC 3) which are needed for lateral control are critical malfunctions. Failure of yaw rate and acceleration sensors is a serious malfunction as presumably estimates from position data can be made for a degraded control mode. A warning malfunction exists if an indication of impending failure is detected.

Longitudinal Measurement Malfunctions

Failures of on-vehicle position sensing is a critical malfunction, or if velocity and acceleration sensors are functioning and these can be used to derive position then position sensor failure will be considered as a serious malfunction. Malfunction of the longitudinal velocity and acceleration sensors is a serious malfunction as estimates of velocity and acceleration derived from position data can be made available for degraded control. A warning exists if there is an indication of impending failure.

Lateral and Longitudinal Control Computer Malfunctions

Computer malfunctions will be considered as a) critical malfunctions in the event that fault-tolerance, i.e., protective redundancy, does not exist or has been exhausted, or b) as serious malfunctions where fault-tolerance exists and thus continued operation, perhaps degraded, is possible.

Position/Navigation Malfunctions

Malfunction of the Position/Navigation function is an issue for RSC's 2 and 3. Periodic position updates to vehicle position are provided from GPS or from wayside position transponders which are interrogated by the vehicle. Failure in ability to receive updated position data is categorized as a serious malfunction in RSC 2 since provision is made for other vehicles in the platoon to transmit accurate position data to any vehicle which has lost the capability to determine its own position. Updates to RSC 3 position data, whether from GPS or wayside transponders, is needed approximately each 1 kilometer, thus reception failure here will also be categorized as serious. Degradation of GPS position quality, which is commonly reported by the GPS receiver, will be classed as a warning.

Displays/Keyboards

This is the human/AHS interface. At some point the vehicle occupants must have communication with the AHS to express desires, request information, or receive information and advisories. This will be classed as a serious malfunction if there is a failure or a warning if a pre-fail condition is detected.

Collision Avoidance Malfunctions

The purpose of collision avoidance is to detect and avoid objects in the roadway and, for RSC 1, it may also provide a backup for headway spacing. For RSC 1 a failure is classified as a serious malfunction in the case where no obstructions are in the roadway in the near vicinity of the malfunctioning vehicle, otherwise, it is a critical malfunction. RSC 3 collision avoidance is based on the vision system used for lane following so a failure in collision avoidance could very well be equivalent to lateral measurement malfunction and is classified as a critical malfunction. A pre-fail indication in any of the RSC's will be classified as a warning.

Power Failure

Complete loss of electrical power is a critical malfunction with potential loss of all control. For RSC 3, if the vision based lane keeping system relies on vehicle lights to illuminate lane lines at night, a power loss or anything which causes light loss at night is a critical malfunction. Alternator failure or battery failure not resulting in total electrical power loss is a serious malfunction. Detected alternator or battery degradation is a warning.

Operator-related Malfunctions

The only identified malfunction attributable to the operator is not being able to assume manual control of the vehicle when required. This is considered to be a critical malfunction if an immediate response from the operator is needed as part of some malfunction management strategy, or this is considered to be a serious malfunction where the request for verification of ability to resume manual control is made well in advance of the time when resumption of manual control is required, e.g., in preparation for exit.

Roadway Infrastructure Malfunctions

Infrastructure malfunction or failures occur for various reasons. There are critical failures, usually resulting from a natural event such as an earthquake or flood. Human subversion can also be a cause of a critical failure of freeway infrastructure, however this is fairly rare in occurrence. Noncritical failures of freeway infrastructure are much more common and can be the result of either a single independent event or normal wear and tear effects of repeated use. Infrastructure failures for freeways can be grouped into three main areas: Roadside Barriers, Pavements, and Bridges. Table 3 lists the malfunctions associated with the roadway infrastructure.

Table 3. Roadway Infrastructure Malfunctions

Category	Element	Malfunction
Critical	Bridges	Not traversable, closed
	Pavements	Not traversable
	Roadside Barriers	Shifts into AHS traffic lane
Serious	Bridges	Traversable, below performance standard
	Pavements	Traversable, below performance standard
	Roadside Barriers	Shifted, deformed
Warning	Bridges	Pre-fail deterioration detected
	Pavements	Pre-fail deterioration detected
	Roadside Barriers	Pre-fail deterioration detected

Roadside Barriers

A roadside barrier is a longitudinal barrier used to shield motorists from natural or manmade hazards located along either side of the roadway. Failure of a barrier is typically noncritical in nature unless the barrier encroaches into the AHS traffic lanes, perhaps due to impact or earthquake. Noncritical failures include degradation of barrier materials due to settlement of the barrier system, expansion and contraction of materials, corrosion, or impact.

Pavements

Pavement failure is defined as a pavement section that does not meet the pavement performance parameters established for the section. In extreme cases, roadways may become untraversable due to pavement distress, this is a critical malfunction. However, a pavement that has “failed” may still be traversable and used by traffic in a degraded mode, this is a noncritical malfunction. Failure criteria for flexible pavements are fatigue cracking, rutting or permanent deformation, and thermal cracking. Failure criteria for rigid pavements are fatigue cracking, pumping or erosion, and rideability. These distress types generally result in rough riding pavements: loss in pavement coefficient of friction, which therefore reduces traveling speeds; and possible lateral control problems.

Bridges

Failures of bridges can be either critical, meaning complete closure of the structure to one or more lanes of traffic; or noncritical, meaning the structure is still traversable, but not at the loads or the travel speeds for which it was designed. Earthquakes and floods pose the greatest threats that could cause the critical failure of a structure. Noncritical malfunctions may be due to settlement of the structure; joint displacement at the abutments; wearing down of the surface of the deck, resulting in polished aggregates which results in a reduction of surface friction; and vehicle impacts which damage the superstructure of the bridge.

Nonroadway Infrastructure Malfunctions

This set of malfunctions consists of all infrastructure components not related to the roadway itself, including roadway electronics, roadway sensors and roadway communications devices which are required for AHS operation. Table 4 lists the malfunctions associated with the non-roadway infrastructure. These malfunctions are categorized as critical, serious, or warning and the RSC's associated with each malfunction are listed.

Sensor Failure Malfunctions

Infrastructure sensors may include roadside radar, infrared, or acoustic devices which can be used to detect obstacles in the roadway and to determine vehicle position and velocity. For RSC 1 and RSC 3, roadside sensors are the primary method for measuring vehicle speed and headway. The failure of a single sensor can be accommodated by placing the sensors at intervals such that range of the sensors overlap allowing adjacent sensors to provide coverage for the area affected by a failure. This is considered a serious malfunction since only one sensor is providing coverage following a failure. The failure of two adjacent sensors is considered a critical failure since there will be a loss of coverage for some section of the highway.

The sensors used for AHS are assumed to have some method of self-test. If the self-test mechanism in the sensors can detect a pre-fail condition, that condition will generate a warning. Maintenance personnel can then replace or repair the sensor before it fails. The primary sensors for RSC 2 will reside on the vehicle. Auxiliary sensors will be placed on the roadway in situations where the roadway grade or curvature prevents the vehicle equipment from sensing a safe distance ahead. The failure of an auxiliary sensor is considered a serious

malfunction. The vehicles may have to slow down in order to compensate for the loss of the infrastructure sensors, but the AHS will remain operational.

Table 4. Nonroadway Infrastructure Malfunctions

Category	Element or System	Malfunction	RSC
Critical	Power	Failure — no standby power available	1, 3
	Roadside processor	Failure — redundancy exhausted	1, 3
	Sensor	Failure — redundancy exhausted	1, 3
	Vehicle-Roadside communications	Failure	1, 3
Serious	Auxiliary sensor	Failure (for curves and grades)	2
	Power	Failure — no standby power available	2
	Power	Failure — standby power available	All
	Roadside processor	Failure — adjacent processors available	1,3
	Roadside processor	Failure — redundancy exhausted	2
	Sensor	Failure — adjacent sensors available	1, 3
	Vehicle-Roadside communications	Failure	2
	Vehicle-Roadside communications	Degradation	All
Warning	Roadside processor	Detects pre-fail condition	All
	Sensor	Detects pre-fail condition	All
	Vehicle-Roadside communications	Detects pre-fail condition	All

Power Failure Malfunctions

The loss of power to infrastructure electronics is considered a critical malfunction for RSC 1 and RSC 3. For these RSC's, the AHS will be completely shut down until power can be restored. If backup power is available, the loss of primary power for RSC 1 and RSC 3 is considered a serious malfunction. The AHS will remain operational on standby power, but maintenance crews must respond immediately to restore primary power.

For RSC 2, the infrastructure will provide advance roadway information to the platoon leader for the purpose of adjusting speed in anticipation of an obstacle or congestion in the roadway ahead or road surface information. The loss of primary power is considered a serious (rather than critical) malfunction for RSC 2, since it will not result in a complete shutdown of AHS. The AHS vehicles will lose their ability to receive advance roadway condition information from the infrastructure, which will cause a reduction in the speed of the AHS lanes.

Vehicle-Roadside Communications Malfunctions

This category of malfunctions is covered in the AHS-specific Vehicle Malfunctions section.

Roadside Processor Malfunctions

In RSC 1, the roadside processor is responsible for performing the control loop calculations for each vehicle within its area of responsibility. The placement of the processors will be determined by the number of vehicles that each processor can handle concurrently. Roadside processors will be spaced at intervals which allow adjacent processors to take over the functions of a failed processor. A malfunction of a roadside processor in RSC 1 is considered serious if adjacent processors are able to take over, and critical if there is currently no backup available. Similarly, the roadside processors in RSC 3 maintain the time-space slots for each AHS vehicle. The spacing of these processors in the infrastructure will allow for redundancy as in RSC 1. Malfunctions are considered serious if adjacent processors are available and critical if adjacent processors are not available. For RSC 2, the roadside processors will be responsible for overall management of a large section of the AHS. The failure of a roadside processor may result in a speed reduction for the section of highway, but the vehicles will retain the ability to function. This is considered a serious malfunction.

Intrusion of Non-AHS Vehicles and Objects

The major events that must be considered are: unauthorized entry of non-AHS vehicles and debris from incidents in the non-AHS lanes. While these events may not result in a failure of any particular AHS component, it is presumed that the AHS is designed to preclude both of these events and, thus, their occurrence can be considered to be a malfunction. Both of these events must be considered critical due to the potential for accidents occurring.

Task 2. Define Malfunction Detection Techniques

The capability to ensure error-free operation of the AHS dictates that equipment malfunctions be prevented or detected in a timely manner to minimize the impact on safe operation of the automated lanes. This task considers the techniques and methods of detecting the malfunctions identified in the previous task. These techniques and methods will be discussed in the same order as the malfunctions of task 1:

- Vehicle malfunction detection.
- Operator-related malfunction detection.
- Roadway infrastructure malfunction detection.
- Nonroadway infrastructure malfunction detection.

Vehicle Malfunction Detection

In modern vehicles, operation of engine, transmission, and fuel functions are monitored by engine control computers and transmission control computers, or an integrated version of these two computers known as a powertrain control module (PCM). Anti-lock brake systems, traction control, variable effort power steering, and adaptive suspension systems are also under computer control. In all of these present day vehicle controllers a considerable amount of malfunction detection capability exists. It is estimated by some sources that 60 percent of the total on-vehicle computing power is devoted to malfunction detection — either of the computers themselves or of the sensors and actuators with which the computers communicate. As AHS is implemented it will be necessary to expand the number of computers or at least expand the computing power resident on the AHS vehicles (or in the infrastructure electronics, depending on the RSC) to include longitudinal control (throttle and brake control) and lateral control (steering control). It will also be necessary to expand the malfunction detection capabilities along with this added computing power. A good example of the direction of future malfunction detection capabilities is that mandated by the California Air Resources Board (CARB) second generation on-board diagnostics (OBD-II) for vehicles of model year 1994. This legislation requires that many of the tasks previously performed by a service bay computer be incorporated in on-board processors to provide continuous, real-time diagnostics under a much wider variety of conditions. In implementing the requirements of OBD-II, a side-benefit applicable to AHS has been reported by some automotive engineers. In addition to the emissions control system malfunctions, which is the primary focus of OBD-II, many powertrain malfunctions can be detected and identified. The current method for

reviewing these PCM malfunction codes is to go to a service facility which has equipment to down-load the malfunction codes that have been stored in the PCM. However, for AHS application there is nothing to preclude the transmission of the malfunction codes to wayside receivers at check-in time or as the vehicle is traveling the AHS lanes.[1]

A literature review of research directed to vehicle fault detection shows extensive activity by researchers in the automobile industry and at various universities. Most of the research reviewed for this study has been done within the past five years.

At another automobile manufacturer a technology that is receiving much attention for application to automotive malfunction detection is Artificial Neural Systems, or Neural Networks. Neural networks have been utilized as trainable pattern classifiers to recognize an extensive set of faults in operating engines from an analysis of the data exchanged between the engine and its controller. In this manner neural networks can be employed as on-board real-time diagnostic systems whose task is to recognize and flag a system malfunction and then to identify the root cause of the malfunction.[2]

In other investigations of vehicle malfunction detection, researchers at a university have shown that, rather than use redundant sensors to determine the validity of the measured output of a control function, a method of analytical redundancy is possible. It is shown using this method that if there are three different quantities to be measured “the basic idea is to build three observers, each of which uses two out of three measurements ... and if one of the sensors fails the error output of only one of the observers will be zero. Thus by knowing which error output is zero and which is not one can identify the faulty sensor.”[3] At another university, research on automobile fault detection has developed and applied a method in which “the fault detection filter is developed to take into account both sensor and actuator faults.”[4]

Research at a well-known automotive research laboratory on detection and diagnosis of sensor failure for on-board vehicle applications has shown in simulation that certain types of sensor failure can be correctly diagnosed within 50 ms. The types of sensor failures considered are: sensor sticking, sensor disconnection, sensor bias, and increased measurement noise. The method can also be utilized for actuator failures and structural system failures.[5]

An interesting concept that is being introduced into manufacturing processes is that of “smart sensors” and “smart actuators”. These sensors and actuators, with on-board intelligence and connected by a bus network, have the capability to monitor processes, communicate with each

other and a central controller, perform self-monitoring of malfunctions, and react to detected malfunctions. The developers of the concept see automobiles as a prime target of the technology because of the current proliferation of sensors and computer control.[6]

General Vehicle Malfunctions

The malfunctions identified in this category in task 1 are those related to powertrain (engine, transmission, and fuel flow), brakes, steering, and tires.

Powertrain Malfunctions

Table 5 shows some of the monitoring functions of a PCM. It should be noted that the focus of the CARB OBD-II requirements, and the main purpose of the PCM data monitoring capabilities, is to improve detection of malfunctions of the vehicle emission controls. This is certain to remain a high priority item. Given the monitoring capabilities shown in this table it appears that nearly all powertrain malfunctions listed in table 1 can be detected by the PCM malfunction detection capability; in addition, engine knock and misfires are derived from this data. An exception to this is the low fuel condition which can be easily detected even with present-day fuel level sensors. A more accurate method of measuring available fuel is to assume maximum fuel availability at fill-up and then monitor fuel usage. Additionally, conversations with automobile company researchers indicate that oil quality monitors continue to be developed which could provide additional pre-failure warning capability in conjunction with the sensors already present on the PCM.

The PCM also performs diagnostics to detect malfunctions of the sensors from which the above data are obtained. These diagnostics include:

- Response / switching times.
- Commanded versus measured states.
- Open/short/intermittent tests.
- Out of range test.
- Rationality/input signal consistency check.
- Circuit continuity check.
- Time in state.

- Time to activate.
- Periodic dynamic tests.
- Illegal switch combinations.

Table 5. PCM Monitored Data

Powertrain component	Data Monitored
Engine	Battery voltage Engine coolant level and temperature Engine load Engine speed Manifold pressure Oil level and pressure Spark timing Vehicle speed
Transmission	Shift solenoids Torque converter clutch (engage state) Torque converter control solenoid Transmission fluid temperature Transmission input speed Transmission output speed
Fuel	Fuel flow Mass Air Flow Throttle position

Brakes

Electronic braking, referred to as brake-by-wire, not only is an enabling technology for AHS, but, in the opinion of brake system designers, allows periodic end-to-end testing of the braking system except for possibly pressure to the brake pads. Since application of pressure to the brake pads will be done frequently while driving, this final part of the dynamic test can be performed at that time. Each time the brakes are applied braking performance can be

compared to expected performance by the longitudinal control computer. Enhanced capabilities are largely dependent on direct pressure measurements, which are not presently made but are a likely enhancement independent of AHS development. Monitoring wheel speed would also provide an end-to-end check on brake performance. Additional sensors that may be needed for a hydraulic brake system are those to measure brake fluid level and temperature.

Detection of brake pad wear in U.S. made vehicles generally relies on a mechanical feeler which provides an audible notification to the operator of excessive wear. For purposes of the AHS it could be desirable to use the European model of an embedded electronic wear sensor that can send a signal to the longitudinal controller or some other computer so that excessive wear cannot be ignored by the operator as is often done with the present U.S. made systems. However, an audio pickup at check-in could be designed to detect the present wear indicator. The detection of excessive brake pad wear could be done exclusively as a check-in test as brake pad wear during one AHS trip would not likely be great.

Brake master cylinders are mechanically redundant in that there are two circuits, each providing brake pressure to a front wheel and a diagonal rear wheel. One brake controller designed for use in commercial vehicles (BOSCH) incorporates two redundant microprocessors controlling each diagonal (front wheel and opposite side rear wheel), with each microprocessor of the pair receiving the same inputs. A constant self-test of RAM, ROM, and accumulators is performed and a watch-dog timer is used to keep track of processing times. Also, wheel speed sensor electronics are monitored for shorts and opens, and in the pressure modulating valves the voltage and current are measured and compared to permissible values. The air gap between sensor and pulse wheel is checked through software monitoring.

Tires

Both direct and indirect indicators of tire pressure loss are possible. Inflation monitors which have been developed, or are being developed for high-end vehicles provide a way of detecting pressure-related tire malfunctions. One of these consists of a module in each wheel containing a sealed pressure sensor with a radio transmitter that signals a receiver when the air pressure drops. This sort of monitoring of tire pressure is currently used with the new generation of run-flat tires. These tires, having thicker, stronger sidewalls than conventional tires, give little visual indication of low pressure and thus need the pressure loss indicator.

Also, ABS wheel speed sensors can be used to determine relative wheel radius and thus deduce low inflation pressures.

Steering

Monitoring of hydraulic pressure and fluid levels can be done if power steering is implemented as at present, although conversations with automotive engineers suggest that electronic steering (steer-by-wire) is likely to be implemented with electric power steering rather than with hydraulic power steering. Failures which result in the steering locking in a single position or result in unstable steering, wherein the vehicle wanders about the desired path, can be detected by the lateral controller monitoring the control error signal. Steering sensors can be monitored using the same methodologies used to monitor engine and transmission sensors by the PCM. The analytical redundancy methods referred to in the opening paragraphs of this task were developed using sensors associated with steering.

AHS Vehicle Malfunctions

The malfunctions identified in this category in task 1 are those related to communication (both vehicle-roadside and vehicle-vehicle), lateral and longitudinal measurement, lateral and longitudinal control computers, display/keyboard, collision avoidance, and power failure.

Communication

Two standard methods are available for performing dynamic testing of communications. One is 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 as a malfunction. The second is a self-test technique known as a loop back test in which a message is fed directly from the unit transmitter to the receiver and a comparison made between the transmitted message and the loop back reception. Loop back tests are often used for fault isolation by looping the signal back at various points in the system. Combining this with a self-test of the processors within the communication system allows a complete fault isolation test to be performed. The transmission of pre-defined test patterns will use a portion of the bandwidth which would otherwise be available for transmission of data. Also, the more frequently a test message is transmitted, the more bandwidth will be used. 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.

Collision Avoidance

If the ranging equipment is radar, periodic tests to determine amplitude and Doppler sensitivity of the system are desirable using targets of known cross-section. One radar which is being used in a military collision avoidance application has implemented a built-in test method similar in nature to the communication loop back test. The output signal from the transmit channel, instead of being sent out of the transmit antenna, is periodically injected through a delay line into the receive channel, producing a target of known characteristics from which calibration can be performed and radar performance can be monitored. Image processing circuitry can be designed to include built-in test functionality, the RF portion can incorporate power sensors in the receiver path to detect correct signal levels, and the transmit path can include detection of local oscillator frequencies to verify functionality. Detection of malfunctions in the processor itself can be done using the methods noted under lateral and longitudinal controllers.

Lateral and Longitudinal Measurement

It is expected that detection of malfunctions of the sensors which are associated with the lateral and longitudinal control function such as accelerometers, yaw rate sensors, steering angle sensors, and magnetometers will be accomplished in essentially the same way as those noted in the discussion of the vehicle PCM capabilities. Actuator malfunctions which result in stuck-at or unstable conditions can also be detected by monitoring the control error signal by the lateral and longitudinal controllers. Detection of malfunctions of longitudinal measurements derived through cooperative ranging using vehicle-vehicle communications is done as noted in the communications paragraph and detection of malfunctions when longitudinal measurements are derived through use of radar is discussed in the paragraph on collision avoidance. Modern video cameras incorporate self-test of the processing electronics as part of the power-on cycle. The sensor arrays can be functionally tested using known images, but this must be performed prior to on-line performance on the automated lanes. Real-time monitoring can be implemented by sampling the output of the sensor periodically to verify that a signal is present and in an acceptable range. This test capability can be designed as part of the subsystem malfunction detection process during normal operation of the unit. Combined with programmable self-test of the processors, difficulties associated with alignment or obscuration that could occur en route may be detected.

Control Computers

The health of the processors required to implement the AHS functions may be monitored via Built-in Test (BIT). BIT may include exercise of the instruction set including an illegal instruction test, watchdog timers to monitor excessive processing times, memory protect test to verify integrity of protected memory, detection of attempted access of illegal addresses, program memory check sum to verify program integrity, RAM pattern test to identify faulty RAM, and monitoring of power supply current/voltage, clocks, and memory write circuits. Integrity of internal data can be verified by implementing parity checks and wrap-around tests. Other methods which allow malfunction detection, such as dual redundancy of processors with comparison, or triple redundancy of processors with data exchange and majority voting, are usually implemented in response to reliability and safety issues. A number of control subsystems in the vehicle may be connected by a bus architecture. The bus, along with its protocol, must be capable of detecting and correcting data transmission errors. A common technique is to employ error detection and correction schemes in either the hardware of the bus itself or the software protocol. These approaches are routinely used in military and space applications but seldom in automotive applications due to the extreme pressure to maintain competitive costs. A careful analysis must be done to determine which of these methods are required to achieve the reliability goals of AHS.

Position/Navigation

For methods using GPS to update position data, present day GPS receivers have the capability to monitor and report on the acquisition of the required satellite signals and to measure the quality of the signals. The receiver's microprocessor undergoes the standard internal tests, output ports are tested, and output data is checked for errors. Several key functions of GPS receivers are compatible with self-test. Among the parameters which may be tested are the position accuracy, signal lock, and signal strength. The ability to measure relative signal strength may be used to determine when a vehicle is entering a shadowed area that has insufficient view of GPS satellites. The ability of the phase-lock loop (PLL) circuitry to track signals from several satellites on multiple channels decreases the time required to accurately determine position. Signal lock is easily detected and can be used with appropriate decision criteria to determine when a receiver is functioning properly. Position accuracy is important in applications requiring close vehicle spacing, and can be verified by checking against stored navigation information such as a map data base or against parallel measurements from an alternate device such as wheel speed sensors. The self-test capability of GPS receivers is still

being developed, but is expected to support the needs of AHS due to the proliferation of programmable units with serial interfaces. A GPS receiver selected to perform safety critical vehicle control functions must have sufficient self-test capability to ensure reliable operation.

Displays/Keyboard

Tests of the keyboards, displays, and other data interchange devices are typically initiated as part of the power-on sequence. The user may be an integral part of the test and may be required to press keys or touch screens to prompt the system to accept test results. A test pattern may be displayed and the user prompted to read the display and respond to a query. The system may provide feedback to the operator when an entry is made for verification of the entry. Errors between intended input and the interpretation by the system will indicate that the data entry unit has malfunctioned. On-line testing of the display is possible, however it may be best to perform real-time tests while the system has automated control of the vehicle to avoid work overload of the user while the driver has manual control or is transitioning to automated control.

Power Failure

Monitoring of on-vehicle battery condition and/or alternator performance has long been implemented on motor vehicles, usually enabling notification of degraded performance well in advance of any major failure. It is likely that monitoring battery and alternator performance must be automated, which is presently not the case.

Operator-Related Malfunction Detection

If the operator is required to assume control of some or all of the vehicle functions as part of a malfunction management strategy there must be periodic checks on operator attentiveness and capability to respond to system prompts. This test could be coordinated with the test of the display/keyboard tests referred to in the AHS Vehicle Malfunction section. The operator may be required to press keys or touch screens to acknowledge readiness. This kind of test may be in conflict with the desire to provide the operator with the ultimate “sit back and relax” driving experience. While some degree of “sit back and relax” may be possible, some attentiveness is still required. An additional check for operator readiness would be an indication that the operator is seated with the seat belt fastened.

A related issue is that of the operator as a malfunction detector. In present day manual operation of vehicles the operator serves as a malfunction detector, using the senses of sight, hearing, touch, and smell. The operator observes road conditions and vehicle gauges with the sense of sight, listens to engine, transmission, and tire sounds with the sense of hearing, feels vehicle movement and vibrations with the sense of touch, and further observes vehicle conditions with the sense of smell. This capability could, and probably should, be utilized even in the automated operation mode and argues for an alert, capable operator. Capabilities should be provided for the operator to communicate to the AHS any observed malfunctions and desired reactions to the malfunctions, e.g., a desire to exit the AHS as soon as possible.

Roadway Infrastructure Malfunction Detection

Current failure detection methods of roadway infrastructure components may evolve into a continual monitoring of key elements of the infrastructure so as to prevent failures from occurring or to detect an actual failure. The detection methods described in the following paragraphs can be implemented as totally automated, continuously monitored functions, or remain as presently implemented — periodic inspections by humans. Since most failures of roadway components are gradual in nature, the automation of detection of such failures would be motivated only by reduced cost, inaccessibility to routine inspection by humans, or reduced impact on AHS operation. Sudden failures, such as those resulting from an impact by a vehicle, would likely be reported by the impacting vehicle or infrastructure position determination function. Detection of failures can be discussed in the following groups: roadside barriers, pavements, bridges, and drainage features of freeways.

Roadside Barriers

Techniques for detecting roadside barrier failures can be categorized into two groups: gradual failure and sudden failure.

Gradual Failure

Gradual failures can be detected by either continual monitoring of certain key contributors, regular visual inspections, user notification or a combination of all these items. Key contributors to gradual failure include: differential settlement, expansion, contraction, and corrosion. Settlement monitoring could be achieved by installation of settlement gauges. Fatigue caused by expansion/contraction could be monitored by strain gauges at expansion joints and correlated to temperature readings. Corrosion of steel members can be determined

by ultrasonic techniques. Due to cost considerations these techniques may not be conducive to monitoring of the whole barrier system, but rather to monitoring at select test locations. It is also noted that regular visual inspections of these barriers along with user notification of potential failures is also a viable gradual failure detection technique.

Sudden Failure

Sudden failures of roadway barrier systems occur when vehicles impact barriers at large approach angles. Generally, after such an impact, barriers must be inspected and replaced as required. Traditional methods of detection of failed barriers include user notification or observations at the scene of accidents. Impacts on barriers can be sensed by impact sensing equipment that would need to be built into the entire length of barriers. Once an impact is detected, visual inspection of the barrier system would be required in order to determine if the barrier system needed repair or replacement.

Pavements

Failed pavements generally result in poor rideability and/or reduced coefficient of friction but can still be traversed by vehicular traffic if adjustments are made for speed. Malfunctions in pavements generally occur gradually over a relatively long period of time and are caused by a variety of contributors as previously discussed. Detection of these contributors will enable timely, appropriate maintenance actions to prevent pavement failures. Based on the above discussion, two strategies for pavement failure detection are discussed: vehicle-based detection and infrastructure-based detection.

Vehicle-Based Detection

Drivers of traditional vehicles adjust speed for various situations resulting from malfunctions in pavement. Vehicles equipped to use AHS lanes, or the AHS infrastructure, should have sensing equipment to make adjustments to speed and spacing in platoons accordingly. This sensing equipment should be able to determine changes in coefficient of friction resulting from bleeding of asphalt, oil accumulation and presence of excess water on the pavement. Detection of pavement rutting could be sensed by resistance to turning as the vehicle turns out of the ruts in the pavement. Vehicle detection of pavement malfunctions will provide continuous monitoring of surface conditions of pavements. Spire Corporation, Bedford, MA, has been awarded a contract for development of indium phosphide-based heterojunction bipolar transistors (HBT's) for millimeter wave applications. This also will involve

development of new metalorganic chemical vapor deposition growth and characterization processes specifically tailored for InP HBT structures. It is anticipated that this research will ultimately lead to an InP-based HBT technology capable of producing high-performance devices for insertion into millimeter-wave imaging radiometers and passive interferometers for guidance and detection. According to Spire researchers, this technology not only has application to collision avoidance systems with improved aperture size and operation under such adverse weather conditions as dust, fog, or smoke; but, placed in vehicle side mirrors, can address the problem of blind spots and also can provide advance warning of road conditions such as ice, oil, and the like.

There is also existing equipment that could be mounted on either special service vehicles or trailers and used to assess pavement condition. The automatic gathering of pavement features and pavement distress types by periodically traversing sections of the AHS with these special vehicles traveling with the regular flow of traffic would allow gathering of the necessary information without closing down or otherwise affecting traffic in the AHS lane.

Video imaging equipment[7], used to gather and analyze pavement condition has been developed. For instance, rutting in asphalt pavements (depressions in the wheel paths) can be detected and measured automatically. The data is analyzed to determine the roadway profile transverse to the direction of travel by use of photo instrumentation (pulse) equipment.

Roughness data can be obtained from non-contact sensors mounted to the vehicle.[8] Surface roughness data can also be obtained through shock absorber meters or from suspension damping sensors which are part of an active suspension system. A computer is used to compare data obtained from meters attached to shock absorbers that measure displacement to maximum and minimum acceptable values. When the pavement roughness values exceed maximum values, the operating agency could schedule either maintenance or rehabilitation activities.

Profilometers may also be used to obtain pavement roughness. Profilometers use an acceler-ometer to establish an inertial reference plane from which vehicle deviations in vehicle dis-placement are measured. [9] Improvements in technology would most likely allow the installation of profilometers to AHS vehicles at reasonable costs or could be part of the special service vehicle or trailer.

Infrastructure Detection

Continuous monitoring of elements of pavement can provide early diagnosis of potential pavement failure. Measurement by in-place sensors of temperature and moisture content of bases and subbases of pavement could indicate the presence of excess water in the bases and subbases which cause pavement failure. Measuring temperature and moisture content of pavement structure would enable prediction of freeze/thaw cycles and their effect on pavement.

Early diagnosis of potential problems in pavement enables pavement structure to be repaired at low demand periods minimizing impacts on operations.

Bridges

Many components of bridges require routine monitoring to ensure that the structure is performing to meet its design parameters and hence prevent any unnecessary closures. Malfunction detection techniques applicable to bridges can be grouped into three categories: traditional monitoring, vehicle-based detection, and infrastructure-based detection.

Traditional Monitoring

Bridges generally undergo routine inspection and monitoring of bearings, expansion joints, deck condition, pier/abutment settlement, and scouring around piers. Inspection of bearings, expansion joints and decks is commonly done visually, which requires no disruption of traffic during inspection if special equipment, such as platforms, is built into the structure. Pier/abutment settlements and scouring around piers is generally monitored using survey and sounding techniques. Since these types of malfunctions are gradual failures, the traditional techniques described above are capable of providing accurate monitoring without disturbing traffic flow.

Vehicle-Based Detection

A vehicle detection system similar to that described for pavements can be used for determining surface malfunctions of bridge decks. This system could determine ride quality over expansion joints and determine if settlements are occurring at these locations.

Infrastructure-Based Detection

Detection of bridge malfunctions with in-place sensors and monitors requires many different installations at key areas of bridges. Many of the techniques described in traditional monitoring can be either partially or fully automated. Behavior of expansion joints can be predicted for various temperatures and therefore failures of expansion joints can be predicted by monitoring the temperature and the amount of expansion and comparing to predicted results. If actual results and predicted results differ significantly there could be a problem with the joint.

Placement of video cameras at all bearings on the bridge, enables constant video monitoring of bridge bearings. Video monitoring techniques could be used in underwater applications to monitor scouring around piers. Video monitoring provides early detection of problems associated with failures indicating need for specific inspection by traditional techniques.

Detection of impact damage to bridge deck elements requires capabilities similar to roadway barrier impact detection requirements. Although impacts to piers and bridge structure are extremely rare, impact sensing equipment installed at strategic locations on piers and bridge structure would provide early detection impacts allowing AHS vehicles to adjust to the situation as quickly as possible.

Drainage

Drainage systems have varying degrees of usage, i.e., the system can be heavily used at times while it can remain idle at other times. Routine monitoring of the system will ensure that, when heavy use of the system occurs, the system will operate correctly. Traditionally, monitoring of drainage systems involves routine inspection of drainage systems to ensure they are in working order. To totally automate this system would require detection sensors at every catch basin, inlet structure, and outlet structure. An early detection system, either manual or automated, should be able to detect ponding of water in ditches or swales so appropriate action can be taken to prevent this water from seeping into the pavement structure causing pavement failure.

Sudden failure occurs when heavy rain causes debris to accumulate rapidly at inlets. This type of failure can be detected either by vehicle-based detection or infrastructure-based detection. Vehicle-based detection should be able to determine excess water on the pavement

and make adjustments to vehicle operations as required. Automated infrastructure detection would require flow meters to measure the amount of inlet and outlet flow to determine if a failure exists so actions can be taken to free up the catch basin.

Nonroadway Infrastructure Malfunction Detection

All of the RSC's defined require a considerable amount of wayside electronics including sensors, processors, and communication devices. As this is true also for AHS vehicles, many of the techniques that are applicable to detecting malfunctions in the wayside electronics have been discussed in the Vehicle Malfunction section. This section presents only those additional comments and techniques which apply to the wayside electronics.

Sensors

Roadside sensors may be used for many functions including incident detection, vehicle position or velocity measurement, or gathering environmental data. Malfunction detection, including that of communication and ranging and radar-based units, is discussed in the section on AHS Vehicle

Malfunctions.

Reliability studies regarding radar subsystems such as transmitters, receivers, and logic circuits have shown that burn-in procedures greatly decrease the failure rate of fielded systems by eliminating the early failures.

Processors

Commercial off-the-shelf (COTS) microprocessors are equipped with self-test capability to verify correct operation of the control ROM, programmable logic arrays, and buffers. The self-test is commonly activated during the power-on cycle. The processors installed at the roadside may be powered on continually, and in this case the self-test must be periodically initiated by the system software during normal operation by controlling designated inputs to the unit to trigger the self-test function. Further discussion of built-in tests is found in the section on AHS Vehicle Malfunctions.

The duration of tests is a function of the processor speed and complexity. A common COTS unit operating at 16 MHz performs its self-test in 30 ms. The length of the self-test may be on

the order of the update rate for the vehicle control loop. The timing of the self-test may be an issue, since the self-test should not be allowed to preempt critical vehicle maneuvers such as emergency braking or lane changes in infrastructure-based control configurations.

Power Supply

Two types of alternating current back-up power supply approaches are available. On-line uninterruptable power supply systems (UPS) provide continuous power with no transfer time when primary power fails. Standby systems switch very quickly to battery back-up, and the switching time is usually transparent to the attached devices. The detection of power failure is an integral part of both back-up power supply approaches. The advantage of uninterruptable supplies is the line conditioning which is provided in series with the ac line power. Line conditioning eliminates voltage sags and spikes which commonly occur on ac power lines. The UPS approach may be preferable in safety-critical roadside processors and communications equipment to avoid loss of computing power or damage to devices during lightening strikes or power surges due to outages elsewhere in the utility system.

Battery powered devices will also require detection of low power conditions to allow timely replacement of primary batteries. Power conditioning circuitry associated with battery powered devices use a voltage level detection technique which generates a logic signal when low battery levels are detected. This logic signal can be used to trigger notification of the battery condition in the periodic status message of the unit. Remote units can be interrogated periodically to verify operational status and maintenance of the battery can be instigated if the low battery message is detected.

Electrical equipment is susceptible to environmental related issues such as temperature extremes, water infiltration, dust, and rodents. Periodic inspection of electrical cabinets would detect the presence of any of the above items and determine what actions would be required to eliminate these problems.

Communications

Communication required by the infrastructure electronics includes vehicle-roadside and controller-controller communication. The communication malfunction detection methods discussed in the AHS Vehicle Malfunctions section are applicable here.

Task 3. Define Malfunction Management Strategies

Defining strategies for management of the malfunctions identified in task 1 can proceed in two steps:

- Define immediate actions by each of the AHS subsystems (wayside electronics and maintenance personnel, roadway maintenance personnel, vehicle, and vehicle operator) which will remove or isolate the malfunction in the safest, least disruptive way possible.
- Define actions which allow recovery from the immediate actions of step 1, restoring the AHS to full operation.

Immediate Actions

Examination of each of the malfunctions listed in task 1 has led to the definition of five basic immediate action scenarios to be performed by the AHS subsystems. Each malfunction is identified with one of these scenarios, or one of these scenarios with some degree of variation. The baseline definition of each of the immediate action scenarios is outlined in the following paragraphs labeled as scenario A through scenario E. In the definition of each of the five scenarios reference is made to the Wayside, meaning the nonroadway infrastructure electronics and any associated maintenance personnel and any maintenance personnel associated with the roadway infrastructure. Reference is also made to the Vehicle, meaning the malfunctioning vehicle. References to the Operator are to be interpreted as the operator of the malfunctioning vehicle. The tables that accompany each of the baseline scenarios define any variations to the baseline scenario required for the individual malfunctions, identify the sources of malfunction detection, state the expected outcome of the actions, and raise issues of concern related to the management of the malfunctions.

In RSC's where access to the AHS lanes is from parallel manual lanes via a transition lane (RSC 3) the immediate action scenarios were constructed assuming that access to the AHS lanes is continuous. Therefore, to not interfere with access to the AHS lanes, it is assumed that the breakdown lane should be the farthest AHS lane from the transition lane. In the other RSC's, since access is intermittent, it is assumed that the breakdown lane is the lane adjacent to the exits. This location facilitates self-clearing of malfunctioning vehicles when possible and simplifies extraction of malfunctioning vehicles by service vehicles when required. This may be a topic for further investigation by roadway operations analysts.

Scenario A — Divert and Clear

Divert malfunctioning vehicle to breakdown lane for clearance by service vehicle or for self clearance.

Wayside:

- Clear path to breakdown lane for malfunctioning vehicle.
- Command vehicle to steer to breakdown lane and continue under own power to exit, if possible.
- Notify operators of affected vehicles of action.
- Notify service vehicle when malfunctioning vehicle must stop in breakdown lane.

Vehicle:

- Notify wayside (all RSC's) and other vehicles of malfunction (RSC 2).
- Request steer to breakdown lane and then steer to lane when permission granted.
- Proceed along breakdown lane to nearest exit if able (RSC 1, 2). Stop in breakdown lane (RSC 3, exit is to manual lanes).

Operator

- No action.

Scenario B — Emergency Braking

Insufficient mobility or controllability of vehicle to allow diversion to breakdown lane, initiate coordinated braking in lane to stop as soon as possible.

Wayside:

- Command preceding vehicles (in own and adjacent lanes) to continue.
- Command coordinated braking for malfunctioning and succeeding vehicles (in own and adjacent lanes if loss of steering).
- Notify operators of affected vehicles of actions.
- Divert following traffic around blocked areas.
- Notify service vehicles.

Vehicle:

- Notify wayside (All RSC's), other vehicles of malfunction (RSC 2).
- Initiate emergency braking (RSC 2, 3).

Operator

- No action.

Scenario C — Prompt Normal Exit

Perform normal exit of AHS at next exit with services.

Wayside:

- Alert operator that vehicle will leave AHS at next exit with services.
- Isolate malfunctioning vehicle from surrounding vehicles, increase space front and rear to provide safe stopping distance. Command vehicle to move to lane most appropriate for managing malfunctions (breakdown lane, lane adjacent to breakdown lane) in anticipation of reaching failure state.
- Initiate checkout procedure.
- Execute usual exit procedure when exit is reached.

Vehicle:

- Notify operator and wayside of warning.
- Exit when required.

Operator

- No action (RSC 1, 2).
- Under manual control (RSC 3) the operator has choice of exiting or continuing on in manual lanes, although exiting is probably the better choice.

Scenario D — Emergency Braking, Revert to Manual Control

Collision avoidance activated as backup longitudinal and lateral control, coordinated braking to stop as soon as possible in lane, followed by reversion to manual lateral control to enable self-clearing if possible.

Wayside:

- Alert neighboring vehicles/platoons.
- Command preceding vehicles (all lanes) to continue on.
- Command succeeding vehicles (all lanes) and malfunctioning vehicle to brake to stop, command coordinated braking as needed.
- Divert following traffic around blocked areas.

Vehicle:

- Collision avoidance activated for longitudinal control, revert to manual lateral control when stopped.
- Execute coordinated emergency braking until stopped.
- Alert operator of necessity to assume manual lateral control when stopped.
- Notify operator to leave AHS at next exit.

Operator:

- Assume manual control when vehicle stopped.
- Steer to breakdown lane and leave at next exit, if able.

Scenario E — Slow, Maintain Lane

Infrastructure component failure or degradation, vehicles continue in AHS lanes, slow if needed.

Wayside:

- Command vehicles in affected section of AHS to slow if needed and stay in designated lanes while in affected section.
- Maintenance personnel replace faulty items.

Vehicle:

- Slow as commanded.
- Maintain lane while in affected section, no exits allowed until out of affected section.
- Notify operator of condition.

Operator

- No action.

Table 6. Scenario A Malfunctions — Divert and Clear

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Engine	Not running	Stop in breakdown lane	PCM, longitudinal controller	Stop in breakdown lane	Braking ability with no engine power
Transmission	No power transfer	Same	Same	Same	
Fuel Flow	Off	Same	PCM	Same	
Fuel Flow	Stuck at, unstable	Same	PCM, longitudinal controller	Same	Longitudinal control maintained by brakes
Brakes	Fail off	Use throttle, transmission, weaving, parking brake to slow	Brake and longitudinal controller	In breakdown lane. Possible minor damage	Down slope control, preceding vehicles change lanes if possible
Engine	Degraded performance		PCM, longitudinal control	Exit AHS, RSC1,2. Breakdown lane, RSC 3	
Transmission	Degraded performance		Same	Same	
Steering	Degraded		Lateral control	Same as above	
Tire	Very low pressure		Tire inflation monitor, brake controller	Same as above	Run-flat tires allows exit from AHS for RSC 1,2
Tire	Blow out	Invoke special steering algorithm, coordinated braking	Same, plus lateral controller	Stop in breakdown lane	Steering algorithm available. Run-flat tires may mitigate
Vehicle-vehicle communication	Degradation, RSC 2		Communications system	Go to breakdown lane and exit	

Table 6. Scenario A Malfunctions — Divert and Clear (continued)

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Lateral Measurement	Rate or acceleration sensors fail		Lateral control	Same as above	Degraded mode with failed data derived from position data
Longitudinal Measurement	Velocity or accel-eration sensors fail		Longitudinal control	Same as above	Same
Lateral or Longitudinal Control Computer	Failure, redundant circuit exists. RSC 2,3		Lateral/Longitudinal control computer	Go to breakdown lane/transition lane and exit	
Position/ Navigation	Receiver failure		GPS self-test or communications	Same as above	
Display/Keyboard	Failure		Self-test, periodic operator action	Same as above	Notification of operator of impending actions
Collision Avoidance	Failure		Self-test	Same as above	
Power	Alternator or battery fail		Power monitors	Same as above	
Vehicle-vehicle communication	Failure. RSC 2	Collision avoidance as back-up longitudinal reference	Communications function of vehicle and surrounding vehicles	Exit AHS. Potential damage to adjacent vehicles	Communication ranging function lost
Longitudinal measurement	Failure. Position RSC 3	Revert to collision avoidance	Longitudinal control	Go to transition lane and exit	
Longitudinal control computer	Failure. RSC 2,3	Collision avoidance as backup longitudinal control	Longitudinal control	Exit AHS	

Table 6. Scenario A Malfunctions — Divert and Clear (continued)

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Vehicle-based communication with wayside RSC 2	Failure	Vehicle slows to default safe speed. Reverts to manual control when operator ready	Vehicle communications	Vehicle leaves AHS at next exit. If operator not capable, vehicle stops in lane	Operator capability to assume manual control. Manual vehicle in AHS lane
Vehicle-based communication with wayside RSC 3	Failure	Same	Same	Same	Same

Table 7. Scenario B Malfunctions — Emergency Braking

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Brakes	Fail on	To breakdown lane if in adjacent lane	Brake controller, longitudinal controller	Blocked AHS lane, possible damage	ABS allows steering control
Steering	Stuck in position	Steer with brakes	Lateral controller and steering sensors	Blocked lanes, damage	Impact on manual lanes, RSC 3. Capability to steer with brakes
Steering	Unstable, no control	Same as above	Same as above	Same as above	Same as above
Vehicle Power	Failure	Operator attempts to gain manual control	Operator, wayside communications	Major damage and casualties	All controllers, communication inoperable. No notification of operator or wayside. Manual capabilities?

Table 8. Scenario C Malfunctions — Prompt, Normal Exit

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Engine Transmission Brakes Steering Fuel Tires Communications — Vehicle-Roadside Communications — Vehicle-Vehicle Lateral Measurement Longitudinal Measurement Lateral Control Computer Longitudinal Control Computer Position/Navigation Display/Keyboard Collision Avoidance Power (Battery or Alternator)	Pre-fail condition detected		As noted in previous tables	Vehicle exits AHS without incident	Operator displeasure when rejected for no discernible reason. Vehicle exits to manual lane (RSC 3) with potential failure

Table 9. Scenario D Malfunctions — Emergency Braking, Revert to Manual Control

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Vehicle-based communication with wayside. (RSC 1)	Failure		Vehicle/Wayside communication	Probable damage, casualties, blocked lanes	
Wayside communication with vehicles. (RSC 1)	Failure	Wayside shuts down affected AHS section All vehicles in affected section stop	Vehicle communication	Probable collisions, casualties, and blocked lanes	Can Operator assume lateral control at some point before complete stop?
Wayside sensor. (RSC 1)	Failure - no redundancy	Same	Wayside electronics	Same	Same
Wayside power. (RSC 1)	Failure - no backup	Same	Same	Same	Same
Wayside processor. (RSC 1)	Failure - no redundancy	Same	Same	Same	Same
Lateral position measurement. (RSC 2,3)	Failure		Lateral control	Same	Same
Lateral control computer. (RSC 2,3)	Failure		Same	Same	Same

Table 10. Scenario E Malfunctions — Slow, Maintain Lane

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Wayside sensor, communication, or processor	Pre-fail detection of failure	Normal AHS operation	Wayside processors, connumications, and sensors	No visible impact	
Wayside sensor. (RSC 1)	Failure, adjacent sensors available	Same	Same	Same	
Wayside power	Failure, standby power available	Same	Same	Same	
Wayside processor. (RSC 1,3)	Failure, adjacent processors available	Same	Same	Same	
Wayside's roadside-vehicle communication	Degraded	Stay in lane	Same	Possible missed exit. No damage/ casualty	
Wayside auxiliary sensor	Failure	RSC 2. Stay in lane	Same	Same	
Wayside power	Failure, no standby	RSC 2. Stay in lane	Same	Same	
Wayside's roadside-vehicle communication	Failure	RSC 2. Stay in lane	Same	Same	
Wayside processor	Failure - no redundancy	RSC 2. Stay in lane	Same	Same	
Wayside communication. (RSC 3)	Failure	Wayside shuts down affected AHS section Collision avoidance for longitudinal control while in affected section	Wayside processors, communications, and sensors	Vehicle passes through affected section, resumes normal operation	

Table 10. Scenario E Malfunctions — Slow, Maintain Lane (continued)

System or Element	Malfunction	Variation	Detection	Expected Outcome	Issues
Wayside power. (RSC 3)	Failure - no backup	Same	Vehicle communication	Same	
Wayside processor. (RSC 3)	Failure - no redundancy	Same	Wayside processors, communication	Same	
Roadside barrier	Shift into AHS lane	Affected lanes shut down, divert vehicles from lane	Roadway infra-structure maintenance function		
Pavement, bridges	Not traversable	Same	Same		
Barriers	Shifted, deformed	Vehicles slow commensurate with conditions	Same		
Pavement, bridges	Traversable, below performance standard	Same	Same		
Barriers, pavements, bridges	Pre-fail deterioration		Same		

Recovery Actions

The immediate actions described in the preceding paragraphs and tables result in one or more of six end results which may require some degree of further recovery actions to restore the AHS to full operation. These end results of the immediate actions and the associated further recovery actions are as follows:

- The malfunctioning vehicle exits the AHS normally and no further action is needed to restore operation.
- The malfunctioning vehicle makes its way to the breakdown lane (or to a second AHS lane that has been designated to be used as the breakdown lane, when required), proceeds to the nearest exit and no further action is needed to restore operation.
- The malfunctioning vehicle makes its way to the breakdown lane and stops.
- The malfunction causes a blocked lane, or a malfunctioning vehicle stops in lane, blocking the lane.
- The malfunction causes blockage to all lanes.
- The malfunction causes collisions of vehicles.

Vehicle Able To Remove Itself From AHS (Self-clearing)

The ideal situation, and the goal in all cases possible, is to have the malfunctioning vehicle exit the AHS before the malfunction causes an impact to the remainder of the system. Second best is to enable the malfunctioning vehicle, even though at a slow speed, to make its way to an exit and leave the AHS. When either of these two actions is possible no further action is required except that the individual operator may need to have the vehicle inspected or repaired at some off-line facility.

Vehicle Stops In Breakdown Lane

The effect when a vehicle makes its way to the breakdown lane and stops depends on whether the breakdown lane is a dedicated breakdown lane or whether it is simply an AHS lane which is utilized as a breakdown lane when necessary. In the latter case, provision must be made to divert traffic, which would ordinarily occupy the lane, around the stopped vehicle. This would require a temporary merge with traffic in the other AHS lanes. This could be accomplished by increasing the interplatoon spacing (RSC 1, 2) or intervehicle spacing (RSC 3) in the unblocked lane(s) to accommodate merging of platoons or vehicles from the blocked

lane. It is also possible, in this case, that vehicles immediately behind the malfunctioning vehicle were required to stop in the lane. A decision must be made whether to leave these vehicles where they are until the malfunctioning vehicle is cleared or to allow these vehicles to maneuver around the stopped vehicle, merge with the traffic in another AHS lane, joining or forming a platoon (RSC 1, 2), and continue on their way. All of these maneuvers would require coordination with the adjacent AHS lanes. Also, in this case and in the event of physically separated AHS lanes, service vehicles sent to retrieve the stopped vehicle may enter the AHS from an upstream entrance ramp and travel with traffic to the stoppage site. In the case of a dedicated breakdown lane, it is conceivable that the service vehicle could enter the AHS from downstream and travel the breakdown lane against traffic to the stoppage. This could also be done with a second AHS lane used as a breakdown lane, but would probably result in a long section of the second lane being blocked to traffic as the section is cleared for the service vehicle to travel on.

Vehicle Stops In Lane

An in-lane vehicle stop may be treated very similarly to the case in the preceding paragraph where the blocked lane is not a dedicated breakdown lane, but is an ordinary AHS lane utilized as a breakdown lane when needed. The same provisions must be made to divert traffic around the stopped vehicle (this presumes at least two adjoining AHS lanes) and vehicles which were required to stop behind the malfunctioning vehicle must be allowed to maneuver around the stopped vehicle, join or form a platoon (RSC 1, 2), and continue their journey. RSC 3 may be treated differently in that no physical barrier is presumed to separate the AHS from non-AHS lanes. In this case it may be advantageous to divert AHS traffic to the transition lane or the manual lanes until the stoppage is bypassed. At that point the AHS could be reentered following the usual procedures. The traffic diverted to the transition lane or manual lanes is from the lane adjacent to the transition lane and is not necessarily the traffic from the blocked lane. This will free up space on the AHS for the necessary diversion. Service vehicles sent to clear the stoppage would likely approach from an upstream entrance. An issue here is that the service vehicle must perform a lane change to get in front of the malfunctioning vehicle to tow it. This is an ordinary AHS maneuver and should present no difficulty. An alternate method is that a section of an AHS lane could be closed and the service vehicle could travel against traffic along the closed section of the lane until it reached the stopped vehicle. This method seems more likely to increase the disruption of traffic flow.

Malfunction Causes Closure Of All Lanes

If all AHS lanes are blocked by malfunctioning vehicles or are closed due to malfunctioning infrastructure equipment, the section of AHS in which the blockage occurs must be closed until the blockage is cleared or equipment repaired. Entrances will be closed which allow access to the blocked section, and the upstream traffic will be diverted from the closed section. For RSC 1 and 2 this will likely mean going through the usual checkout procedure and exiting the AHS to surface streets. For RSC 3 this could be accomplished by exiting to the manual lanes, traveling past the blocked section and then reentering the AHS. There may be some number of vehicles behind the blockage which cannot exit the AHS and which must wait until the blockage is cleared to proceed. When the blockage is cleared these vehicles, if they have not been involved in a collision and if, through the usual detection methods, they give no indication of any malfunctions, will be formed in platoons (RSC 1, 2) or assigned time slots (RSC 3) and restarted in sequence. The restart sequence is: wayside and vehicle verify no known malfunctions in affected vehicles (including operator readiness), wayside notifies all affected vehicles of imminent restart, forms platoons (RSC 1, 2) or assigns time slots (RSC 3) and notifies vehicles of immediate restart, first platoon or vehicle starts and accelerates to speed (utilize coordinated acceleration), as safe interplatoon or intervehicle spacing is reached, the second platoon or vehicle starts and accelerates to speed. This procedure continues until all vehicles in the blocked section are at speed. At this time the section can be reopened.

Malfunction Causes Collisions Of Vehicles

Any vehicle that collides with another vehicle or object must exit the AHS and pass the required check-in procedure before being readmitted to the AHS. This applies whether the vehicle is able to exit the AHS under its own power or has need to be cleared by a service vehicle.

On present-day highways, accident investigation can cause lanes to remain blocked for hours. With the automation of the highway it is expected that the history of the state of most subsystems of the AHS, including malfunction codes, can be preserved in memory for a time interval sufficient in length to allow the affected vehicles to be immediately cleared from the AHS and the accident investigation to proceed off-line.

Intrusion of Unauthorized Vehicles

The vehicle malfunctions discussed to this point have been for AHS vehicles which passed check-in and failed while on the AHS. The malfunction management system must also be designed to respond to a second category of vehicles which will be called intruding vehicles. The intruding vehicles can be of two types: Those that are equipped for entry on the AHS, fail to pass check-in, and manage to enter the AHS lanes anyway, and those that are not equipped for AHS entry yet manage to elude the check-in safeguards. In either case the intruding vehicle must be considered as a danger to the remaining vehicles on the AHS, either because the vehicle exhibits some malfunction and was therefore declared ineligible to enter the AHS, or because the vehicle is not equipped to travel in the AHS environment. Detection of unauthorized vehicles is performed by the check-in facility if the vehicle is the first type mentioned. Otherwise, detection can be performed by the wayside sensors and communication equipment, and the communication equipment of the other AHS vehicles in that a vehicle is detected which does not respond to queries or commands. Detection could also be through the vehicle collision avoidance system. Platoons or individual vehicles must be separated from the intruding vehicle by safe stopping distances, both in the lane occupied by the intruder and in the adjacent lanes, in preparation for sudden uncontrolled lane changes, and the distances must be maintained until the intruder exits the AHS. If the intruder is slower than the normal AHS vehicle or platoon, preceding vehicles can be allowed to proceed normally, while following vehicles must slow down to provide adequate separation. If the intruder is traveling faster than normal AHS speeds, following traffic may be allowed to proceed normally while preceding traffic may have to exit the AHS. A moving, closed segment which includes the intruder can be implemented by closing entrances to the AHS, both before and behind the intruding vehicle, for a time to further isolate it from the other vehicles on the AHS. It may be necessary to dispatch AHS-qualified security vehicles to isolate the intruder and attempt to encourage the intruder to exit the AHS. An automated version of present day pursuit methods can be implemented in which security vehicles maintain contact with the pursed vehicle but don’t try to force the intruding vehicle from the AHS unless actions by that vehicle are found to be a clear danger to other vehicles on the AHS. Another plan that has been suggested is that of a series of barriers, placed at intervals along the AHS roadway, that are erected only in the case of intruders and shunt the intruder from the AHS to an exit.

Task 4. Define Measures of Effectiveness

This task will provide guidelines for evaluating the malfunction management strategies proposed in this activity report. Measures of Effectiveness (MOE's) are derived from the design goals of the system being developed. The MOE's must be carefully selected to reflect the specific performance requirements, in order to effectively analyze the candidate malfunction management techniques. A variety of approaches for measuring effectiveness of malfunction management strategies exist. The primary consideration in this discussion is system safety. Other system design parameters such as capacity, throughput, or travel time can also be used to analyze the MOE's. Market penetration is another factor which can be affected by the approach to malfunction management due to its relationship with cost and consumer acceptance.

The measures of effectiveness identified include two classical standards, probability of detection and false alarm rate. Other typical MOE's, such as performance degradation and service availability are also discussed. Cost is a measure that can be used to differentiate between two strategies with similar technical attributes and identical safety ratings. The MOE's for malfunction management strategies are summarized in table 11 and categorized in relationship to their relative impact on three major system attributes: safety, throughput, and consumer acceptance.

The MOE's which are closely linked with maintaining system safety will be indicated as safety critical. Each MOE within the safety category is given a ranking indicating its relative importance with respect to system safety. A weight of 10 indicates the most safety critical measure, while 1 indicates the measure that is least significant relative to all others in the safety category. Measures which have the greatest impact on system throughput are weighted in a similar manner, with 10 indicating the highest relative importance within the throughput category. The remaining MOE's are not critical to safety or throughput, and are placed in the category of market penetration. Their relative weights are also assigned, with 10 corresponding to the most important MOE within the category.

Safety Critical

Probability of Detection

The ability of the system to correctly identify a malfunction is one measure of effectiveness. The probability of detection must be defined in terms of the desired impact the management

strategy is intended to have on system performance. The probability of detecting a malfunction which compromises the safety of the system must approach 100 percent. The probability of detecting a malfunction which limits access to the system might be acceptable at 95 percent. Tradeoffs will occur between the cost of implementing more accurate detection techniques and the benefit to system performance. This MOE is indicated as safety critical because the ability to accurately identify malfunctions is the key to effective management. As the number of malfunctions not detected by the system increases, the likelihood of a hazardous condition increases. The probability of detecting a critical or serious malfunction is directly related to safe operation of the system.

Table 11. MOE's Summarized by Category

MOE	Description	Weight	Justification
Safety Critical			
Probability of Detection	Measure of the number of malfunctions which are not detected (False Negative)	10	Undetected malfunctions cause potentially severe safety hazards
Damage Control	Measure of the likelihood of a collision occurring	9	Collisions jeopardize lives and increase risk of injury
Operator Interface Complexity	Measure of the workload delegated to the driver to handle malfunction strategy	8	Drastic increase in workload affects driver's ability to make safe decisions
Response Time Delay	Measure of the amount of time required for the system to respond to a detected malfunction	5	Maximize safety by minimizing time system operates with a component malfunction
Throughput Significant			
Service Availability	Measure of the amount of time required to bring system back to 100% performance	10	Downtime or period of reduced system capability should be minimized
Performance Degradation	Measure of the level of service following management action	8	Reduction in capacity or throughput may occur as a result of malfunction
Impact to System Operation	Measure of the severity of the effect on system operation during malfunction	6	Malfunction can impact reliability, false alarm rate, probability of detection
False Alarm Rate	Measure of the number of incorrectly detected malfunctions (False Positive)	5	Minimize intervention by system which impacts optimum performance
Market Penetration Sensitive			
Consumer Acceptance	Acceptability of alternative actions taken	10	Convenience of options will affect user base

Cost	Relative expense of implementation	8	Cost used as tie breaker between equivalent options

Damage Control

The ability to minimize injury, death, or economic loss caused by a system malfunction is an important measure of the effectiveness of a management strategy. Malfunctions with the potential to cause major collisions must be dealt with using techniques that limit the risk of damage to vehicles, occupants, and the system. Minor collisions may be acceptable if damage to property is negligible and injuries do not occur. The damage caused by minor collisions between vehicles in a close vehicle following mode can be nonexistent if the difference in traveling velocity of the vehicles involved is small. The acceptability of a management strategy that allows collisions of this type may involve consumer opinion to a large extent.

Operator Interface Complexity

The level of complexity the management strategy introduces to the operator interface is a primary
consideration. The operator may be involved in the process of mitigating a malfunction, and may be required to perform some manual operation while the vehicle is in the automated lane. An ineffective approach to resolving the malfunction may place an inappropriate work level on the driver. Management techniques must take into consideration the wide variety of reaction times in the driving population and ensure that safety is not compromised by involving the operator in the malfunction abatement process. This MOE is identified as safety critical because of the high correlation between conventional accidents and human error. The malfunction management strategy must not transfer control of safety-critical vehicle functions to the driver in situations where the likelihood of operator error is high. Extremely hazardous conditions might include reverting to manual steering or braking in close vehicle following mode at high speeds.

Response Time Delay

The time the system consumes in the process of identifying a malfunction and implementing the management strategy is termed the response time delay. This MOE is important because it is integral to the ability to maintain system performance. Excessive delay in responding to a potential malfunction can increase safety hazards or reduce the level of service of the AHS.

This MOE is categorized as safety critical due to its potential impact on system safety. The management technique must balance the ability to react quickly enough to avoid hazardous con-ditions while minimizing the risk to system operation. A tradeoff must occur to allow the malfunction

evaluation to be timed to provide the most efficient response in terms of maximizing throughput and capacity while maintaining the desired safety level.

Throughput Significant

Service Availability

The period of time the system is at limited functionality due to a malfunction is also an MOE. This measure combines the effects of both Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR). Service availability is expressed as (MTBF – MTTR) / MTBF. A high MTBF is associated with high reliability, and low MTTR indicates the ability to quickly fix a failure. As MTBF increases and MTTR decreases, the service availability figure will approach 100 percent. Frequent loss of full operating capability will reduce the overall system availability figure. System down time will have an adverse impact on user perception and maximizing the system availability will be a significant measure of the effectiveness of a management strategy. This MOE is identified as throughput significant, indicating a close relationship to efficient operation. The period of time during which the system operates at less than optimum safety must be minimized. The approach to system availability must allow a tradeoff between bringing the system back up to full capability in a timely manner without increasing the safety risk.

Performance Degradation

The level of service the AHS can provide following a malfunction is another measure of the effectiveness of management strategies. A highly effective management strategy will allow the malfunction to be transparent to mainstream operation of the AHS. A less effective method might require the travel speed to be decreased until the malfunction is rectified. This MOE is throughput significant due to the emphasis on limiting system performance for the benefit of optimized safety. Given a specific standard for system safety, the candidate management strategies can be evaluated on their relative ability to prevent degradation of performance.

Impact to System Operation

The effect of a particular management approach on the operation of the system during the malfunction is another MOE. System reliability is an area which may bear the impact of the

management approach. An example might involve redundant system components. Designing a system to provide redundant coverage by one or more sensors can allow an adjacent sensor to provide backup capability in the event of a sensor failure. The overall system reliability will be reduced in the event of a sensor failure until it can be corrected, even though system performance is not affected by a single point failure. This phenomena is due to the fact that the redundant sensor also has a finite risk of failure and will cause system malfunctions in the event of a failure prior to correction of the first defect. Similarly, the probability of detecting additional malfunctions may be reduced until a single point failure is resolved. This MOE is throughput significant since the primary effects will be limited to reduced system capability, and safety is not expected to be affected.

False Alarm Rate

The likelihood of indicating a malfunction when none exists is related to the probability of detection. Certain malfunctions which affect the safety of the system will require an extremely high probability of detection. The possibility of false alarms can increase when the possibility of not detecting a malfunction can not be tolerated. The accuracy of the detection technique will affect the ability to reduce the false alarm rate without compromising probability of detection. This MOE is categorized as throughput significant since false positive malfunction indications will not affect system safety but may compromise efficient operation. The primary results of a high false alarm rate may include reduced level of service or driver inconvenience in being denied access to the system. An approach which allows the false alarm rate to err on the side of safety will have a greater impact on throughput. The false alarm rate can be designed to maximize throughput at greater risk to safety, and this type of approach might be categorized as safety critical. The assumption is made for this analysis that safety is optimized first and throughput is secondary.

Market Penetration Sensitive

Consumer Acceptance

The user perception of management strategies is one of the least important MOE's in terms of safety. Market penetration is highly dependent on consumer acceptance of AHS implementation, but in the event of a malfunction, the alternatives must be developed to enhance safety. Two options which provide identical levels of safety but which have greatly disparate effects on the convenience offered by the AHS can be weighed using this measure.

Cost

The cost of implementation can be used to differentiate between two strategies with similar technical attributes in terms of efficient operation and identical safety ratings. The development cost can be used to trade off different approaches to increasing probability of detection or system availability with equivalent safety ratings. Implementation costs can also be used to evaluate similar technical approaches to reducing false alarm rate or the complexity of the human interface. The safety of the system can not be compromised in favor of reducing the cost of a candidate strategy. The cost may be used to evaluate diminishing returns of increased throughput in light of potential market penetration.

Task 5. Evaluate the Management Strategies

Evaluating the Malfunction Management Strategies requires that tools for the evaluation be obtained or developed and that the tools be applied to the management strategies. The following two sections describe the tools to be used and their application to the evaluation of the management strategies.

Evaluation Tools

The evaluation of the Management Strategies is based on the Measures of Effectiveness (MOE) defined in task 4 and on severity scales that are developed for each of the MOE's. In task 4 the MOE's are ranked according to importance within their respective categories and a numerical value is also assigned to each of the MOE's which, along with numerical values assigned to the MOE severity scale, can be used to compute an effectiveness score for each of the management strategies. The scores thus developed can be used to compare the effectiveness of alternative management strategies for a malfunction and can also be used to aid in identifying those malfunctions that are difficult to manage and therefore must be prevented from occurring.

A severity scale for the Safety Critical MOE's and one for the Throughput Significant MOE's are shown here. These severity scales are based on the scales developed at the Vehicle Operations mini-conference of 20 July 1994. The naming of each scale division and the definition of the scale divisions are those arrived at during discussions held at that mini-conference. In this analysis a numerical value is also assigned to each division of the severity scale for convenience in using the scales to evaluate the management strategies and are an

indication of the relative weight of each scale division. The severity scale developed for safety is shown in table 12 and the severity scale developed for throughput or performance is shown in table 13. In this analysis no attempt is made to devise a severity scale for the Market Penetration Sensitive MOE's and no evaluation of the management strategies with respect to these MOE's will be done. It is judged that at this point cost and consumer acceptance of management strategies are not sufficiently well known to allow an assessment of management strategies in these areas.

Table 12. Safety Scale

Scale Division	Definition	Severity Index
No Impact	User annoyance/comfort, forced off, not allowed on	0
Negligible	Less than minor injury or system damage; user discomfort	1
Moderate	Minor injury with moderate equipment damage	3
Major	Severe injury or death, major damage	8
Catastrophic	Multiple deaths and major damage; system shutdown	10

Table 13. Throughput Significance Scale

Scale Division	Definition	Severity Index
No Impact	No perceptible effect on performance	0
Negligible	Minor delay to few vehicles (<2%), minor loss of throughput, not sustained	1
Moderate	Moderate delays (10–20% of vehicles)	3
Major	Major delays (40–60% of vehicles); system shutdown <2 hour	8
Catastrophic	System shutdown >2 hour	10

With the numerical values assigned to the MOE's and to the severity scales, it is possible to assign a safety score and a throughput (or performance) score to each of the management strategies that were developed in task 3. It should be emphasized that the only meaning that should be given to the numerical values attached to the MOE ranking and severity scales is that of providing a convenient method of computing a score to facilitate making qualitative

comparisons or rankings of the management strategies. These scores are computed by the equation

$$\text{Score} = \sum_{\text{MOE}} (\text{Weight}_{\text{MOE}}) \times (\text{SeverityIndex}_{\text{MOE}}) \quad (1)$$

That is, the score is computed as the product of MOE weight and MOE severity index, summed over all MOE's within a category. With the numerical weighings of MOE's and severity scales as shown above, effective management schemes will have low scores. A perfect management strategy would have a score of 0 with larger scores indicating less effective strategies.

Application of Evaluation Tools

For this task the malfunction strategies will be evaluated utilizing the MOE's defined as being Safety Critical and the MOE's defined as Throughput Significant only. Furthermore, within the Safety Critical and Throughput Significant categories those MOE's that will be utilized in this evaluation are: Damage Control and Operator Interface Complexity in the Safety Critical category, and Service Availability, Performance Degradation, and Impact to System Operation in the Throughput Significant category. These are the MOE's that are judged to be sufficiently design-independent to allow some estimate of management strategy effectiveness. When a more detailed design of the malfunction management system is made, the additional Safety Critical MOE's, Probability of Detection and Response Time Delay, as well as the additional Throughput Significant MOE, False Alarm Rate, can be included in this evaluation process.

The results of the evaluation are shown in tables 14 through 18 and are organized by management scenario as was done in task 3. For each of the identified malfunctions, the tables show the ranking on the severity scale for each MOE considered and the computed scores for Safety and Performance (Throughput). In these tables the larger scores indicate the less effective management strategies.

As an example of the use of equation 1, the Safety Critical Score for the brake element with fail off malfunction in table 14 will be evaluated. The Operator Interface Complexity MOE has a weight of 8 and the Damage Control MOE has a weight of 9 from table 11. Within table 14 the MOE's are evaluated as affected to the No Impact level and the Moderate level, respectively, for the malfunction being considered. These two levels are associated with the

Severity Index values 0 and 3 in table 12. Thus the score, which is the sum of the products of MOE Weight and MOE Severity Index, is evaluated as:

$$\text{Score} = 8 \times 0 + 9 \times 3 = 27 \quad (2)$$

Table 14. Scenario A Evaluation - Divert and Clear

System or Element	Malfunction	Safety Critical			Throughput Significant			
		Operator Interface Complexity	Damage Control	Score	Performance Degradation	Impact to System Operation	Service Availability	Score
Brakes	Fail off	No Impact	Moderate	27	Moderate	Negligible	Moderate	60
Engine	Not running	No Impact	Negligible	9	Negligible	Negligible	Moderate	44
Engine	Degraded performance	No Impact	No Impact	0	No Impact	Negligible	Negligible	16
Fuel Flow	Off	No Impact	Negligible	9	Negligible	Negligible	Moderate	44
Fuel Flow	Stuck at, unstable	No Impact	Negligible	9	Negligible	Negligible	Moderate	44
Lateral Measurement	Rate or acceleration sensors fail	No Impact	Negligible	9	No Impact	Negligible	No Impact	6
Lateral or Longitudinal Control Computer	Failure, redundant circuit exists	No Impact	No Impact	0	No Impact	No Impact	No Impact	0
Longitudinal Measurement	Velocity or acceleration sensors fail	No Impact	No Impact	0	No Impact	Negligible	No Impact	6
Position/Navigation	Receiver failure	No Impact	No Impact	0	No Impact	No Impact	No Impact	0
Steering	Degraded	No Impact	Moderate	27	Negligible	Negligible	Negligible	24
Tire	Very low pressure	No Impact	No Impact	0	Negligible	Negligible	No Impact	14
Tire	Blow out	No Impact	Moderate	27	Moderate	Negligible	Moderate	60
Transmission	No power transfer	No Impact	Negligible	9	Negligible	Negligible	Moderate	44
Transmission	Degraded performance	No Impact	No Impact	0	No Impact	Negligible	No Impact	6
Vehicle-vehicle communication. (RSC 2)	Degraded	No Impact	Negligible	9	No Impact	Negligible	No Impact	6

Table 14. Scenario A Evaluation - Divert and Clear (continued)

System or Element	Malfunction	Safety Critical			Throughput Significant			
		Operator Interface Complexity	Damage Control	Score	Performance Degradation	Impact to System Operation	Service Availability	Score
Collision Avoidance	Failure	No impact	No impact	0	No impact	Negligible	No impact	6
Display/Keyboard	Failure	No impact	No impact	0	No impact	No impact	No impact	0
Power	Alternator or battery fail	No impact	No impact	0	No impact	No impact	No impact	0
Longitudinal control computer. (RSC 2,3)	Failure	No impact	Negligible	9	Negligible	Negligible	Negligible	24
Longitudinal measurement. (RSC 3)	Failure - position	No impact	Negligible	9	No impact	Negligible	No impact	6
Vehicle-vehicle communication. (RSC 2)	Failure	No impact	Negligible	9	Negligible	Negligible	No impact	14
Vehicle-based communication with wayside. (RSC 2)	Failure	Moderate	No impact	24	No impact	Negligible	No impact	6
Vehicle-based communication with wayside. (RSC 3)	Failure	Moderate	No impact	24	No impact	Negligible	No impact	6

Table 15. Scenario B Evaluation — Emergency Braking

		Safety Critical			Throughput Significant			
System or Element	**Malfunction**	**Operator Interface Complexity**	**Damage Control**	**Score**	**Performance Degradation**	**Impact to System Operation**	**Service Availability**	**Score**
Brakes	Fail on	No impact	Moderate	27	Moderate	Moderate	Moderate	72
Steering	Stuck in position	No impact	Major	72	Major	Major	Major	192
Steering	Unstable, no control	No impact	Major	72	Major	Major	Major	192
Vehicle Power	Failure	No impact	Catastrophic	90	Catastrophic	Catastrophic	Catastrophic	240

Table 16. Scenario C Evaluation — Prompt, Normal Exit

System or Element	Malfunction	Safety Critical			Throughput Significant			
		Operator Interface Complexity	Damage Control	Score	Performance Degradation	Impact to System Operation	Service Availability	Score
Engine	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Transmission	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Brakes	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Steering	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Fuel	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Tires	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Communications — Vehicle-Roadside	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Communications — Vehicle-Vehicle	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Lateral Measurement	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Longitudinal Measurement	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Lateral Control Computer	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Longitudinal Control Computer	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Position/Navigation	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Display/Keyboard	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Collision Avoidance	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0
Power (Battery or Alternator)	Pre-fail condition detected	No impact	No impact	0	No impact	No impact	No impact	0

Table 17. Scenario D Evaluation — Emergency Braking, Revert to Manual Control

System or Element	Malfunction	Safety Critical			Throughput Significant			
		Operator Interface Complexity	Damage Control	Score	Performance Degradation	Impact to System Operation	Service Availability	Score
Vehicle-based communication with wayside. (RSC 1)	Failure	Negligible	Major	80	Major	Major	Major	192
Wayside communi-cation with vehicles. (RSC 1)	Failure	Negligible	Catastrophic	98	Catastrophic	Catastrophic	Catastrophic	240
Wayside sensor. (RSC 1)	Failure. No redundancy	Negligible	Catastrophic	98	Catastrophic	Catastrophic	Catastrophic	240
Wayside power. (RSC 1)	Failure. No backup	Negligible	Catastrophic	98	Catastrophic	Catastrophic	Catastrophic	240
Wayside processor. (RSC 1)	Failure. No redundancy	Negligible	Catastrophic	98	Catastrophic	Catastrophic	Catastrophic	240
Lateral position measurement. (RSC 2, 3)	Failure	Negligible	Moderate	35	Moderate	Moderate	Moderate	72
Lateral control computer. (RSC 2, 3)	Failure	Negligible	Catastrophic	98	Major	Major	Major	192

Table 18. Scenario E Evaluation — Slow, Maintain Lane

System or Element	Malfunction	Safety Critical			Throughput Significant			
		Operator Interface Complexity	Damage Control	Score	Performance Degradation	Impact to System Operation	Service Availability	Score
Wayside sensor, communication, or processor	Pre-fail detection of failure	No impact	No impact	0	No impact	No impact	No impact	0
Wayside sensor. (RSC 1,3)	Failure, adjacent sensors available	No impact	No impact	0	No impact	No impact	No impact	0
Wayside power	Failure, standby power available	No impact	No impact	0	No impact	No impact	No impact	0
Wayside processor. (RSC 1,3)	Failure, adjacent processors available	No impact	No impact	0	No impact	No impact	No impact	0
Wayside's roadside-vehicle communication	Degraded	No impact	Negligible	9	No impact	Moderate	No impact	18
Wayside auxiliary sensor. (RSC 2)	Failure	No impact	Negligible	9	No impact	Moderate	No impact	18
Wayside power. (RSC 2)	Failure, no standby	No impact	Negligible	9	No impact	Moderate	No impact	18
Wayside's roadside-vehicle communication. (RSC 2)	Failure	No impact	Negligible	9	No impact	Moderate	No impact	18
Wayside processor. (RSC 2)	Failure - no redundancy	No impact	Negligible	9	No impact	Moderate	No impact	18
Wayside communication. (RSC 3)	Failure	No impact	Negligible	9	Major	Major	Moderate	142

Table 18. Scenario E Evaluation — Slow, Maintain Lane (continued)

System or Element	Malfunction	Safety Critical			Throughput Significant			
		Operator Interface Complexity	Damage Control	Score	Performance Degradation	Impact to System Operation	Service Availability	Score
Wayside power. (RSC 3)	Failure - no backup	No impact	Negligible	9	Major	Major	Moderate	142
Wayside processor. (RSC 3)	Failure - no redundancy	No impact	Negligible	9	Major	Major	Moderate	142
Roadside barrier	Shift into AHS lane	No impact	Moderate	27	Major	Major	Major	192
Pavement, bridges	Not traversable	No impact	Moderate	27	Major	Major	Catastrophic	212
Barriers Shifted, deformed. Pavement, bridges	Traversable, below performance standard	No impact	Negligible	9	Moderate	Moderate	Major	122
Barriers, pavements, bridges	Pre-fail deterioration	No impact	No impact	0	No impact	Moderate	Negligible	28

Examination of the scores computed in these tables clearly indicates that most malfunctions are manageable with small impact on either safety or performance, but malfunctions brought about by failures in equipment that affects lateral control are very difficult to manage effectively and thus must be prevented from occurring.

The next most difficult malfunctions to manage are those associated with brake failures, tire failures, and failures of roadway pavements, barriers, and bridges.

As would be expected, malfunctions that have large safety scores also have large performance scores. In addition, the malfunctions which require closing, even temporarily, one or more AHS lanes have large performance scores.

CONCLUSIONS

A count of the items on the malfunction lists of task 1 reveals approximately 70 malfunctions, distributed as follows:

- General vehicle malfunctions — 19.
- AHS-specific vehicle malfunctions — 28.
- Wayside electronics malfunctions — 15.
- Roadway malfunctions — 9.

Operator malfunctions identified for the RSC's defined are limited to the operator not being prepared to assume manual control on checkout.

Methods and technologies have been identified which enable detection of each of the identified malfunctions. A survey of current research found that a considerable amount of research is being conducted in industry and in universities with the aim of improving malfunction detection capabilities.

Analysis needs to be done to determine which of the identified detection methods are practical and cost-effective for use on AHS. Some of the methods and technologies identified are commonly used for malfunction detection in military and space applications, but may be too costly for AHS application. An example would be triple redundant processors with data sharing and majority voting.

Methods for automating the detection of roadway malfunctions, which are presently detected by manual inspection, were identified. Further analysis should be performed to determine which malfunctions require automated detection to meet safety and performance goals and which malfunctions are detected more cost-effectively by automated detection than by manual inspection.

The management strategy for each malfunction can be divided into two parts: a set of immediate actions to contain the malfunction and a set of actions to restore AHS operation. Five sets of immediate actions were defined that cover all of the malfunctions and five sets of actions to recover from the effects of these immediate actions were also defined.

In RSC's where access to the AHS lanes is from parallel manual lanes via a transition lane (RSC 3) it was assumed that the AHS lanes are continuous. To not interfere with access to the AHS lanes, the breakdown lane was placed as the farthest AHS lane from the transition lane. In the other RSC's, since access is intermittent, it is assumed that the breakdown lane is the lane adjacent to the exits so as to facilitate self-clearing of malfunctioning vehicles when possible and to simplify extraction of malfunctioning vehicles by service vehicles when required. This should be a topic for further investigation by roadway operations analysts.

The evaluation of management strategies shows that most malfunctions can be managed effectively by the strategies defined. In the evaluation of malfunction management strategies for malfunctions which result in loss of lateral control, the scoring of Safety Critical items show that these malfunctions are difficult to manage. This results from having no identified adequate backup for lateral control. The RSC most affected by malfunctions resulting in loss of lateral control is RSC 1. In this RSC a large part of the control function resides with the wayside. A failure in this function affects multiple vehicles. Collision avoidance systems are assumed to be an adequate backup for longitudinal control to the extent that they are realized as redundant and separate systems. An investigation of what is required to provide backup for lateral control should be undertaken. Perhaps side-collision warning systems can be adapted.

From a Safety Critical standpoint the next most difficult malfunctions to manage are those associated with brake failures, tire failures, and failures of roadway pavements, barriers, and bridges.

Malfunctions that are difficult to manage for safe operation also are difficult to manage for maintenance of performance. Malfunctions that can be managed for safe operation but that require closing of AHS lanes, or even entire AHS sections, also have a large impact on performance

On the nonautomated highway the operator is presently the major detector of malfunctions and implementor of malfunction management. Intuitively, it seems that the operator could continue to play some role in the detection of malfunctions, that there are some malfunctions that the operator could detect better than, or at least as well as, the automated detection system, and therefore the operator should serve as a backup or alternative detector. One item that continually is brought up in discussions of the subject is that of animals on the roadside that may jump in front of the vehicles and how the operator may be better able to anticipate

the animals movements than the automated detection system. Some further investigation of the operator's role in malfunction detection should be carried out, as well as a determination of how the operator can indicate the perceived malfunction and desired management actions to the AHS.

Results from studies of operator reaction capabilities suggest that virtually no operator participation in malfunction management be allowed in the mature AHS RSC's assumed in this activity report. The discussion found in activity D, task 5 reviews studies of driver reaction time and the possibilities of driver intervention in case of automatic control failure. The long reaction times shown in that task and accounts of accidents due to improper operator reaction or over-reaction to malfunctions (blowouts, drifting out of lane) when the driver has had continual control seems to preclude sudden resumption of lateral control after a long period of no driver involvement with vehicle control. The analysis of this activity assumes that the operator will not have a role in any management strategies except in those cases where control can be assumed at the operator's leisure. The operator is allowed a role only in those cases where the vehicle can be brought to a complete stop before the operator assumes control, or where the vehicle can continue to operate in a near-normal fashion until the operator can assume control. If it could be shown that under some benign set of conditions, short of coming to a complete stop, the operator could safely assume control, this may mitigate some of the difficulty with managing loss of lateral control.

REFERENCES

1. B. Visnic, “OBD-II: No longer a nightmare”, WARDS Auto World, August 1994.

2. K. A. Marko et al, “Vehicle Applications of Artificial Neural Systems: Diagnostics and Control”, IEEE Roundtable Discussion on Fuzzy and Neural Systems, and Vehicle Applications, paper 1, November, 1991.

3. S. Patwardhan and M. Tomizuka, “Robust Failure Detection in Lateral Control For IVHS”, Proceedings of 1992 American Control Conference, volume 2, pages 1,768 through 1,772, Piscataway, NJ., 1992.

4. J. Park, “A Unified Theory of Fault Detection and Isolation in Dynamic Systems”, Dissertation Abstracts International, page 3,808.

5. C. D. de Benito, “On-board Real-Time Failure Detection and Diagnosis of Automotive Systems”, Transactions of the ASME, Journal of Dynamic Systems, Measurement and Control, volume 112, number 4, pages 769 through 773.

6. Charles J. Murray, “Dawn of the Smart Sensor”, Design News, 9 May 1994.

7. J. Balar, B. Dahlstrom, K. Longenecker, and T. Buu, “Video Image Distress Analysis Technique for Idaho Transportation Department Pavement Management System”, Transportation Research Record 1,117, 1987.

8. C.A. Lenngren, “Some Approaches in Treating Automatically Collected Data on Rutting”, Transportation Research Record 1196, 1988.

9. D. L. Huft, D. C. Corcoran, B. A. Lunde, and P. A. Orth, “Status of South Dakota Profilometer”, Transportation Research Record 1,117, 1987.