Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Activity Area E Malfunction Management and Analysis

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-95-030
November 1995

FOREWORD

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

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

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

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

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

NOTICE

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

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

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-RD-95-030		

4. Title and Subtitle	5. Report Date
PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS Activity Area E—Malfunction Management and Analysis	November 1995
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
Steven R. Nelson, Graham Alexander, John Herridge	
9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Battelle Transportation Systems 505 King Avenue Columbus, Ohio 43201 614-424-4748	11. Contract or Grant No. DTFH61-93-C-00195
12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Federal Highway Administration Finance Division, Room 4314 400 Seventh Street, S.W. Washington, D.C. 20590	Resource materials 8/93 - 11/94
	14. Sponsoring Agency Code FHWA

15. Supplementary Notes

Contracting Officer's Technical Representative (COTR) – Dick Bishop (HSR-12)

16. Abstract

Increasing the safety of travel is a principal goal for an AHS and one of the baseline assumptions on which this study is based. Establishing the safety parameters and manner in which vehicle, highway, and human failures can be moderated to produce the minimum harm is likely to be one of the main drivers in selection of AHS architectures and system/vehicle implementations. A good understanding of the issues must be developed early in the program. The importance of this malfunction management and analysis task cannot be overestimated.

Normal operation of the AHS will significantly increase public safety by removing the driver from the loop, thus eliminating more than 80 percent of accidents which are caused by improper driving. An AHS will compliment or supplant freeways and thus must provide a level of safety greater than driver-operated vehicles on these already relatively safe roads currently enjoy. Introduction of the AHS also introduces a potential new cause of accidents—malfunction of the AHS. This study seeks to increase safety by identifying and analyzing the possible malfunctions associated with an AHS, and developing strategies to handle these malfunctions.

This document type is resource materials.

17. Key Words	18. Distribution Statement
Automated Highway Systems AHS	This document is available to the public through the National Technical Information Services (NTIS), Springfield, Virginia 22161—Telephone (703) 487-4650

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	238	

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS/ABBREVIATIONS

AARP	American Association of Retired Persons
AASHTO	American Association of State Highway and Transportation Officials
ABS	Antilock Braking System
ADT	Average Daily Traffic
AE	Architectural Engineer
AHMCT	Advanced Highway Maintenance and Construction Technology Program
AHS	National Automated Highway System
AICC	Autonomous Intelligent Cruise Control
ANSI	American National Standards Institute
APTS	Automated Public Transportation System
ARPA	Advanced Research Project Agency
ARTS	Automated Rural Transportation System
ASTM	American Society for Testing Materials
ATIS	Automated Traffic Information System
ATMS	Advanced Traffic Management System
AVCS	Automatic Vehicle Control System
AVI	Automatic Vehicle Identification
AVLS	Automatic Vehicle Location System
BBS	Bulletin Board System
CASA	Computer and Automated System Association
CE	Civil Engineering
CI	Configuration Items
CVO	Commercial Vehicle Operation
DC	Direct Current
DCAA	Defense Contract Audit Agency
DOT	Department of Transportation
DVI	Driver Vehicle Interface
EPS	Electric Power Steering

FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FMEA	Failure Modes Effects Analyses
FMVSS	Federal Motor Vehicle Safety Standard
FOT	Field Operational Test
FREE-SIM	Freeway Simulation
FTA	Federal Transit Authority
FY	Fiscal Year
GIS	Geographic Information System
GPS	Global Positioning System
HOV	High Occupancy Vehicle
HW	Hardware
IAVD	International Association of Vehicle Dynamics
IEEE	Institute of Electrical and Electronic Engineers
IR	Infrared
IR&D	Independent Research and Development
ISO	International Standards Organization
ISTEA	Intermodal Surface Transportation Efficiency Act
IVHS	Intelligent Vehicle Highway Systems
MOE	Measure of Effectiveness
MOP	Measure of Performance
MPR	Mean Personal Rating
MTBCF	Mean-Time Between Critical Failure
MTBF	Mean-Time Between Failures
MVMT	Million Vehicle Miles Traveled
NADS	National Advanced Driving Simulator
NAHTSA	National Automotive Highway Transportation Society of America
NDS	National Driving Simulator
NES	National Energy Strategy

NHTSA	National Highway Traffic Safety Administration
NSC	National Safety Council
OEM	Original Equipment Manufacturer
PC	Personal Computer
PBMS	Performance Based Measurement System
PSA	Precursor Systems Analysis
QFD	Quality Function Deployment
R&D	Research and Development
SAE	Society of Automotive Engineers
TMC	Traffic Management Center
TRB	Transportation Research Board
TRAF-NET	Traffic Network Simulation
UL	Underwriters Laboratories
USG	United States Government
V&V	Validation and Verification
VMT	Vehicle Miles Traveled

EXECUTIVE SUMMARY

Objective and Scope

Increasing the safety of travel is a principal goal for an AHS. Accordingly, the objective and scope of activity area E efforts were coordinated with activity area N efforts (i.e., AHS safety issues) to assure comprehensive coverage of this critical pair of issues. Briefly stated, the overall objective for activity area E was to identify and evaluate the management strategies that can be used to *reduce the number of, or mitigate the effects of, potential AHS system malfunctions*. By way of contrast, activity area N efforts were directed at providing AHS users with a *collision-free driving environment in the absence of malfunctions*. The scope of this activity area E search for pertinent malfunction management strategies was restricted to looking for malfunctions that might occur with the various subsystems and human participants anticipated in the team's selected group of RSCs.

In addition to coordination with area N, the activity area E staff coordinated at differing levels with project staff for the six other activity areas analyzed by this program team. One of the focal points for collaboration and discussion was the development of the team's set of RSCs. In general it was found that the area E subteam had to describe the RSCs in much more detail than was required by the other subteams. Some subteams could consider an entire AHS vehicle/traveling unit as essentially a "black box." To do a meaningful job of anticipating and mitigating potential malfunctions, however, the area E subteam had to visualize what *sorts* of systems and subsystems would accomplish the required AHS functions, maneuvers, etc. In pursuing relative depth, the area E subteam did not get into design details, just "functional concepts."

The scope of those efforts included potential malfunctions for the human elements (e.g., vehicle drivers and AHS operational staff) as well as the hardware/software/equipment in the vehicles and the roadway infrastructure. In general, the analyses were restricted to the representative systems within the program team's selected set of RSCs. One exception to the scoping consideration was that some thought was given to potential malfunctions of AHS systems while the AHS vehicles were intended to be under manual control (e.g., while being operated on non-AHS roadways).

Methodology

While participating in formulation of the program team's RSCs, the area E subteam simultaneously fleshed out its intended approach to systematically:

- Identify and analyze major malfunctions.
- Identify requirements and strategies to manage malfunctions.
- Assess consequences of collisions.

- Develop and utilize measures of effectiveness to select the more promising malfunction strategies.

An initial step in this process was to search for relevant information in the relatively sparse existing and emerging literature for AHS and IVHS systems. With this background and the program team's RSCs as a point of departure, the area E subteam formulated a functional block diagram to begin its visualization of the specific AHS systems that might be selected and that might malfunction. Many of the systems so identified shared a basic structure as follows:

- A sensor which receives or detects vital input information for the control of the AHS vehicle (or AHS facility).

- One or more communication links which carry this information to the control elements in the vehicle (or AHS facility).

- A control unit, driver, or controller which/who must interpret and/or process this information and generate or send appropriate command signals or actions.

- One or more actuators to execute the AHS commands.

Each of these elements is a node in the system and potential failures can occur at any of the nodes or the interfaces between them.

The initial analysis of the functional AHS elements was performed using the well known system safety technique known as fault tree analysis (FTA). This technique begins with the identification of a major undesirable outcome (e.g., a serious fault) at the top of what will become a tree-shaped figure. The expanding triangular base of the tree is comprised of the possible subfaults that could lead to the main fault and, in turn, the sub-sub faults that might cause the sub-faults in the tier above them, and so on. While FTA is a comprehensive form of analysis, to develop a more comprehensive/thorough understanding of the various systems, their interactions, when their actions and interactions occur, etc., the area E subteam also developed action timelines. This tool provided an organized means of describing (for each RSC) a series of functions or events needed to be performed by the driver, the vehicle, the infrastructure, and any intervening communication links during each phase of a hypothetical trip on the subject RSC.

Once the action timelines were developed, the required functions in the action timelines were analyzed to develop the potential operational malfunctions that would occur given the negation of the required function. The results from this effort were organized as a set of malfunction timelines.

The efforts described above provided a foundation for understanding what systems were likely to be involved, what their key intended interactions were, and how they might fail to perform their intended functions. The area E tasks that followed were then aimed at identifying and

assessing appropriate countermeasures (i.e., methods to manage these malfunctions). Some of the key steps involved in this phase of the work included development and use of scoring techniques to assess the probability and severity of the identified malfunctions in the *absence* of any malfunction management strategies. Specific malfunction management strategies (e.g., use of higher reliability components, use of redundancy, and use of adaptive type controls) were then conceived to mitigate each of the identified malfunctions (with emphasis on the malfunctions scored as being the most critical). (In this context criticality refers to the product of probability and severity.) By structuring this scoring process to include such measures of effectiveness as cost, convenience, and capacity, as well as safety, it was possible to begin the process of rank ordering the various countermeasures. The scoring activities in area E were performed independently by three area E staff members having extensive experience in automotive and/or hydromechanical control systems.

Synthesizing the results of the above activities yielded final activity area products in the form of recommended AHS vehicle system countermeasures, recommended AHS infrastructure countermeasures, and recommended AHS operational malfunction countermeasures, which together comprise the malfunction management strategy (MMS) for each RSC.

Results

The following points highlight the findings for activity area E. Additional findings and supporting material are presented in the main topical report for area E.

Malfunction Management Strategy Needs and Adequacy

Potentially serious malfunctions (i.e., malfunctions that could result in death or serious injury and/or could involve 13 or more vehicles) could occur during operation of any of the four AHS RSCs investigated. However, reasonable malfunction management strategies were identified to significantly mitigate the consequences of the malfunctions and/or make the serious malfunctions significantly less likely to occur for all of the RSCs examined. The recommended malfunction management strategies (MMSs) are based on a “defense-in-depth” approach to achieving a desired level of safety—i.e., the likelihood of a potentially serious malfunction is minimized by use of reliable components and one or more levels of redundancy on 11 of the 26 major vehicle and infrastructure elements. One element, the zone control element, was judged sufficiently critical to warrant the use of three levels of redundancy. Considering the large number of current accidents in which human error causes or contributes to the accident (i.e., approximately 80 percent of current highway accidents are attributed to improper driving), an AHS that eliminates these kinds of accidents and incorporates a well designed, tested, and maintained set of malfunction management measures should be able to offer a level of safety much higher than that attained on current freeways.

Mixed Traffic

Mixed traffic (i.e., a single lane carrying both manually driven vehicles and vehicles under AHS control) is a situation that must be addressed by a malfunction management strategy even if it is not part of the RSC's normal operational mode. This is true because the potential for a) a failure that eliminates the ability of the AHS to control a vehicle or b) a non-AHS vehicle deliberately or accidentally penetrating the AHS-only environment will always exist. Also, a transition lane (in which a manually driven vehicle merges into the transition lane, is accepted into the automated system within the lane, and then changes lanes to a fully automated lane under AHS control) is a feature of many scenarios. This is an example of mixed traffic common to many RSCs. Therefore, mixed traffic must be accommodated.

Work done in support of IVHS has shown that vehicle systems to help the driver to avoid collisions or run off the road can be of substantial benefit. Extensions or modifications of some of these systems could be employed in an AHS to allow mixed traffic situations with reasonable levels of safety. It is the opinion of the area E team that mixed traffic scenarios probably possess levels of safety intermediate between current freeways and a potential AHS based on the total separation of manual and automated lanes.

Driver-In-The-Loop

The driver or passengers of an AHS vehicle should be able to make inputs to the AHS in certain cases, but the AHS cannot be designed to rely on these inputs for safe normal operation or to counter malfunctions. A basic assumption of the AHS is that the driver can be less alert (e.g., to read a newspaper) during the period that the vehicle is under automatic control; this cannot be violated. However, the driver/passenger must be able to alter some AHS processes such as the originally set destination to accommodate human “malfunctions” which could not be detected by the AHS (e.g., illness of a passenger). The AHS equivalent of the aircraft “pilot report” could increase safety and reliability of the AHS. In most cases, the driver should be allowed to move a malfunctioning AHS vehicle along the breakdown lane to the next exit after the automatic systems have responded to a malfunction by stopping the vehicle in the breakdown lane. This prevents the need for an AHS response team to respond to every minor AHS vehicle failure. Other examples exist but basically, driver inputs can a) improve the capacity of the AHS, b) increase the probability of completing the trip without significant outside intervention, c) reduce AHS cost of operation, and d) increase the convenience of the AHS experience.

Pallet Based AHSs

From a malfunction management viewpoint, pallets are a viable option possessing unique advantages and disadvantages. Advantages include a) control of pallet maintenance by a central authority results in a better maintained pallet compared to a privately owned AHS vehicle, b) higher utilization of the pallet compared to a private AHS vehicle allows greater investment in each pallet (i.e., one can afford more redundancy and/or more expensive/higher reliability systems), and c) because pallets only operate on the AHS, they can be optimized for that environment. Disadvantages include a) higher center of gravity which likely results in a

less stable vehicle, b) additional functions (e.g., vehicle load/unload and associated facilities, vehicle lockdown on the pallet, etc.) that are pallet-unique provide additional opportunities for malfunctions, and c) there will probably be a need for additional response teams to recover pallets with minor malfunctions. It is the opinion of the project team that, from a malfunction management viewpoint, the advantages of pallets probably outweigh their disadvantages.

Multi-Vehicle Incidents

The program team believes that it is very important to minimize the possibility of a significant multi-vehicle accident because of the impact on perceived safety of the system. The occurrence of one or more 10- to 20-vehicle accidents in the early stages of AHS introduction would tend to devastate public confidence in system safety and reliability, probably delaying widespread introduction for decades. The communications linkage of all AHS vehicles to a central authority provides the basis for minimizing the number of vehicles involved in such accidents. The basic responsibility of any vehicle involved in a collision or experiencing a malfunction that has a reasonable probability of leading to a collision is to inform the central authority of the situation immediately. The central authority can then take various actions (e.g., limiting travel speeds, stopping potentially affected vehicles, requesting driver input, rerouting traffic, etc.) very quickly that minimize the probability that numerous other vehicles will become involved.

Safety is an Imperative

Safety is the most important major AHS attribute. An RSC cannot be considered *good* unless it provides a degree of safety significantly beyond that provided on current freeway systems. In choosing components, systems, or techniques for the AHS, the predisposition of the program team is to include anything that can contribute to safety. Only if the inclusion of the item will substantially reduce system capacity, decrease convenience, or substantially increase cost should the item be excluded.

Capacity

Capacity is important, especially in urban areas. In urban areas, capacity and convenience are nearly synonymous. Most rural highways do not face a capacity crises, which makes increasing capacity over current levels much less important. This precursor study recognizes that the importance of increasing capacity varies between urban and rural AHS implementations; however, the project team has chosen not to explicitly evaluate any of the RSCs based on only urban or only rural implementation. Such an evaluation should be done in the future when the target RSCs are better defined. At this point it would detract from some of the other areas that must be covered (e.g., given fixed resources, evaluating each of the RSCs in both urban and rural environments might result in less consideration being given to identifying and assessing potential malfunctions or malfunction management strategies).

Therefore, this precursor study treats all examined RSCs as though they will be implemented with a single set of malfunction management strategies in both urban and rural settings.

Driver Training

The driver needs to possess an AHS driver's license to participate in the AHS system. It is this team's view that the driver will not inherently know how to do the basic driver functions—i.e., how to get on the system, enter the desired destination, relinquish control to the system, resume control at the end of the AHS ride, and exit the system. Still further training is anticipated with regard to the driver's responsibilities for vehicle maintenance and procedures/requirements appropriate in the event of an infrastructure malfunction or shutdown or collision with another vehicle. It is expected that drivers will also need instruction on how to respond to perceived unusual operation of their vehicle or the system—e.g., serious degradation of their vehicle, illness of a passenger, observation of deer or other animals in the median, etc.

Extracurricular AHS System Malfunctions

The introduction of AHS components or systems brings with it the potential for those systems to malfunction and cause, or contribute to, collisions or other unfavorable incidents. These malfunctions may not be limited to AHS vehicles operating under AHS control on AHS roadways, but could be induced by unwanted activation of AHS features or modes in "extracurricular" situations (e.g., normal manual operation of an AHS vehicle on residential streets).

INTRODUCTION

Increasing the safety of travel is a principal goal for an Automated Highway System (AHS) and one of the baseline assumptions of this study. Establishing the safety parameters and manner in which vehicle, highway, and human failures can be moderated to produce the minimum harm is likely to be one of the main drivers in selection of AHS architectures and system/vehicle implementations. A good understanding of the issues must be developed early in the program.

Normal operation of the AHS will significantly increase public safety by removing the driver from the loop, thus eliminating 70 to 80 percent of accidents caused by improper driving. An AHS will complement or supplant freeways and thus must provide a level of safety greater than driver-operated vehicles on already relatively safe roads. Introduction of the AHS also introduces a potential new cause of accidents - malfunction of the AHS infrastructure components and/or malfunctions of the AHS vehicle components. This task seeks to identify and analyze the major malfunctions associated with the four representative configurations (RSC), then develop and evaluate potential strategies to handle these malfunctions.

Scope of Study

The Automated Highway System (AHS) is a combination of vehicles and infrastructure designed to allow “hands-off” transportation from selected entry point to the selected exit point of the AHS. The complete system includes the vehicles, roadway, sensors, communications, and decision-making personnel and devices that permit this “hands-off” operation. Certain gray areas exist in this definition. For example, one could argue that the normal equipment on the car (e.g., engine, transmission, brakes, tires, etc.) either a) should, or b) should not, be included in the system. The team has chosen to include these components as part of the system because failures of these components would result in the vehicle not being able to reach its originally selected exit point from the system without manual intervention in many cases. However, the team has not emphasized developing malfunction countermeasures, but rather concentrated on those new parts of the system that are uniquely AHS in nature.

The purpose of this effort is to maintain the reliability, capacity, and safety of transportation on the AHS in the presence of malfunctions. The team has defined a malfunction as anything that causes the system to operate imperfectly. To accomplish this a malfunction management strategy (MMS) is required that will a) reduce the probability of malfunctions occurring, and b) reduce the adverse consequences of those malfunctions that do occur. The MMS for each RSC is a combination of several different types of countermeasures, each addressing a range of potential malfunctions.

Issues Addressed

Early in the program, this task area identified certain issues that would be addressed by the analysis. Later these were somewhat modified in light of interim research results as shown in table 1.

Table 1. Issues addressed by task area E.

Identification and categorization of potential malfunctions	The use of Fault Trees to identify the malfunctions are the major approach used. A limited amount of quasi-Failure Mode and Effects Analysis is also used.
Establishment of safety, performance and reliability requirements	General issues such as inspection and built-in-test are addressed. Certain performance levels and reasonable reliability are assumed. However, we did not plan to specify that to meet the AHS safety requirements the vehicle must have a MTBF of 10^6 hours or be able to accelerate from 40 to 60 mph in 1.4 seconds.
Estimation of collision consequences	"Collision" is used in a generic sense. We have estimated the consequences of the various malfunctions developed above. This procedure involves estimating the subjective probability of the malfunction occurring, the severity category of the most likely outcome of the malfunction, and the number of vehicles likely to be involved given the malfunction.
Collision Type	After further consideration, this is probably not as important as originally thought and possibly beyond our capability to do given the limitations of available information. Not performed.
Definition of MOEs	These were defined based on inputs from other precursor studies, and our Senior Technical Review Panel. The selected categories are Safety, Capacity, Convenience, and Cost. These categories were used to evaluated the various alternative proposed malfunction countermeasures.
Investigation of malfunction detection techniques	These have been investigated at a conceptual level (not at a specific hardware level) as a subset of development of malfunction management strategies. Not intended to select between detection techniques (e.g., selection of radar over vision as a headway sensor).
Development of malfunction management strategies	For each set of malfunctions for each RSC, a strategy is developed to either a) reduce the probability of the malfunction and/or b) reduce its consequence. This can include steps to detect the malfunction, decide the proper action to take, and implement that action. For some (but not all) malfunctions, alternative strategies are considered.
Human Intervention	The task E subteam staff now believes that human intervention should be allowed and encouraged within certain limits on the AHS. This intervention should not take the place of an automated MMS designed to bring the vehicle to a safe state, but it should allow the driver to participate in correcting unusual, breakdown, or emergency situations as appropriate.

Approach

Several approaches are viable for this precursor study. The team selected to define four representative system configurations (RSCs) to a level of detail necessary to define specific, relatively detailed, malfunctions of the AHS for each RSC. This approach allows the identification of specific, potentially appropriate MMSs for each RSC.

The sub-tasks accomplished during this study are briefly listed below:

- Developed an information base using other AHS precursor studies, PATH studies, IVHS information, and other transportation related sources.

- Developed four baseline RSCs and two variations for one of these RSCs. Included in these baseline RSC descriptions are the a) functions each RSC would need to perform and b) the systems or components needed to perform each function.

- Characterized a set of potential malfunction for each of the four baseline RSCs both from a) an operational/functional and b) a component/systems viewpoint. These malfunction sets were screened to select the ones most likely to involve safety; these became the malfunctions on which continuing analysis was performed.

- Estimated the seriousness of each of the potential malfunctions in the absence of an MMS _ i.e., what would happen if there was no means of correcting the situa tion. This provided a baseline against which the final set of MMSs could be compared.

- Developed countermeasure set(s) for each of the functional and systems malfunctions.

- Developed a set of measures of effectiveness (MOE) that allowed the team to subjectively judge how well each countermeasure set performed when applied to a malfunction or malfunction set. The four selected MOEs are safety, capacity, convenience, and cost.

- Rated each of the operational and component/systems countermeasures with respect to the four MOEs.

- Selected the best countermeasure set for each malfunction set (i.e., the one that rated highest when evaluated against the MOEs). This countermeasure set is the RSC's malfunction management strategy.

Figure 1 graphically illustrates this approach.

Assumptions

The following list provides the primary assumptions on which this study was based. Secondary assumptions, necessary for some smaller portion of this study, are described in the appropriate sections.

1. Normal operation of the AHS will significantly increase public safety by removing the driver from the loop thus eliminating a large proportion of current accidents which are caused by improper driving. An AHS will compliment or supplant freeways and thus

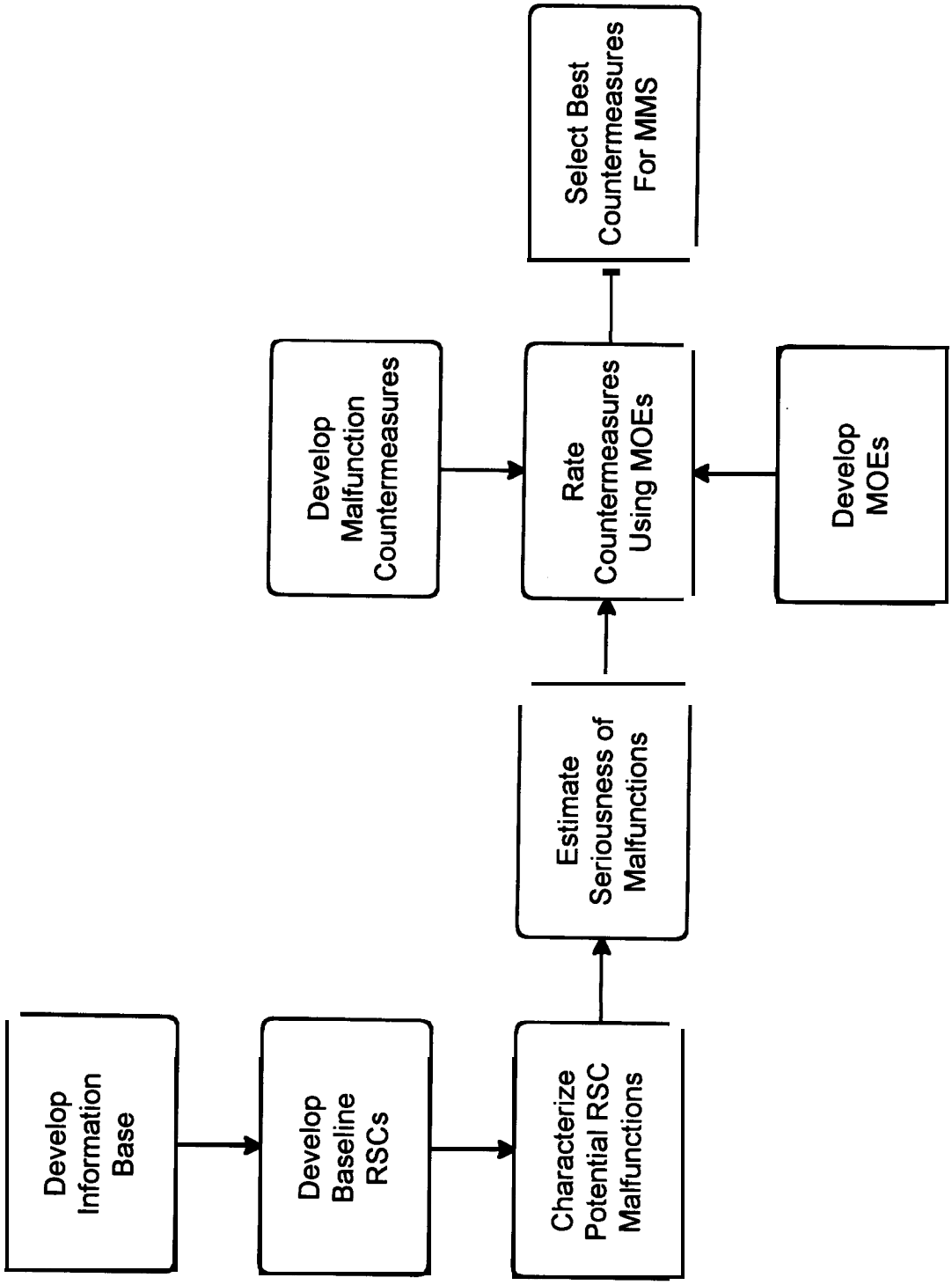


Figure 1. Subtasks of malfunction management study.

must provide a level of safety greater than driver-operated vehicles on these already relatively safe roads currently enjoy. Introduction of the AHS introduces a potential new cause of accidents - malfunction of the AHS. This task seeks to increase safety by identifying and analyzing the possible malfunctions associated with the four representative configurations (RSC), and developing strategies to handle these malfunctions.

2. One of the basic premises of the AHS is that safety will increase if one can eliminate the driver caused or influenced accidents. Since these accidents represent a large fraction of all accidents, this seems to be a reasonable premise - if two other assumptions are true.

.

of this premise is that the various operational functions that need to occur on the AHS (e.g., not running into other vehicles or roadway obstacles such as deer, tracking the lane centerline, commanding gaps to form in the vehicle traffic flow and having them form, and all the other required functions) actually can be made to occur with reasonable performance and at an affordable cost. The public will not be willing to repair or replace major portions of the AHS vehicle system during a normal operational life. Therefore, the AHS vehicle systems will have expected lifetimes at or greater than the expected operational life of the vehicle on the AHS.

.

either a) will not be used off the AHS, or that b) accidents caused by the use of AHS components off the AHS will not be counted against them. If AHS components are to be used off the AHS, then the possibility arises that failures of these components off the AHS will result in accidents. It would be fair to include these potential malfunctions against the AHS safety record only if one were also to explore the potential safety benefits of using the AHS components off the AHS. Both of these activities are beyond the coverage of this precursor study.

Representative System Configurations (RSC)

For the purpose of this document, the research team considered four primary representative system configurations (RSCs). Detailed descriptions of these RSCs can be found in the AHS Precursor Systems Analyses Overview Report. Only the characteristics of these RSCs relative to the research in this activity area are contained herein.

In general terms, the RSCs can be summarized as follows:

Table 2. Representative system configurations.

RSC	Traveling Unit	Headway Policy	Vehicle Intelligence	Guideway Intelligence
1. Average Vehicle Smart Highway	Individual Vehicle	Uniform	Average	Active
2. Smart Vehicle Average Highway	Individual Vehicle	Platoon	Autonomous	Passive
3. Smart Pallet Average Highway	Pallet	Uniform	Autonomous	Passive
4. Smart Vehicle Passive Highway	Individual Vehicle	Independent	Autonomous	Passive

Note: [1]RSC 2 consists of three lane configuration variations, resulting in a total of six specific RSCs.

Each RSC used in this research requires a specific definition of the associated roadway configuration. Three of the four primary RSCs (i.e., 1, 3, 4) were assigned only one roadway configuration, and one of the RSCs (i.e., 2) was assigned three different roadway configurations. The result is a total of six variations of the four primary RSCs, described by their *mainline, AHS access,* and *separation characteristics*.

Mainline

None of the RSCs investigated in this research effort involved a roadway which is completely AHS for all lanes, with no provisions for non-AHS vehicles. However, three distinctly different mainline roadway configurations were associated with the target RSCs and considered:

1. Two lanes in each direction, with the left lane in each direction serving mixed AHS and non-AHS traffic.

2. Three lanes in each direction with the left lane in each direction serving only AHS traffic.
3. Two lanes in each direction serving non-AHS traffic and a reversible lane between the non-AHS lanes serving only AHS traffic.

AHS Access

Access to the lane in which AHS is provided can involve a variety of entry/exit designs, some of which require maneuvering through non-AHS traffic to get to the AHS lane. Others simply provide direct access to the AHS lane via an exclusive ramp system.

For the sake of this research, entry and exit facilities were addressed only at a high level to determine compatibility with roadway design strategies. The main interest in entry/exit for this effort is simply to acknowledge whether a ramp system is on the left or right side of a lane set, spacing between terminals, and whether the ramp is intended for mixed or exclusive AHS flows. Other research teams have conducted detailed studies of entry/exit facilities (Area J—Entry/Exit Analysis) and their deployment, and have documented those results in other reports.

The following AHS lane access components were considered germane to the RSCs in this research:

1. Mixed Ramps—AHS vehicle enters/exits the freeway facility by using the same ramp facilities as non-AHS vehicles. Special lanes may be provided for AHS vehicles on the ramps to facilitate check-in and check-out, but the AHS vehicle must maneuver through non-AHS lanes when traveling between the AHS lane and the ramp system.

2. Exclusive Ramps—All entry and exit points serving the AHS are provided by ramps intended exclusively for the use of AHS vehicles only and are physically located such that no maneuvers by AHS vehicles through non-AHS traffic are necessary to reach the AHS lane.

3. Transition Lane—Similar to the mixed ramp concept where AHS and non-AHS vehicles utilize the same ramps, but includes a transition lane located adjacent to the AHS lane. The transition lane is used for maneuvers into and out of the AHS lane. Traffic flow in the transition lane may be AHS only or mixed flow, and AHS vehicles must maneuver through non-AHS lanes and traffic to reach the AHS lane.

Lane Separation

The means by which separation of AHS and non-AHS traffic is accomplished is closely associated with how entry/exit may be accomplished. In terms of the RSCs considered for this research, the following two concepts were considered:

1. None—Separation of AHS and non-AHS traffic is accomplished by signing and striping only.

2. Barrier—Physical barrier used to separate AHS and non-AHS traffic streams along the length of the AHS lane.

Using these characteristics, the resulting six variations of the four primary RSCs are summarized as follows:

Table 3. Global RSC characteristics.

RSC	Mainline Roadway Configuration	AHS Lane Access			Lane Separation	
		Mixed	Exclusive Ramps	Transition Lanes	None	Barriers
1	3 Lanes each direction Exclusive AHS Lt. lane	X		X	X	
2A	3 Lanes each direction Exclusive AHS Lt. lane	X			X	
2B	3 Lanes each direction Exclusive AHS Lt. lane		X			X
2C	2 Non-AHS lanes each direction Reversible excl. AHS center lane		X			X
3	3 Lanes each direction Exclusive AHS Lt. lane		X			X
4	2 Lanes each direction Mixed traffic Lt. lane	X			X	

The graphics on the following sheets illustrate the general roadway configurations of the six variations of RSCs used in this research. The basic assumptions as to how each RSC would operate in summarized in Table 4. Detailed descriptions of characteristics beyond the roadway deployment characteristics may be found in the AHS precursor systems analyses overview report.

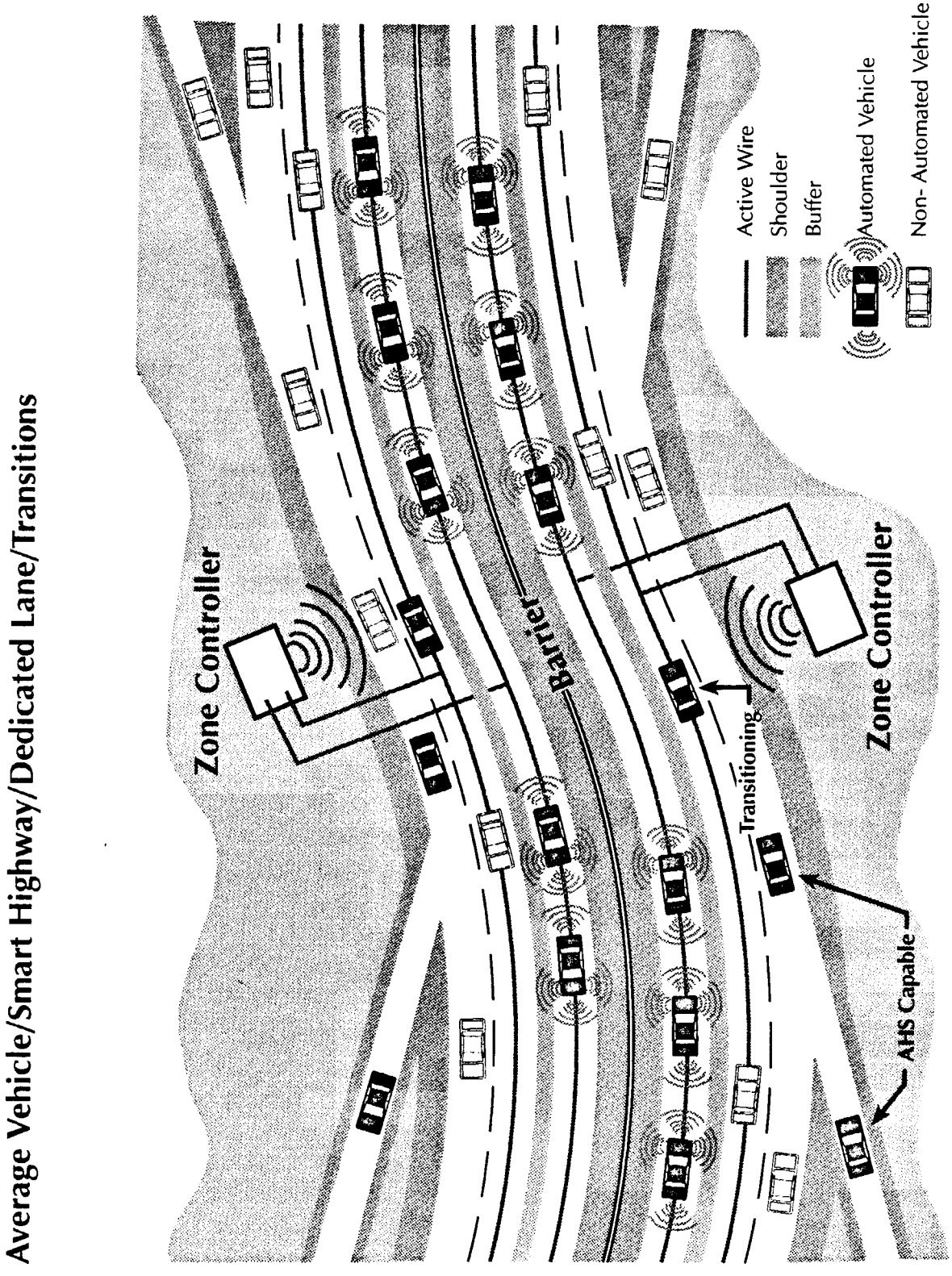


Figure 2. RSC 1.

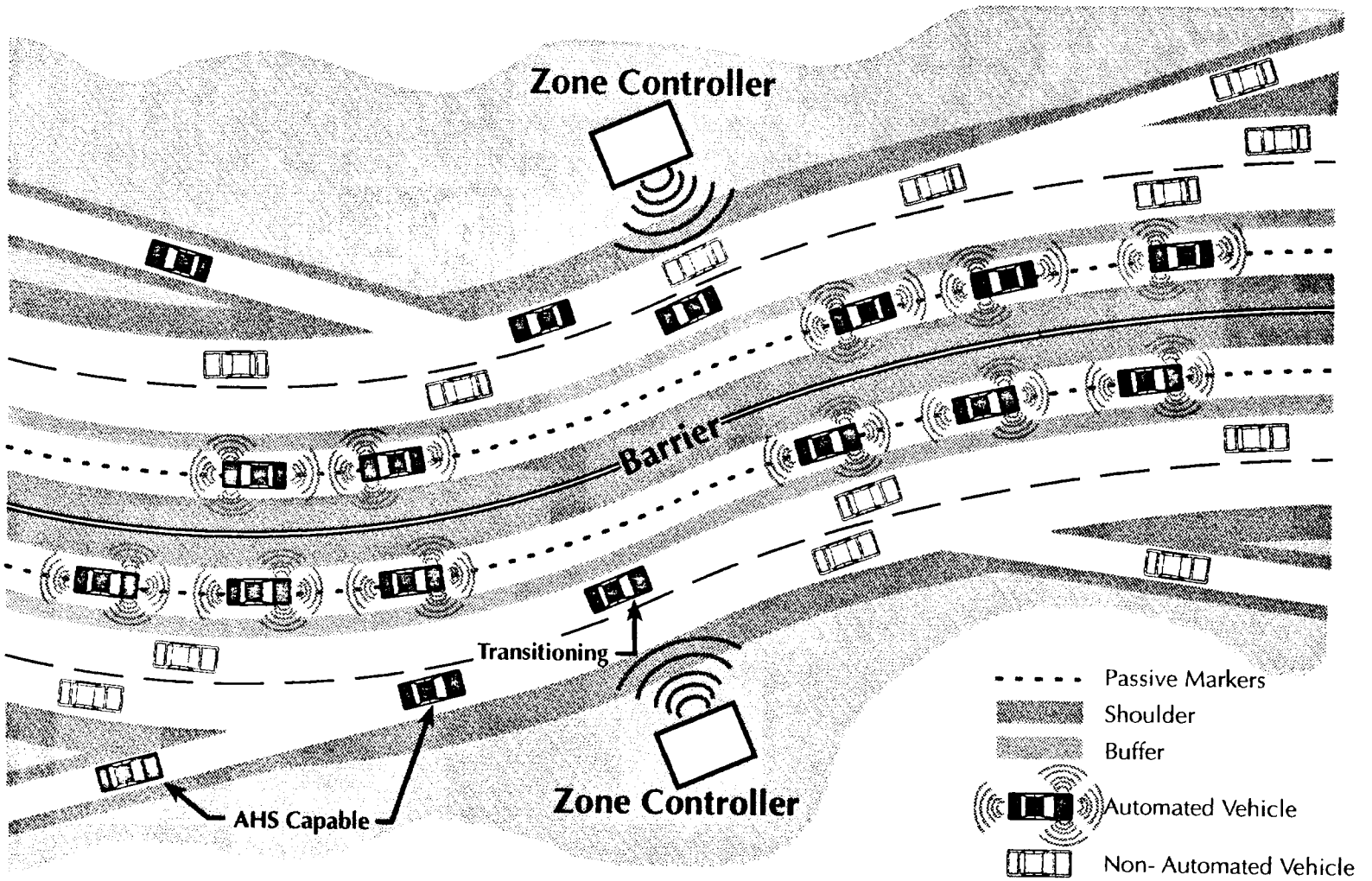


Figure 3. RSC 2A.

Figure 4. RSC 2B.

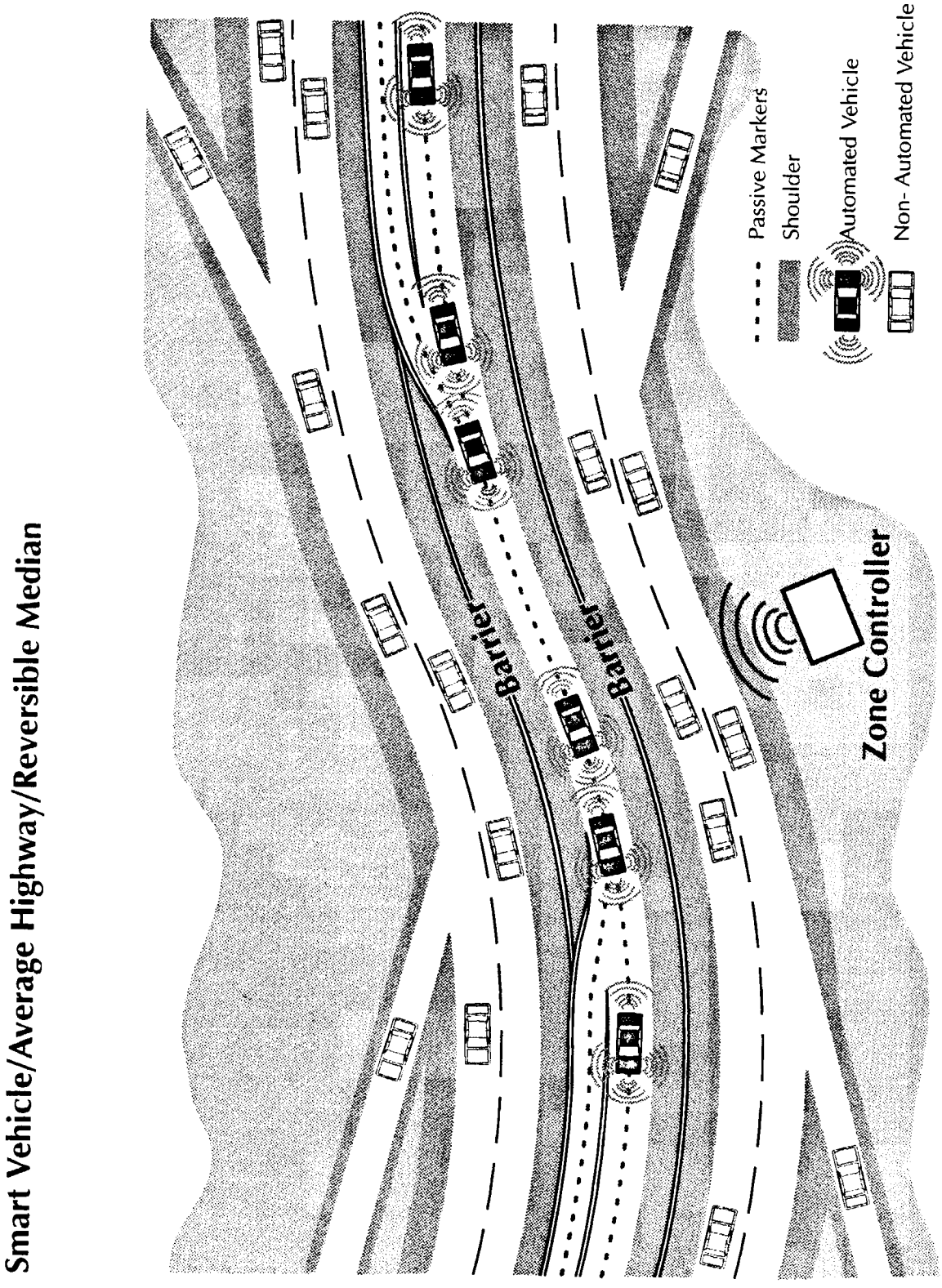


Figure 5. RSC 2C.

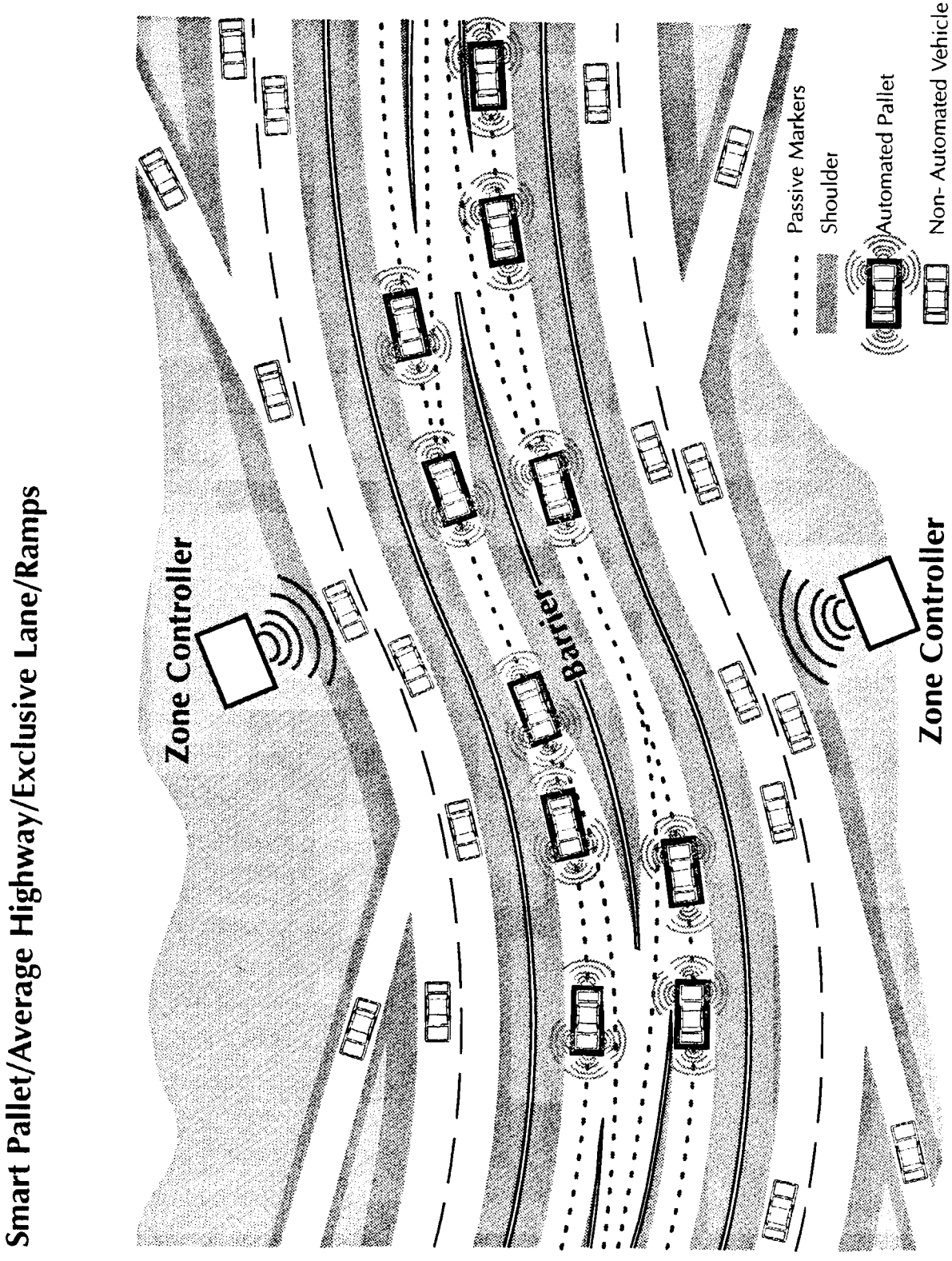


Figure 6. RSC 3.

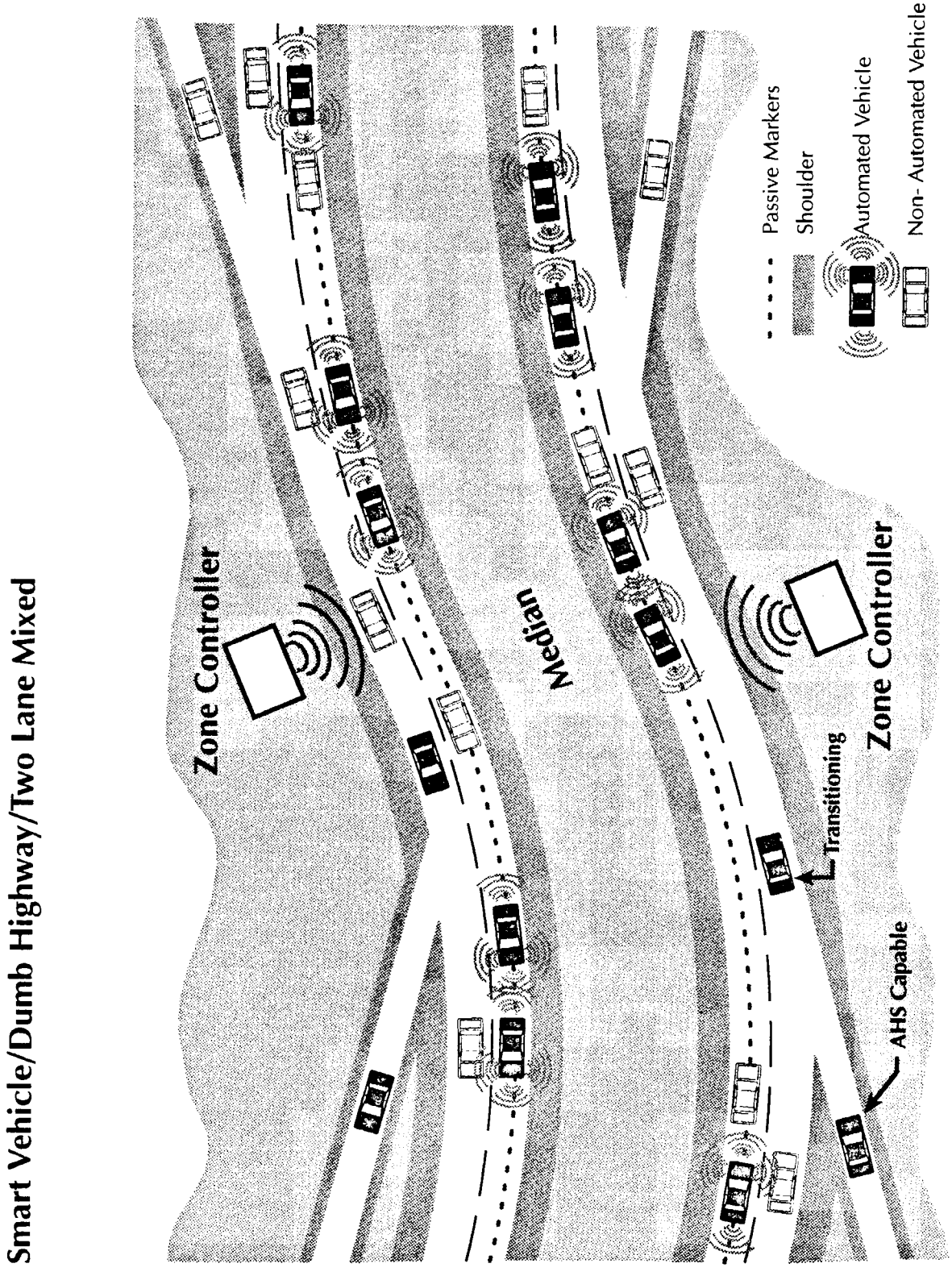


Figure 7. RSC 4.

Table 4. RSC assumptions.

Parameter	RSC 1	RSC 2	RSC 3	RSC 4
Vehicle Type	Individual Passenger Car	Individual Passenger Car	Single Car Pallet, Automatic Control Only	Individual Passenger Car
Headway Policy	Uniform	Platoon	Uniform	Independent
Vehicle Intelligence	Good	Smart	Smart	Very Smart
Roadway Intelligence	Good	Average	Average	Dumb
Lane Configuration	Mixed traffic on inside AHS lane with manual traffic on outside lane	Dedicated AHS lane(s) with transition lane and manual lane(s)	Dedicated reversible AHS lane with pullover space adjacent to AHS lane	All lanes mixed traffic
Barriers	None	None	Between AHS and Non-AHS Lanes Only	None
Entry/Exit Ramps	Current Type	Current Type	Current Types for Non-AHS Dedicated for AHS	Current Type
Transition to AHS	Where: In AHS lane When: At driver command after sector control OK How: Manual switch	Where: In Transition Lane When: At driver command after sector control OK How: Manual switch	Where: In Pallet Attach & Detach Area When: Upon link to pallet How: Automatic with link	Where: In AHS lane When: At driver command after sector control OK How: Manual switch
Check-Out of AHS Vehicle Systems	Combination of periodic certification and polling of internal sensors	Combination of periodic certification and polling of internal sensors	Pallets under control of central authority—Inspected before allowing on AHS	Combination of periodic certi-fication and polling of internal sensors
Failure to Transition Results In:	Driver must continue under manual control	Driver must continue under manual control in transition lane or re-enter manual lane	Essentially cannot fail to transition unless driver refuses to enter destination	Driver must continue under manual control

MALFUNCTIONS

The American Heritage Dictionary defines malfunction as 1) to fail to function, or 2) to function abnormally; perform imperfectly. As applied to the Automated Highway System, a malfunction occurs when the automated highway system fails to function or functions imperfectly. This can happen if the system does not fulfill any of a number of goals; for example:

- The system could fail to handle the specified number of vehicles per hour.
- The system could route vehicles to the wrong destinations.
- The system could not meet the safety levels expected.

Of the possible failures, not meeting the expected safety level is the most serious and deserves the most attention early in the program.

Not all problems or failures necessarily lead to malfunctions, even in the absence of a malfunction management strategy. Deterioration in the range resolution of an external sensor might place that sensor outside of its specified tolerance; however, it is not a malfunction unless the operation of the AHS is affected by this change.

Functioning of the RSCs

To identify potential malfunctions of the individual RSCs, one must understand how each RSC functions. The team's summary document describes the functions of the four RSCs explored in this study. The team does not have a task to detail design a complete AHS. In any event, such a task would be premature given the current degree of certainty concerning what AHS concept should be followed (e.g., individual vehicle platooning, mixed traffic independent headway, pallets controlled from a central location, etc.). The RSCs have been established in an attempt to provide a wide, but not exhaustive, range of concepts for evaluation purposes. We have established the definition of these systems at relatively high levels but containing sufficient detail so that the analysis of the malfunctions and possible management strategies will be of use to those who will make the decision concerning the future directions for the AHS.

The AHS is designed to allow a properly equipped vehicle to move from point to point on a freeway-type roadway without the need for the driver's intervention or close attention. This requires that the AHS perform those functions that the driver currently performs on manual roadways:

- Sense the vehicle's surroundings.

- Determine what maneuvers are appropriate given its navigational requirements and information about the vehicle's surroundings.

- Implement those maneuvers by using the ability to:

Additionally, the AHS must accomplish certain functions not presently required of a driver:

- Take control of vehicle movements from the driver at the appropriate time.

- Relinquish control of vehicle movent to the driver at the appropriate time.

- Recognize and safely handle conditions of driver inability to control the vehicle.

Because some of the studied RSCs envision that certain functions (e.g., determining what maneuver is appropriate) will be split between the vehicle and the infrastructure, the final requirement is the ability to:

- Communicate between the vehicle and infrastructure.

Failure to perform any of these functions adequately can be considered a malfunction with potentially serious consequences.

Identification of Malfunctions

To identify the various malfunctions possible for each of the RSCs, a functional block diagram showing the systems that would be needed to perform the AHS functions and the approximate location of those systems (i.e., in the vehicle or in the infrastructure) was prepared as shown in figure 8. Component or system based malfunctions can be easily defined once the system architecture has been established. These malfunctions involve failures in the various subsystems or components necessary for the functioning of the

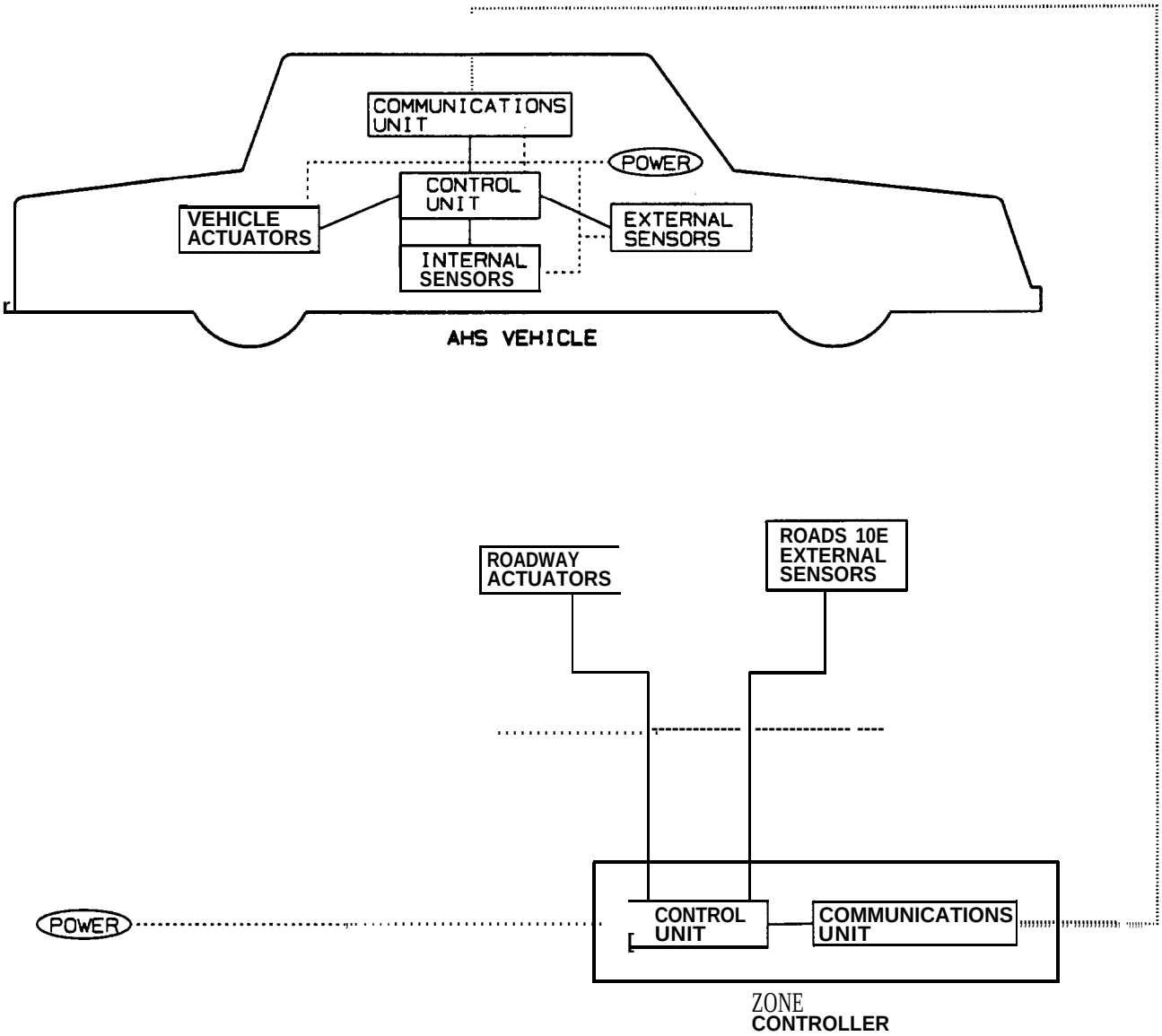


Figure8. AI- R3systemarchitectu reschematic.

RSC. At the most basic level a system comprised of two components, A and B, connected by a communications link can have the following mechanical malfunctions:

- Component A can fail.
- Component B can fail.
- The communications link can fail.

Because the purpose of developing the malfunctions for the RSCs is to allow the identification, development, and evaluation of various malfunction management strategies, it is necessary to develop the malfunctions beyond this most basic level. Simply understanding that the brake system of the vehicle may fail is insufficient. One must understand that the potential failure modes include:

- The brakes may be applied (fully or partially), regardless of control inputs.
- The brakes may not respond to a control input to activate.
- The brakes may respond to the control inputs but not at the proper level of force.
- The brakes may intermittently activate and de-activate, regardless of control inputs.

Each of these failure modes may require, or allow, its own malfunction management strategy.

The primary method used to define the component malfunctions is the fault tree. In the fault tree, the main fault is listed as the top of the tree (e.g., loss of lateral control), and the possible sub-faults that could lead to this consequence are connected to the fault via boolean operators. Because the purpose of these fault trees is to identify potential malfunctions, only OR gates are used. In developing these fault trees, the team has sought to evolve each to a level that will allow a reasonably technically sophisticated reviewer to appreciate the possible consequences of each failure mode without delving into component or subsystem design issues. The specialized fault trees developed for the subject RSCs is shown in appendix A of this report.

The major faults that would almost certainly lead to a collision or other unwanted consequence had been identified using the fault tree approach. It was originally thought that the malfunction (e.g., a flat tire) would lead rather straighforwardly to a consequence (e.g., a collision). After some consideration however, the team decided that it is not possible to directly connect the malfunction and the consequence without specific information about the RSC and the specific roadway. The consequences of a malfunction such as loosing track of the lane centerline depend upon the state of the roadway at the time of signal loss. If the weather conditions are good and the road is straight, the probable outcome will be an automatic braking to a stop in the AHS lane without leaving the lane and no collision with

other vehicles or fixed obstacles. If the weather renders the roadway slippery and the road is significantly curved, the probable outcome will involve leaving the confines of the AHS lane before the vehicle can brake to a stop. The possibility of striking another vehicle or fixed obstacle depend upon the presence of such targets.

The team wanted to make sure that no serious consequence was overlooked. In order to more closely link the identified malfunctions to the implementation of each RSC, the Battelle team developed a set of action timelines each describing a series of functions or events needed to be performed by the driver, vehicle, infrastructure, or communications links during each phase of the vehicle's journey on each RSC. These action timelines are presented in appendix B; one table for each of the four RSCs considered in this study.

Inspection of the required functions in the action timelines allowed the development of the operational malfunctions by negation of the required function. For example, for the required function *AHS destination set*, the associated malfunction would be *AHS destina tion not set.*. The analyst can identify what AHS components might be involved in the failure to set the AHS destination by reference to the AHS system architecture schematic. In RSC 2B the driver sets the destination on the AHS control panel and this information is transmitted to the zone controller where it is interpreted. Thus if the driver, vehicle control unit, vehicle internal communications bus, vehicle communications unit, zone controller communications unit, or zone controller control unit failed to perform its function to generate, relay, receive, or interpret the necessary information, the AHS destination would not be set. This information is shown in appendix C as malfunction timelines (so named because these malfunctions are tied directly to the actions in the action timelines).

Operational malfunctions have been limited to those malfunctions that directly involve some AHS operation. For example, in an RSC defined with parallel manual and AHS lanes, one could define a collision between two manually operated vehicles in a manual lane as an operational malfunction. The team has chosen not to consider such issues unless they directly affect the operation of the AHS traffic (e.g., parts from the collision intrude on the AHS lanes). This limitation allows the team to focus more closely on those issues unique to the AHS.

Seriousness of Malfunctions

Each of the failures to perform some AHS related function identified in the malfunction timelines was subjectively analyzed to determine whether it would likely result in a safety related consequence. The results of that analysis is shown on the Malfunction Timeline sheets. Those malfunctions that were judged to be potentially safety related were retained for further analysis while those judged not to be safety related were dropped from further consideration.

For each RSC, a matrix was developed which showed the various AHS components and subsystems along the horizontal axis and the selected malfunctions along the vertical axis. A complete set of these matrices are shown in appendix D. These matrices identify potential

involvement of components or subsystems in the selected malfunctions by placing a X at the intersection of the row and column representing the malfunction and the component, respectively. For example, the malfunction *Driver not aware of rejection* could be caused by a failure of the zone control control unit, the zone control communications unit, the power source for the zone controller, the vehicle AHS power source, the vehicle communications unit, the vehicle internal bus, the vehicle control unit, or the driver - and Xs are shown in the appropriate blocks.

A set of criteria were developed to allow the team to rate the seriousness of each malfunction. Three independent variables were selected; probability, scope, and severity. Probability is a measure of the chances that a particular component or system will malfunction. Scope is a measure of how many people or vehicles a malfunction will affect (assuming the malfunction occurs). Severity is a measure of the importance placed on avoiding the consequence of the malfunction (i.e., death is more severe than property damage because society places a higher value on life than on possessions). The scoring criteria used to rate each of these parameters is shown in tables 5, 6, and 7.

The team initially scored each of the RSCs based on no special malfunction management strategies being in place, but assuming that each RSC was designed with some minimal (unspecified) method of handling problems. Without this assumption, every minor problem would probably lead to a major consequence. No component or subsystem redundancy was assumed, but each system was assumed to be designed to a necessary high level of reliability (e.g., the vehicle control unit was assumed to have similar reliability to vehicle engine control computers today).

Initially, the assumption was that the team would have to place a score for each of the Xs in appendix D. This would have required placing nearly one thousand separate scores for RSC 1 alone. However, after some initial scoring using this method a pattern emerged. The scores for the probability and scope for a particular component or subsystem did not vary significantly regardless of the malfunction considered. Further, the scores for the severity for a particular malfunction did not vary significantly regardless of the equipment or subsystem involved. The matrices in appendix D were modified to allow scores for probability and scope associated with each component or subsystem and a score for severity associated with each malfunction.

Table 5. Probability.

Think in terms of five year blocks of time applied to subject unit (i.e., if the malfunction relates to a vehicle, think about a five year period in the vehicle's life; for an infrastructure malfunction, think of five years of infrastructure use).

Score	Rank	Probability of Occurrence	Description
5	High	>50%	Used to describe something that is quite likely to happen
4	Moderate	05 - 50%	Used to describe something that one is not surprised happened
3	Low	01 - 05%	Used to describe something that one is somewhat surprised happened
2	Very Low	0.1 - 01%	Used to describe something that one is very surprised happened
1	Remote	<0.1%	Used to describe something that one would have thought would not happen

Table 6. Scope.

How many vehicles is the malfunction likely to significantly affect?

Score	Number of Vehicles Affected	Description
4	>50	A widespread malfunction, likely involving the loss of the infrastructure control functions, that affects a very large number of vehicles (earthquake, major systemwide power loss)
3	13 - 50	A malfunction that is likely to involve more than a few nearby vehicles and spread to even more (possibly two platoons colliding)
2	4 - 12	A malfunction that is likely to involve one or two vehicles and then could reasonably spread to all those vehicle in the immediate vicinity (a loss of vehicle control resulting in a v/v crash and spilling into other lanes)
1	<4	A malfunction that is likely to directly affect one vehicle but could involve one or two other nearby vehicles because of the effect on the first vehicle (temporary loss of vehicle control resulting in one or two other vehicles bumped before the control system can bring the malfunctioning vehicle to a stop in the breakdown lane)

Table 7. Severity.

Think about the most likely outcome of the malfunction. One could say that a flat tire could lead to an accident involving multiple deaths; however, a more likely scenario is that it leads to a short, sharp transient which the control system is able to handle and move the vehicle over to the breakdown lane. Thus it would be scored a 2 rather than a 4.

Score	Description
4	A reasonable chance that a malfunction will lead to death or bodily injury. Characterized by high accelerations, fast changes in direction, loss of vehicle control that is not handled by the control system.
3	A reasonable chance that a malfunctions will lead to property damage. Characterized by medium to high accelerations, some loss of vehicle control but regained by the control system in a few seconds.
2	A reasonable chance that a malfunction will be limited to causing a delay. Characterized by low accelerations or a short,sharp transient, no loss of vehicle control or control re-established almost immediately, vehicle must be moved to breakdown lane or out of AHS.
1	A reasonable chance the malfunction will be nothing more than a nuisance. Characterized by low to very low accelerations or modest transients, no loss of vehicle control, driver/passengers may be startled, no need to leave AHS.

Key Results, Conclusions, or Issues

1. Potentially serious malfunctions (i.e., malfunctions that could result in death or serious injury and/or which could involve large numbers of vehicles) which could occur during operation of any of the AHS RSCs investigated exist. Therefore, a set of malfunction management strategies are required.

2. Rating each potentially serious malfunction for each RSC with regard to a) probability of the malfunction occurring, b) severity of the consequence if the malfunction did occur, and c) scope of the malfunction (i.e., the number of vehicles likely to be affected by the malfunction) provides the information needed to judge the seriousness of a potential malfunction.

3. Advantages are realized from viewing malfunctions in two different ways; a) failure of an AHS system or component or b) failure of a required function or operation to occur.

4. Probability of malfunction and the scope of the malfunction are mainly related to the failure of a component or subsystem while the severity of the consequence of the malfunction is mainly related to the effect on the operation of the AHS that results from the malfunction.

MALFUNCTION MANAGEMENT STRATEGIES

An MMS provides a method of handling events that interfere with the operation of the AHS. The MMS can either a) reduce the probability that a malfunction will occur, or b) reduce the adverse consequences of the malfunction when it does occur. With a complex system such as the AHS, the strategy is comprised of a collection of countermeasures, each addressing certain issues. Often these countermeasures overlap and provide multiple points of intervention in the malfunction process. The following general techniques were used to develop the countermeasures.

Reliability

Designing and producing components and subsystems having high levels of reliability will reduce the probability that a malfunction will occur. The adoption of high reliability Mil-Spec products by the armed services provides an excellent illustration of the advantages and disadvantages of using high reliability items to increase the chances of successful mission completion. High reliability Mil-Spec products are designed and produced to a high standard of quality and rigorously inspected to assure that they meet the required standard. As a result, these products demonstrate higher levels of reliability than would other products operated in the same manner and environment. These products also usually cost significantly more than other products that accomplish essentially the same function. Also, these products are often behind the most recent advances in commercial technology because of the long design/testing cycle required and the high cost of development and certification.

High reliability can also be achieved by regular maintenance and inspection of good quality commercial components. A major factor in Mercedes automobiles having such long lives and high reliability is that most Mercedes owners carefully follow the suggested maintenance schedule, which requires comparatively frequent inspection and maintenance intervals. Small problems can be caught and rectified before they cause a problem on the road. However, these comparatively frequent service calls cost and inconvenience the owner. The project team doubts that the general public would be willing to subject their vehicle to a set of frequent inspections for the ability to travel on the AHS, unless the AHS provided great benefits compared to other modes of travel.

Reliability improvement alone is insufficient for system components or links that provide single point catastrophic failure potential, unless reliability is improved to a very high order or other countermeasures are impossible or impractical. Secondary countermeasures must be implemented to handle the malfunction on those occasions that it does occur.

Passive Redundancy

Passive redundancy exists when the failure of one system component or link does not degrade system capability because other system components or links exist to carry the load without the need to switch in backup systems. This is a second technique that can be used to reduce the probability of a malfunction. An example of passive redundancy is the use of four or five bolts to hold on a wheel when two or three would be adequate to carry the maximum load envisioned.

Sometimes, passive redundancy implies no loss of rated system capacity (i.e., the system should still be able to function to its maximum rated limit). However, some loss of overload protection is lost. If the wheel is designed to withstand 3000 pounds of sideload with all bolts in place, it should be able to withstand that same amount of sideload with one bolt missing or broken. However, this probably means that the wheel could have withstood 4000 pounds of sideload with all bolts in place and properly tightened. Thus full rated capacity is maintained but some overload protection is lost.

Sometimes rated system capacity is lost. For example, one form of passive redundancy incorporated into current vehicles is the dual brake system. Two wheel brakes are on one hydraulic circuit while the other two brakes are on second circuit. Loss of one brake line does not eliminate the braking capability of the vehicle, however it does reduce the braking capability.

There are advantages and drawbacks to both active and passive redundancy. Under passive redundancy the partial failure often remains undetected and there is a loss of reserve capacity. The next partial failure could cause a malfunction. Ideally, the partial failure should be detected and a warning issued so that the level of reserve capacity is maintained. However, this requires some type of sensor, or a more frequent inspection interval, to detect the failure - which costs more and increases system complexity. In cases where passive redundancy is attractive, it often costs less than active redundancy because no system need exist to recognize the loss of the primary component and switch in the backup component.

Some specific examples of passive redundancy that might apply to the AHS include:

- A vehicle computer that has three independent sections. Each section votes on the proper command to issue. If all three agree, within a set tolerance zone, the computer is assumed to be functioning properly. If one section is outside the tolerance limits set by the other two sections agreement, that section is assumed to have failed and will not be allowed to control any AHS operations.

- The zone controller may locate vehicles on the roadway via the use of vision devices (cameras). The zone of coverage of these vision devices may overlap by 50 percent. The failure of a single vision device would still allow the entire roadway to remain under observation from the adjacent vision devices (under specified visual conditions).

Active Redundancy

Active redundancy exists when the failure of one system component or link can be compensated for by the activation of a backup component or link. Active redundancy is a technique that can be used both to a) reduce the probability of a malfunction, and b) reduce the consequences of a malfunction. An example of active redundancy is the activation of a backup power supply to provide power to a computer in the event of a power failure on the main circuit. If the backup power supply switched in before the operation of the system was affected, and it is capable of handling the entire power needs of the system, this is an example of reducing the probability of a malfunction. If the backup power supply switched in after the operation of the system was affected, or if the power supply can only handle part of the needs of the system, this is an example of reducing the consequences of a malfunction (i.e., limiting the duration of the malfunction). There is a tradeoff between the amount of capacity retained by the backup system and the cost of that system; backup systems with no loss of system capacity usually cost more than ones that accept some loss of capacity.

Some specific examples of active redundancy that might apply to the AHS include:

- The provision of dual actuators for steering control. The primary actuator is normally used to position the wheels under control of the vehicle control unit. A secondary, or backup, actuator can be switched in should the primary actuator fail.

- The provision of two cables linking the roadway sensor to the zone control. If one cable should fail, the second can be used to continue communications.

Adaptive Control

An adaptive control strategy changes the method used to control the system based on those parts of the system that are still operating. It is a techniques used to limit the adverse consequences of a malfunction. This technique can be applied at multiple levels in the system. At the unit level, modern fly-by-wire aircraft may be able to compensate for the loss of certain control surfaces by using others in a non-standard manner (e.g., if ailerons become inoperative, the system might be able to use differential elevons for roll control). At the overall system level, the aircraft experiencing the aileron failure may be given a different set of rules to follow (i.e., the need to strictly follow a flight path may be relaxed; other traffic will be diverted).

Depending upon the failure, and the robustness of the control system, adaptive control may or may not result in the loss of system capacity or performance. In the example above, with ailerons fully operational, the aircraft might have a roll rate capability of 90^{o} per second. Using only differential elevons that rate might be reduced to 60^{o} per second. Adaptive control requires the ability to sense the failure of part of the control system and alter the normal way of doing business to retain the maximum amount of critical control functionality.

Some specific examples of active redundancy for the AHS include:

- The potential use of downshifting the transmission and using engine braking in the event of a loss of braking function.

- The stopping, slowing, or rerouting of the AHS traffic flow in response to a collision or breakdown on the AHS.

A Comparison of Countermeasure Techniques

Table 8 provides a comparison of the various countermeasure techniques with respect to means of detection, decision, and intervention. As one moves further along the continuum of countermeasure techniques, the complexity involved in providing the countermeasure increases.

Table 8. Comparison of malfunction countermeasure techniques.

	Reliability	Passive Redundancy	Active Redundancy	Adaptive Control
Detection	_	Potentially required to avoid loss of reserve capacity	Sensor required	Sensor required
Decision	_	_	Moderate intelligence required	High intelligence required
Implementation	Design, production, and inspection	Design, production, and inspection	A - B switch	Normal components or systems used differently

Developed Countermeasures

Sets of countermeasures were proposed for both the component/system malfunctions and the operational malfunctions identified. These malfunction countermeasures are shown in appendix E for the Equipment/Component Countermeasures and Appendix F for the Operational Countermeasures. In referring to these appendices, one will see ratings attached to each countermeasure. Those ratings, and the process by which they were developed, are described in the section of this report entitled *Evaluation and Selection of Countermeasures*.

MEASURES OF EFFECTIVENESS

In any program that seeks to choose between several possible courses of action, a set of criteria must be established by which the various alternatives can be evaluated. In this program, these criteria are known as measures of effectiveness (MOE). Any MOE can be viewed as a cost/benefit ratio; the cost of installing the malfunction management strategy must be smaller than the benefit derived therefrom.

Criteria

In deciding what MOEs should be used, the program team referred to the RFP, the results from the interim meeting, and internal discussions (especially those involving our senior technical review panel). Given these sources, the characteristics that seemed to be of most importance were to maximize safety, capacity, and convenience while minimizing cost.

A balance must be struck between these four characteristics. The program team has identified safety as being the most important of these characteristics, however exceptional safety without reasonable capacity, publicly acceptable convenience, and affordable cost is useless because without balance very few will use the Automated Highway System. In making decisions concerning the makeup of the AHS, the program team decided to use the following guidelines.

- Safety is the most important of the four major AHS characteristics. An RSC cannot be considered viable unless it provides the public with a degree of safety at least comparable to the current freeway system. An RSC cannot be considered good unless it provides a degree of safety significantly beyond that provided on current freeway systems. In choosing components, systems, or techniques for the AHS, the predisposition of the program team is to include anything that can contribute to safety. Only if the inclusion of the item will substantially reduce system capacity, decrease convenience, or increase cost will the item be excluded.

- Capacity is important, especially in urban areas. In these urban areas, capacity and convenience are nearly synonymous. Most rural highways do not face a capacity crises, which makes increasing capacity over current levels much less important. This precursor study recognizes that the importance of increasing capacity varies between urban and rural AHS implementations, however, the project team has chosen not to explicitly evaluate the RSC based on urban versus rural implementation. Such an evaluation should be done in the future when the target RSC is better defined, however, at this point it would detract from some of the other areas that must be covered (e.g., given fixed resources, evaluating the RSCs in both urban and rural environments might result in fewer malfunctions or malfunction management strategies being considered). Therefore, this precursor study treats all examined RSCs

as though they will be implemented with a single set of malfunction management strategies in both urban and rural settings.

- Convenience of use is necessary to gain public acceptance of the AHS. A prime driver for the AHS is freeing time for the motorist; by decreasing the time required for the trip and by freeing the motorist to concentrate more on non-driving activities during the AHS trip. An AHS that requires substantial time on the motorists part, either during the trip (e.g., a long check-in period) or offline (e.g., frequent mandatory inspections), is not likely to be popular or widely adopted. The project team has tried to include features in the final RSCs that will maximize convenience while not significantly impacting safety.

- Cost of individual participation in the AHS will significantly impact the propor tion of the population that will or can participate. This is unsurprising because cost is the most common way we ration in our society. In the case of the AHS, however, the project team believes that the cost of individual participation must be affordable to the large majority of the public that currently use private automobiles or the public will not support the project. Therefore, measures that would cost a significant amount to implement are not rated very highly.

The criteria above are used to rate each of the countermeasures developed in appendices E and F of this report. The scoring process and rating system are shown in the next section.

Accident Reduction Goals

A major feature of the AHS is that it will have fewer and less severe accidents than are currently experienced. The AHS will, at least initially, replace or supplement parts of the interstate highway system, thus safety comparisons should be made to that system. The AHS introduces automation to reduce/eliminate driver-caused accidents. Thus one wants to have the number of automation failures to be fewer than the number of driver failures currently seen on freeways. This section seeks to define a rough order-of-magnitude goal for AHS vehicle system reliability to reduce the number of accidents caused by malfunctions of the AHS.

Basic assumptions include:

- Only AHS vehicle system failures leads to an accident.

- All AHS vehicle system failure lead to an accident.

Table 9, based on data drawn from *Accident Facts*, National Safety Council 1990 edition, shows the number and severity of accidents experienced on the interstate highway system. *Accident Facts* also indicates that 72.7 percent of all accidents involve improper driving. The following results conclusions can be drawn from this information.

· The number of vehicle accidents on interstates is approximately one accident per 375,000 vehicle miles traveled.

Table 9. Accidents by class of trafficway, 1989.

	Fatal Accidents	Injury Accidents	Property Damage Accidents	Deaths	Injuries
All Trafficways	41,300	1,100,000	11,700,000	46,900	1,700,000
URBAN					
Total Number	14,500	740,000	8,700,000	16,400	1,090,000
% on Interstates	17.7%	11.8%	9.5%	18.0%	12.0%
Number on Interstates	2,567	87,320	826,500	2,952	130,000
RURAL					
Total Number	26,800	360,000	3,000,000	30,500	610,000
% on Interstates	11.5%	9.8%	10.4%	11.7%	10.0%
Number on Interstates	3,082	35,280	312,000	3,569	61,000
COMBINED					
Total Number	41,300	1,100,000	11,700,000	46,900	1,700,000
% on Interstates	13.68%	11.15%	9.73%	13.90%	11.28%
Number on Interstates	5,649	122,600	1,138,500	6,521	191,800
Rate per 100M Vehicle Miles (assumes same proportion of travel on interstates in 1989 as in in84, i.e. 20.5%)	1.32	28.72	266.75	1.53	44.94

Accident Facts, National Safety Council, 1990 Edition.
Source based on five state traffic authorities.

· If elimination of the improper driving prevents the accident from occurring, then malfunctions of the AHS must not allow an accident more often than every 516,000 vehicle miles traveled.

Since the goal of the AHS is to have fewer accidents than current roadways, an initial goal of one malfunction-caused accident every 1,000,000 vehicle AHS miles traveled appears reasonable (i.e. the AHS eliminates improper driving accidents and for every two improper driving accidents that occur on current interstates we would allow one malfunction-caused accident on a future AHS). This would result in approximately a 36 percent reduction in accidents on the AHS compared to current interstates (i.e., those accidents not caused by improper driving would not be affected). Some may believe that the initial goal should be set higher, and indeed it probably should, but this discussion is meant to set a minimum goal beyond which the AHS must leap just to qualify for consideration.

The AHS vehicle will probably command a significant price premium over the same type vehicle without AHS equipment, therefore an individual is not likely to purchase the AHS vehicle unless he plans to make substantial use of its AHS capability, say 20 percent of the time spent in AHS mode. The average American vehicle currently has an expected life of roughly 100,000 miles (a figure that may well increase over time), thus the AHS life might be

roughly estimated at 20,000 miles. This is equivalent to approximately 333 hours at 60 miles per hour.

So, if one malfunction-caused accident is allowed every 1,000,000 AHS miles driven, and the average life expectancy of the AHS vehicle is 20,000 miles, then only 1 in 50 AHS vehicles can experience an AHS malfunction-caused accident. Another way of saying this is that 98 percent of AHS vehicles will never be involved in an AHS malfunction-caused accident, or that 2 percent of AHS vehicles will be involved in an AHS malfunction-caused accident.

The AHS vehicle likely must have the following systems to be able to operate in an automated mode:

- A sensor to determine forward gap.
- A sensor to determine lane centerline.
- A steering actuator.
- A brake actuator.
- A throttle actuator.
- A control unit to decide what should be done.
- A communications unit to link the vehicle to the infrastructure and other vehicles.
- An internal communications bus to link the systems above.
- A power source for the units above.

Thus we see that, at a minimum, each AHS vehicle (with 9 critical sub-systems) must be 98% reliable over a 20,000 mile (333 hour) life. If we assume that:

- Each sub-system is independent.
- Each sub-system has an equal chance of failure.
- The sub-systems are operating in the constant failure rate portion of the bathtub curve.

Then we can use the mean time between failure (MTBF) concept and estimate how long an MTBF would be required for each sub-system.

Since: P(vehicle life of 333 hours) = .98
Then: P(sub-system life of 333 hours) = .9978

To obtain this reliability for an expected life of 333 hours, each sub-system must have an MTBF of approximately 150,000 hours. Given the complexity of the tasks involved, and the maturity level of the sub-systems involved, this is probably an unreasonable goal.
One could allow a simple duplication of each sub-system function to reduce the required MTBF. The operational requirement could then be stated that

> "The failure of an AHS vehicle sub-system will require the AHS vehicle to remove itself from the AHS within 1 hour after the failure and not to return until the failure is repaired."

Thus, one is now examining the probability of, for example, a second communications unit failing within a one hour time span of the first communications unit failing. This probability is approximately that of a single communications unit failing within any one hour period during the AHS life of the vehicle. Then, instead of requiring a sub-system to have a MTBF of 150,000 hours, the requirement is reduced to a MTBF of 454 hours.

The MTBF for each sub-system would probably need to be higher than this if one wanted to sell many AHS vehicles. With an MTBF of 454 hours, and an expected AHS vehicle life of 333 hours, one would expect to replace or repair about 25 percent of the AHS vehicle sub-systems during the life of the vehicle. If the MTBF could be raised to 1000 hours, then one would expect to replace or repair only about 5 percent of the AHS vehicle systems during the life of the vehicle. This 1000 hour MTBF translates to probably 1 AHS vehicle system repair during the vehicle's life compared to 4 or 5 if the MTBF were 454 hours. A 1000 hour MTBF would also increase the sub-system reliability over 333 hours to .999, which increases vehicle reliability to approximately 99 percent, thus reducing the accident rate even further.

Therefore, malfunction management strategies such as redundancy and adaptive control need to be incorporated into the AHS for it to meet the target specification (i.e., that there are fewer accidents as a result of the malfunctioning of the AHS compared to the failure of the human driver on today's freeway system).

EVALUATION AND SELECTION OF COUNTERMEASURES

The countermeasures developed to manage the malfunctions identified for each RSC are shown in appendices E and F. Each countermeasure is method to handle an identified potential malfunction; together the sum of all the countermeasures for an RSC make up the malfunction management strategy for that RSC. These countermeasures were each evaluated by the project team using the scoring system shown in the Appendices.

As a result of these ratings, the project team has prepared a set of malfunction management strategies for each investigated RSC. Due to the manner in which the equipment portion of the RSCs were defined, all four RSCs can be covered with a single table providing the team's recommended AHS Vehicle Systems (table 10). Likewise the same can be accomplished for the for the Recommended AHS Infrastructure (table 11). These two tables provide countermeasures relying primarily on reliability and redundancy to minimize the potential for a failure that can adversely affect the operation of the AHS. Recommended operational AHS malfunction countermeasures are shown for all the RSCs in table 12. The countermeasures in this table are directed towards minimizing the consequences of an failure, once the failure has occurred. Together, these tables provide the team's suggested malfunction management strategy for each RSC investigated.

The consensus opinion within the team is that the malfunction management strategy selected for a particular embodiment of the AHS should be based on a defense-in-depth principle. Initially, techniques such as reliability, passive redundancy, and active redundancy should be used to limit the number of failures that affect the operation of the AHS to the lowest level that are economically practical. Since it is probably cost prohibitive to eliminate the possibility of failure, other techniques such as adaptive control should be used to limit the consequences of the malfunctions that do occur.

Table 10. Recommended AHS vehicle systems.

DESCRIPTION	COUNTERMEASURE
Rear Gap Sensor (RSC 4 only)	No backup required. Sufficient built-in-test should be provided to alert driver to failure of the unit. This unit is used to trigger lights/horn if a Non-AHS vehicle is approaching too closely and too rapidly from the rear. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS.
Lateral Sensors (4 used)	No backup required
Vehicle Control Unit including Driver Interface	Three independent control units and vehicle interfaces. The units continually vote on required actions, if one disagrees with the other two (outside a tolerance zone) it is considered failed and will not be allowed to participate in any more control decisions. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS.
Vehicle Communications Unit	Two independent communications units and interfaces with error detection in messages (error detection eliminates need for third unit). In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS. Platooning depends so highly on intravehicle communications that such vehicles might warrant and additional communications unit or communications units of higher reliability.
Brake Actuator	Two independent actuators. If the operational actuator does not adequately respond to control inputs it will be deactivated and the other actuator will be activated. The actuator should be designed so that it cannot fail with the actuator holding the brakes in a partly or fully activated condition. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS. Anticipated brake-by-wire system eliminates need for brake pedal cutout.
Steering Wheel Cutout (not required on RSC 3)	Two independent cutouts are placed in series in the steering wheel shaft. Each unit operates like a magnetic clutch. When the unit is operating (i.e., in the AHS mode), it disconnects the upper and lower shafts from each other. When the unit is off (or has failed), the upper and lower shafts are mechanically connected. In the event of a unit failure, maintenance will be required before the vehicle will be allowed back on the AHS. In the very unlikely event that both independent units fail during a single trip, then the upper and lower steering shafts will be connected, and a manual steering capability will exist. Failure does not prevent the AHS from steering the vehicle; however, it does allow the driver to steer the car and override the AHS steering commands in the event of another emergency or failure occurring.
Steering Actuator	Two independent actuators. If the operational actuator does not adequately respond to control inputs it will be deactivated and the other actuator will be activated. The actuator should be designed so that it cannot fail by locking the steering in one position. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS.
Throttle Actuator	Two independent actuators. If the operational actuator does not adequately respond to control inputs it will be deactivated and the other actuator will be activated. The actuator should be designed so that it cannot lock the throttle in one position. In the event of a failure, maintenance will be required before the vehicle will be allowed back on the AHS. Anticipated computer control of throttle position eliminates need for throttle cutout.
Forward Gap Sensor	If the sensor is of relatively low cost, the unit should be designed to provide three independent measures of gap. The units continually vote, if one disagrees with the other two (outside a tolerance zone) it is considered failed and will be ignored. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS.
	If the sensor is of higher cost, the unit should be designed to provide two independent measures of gap and incorporate sufficient built-in-test to identify a failed unit. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS.

Table 10. Recommended AHS vehicle systems (continued).

DESCRIPTION	COUNTERMEASURE
Centerline Sensor	The sensor should be designed to provide three independent measures of centerline position. The units continually vote, if one disagrees with the other two (outside a tolerance zone) it is considered failed and will be ignored. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS. (Team believes this will be a relatively low cost sensor).
Vehicle Communications Bus	Two independent communications buses with error detection in messages (error detection eliminates need for third unit). In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS.
Driver	AHS specific training required, including normal, emergency, and unusual situation procedures. Periodic retraining and recertification may be required.
Vehicle Lockdowns (4 used) (RSC 3 only)	These lock the vehicle to the pallet by attaching themselves to each vehicle wheel. No redundancy required. Normal pallet maneuvering limited so that if one or two of the four lockdowns has a solid lock the vehicle should remain on pallet. System to assure vehicle is locked to pallet before pallet moves from loading dock.
External AHS Vehicle Lights and Directional Siren (RSC 4 only)	No backup required.
AHS Power Supply	Normally drawn from vehicle with a separate battery backup on an independent circuit. In the event of a failure, driver will be informed and maintenance will be required before the vehicle will be allowed back on the AHS.

Table 11. Recommended AHS infrastructure.

DESCRIPTION	COUNTERMEASURE
Zone Control Personnel	Special training and periodic retraining and recertification. Duty aids such as computer based checklists and expert system/fuzzy logic assistance. More than one person per zone control station on each shift.
Centerline Wire (RSC 1 only)	Wire must have a backup. To the extent possible, wires should be "insulated" from exterior forces such as earth movement, freeze/thaw cycles, and animal attack.
Markers (RSCs 2, 3, and 4)	Magnetic markers should be spaced so that at least one can be missed without allowing the vehicle to move out of the acceptable centerline track tolerance.
Environmental Sensors	Realistically located to pick up important environmental conditions such as sleet, snowfall, wind, temperature, rain, fog, etc. Sufficient coverage for adequate condition reporting. Sufficient number of environmental sensor stations exist so that the non-provision of data from a sensor or two at a single station for a few hours likely is of small consequence.
Link from Environmental Sensor to Zone Control	Single land line from each sensor station to zone controller. No backup required. Sufficient number of environmental sensor stations exist so that the non-provision of data from a single station for a few hours likely is of small consequence.
Roadway Sensors	Realistically located to pick up important roadway conditions such as traffic density, roadway surface conditions (including ice), animals on road, etc. Visual systems have overlap during normal visibility conditions. Thermal imagers for night and bad weather (probably won't have full coverage under these conditions). Sufficient number of sensor stations exist so that the non-provision of data from a single station, for a few hours likely is of small consequence.

Table 11. Recommended AHS infrastructure (continued).

DESCRIPTION	COUNTERMEASURE
Link from Roadway Sensor to Zone Control	Single land line from each sensor station to zone controller. No backup required. Sufficient number of roadway sensor stations exist so that the non-provision of data from a single station for a few hours likely is of small consequence.
Zone Control Control Unit	Four independent control units and interfaces. The units continually vote on required actions, if one disagrees with the other three (outside a tolerance zone) it is considered failed and will not be allowed to participate in any more control decisions. Three control units would have to fail (or two units simultaneously and in a manner that produces identical errors) before the zone control output would be affected. In the event of a failure, maintenance will be initiated immediately to return control unit to full status as quickly as possible. Team believes this likely is the most critical infrastructure function and affects largest number of vehicles with even a small failure.
Zone Control Communications Unit	Two independent communications units and interfaces with error detection in messages (error detection eliminates need for third unit). In the event of a failure, maintenance will be initiated immediately to return communications unit to full status as quickly as possible.
AHS Power	Normally supplied by regular electric grid. UPS sufficiently large to handle full load for a period sufficient to try to start standby generator several times and then effect an orderly shutdown of roadway. Standby generator to take over from UPS, normally within a few minutes. Priority on repair of main electric grid.
Dock System (RSC 3 only)	No backup required. Multiple loading stations available at a single loading location, some proportion of these stations will always be under repair.

Table 12. Recommended operational AHS malfunction countermeasures.

The following countermeasures assume that a failure has occurred that will negatively affect the performance of the AHS. Given the redundancies built into the vehicle and infrastructure as outlined in Tables 6 and 7, these failures should be a very infrequent occurrence. However, given that such failures can occur, they must be dealt with in a manner to limit the degree to which the failure affects the AHS.

Since the team determined that safety is of significantly higher importance than convenience or capacity, the countermeasures were conceptualized to introduce the maximum amount of safety in as wide a range of scenarios as possible. In general, the countermeasure seeks to place the subject vehicle in a safe state (one in which the vehicle possess low energy and a predictable location - this usually means stopped) as quickly as possible.

Several countermeasures react to loss of sensor or control function by stopping the vehicle in its assigned lane as quickly as possible. Other alternatives exist, but these alternatives are usually situationally dependent and take time that might not be available. For example, a failure could trigger the vehicle to check with the zone control to determine if a clear path is open to the breakdown lane or shoulder and take that path immediately rather than stop the vehicle in the AHS lane. However, if the AHS speed is 60 mph and it takes one-quarter second to check if a path is open, under this alternative the vehicle will move 22 feet before any countervailing action is attempted. That delay may spell the difference between attaining a safe state and a collision. Also, the path to the breakdown lane will not always be open, in these situations the vehicle would have to come to a stop in the AHS lane to await path opening. The team has tried to choose maximum safety in selecting these countermeasures, even when it interferes with the capacity or convenience of the AHS.

All RSCs

The following measures and countermeasures are recommended as part of the MMS for all of the RSCs investigated.

1. The driver must have specialized training on how to use the AHS properly. This training will include normal AHS operations, emergency and other non-standard situations on the AHS. Periodic driver recertification may be necessary. Part of the AHS check-in procedure should involve the driver inserting his valid AHS license into the vehicle control unit to verify to the AHS zone control that a valid licensed AHS driver is in control of the vehicle.

   It may be necessary to acquaint all drivers with some of the changes made necessary by the introduction of the AHS. In scenarios where AHS vehicles and manually driven vehicles are not separated by physical barriers this instruction is especially important.

2. The driver should have the ability to interact with the AHS in, at least, the following ways:

   2.1 The driver can request exit from the AHS as soon as possible or at the next exit. This allows the driver to handle emergencies that occur among the vehicle's occupants (e.g., illness of a passenger) that would be unreasonable to assume the AHS could detect.

   2.2 The driver can request a panic stop (which will bring the vehicle to a stop in the AHS lane at the maximum allowable AHS braking rate). The zone control will alert other affected vehicles to take appropriate action. The zone control personnel will contact the driver and inquire as to the nature of the emergency. If no emergency exists, penalties can be imposed on the driver. This allows the driver to influence his fate should he see that the AHS is malfunctioning. This ability is probably necessary for near term public acceptance.

   2.3 The driver has the ability to contact the zone control to alert them to situations of which they might be unaware (i.e., provision of a “pilot report”). This allows the driver to provide information to the AHS that it may not be able to obtain through its own sensors (e.g., pothole in the road, armadillo crossing the highway. etc.).

   Strong consideration should be given to the use of the driver as either a permissive or restrictive link in the system (at least in the early implementation of the AHS). As a permissive link, the driver would have to give his permission for certain actions to be taken by the AHS. As a restrictive link, the driver would be able to prevent the AHS from taking certain actions. Examples of these actions might include changing lanes, changing from one highway to another, exiting the AHS, joining a platoon, and leaving a platoon. Normal centerline tracking and gap maintenance would be entirely under AHS control with no driver permissions required.

A major problem is that the interaction between the driver and the AHS is limited by the human/
machine interface. A system that could listen to a driver's verbal input (e.g., “I’m about to hit a deer.”) and correctly interpret this message would be ideal. However, especially since different drivers will express the same thought in different ways, such a system remains for the future.

As currently envisioned, the driver can interact with the AHS by a) pressing a button to execute an emergency stop in the current lane, b) pressing a button to get off the AHS as soon as possible, c) pressing a button to get off the AHS at the next exit, or d) calling the zone control personnel on the radio and talking to them. The first three methods are quick and unambiguous but convey little information by themselves. The fourth is slow and subject to interpretation and mistakes but allows the conveying of a great deal of information.

In no case is the team advocating that the driver be included in the loop to bring the vehicle to an initial safe state (i.e., at a low energy state and with a predictable path - usually stopped) after a malfunction occurs that affects the operation of the AHS. Even if a switch were available to the driver that, upon activation, would return total vehicle control to the driver, the short time in which a malfunction can develop and lead to an accident would prevent the driver from taking effective countermeasures in most cases. In addition, the unpredictability of the driver could easily lead to other problems. Therefore, the team believes that automatic handling of a malfunction to bring the vehicle to a safe state combined with the possibility of driver intervention a few moments later to remove the malfunctioning vehicle from the AHS traffic lane, offers a good balance between safety , convenience, capacity, and cost.

3. In the event of a loss of vehicle control beyond a set threshold (i.e., longer than *n* milliseconds, with a delta V greater than *x* feet/second, with accelerations above *y* Gs, etc.) the vehicle should reduce its speed as quickly as possible, try to maintain itself in the assigned lane, and immediately inform the zone control unit of its situation. The zone control unit will alert other affected vehicles to take appropriate action (slow, stop, change lanes, reroute, etc.). This will reduce the probability of other vehicles being involved in the same adverse situation as the reporting vehicle. After the vehicle has stopped (achieved a safe state) the zone control personnel will contact the driver and inquire as to the nature of the situation and dispatch aid as necessary. Vehicle may be moved off the road under automated or manual control, or even allowed back onto the manual lanes under some circumstances.

4. In the event of a complete failure of information from the gap and/or centerline sensors, the vehicle should reduce its speed as quickly as possible, try to maintain itself in the assigned lane, and immediately inform the zone control unit of its situation. The zone control unit will alert other affected vehicles to take appropriate action (slow, stop, change lanes, reroute, etc.). This will reduce the probability of other vehicles being involved in an accident with the failed vehicle. After the vehicle has stopped (achieved a safe state) the

zone control personnel will contact the driver and inquire as to the nature of the situation and dispatch aid as necessary. Vehicle may be moved off the road under automated or manual control, or even allowed back onto the manual lanes under some circumstances.

5. If vehicle detects a malfunction, collision, or any other unexpected event, it reports to the zone control immediately. The zone control will alert other affected vehicles to take appropriate action (slow, stop, change lanes, reroute, etc.). This will reduce the probability of other vehicles being involved in the same adverse situation as the reporting vehicle. The zone control personnel will contact the driver and inquire as to the nature of the situation and dispatch aid as necessary. Vehicle may be allowed to continue on AHS, moved off AHS into manual lanes, or moved to the shoulder as circumstances suggest. The ability of the vehicles to keep the zone control informed with respect to their status provides a significant measure of security from the "lemming syndrome" in which multiple vehicles collide because they have experienced a situation for which the AHS was not designed or that exceeds the AHS capacity.

6. Active redundant steering, brake, and throttle actuators are specified in Table 6. An arrangement for varying the use of these actuators should be employed. For example, this time when using the AHS the vehicle control unit will select to use steering, brake, and throttle actuators A; next time the control unit will select actuators B. This technique spreads the operation over two actuators instead of one and prevents the “flat spare tire” syndrome.

7. Information about the status of individual vehicles under AHS control that is stored in the zone control computer should be rechecked on a periodic basis. If information does not agree, or is found to be in error or missing, valid information should be immediately obtained. If not possible to immediately obtain valid critical information, a buffer zone is established around the vehicle and the subject vehicle is routed off the AHS as soon as possible.

8. Whenever a vehicle is given a command by the zone control, the vehicle is required to acknowledge the command, carry out the command, and report the completion of that command to the zone control. If the zone control does not have confirmation within an expected time it will check with the vehicle. Appropriate action can then be initiated.

9. Communication between the zone control and vehicle is very important. This communications link should be tested periodically to assure its availability when needed. The frequency of the test depends on RSC, some might need a check once per second while others might only require a check once per minute. If the communications is lost, the vehicle should be programmed to stop in the assigned lane and await assistance. This assistance may be rendered via the following AHS vehicle being provided a special code to release the communications faulted vehicle from AHS control once the path between the communications faulted vehicle and the shoulder or a manual lane has been cleared.

RSC 1.

The following additional countermeasures are recommended as part of the MMS for RSC 1.

1. Some method needs to be developed to assure that the active wire is very reliable. The failure of this system will affect every AHS vehicle operating in the affected zone. The failure of this wire will cause each individual AHS vehicle to brake at its maximum rate with its front wheels locked at the last commanded angle until the vehicle stops. Control will then be turned over to the drivers and vehicles will be allowed to proceed manually more than a momentary wire shutdown is anticipated. Upstream zone controllers will be contacted so they can transition their vehicles to manual control smoothly.

2. The transition from the AHS Lane to the Transition Lane under AHS control is fraught with failure potential. Since the driver has already passed the awareness test (or this transition would not be undertaken) the potential exists to have the driver participate by visually clearing the transition lane and informing the zone control when he believes it is safe to change lanes via a pushbutton input on the steering wheel. The lane change will not occur unless both the driver and zone controller believe it is safe to do so. (See Item 2.4 under All RSCs above.)

RSC 2.

There were no additional countermeasures recommended as part of the MMS for RSC 2.

RSC 3.

The following additional countermeasures are recommended as part of the MMS for RSC 3.

1. A positive method must be developed to assure that the vehicle is securely locked to the pallet. Possible the use of inexpensive load cells under each of the locking points joining the pallet and vehicle could provide this indication. In the event that the vehicle partially or fully unlocks from the pallet, the pallet maneuvering could be kept to a minimum and the pallet routed off the AHS at the earliest opportunity.

2. The driver must be able to contact the personnel at the pallet mate/demate facility easily and quickly to alert them to potentially dangerous situations of which they might be unaware. This communication cannot always be achieved via the portable AHS control panel that controls the pallet's movement because that panel may not be available when the driver needs it. Therefore, fixed microphones should be placed in the mate/demate facility allowing the driver to be heard whenever he is in vehicle loading/unloading area.

3. In the most extreme case, the driver should have a way of manually unloading his vehicle from the pallet. Thus, if the system had to be shut down for a wide scale emergency (e.g., earthquake) the drivers could unload their vehicles and proceed manually.

RSC 4.

The following additional countermeasures are recommended as part of the MMS for RSC 4.

1. A method should be developed to discourage manual drivers from harassing AHS vehicles, possibly by making such harassment illegal. The AHS driver can establish voice communications with the zone control personnel to report harassment. Zone control personnel can take the appropriate action by dispatching police, or possibly taking a photo of the offending vehicle and driver if the road is under visual surveillance. If the AHS vehicle uses a vision system for collision avoidance, the vision system may be able to provide the visual evidence needed.

2. AHS vehicle is equipped with sensors to determine position and relative vectors of all nearby vehicles (forward gap sensor, lateral obstacle sensors, and rear gap sensor). In the event that a target vehicle meets certain criteria programmed into the vehicle control unit suggesting that the target vehicle is on a likely collision course with the AHS vehicle, the AHS vehicle will fire a strobe light and/or sound a directional siren at the target vehicle to alert target vehicle driver. The AHS vehicle will make an attempt to avoid the collision if is safe to make the avoidance maneuvers.

   This same system can be used to induce a manually driven vehicle to maintain a reasonable following distance. It should not be difficult to provide a means for determining whether the following vehicle is under AHS control (e.g., the zone control may provide the information or there may be a distinct signature radiated from each AHS vehicle). If the following vehicle is not identified as under AHS control, the AHS vehicle can trigger its rear strobe or a special light to indicate that the vehicle is following too closely for safety under current speed, roadway, and environmental conditions.

3. The results of the use of a panic button by the AHS driver in this mixed traffic scenario will need to be modified compared to those scenarios in which all of the other vehicles in a lane are under AHS control and linked to the zone control. If all the vehicles in a lane are linked to the zone control, and/or have forward gap sensors that prevent them from following the vehicle ahead too closely for the prevailing roadway and environmental conditions, then a panic stop using maximum AHS braking can be accomplished in safety. However, if manually driven vehicles are mixed in the same lane, the possibility of driver errors such as following too closely and driver inattention make such a maneuver more risky.

   An AHS vehicle undergoing maximum braking (say 0.8G) in response to a panic button activation would stop in approximately 150 feet; a level of braking generally achievable by most modern cars. An AHS vehicle trailing the panic stop AHS vehicle, even without relying on being warned by the zone control about the panic stop, should still be able to stop without a collision, given a 0.3 second reaction time and an initial 50 foot gap at an initial speed of 60 mph. However, a manually driven vehicle following the panic stop AHS vehicle may not be able to stop without a collision. Given a 1.5 second man/machine reaction time, an initial speed of 60 mph, a standard six car length following distance (96 feet), and a 0.8G braking rate - a collision will result.

The man/machine reaction time must fall to less than 1.1 seconds to avoid a collision. This reaction time is approximately equal to the mean “surprise” reaction time identified by Olson in “Parameters Affecting Stopping Sight Distance”, TRB Report No. 270, June 1984. This means that approximately half of the time a collision will result given the parameters above.

Olson identified the 2 to 98 percentile “surprise” reaction time as spanning the range from 0.81 to 1.76 seconds. If we assume that a 2 percent collision rate is acceptable and that most drivers can be induced to follow no closer than 1 car length for every 10 mph, then most rear end collisions should be avoidable by adopting one of the following methods:

- An extra delay could be introduced into the AHS vehicle's panic stop mode. Once the AHS panic stop vehicle's brake lights have illuminated, the vehicle would not actually apply a 0.8G braking rate for 0.7 seconds. This would allow 98 percent of manually driven vehicles to stop without collision given Olson's data and a 0.8G brake rate.

- The AHS panic stop vehicle could be limited to a braking rate of approximately 0.55G. The AHS panic stop vehicle would stop in a distance of 220 feet, the manually driven vehicle would continue for 1.76 seconds at 88 feet/second (155 feet) then apply a 0.8G brake rate and stop in 150 feet - thus the manually driven vehicle could be following as closely as 85 - 90 feet and still avoid a collision.

Either of these techniques imposes a severe restraint on the AHS vehicle; it must use much less than its maximum performance brake rate just so that if it happens to be followed by a manually driven vehicle, the following vehicle can stop without a collision. A potentially better solution is to limit the performance of the AHS vehicle only if it needs to be limited and can be limited with reasonable safety.

If the AHS vehicle has forward and rear gap sensors then the distance and closing rate to the obstacle in front of the AHS vehicle and distance and closing rate of the vehicle to the rear of the AHS vehicle can be measured. The AHS panic stop vehicle can use maximum performance unless it detects a vehicle closing from the rear at a rate and distance that would portend a significant collision. In that case, the distance and closing rate to the forward obstacle would be measured and, if it could be done so with reasonable safety, the AHS panic stop vehicle would reduce its braking rate.

Of course, this countermeasure cannot handle all possible situations. Dips and curves in the road can mask both vehicles closing from the rear and obstacles ahead. The reason for the panic stop may involve a large hole in the road ahead rather than an obstacle, this situation could fool the vehicle into braking at a lower rate than required to avoid the hole. However, given that this countermeasure would only come into play in the event of a panic stop with a fast closing vehicle from the rear, it seems reasonable to postulate that if provides a reasonable degree of safety.

4. It will be necessary to acquaint all drivers with AHS related procedures if they are to travel the same lanes as AHS vehicles. Instruction concerning safe following distance and how the AHS vehicle may help you maintain that distance (see item 2 in this RSC), and the concept that the AHS vehicle may brake suddenly and hard should be given.

Other Considerations

1. As used in this study, a malfunction occurs when the system does not perform as it was designed. The question of software malfunctions has been raised on several occasions. By the definition used in this study, a software malfunction occurs only if the software commands "A" and the vehicle does "B". Even if "A" is a non-optimum choice (e.g., if the gap falls below the setpoint, decelerate the vehicle at the maximum possible rate) if the vehicle does "A" when commanded to do so, it is not a malfunction. This means that the AHS will have to be carefully specified, designed, constructed, and thoroughly tested before introduction to the public.

2. Another reason for testing is that the suggested operational countermeasures selected for the final MMS for each RSC represent Battelle's current best estimate of an appropriate operation response to a particular malfunction. However, there may be better responses available that will only be shown through testing of an operational system.

3. It is not possible to directly connect the malfunction and the consequence without specific information about the RSC and the specific roadway. The consequences of a malfunction such as loosing track of the lane centerline depend upon the state of the roadway at the time of signal loss. If the weather conditions are good and the road is straight, the probable outcome will be an automatic braking to a stop in the AHS lane without leaving the lane and no collision with other vehicles or fixed obstacles. If the weather renders the roadway slippery and the road is significantly curved, the probable outcome will involve leaving the confines of the AHS lane before the vehicle can brake to a stop. The possibility of striking another vehicle or fixed obstacle depend upon the presence of such targets.

   One could construct a table covering all of the significant factors influencing the consequence of a particular malfunction; weather conditions, condition of the roadway, and roadway geometry (grade, curves, etc.). The proportion of time each of these conditions exist, and their influence on the probability of a collision or other adverse consequence can be used to simulate the operation of the AHS in the presence of specific malfunctions. This process would allow the replacement of the subjective severity ratings in Appendices D and G with more objective data.

4. The possibility exists that the AHS systems may malfunction while the vehicle is not on the AHS. In this case, the malfunction should be brought to the attention of the driver so that the necessary repairs can be scheduled. More importantly, the malfunction cannot be allowed to cause an accident or incident. The AHS system must be designed so that it cannot take control of the vehicle's steering, brakes, throttle, or any other sub-system

unless there is a positive request by the driver for that takeover, and the vehicle is in the appropriate place, with the appropriate vehicle status for a safe takeover of control.

5. Pallets possess unique advantages and disadvantages compared to other types of AHS traveling units investigated during this study. The list below compares pallets to private vehicles on several characteristics that pertain directly to malfunction management.

Pallets	Private Vehicles
Control of pallet maintenance by a central authority enrolls each pallet in an organized program of preventative maintenance and inspections	The need to maintain and periodically inspect AHS vehicle systems falls entirely onto the owner; some will do excellent jobs and some will do poor jobs
By design, pallets spend full time on the AHS. Pallets can be equipped with more expensive and robust AHS vehicle systems and still maintain a reasonable cost/mile depreciation rate	Private vehicles spend part of their time on the AHS and part on conventional streets, average AHS utilization is less than pallets, private vehicles likely must be equipped with less expensive AHS vehicle systems to keep depreciation cost/mile reasonable
Pallets operate only on the AHS and can be optimized for that specific environment	Private vehicles must be able to operate on the AHS and on conventional streets
Pallets have a straightforward transition of control to and from the AHS.	Transition to and from AHS control is less straightforward.
Pallets can handle a disabled driver best of all the systems studied	Adequate methods of handing a disabled driver can be implemented
Pallets can be designed to be safe and stable, but the pallet/vehicle traveling unit probably will have a higher center of gravity compared to the private vehicle alone	Lower center of gravity, probably more stable
Additional traveling unit based functions (e.g., vehicle lockdown) and infrastructure based functions (e.g., vehicle load/unload docks) introduce additional points of failure	Fewer traveling unit and infrastructure based functions required
The pallet has no mobility off the operating AHS, therefore the central authority will likely need to respond to most malfunctions that leave the pallet without AHS capability via the dispatch of a response team	Upon loss of AHS capability, private vehicles could be allowed to move in the breakdown lane to an exit, or could be routed onto the manual section of the freeway without need for a response team

Overall, the team believes that the pallets have an edge over the private vehicle based systems in terms of malfunction management. Control of pallet maintenance by a central authority and the ability to equip the pallets with more expensive and robust AHS vehicle systems subjectively outweigh the disadvantages listed for the pallets.

APPENDIX A AHS FAULT TREES

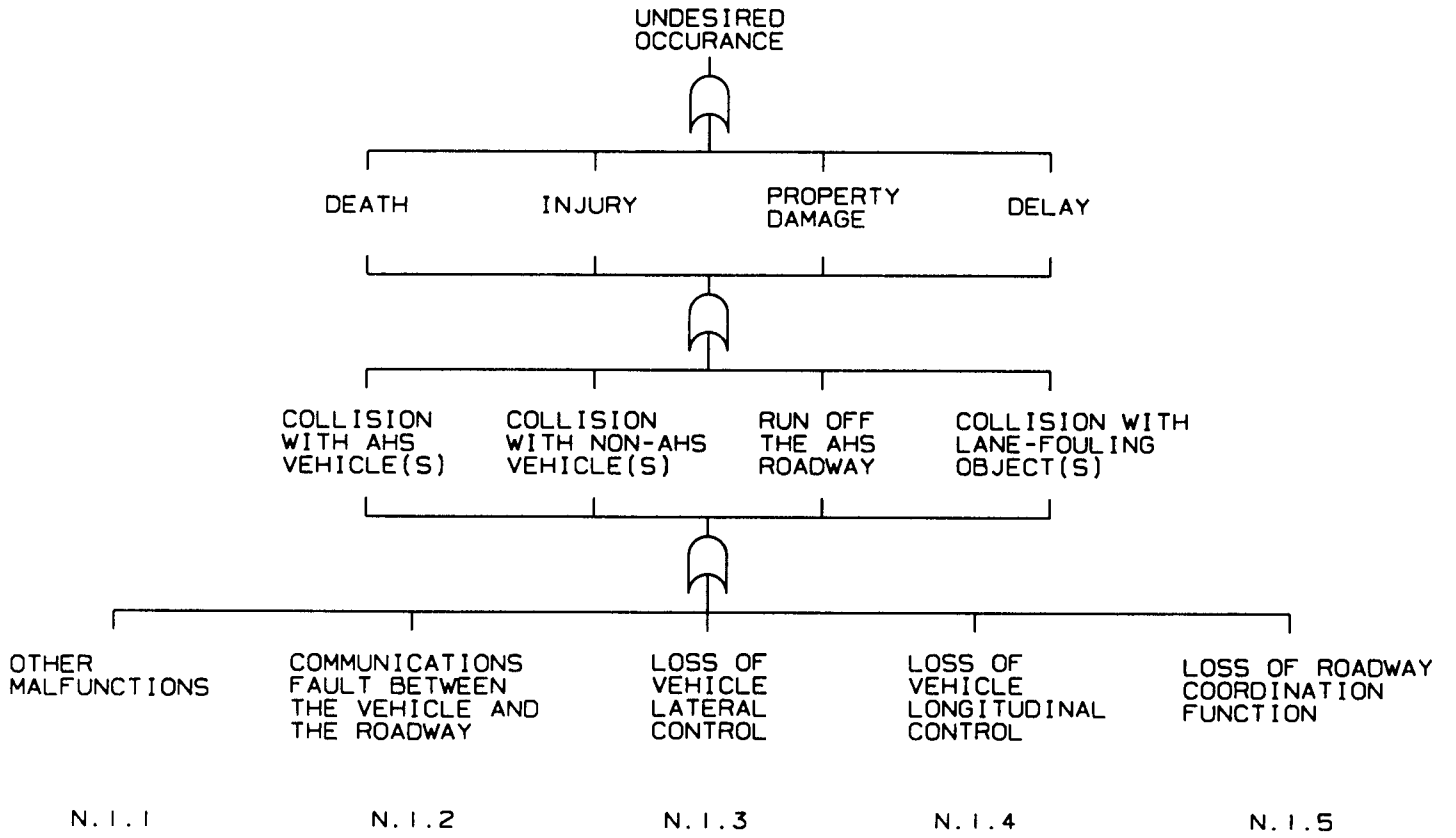
The primary method used to define the component malfunctions is the fault tree. In the fault tree, the main fault is listed as the top of the tree (e.g., loss of lateral control), and the possible sub-faults that could lead to this consequence are connected to the fault via boolean operators. When sufficient information is available about the reliability of sub-systems and components, the fault tree can be used to calculate the reliability of the overall system. In this study, the fault trees are most useful in showing the relative, rather than the absolute, importance of various sub-systems and components.

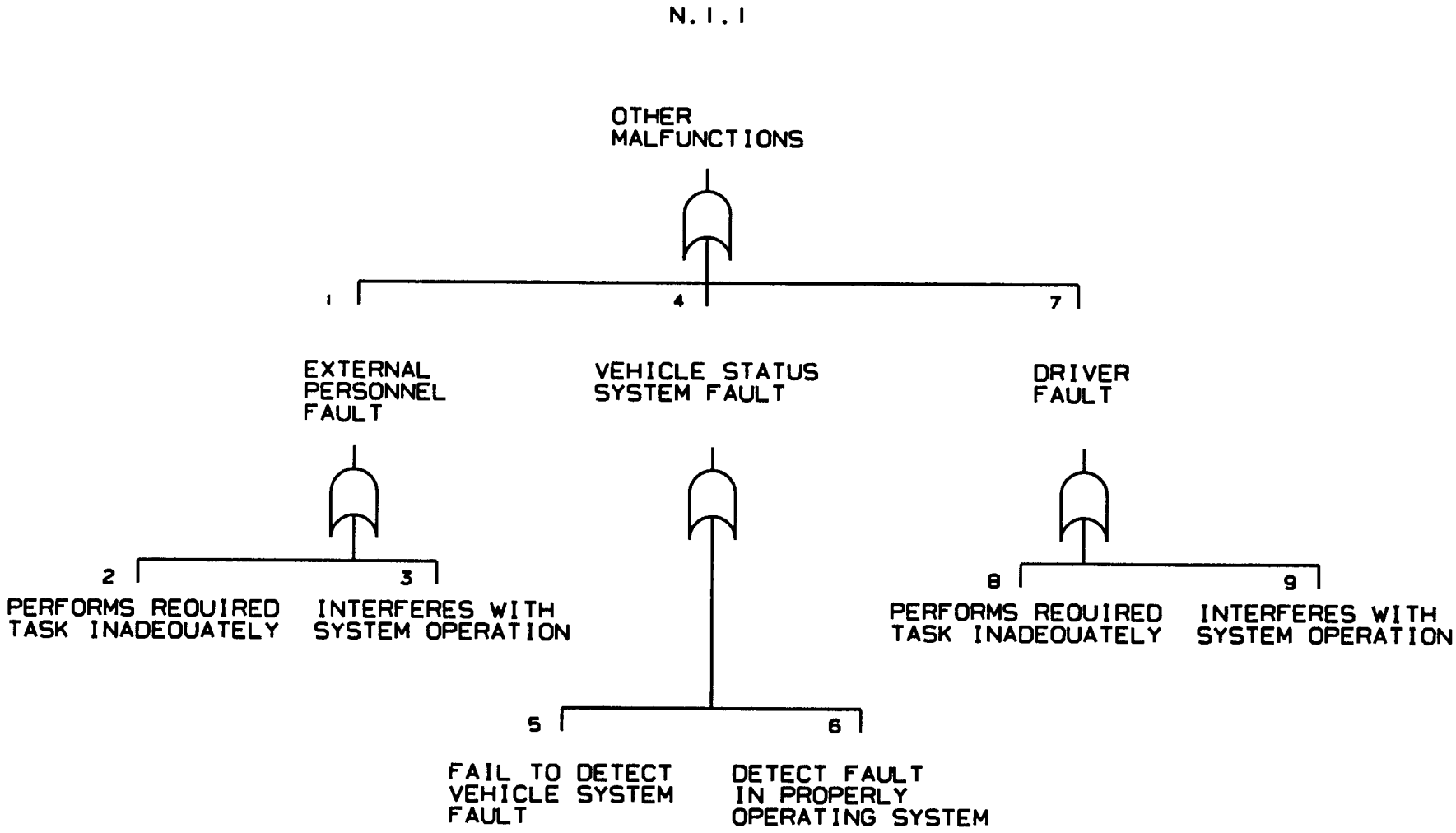
The specialized fault tree developed for the subject RSCs is shown in this appendix. A brief explanation of some conventions used is needed to understand and link the various pages of this complex document.

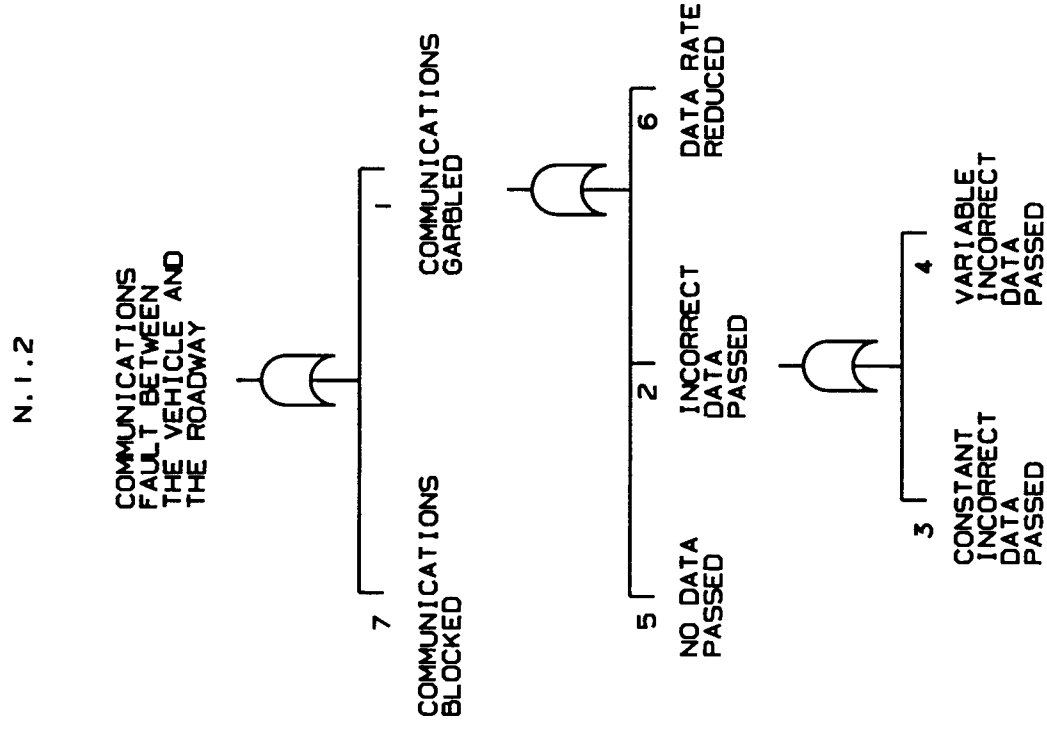
The top of the fault tree is shown on page 48 with “Undesired Occurrence” as the primary fault or result. Below this fault is a symbol that is an “OR” gate; it signifies that an undesired occurrence has happened if “Death,” OR “Injury,” OR “Property Damage,” OR “Delay” has occurred.

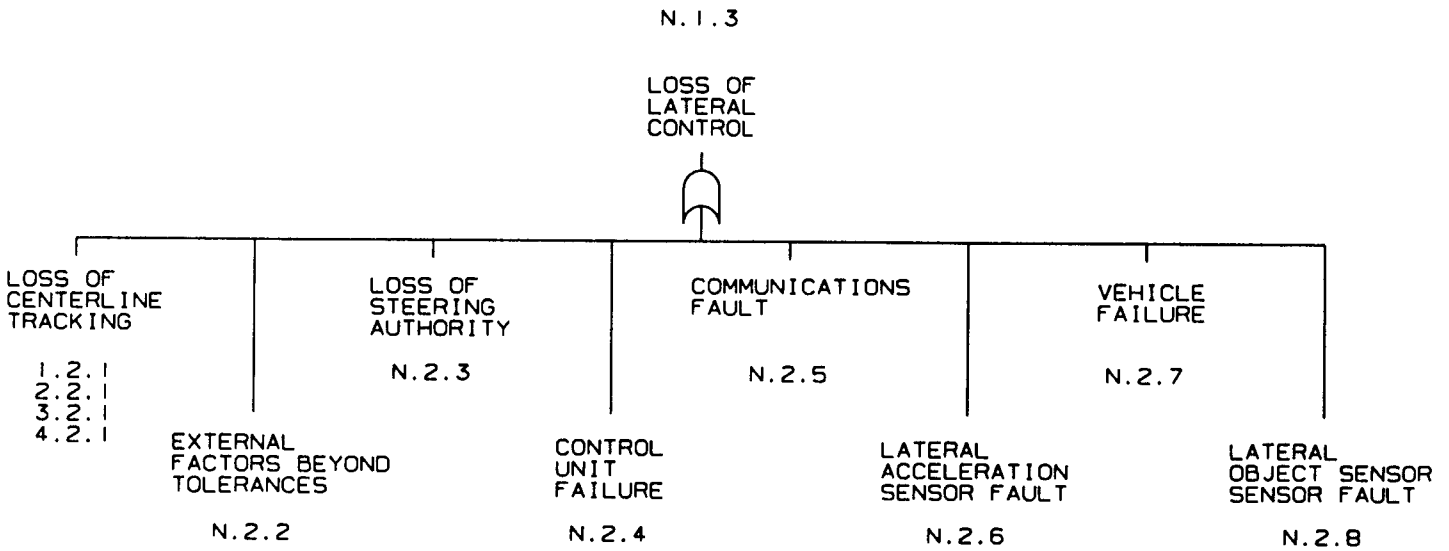
Normally, each result on each level of the fault tree is described by a series of possible events that could cause the fault (see page 49 for a more typical fault tree). The lines extending down from the second level of the fault tree are connected to another OR gate which, in turn, leads to the third level starting with “Collision with AHS Vehicle(s).” This notation is used to signify that any of the events shown on the third level can lead to any of the consequences shown on the second level (and any of the events in the fourth level can lead to any of the consequences in the third level). Thus, a loss of vehicle lateral control could lead to a collision with an AHS vehicle and result in property damage. In a different set of circumstances, the same loss of lateral control could lead to the vehicle departing from the AHS roadway and result in one or more deaths.

At the bottom of the first fault tree page are the designations N.1.1 through N.1.5. To find the part of the fault tree that continues below “Loss of Vehicle Lateral Control,”one would look for the page that has N.1.3 at the top (in this case, page 51). Subsequently, if one wished to follow this tree to a lower level, say below “Loss of Steering Authority,” one would look for the page with N.2.3 at the top (i.e., page 54).

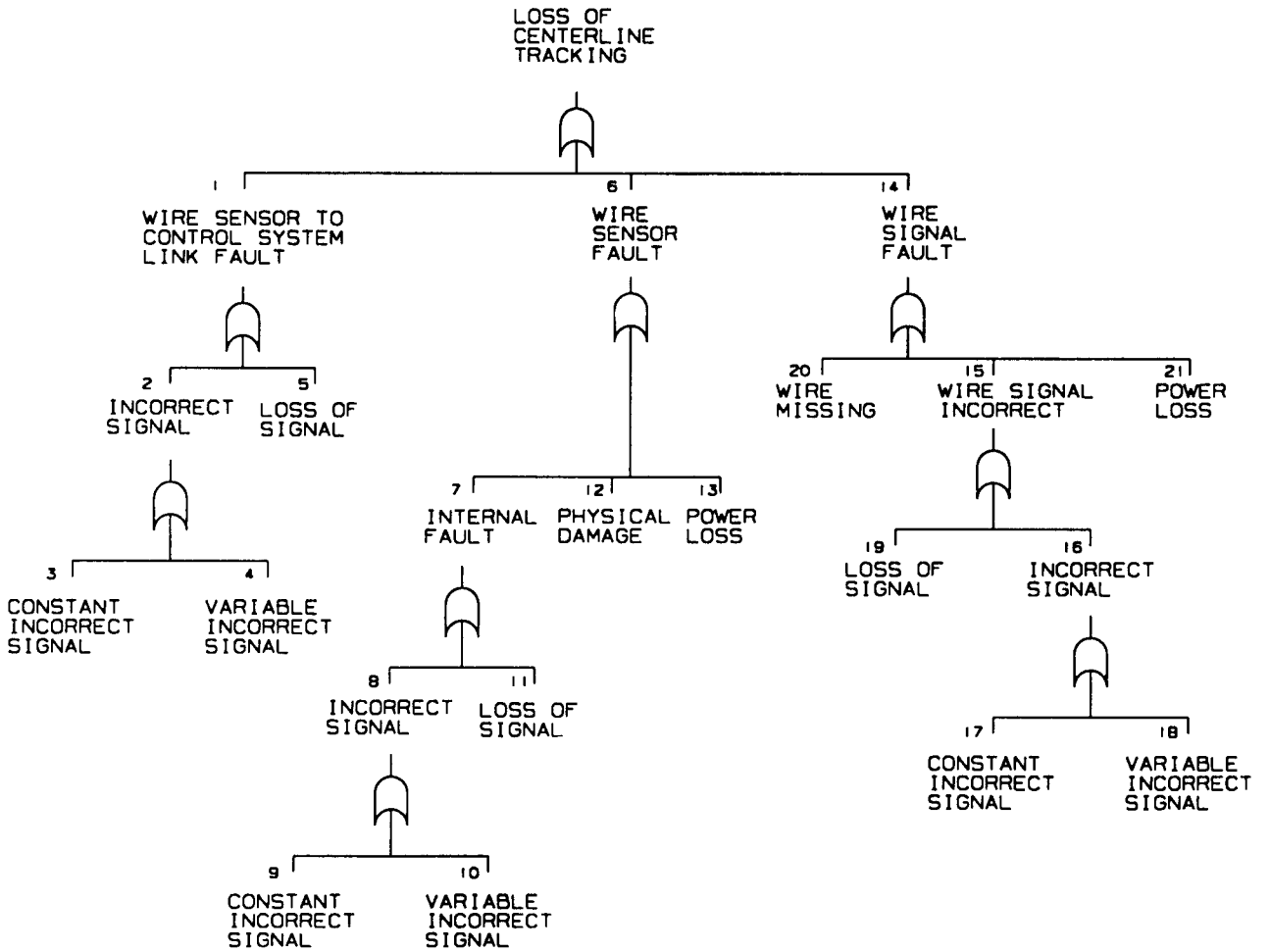

UNDESIRED OCCURANCE
DEATH
INJURY
PROPERTY DAMAGE
DELAY
COLLISION WITH AHS VEHICLE(S)
COLLISION WITH NON-AHS VEHICLE(S)
RUN OFF THE AHS ROADWAY
COLLISION WITH LANE-FOULING OBJECT(S)
OTHER MALFUNCTIONS
COMMUNICATIONS FAULT BETWEEN THE VEHICLE AND THE ROADWAY
LOSS OF VEHICLE LATERAL CONTROL
LOSS OF VEHICLE LONGITUDINAL CONTROL
LOSS OF ROADWAY COORDINATION FUNCTION
N.1.1
N.1.2
N.1.3
N.1.4
N.1.5


N.I.1
OTHER MALFUNCTIONS
1
4
7
EXTERNAL PERSONNEL FAULT
VEHICLE STATUS SYSTEM FAULT
DRIVER FAULT
2
3
8
9
PERFORMS REQUIRED TASK INADEQUATELY
INTERFERES WITH SYSTEM OPERATION
PERFORMS REQUIRED TASK INADEQUATELY
INTERFERES WITH SYSTEM OPERATION
5
6
FAIL TO DETECT VEHICLE SYSTEM FAULT
DETECT FAULT IN PROPERLY OPERATING SYSTEM

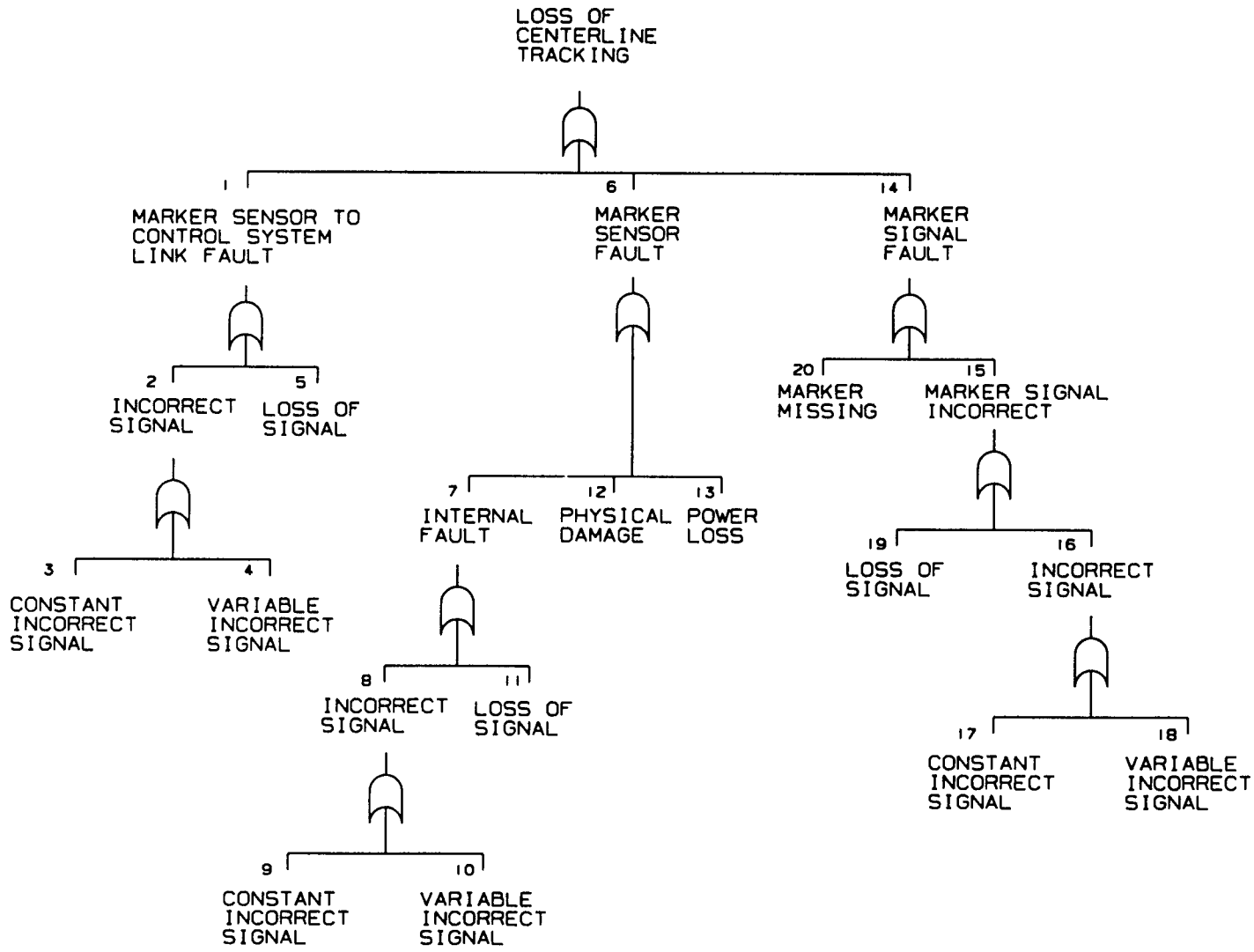

N.I.2
COMMUNICATIONS FAULT BETWEEN THE VEHICLE AND THE ROADWAY
1
COMMUNICATIONS GARBLED
7
COMMUNICATIONS BLOCKED
6
DATA RATE REDUCED
2
INCORRECT DATA PASSED
5
NO DATA PASSED
4
VARIABLE INCORRECT DATA PASSED
3
CONSTANT INCORRECT DATA PASSED


N.1.3
LOSS OF LATERAL CONTROL
LOSS OF CENTERLINE TRACKING
1.2.1
2.2.1
3.2.1
4.2.1
EXTERNAL FACTORS BEYOND TOLERANCES
N.2.2
LOSS OF STEERING AUTHORITY
N.2.3
CONTROL UNIT FAILURE
N.2.4
COMMUNICATIONS FAULT
N.2.5
LATERAL ACCELERATION SENSOR FAULT
N.2.6
VEHICLE FAILURE
N.2.7
LATERAL OBJECT SENSOR SENSOR FAULT
N.2.8

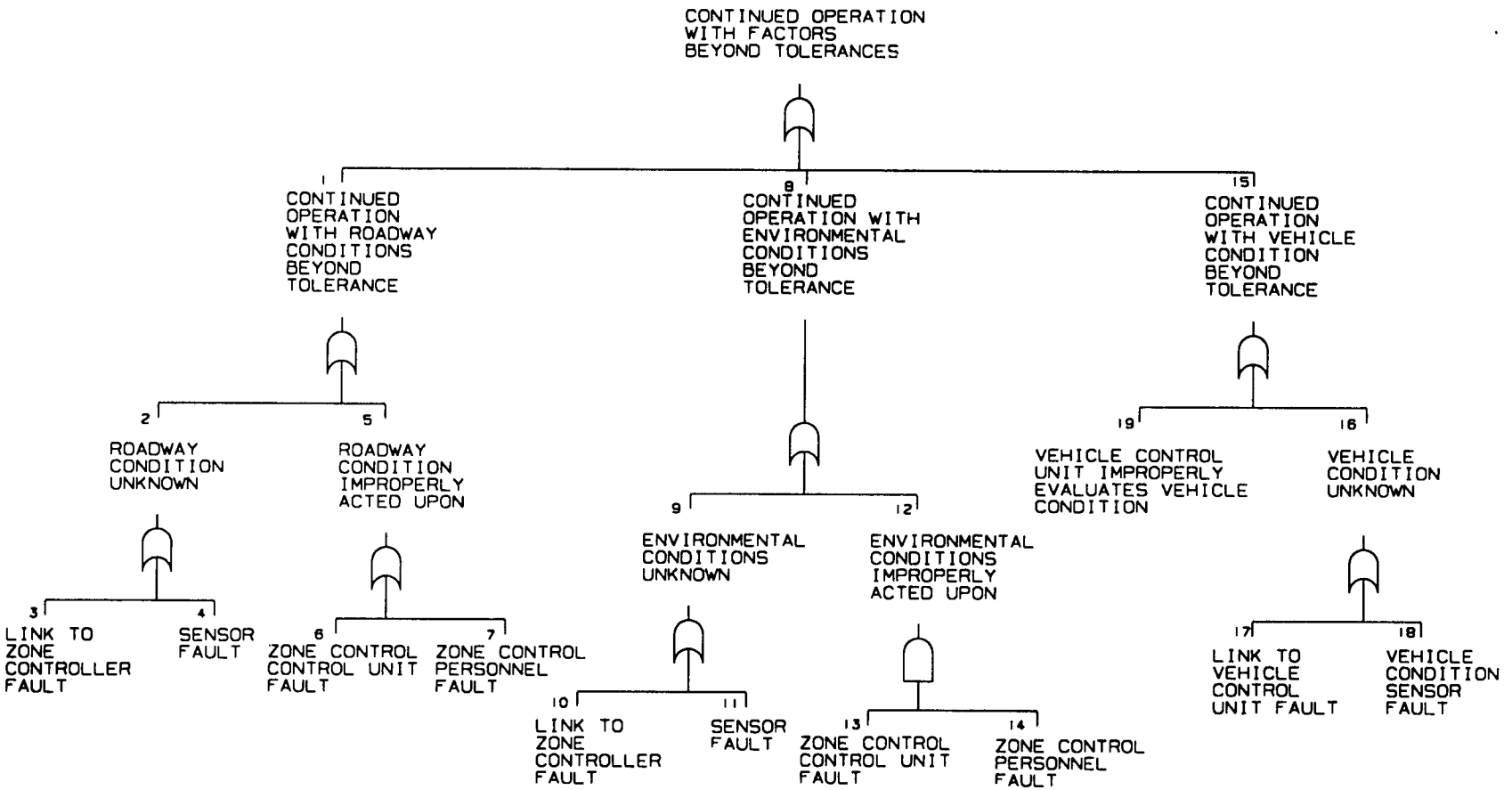
1.2.1


LOSS OF CENTERLINE TRACKING
1
WIRE SENSOR TO CONTROL SYSTEM LINK FAULT
6
WIRE SENSOR FAULT
14
WIRE SIGNAL FAULT
2
INCORRECT SIGNAL
5
LOSS OF SIGNAL
3
CONSTANT INCORRECT SIGNAL
4
VARIABLE INCORRECT SIGNAL
7
INTERNAL FAULT
12
PHYSICAL DAMAGE
13
POWER LOSS
8
INCORRECT SIGNAL
11
LOSS OF SIGNAL
9
CONSTANT INCORRECT SIGNAL
10
VARIABLE INCORRECT SIGNAL
20
WIRE MISSING
15
WIRE SIGNAL INCORRECT
21
POWER LOSS
19
LOSS OF SIGNAL
16
INCORRECT SIGNAL
17
CONSTANT INCORRECT SIGNAL
18
VARIABLE INCORRECT SIGNAL

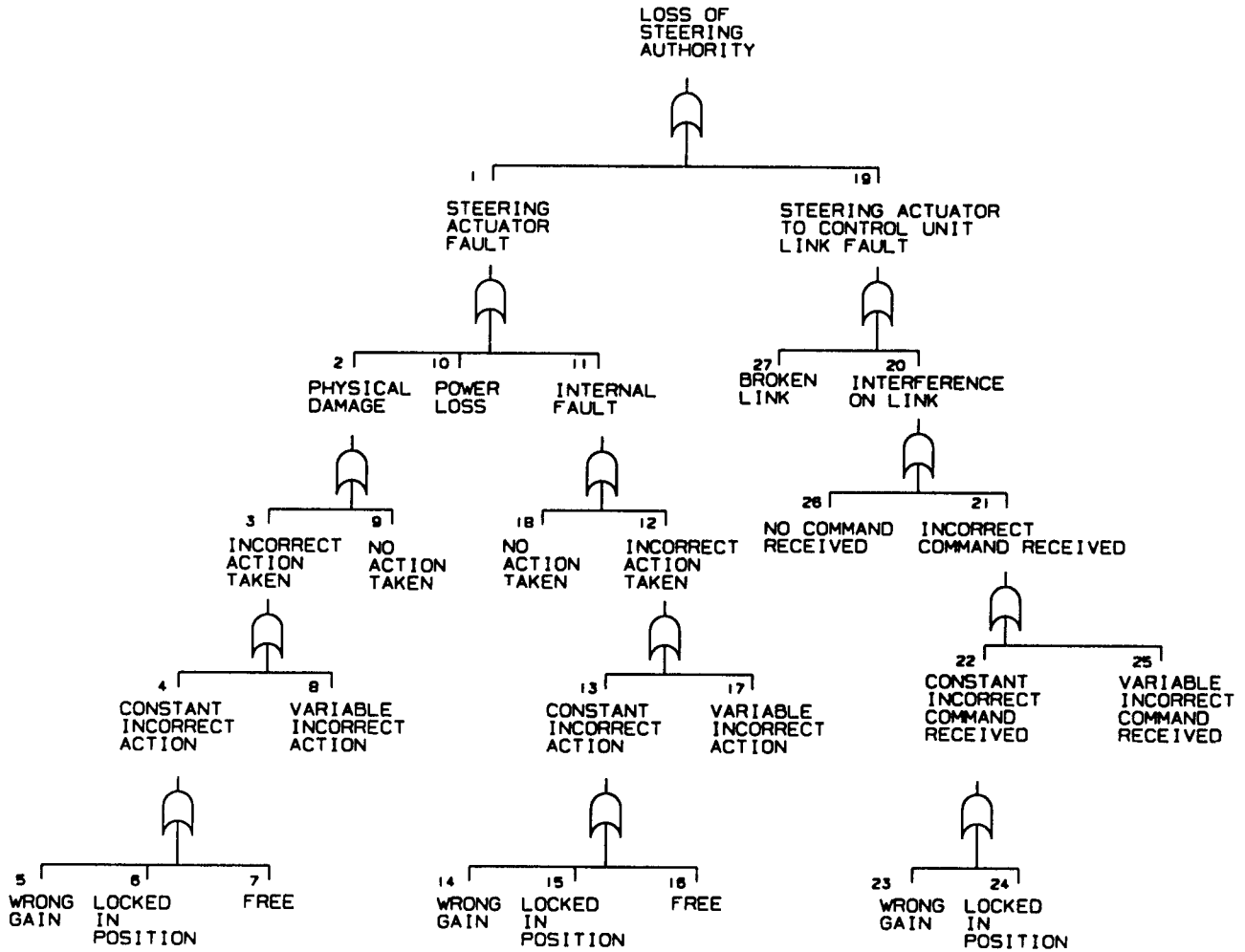
2.2.1
3.2.1
4.2.1

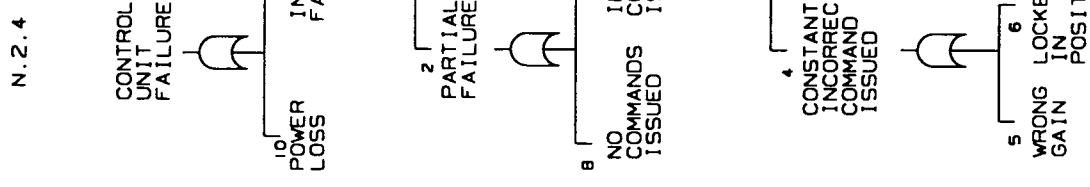

LOSS OF CENTERLINE TRACKING
1
6
14
MARKER SENSOR TO CONTROL SYSTEM LINK FAULT
MARKER SENSOR FAULT
MARKER SIGNAL FAULT
2
5
INCORRECT SIGNAL
LOSS OF SIGNAL
3
4
CONSTANT INCORRECT SIGNAL
VARIABLE INCORRECT SIGNAL
7
12
13
INTERNAL FAULT
PHYSICAL DAMAGE
POWER LOSS
8
11
INCORRECT SIGNAL
LOSS OF SIGNAL
9
10
CONSTANT INCORRECT SIGNAL
VARIABLE INCORRECT SIGNAL
20
15
MARKER MISSING
MARKER SIGNAL INCORRECT
19
16
LOSS OF SIGNAL
INCORRECT SIGNAL
17
18
CONSTANT INCORRECT SIGNAL
VARIABLE INCORRECT SIGNAL

N.2.2

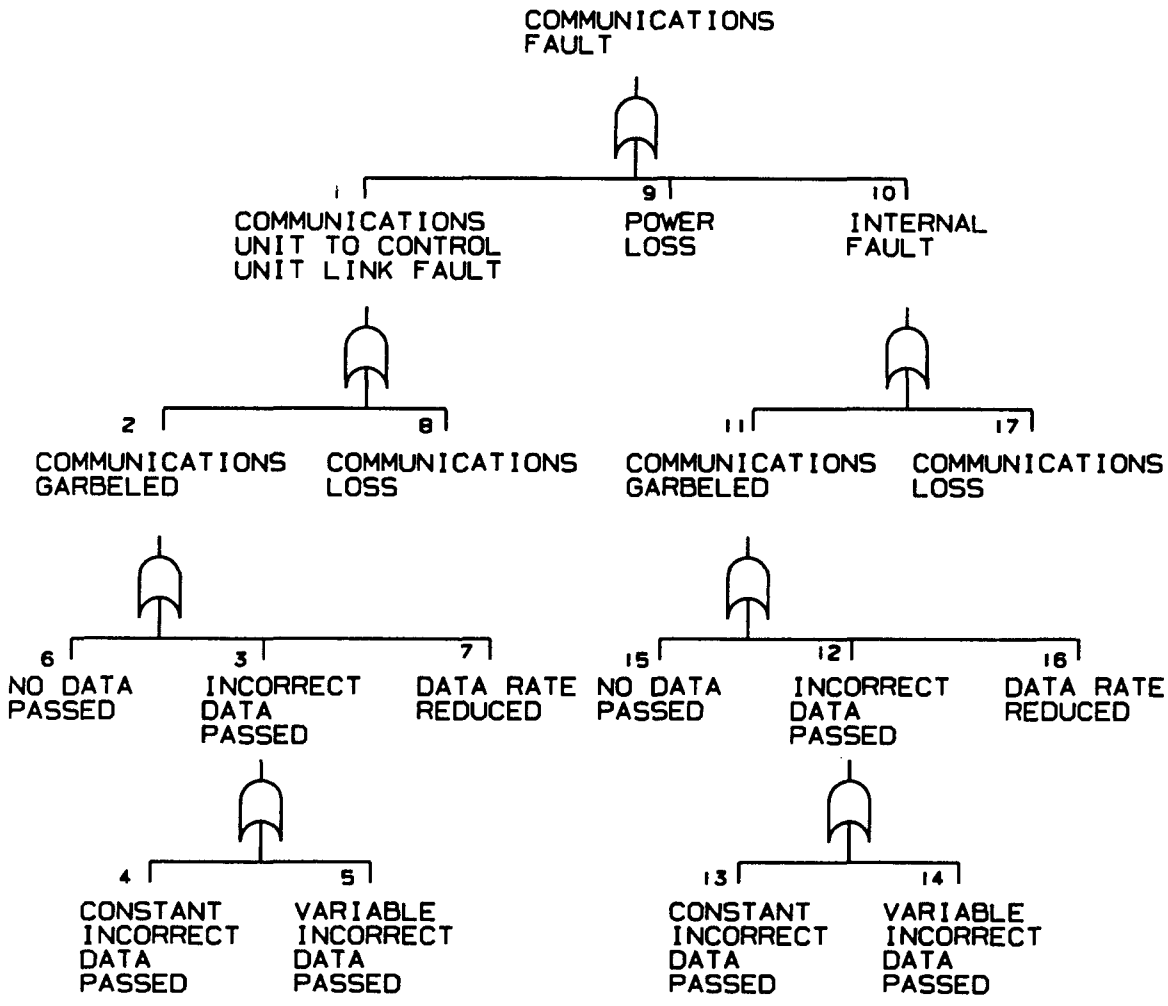

CONTINUED OPERATION WITH FACTORS BEYOND TOLERANCES
1
CONTINUED OPERATION WITH ROADWAY CONDITIONS BEYOND TOLERANCE
8
CONTINUED OPERATION WITH ENVIRONMENTAL CONDITIONS BEYOND TOLERANCE
15
CONTINUED OPERATION WITH VEHICLE CONDITION BEYOND TOLERANCE
2
5
ROADWAY CONDITION UNKNOWN
ROADWAY CONDITION IMPROPERLY ACTED UPON
9
12
ENVIRONMENTAL CONDITIONS UNKNOWN
ENVIRONMENTAL CONDITIONS IMPROPERLY ACTED UPON
19
16
VEHICLE CONTROL UNIT IMPROPERLY EVALUATES VEHICLE CONDITION
VEHICLE CONDITION UNKNOWN
3
4
LINK TO ZONE CONTROLLER FAULT
SENSOR FAULT
6
7
ZONE CONTROL CONTROL UNIT FAULT
ZONE CONTROL PERSONNEL FAULT
10
11
LINK TO ZONE CONTROLLER FAULT
SENSOR FAULT
13
14
ZONE CONTROL CONTROL UNIT FAULT
ZONE CONTROL PERSONNEL FAULT
17
18
LINK TO VEHICLE CONTROL UNIT FAULT
VEHICLE CONDITION SENSOR FAULT

N.2.3

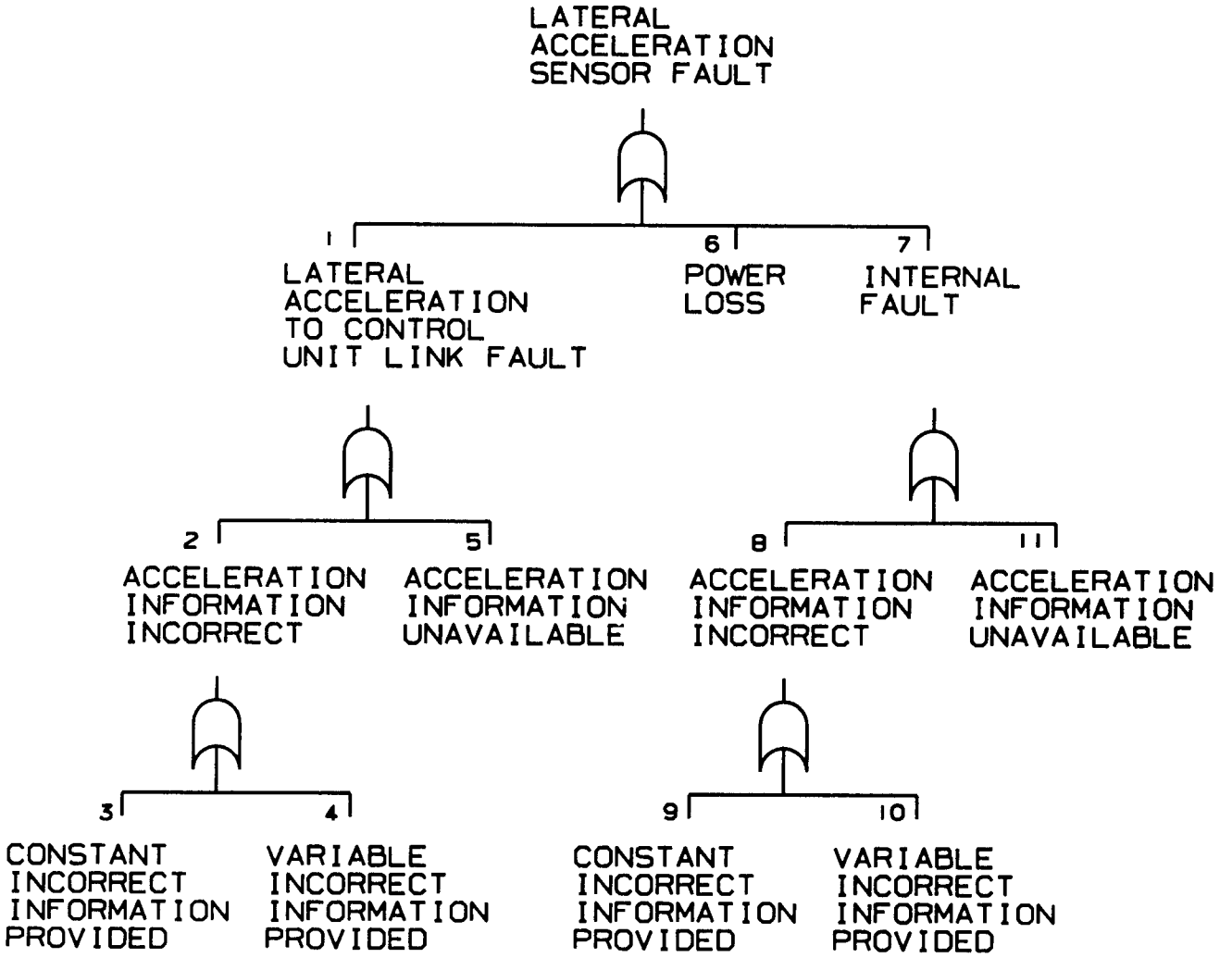

LOSS OF STEERING AUTHORITY
1
19
STEERING ACTUATOR FAULT
STEERING ACTUATOR TO CONTROL UNIT LINK FAULT
2
10
11
PHYSICAL DAMAGE
POWER LOSS
INTERNAL FAULT
27
20
BROKEN LINK
INTERFERENCE ON LINK
3
9
18
12
26
21
INCORRECT ACTION TAKEN
NO ACTION TAKEN
NO ACTION TAKEN
INCORRECT ACTION TAKEN
NO COMMAND RECEIVED
INCORRECT COMMAND RECEIVED
4
8
13
17
22
25
CONSTANT INCORRECT ACTION
VARIABLE INCORRECT ACTION
CONSTANT INCORRECT ACTION
VARIABLE INCORRECT ACTION
CONSTANT INCORRECT COMMAND RECEIVED
VARIABLE INCORRECT COMMAND RECEIVED
5
6
7
14
15
16
23
24
WRONG GAIN
LOCKED IN POSITION
FREE
WRONG GAIN
LOCKED IN POSITION
FREE
WRONG GAIN
LOCKED IN POSITION


N.2.4
CONTROL UNIT FAILURE
1 INTERNAL FAULT
10 POWER LOSS
9 COMPLETE FAILURE
2 PARTIAL FAILURE
3 INCORRECT COMMANDS ISSUED
8 NO COMMANDS ISSUED
7 VARIABLE INCORRECT COMMAND ISSUED
4 CONSTANT INCORRECT COMMAND ISSUED
6 LOCKED IN POSITION
5 WRONG GAIN

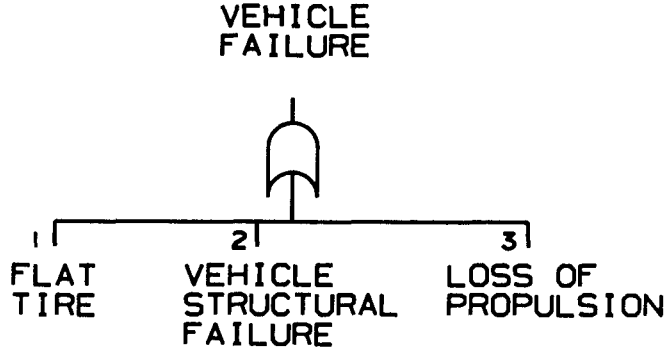
N.2.5


COMMUNICATIONS FAULT
1
COMMUNICATIONS UNIT TO CONTROL UNIT LINK FAULT
9
POWER LOSS
10
INTERNAL FAULT
2
COMMUNICATIONS GARBELED
8
COMMUNICATIONS LOSS
11
COMMUNICATIONS GARBELED
17
COMMUNICATIONS LOSS
6
NO DATA PASSED
3
INCORRECT DATA PASSED
7
DATA RATE REDUCED
15
NO DATA PASSED
12
INCORRECT DATA PASSED
16
DATA RATE REDUCED
4
CONSTANT INCORRECT DATA PASSED
5
VARIABLE INCORRECT DATA PASSED
13
CONSTANT INCORRECT DATA PASSED
14
VARIABLE INCORRECT DATA PASSED

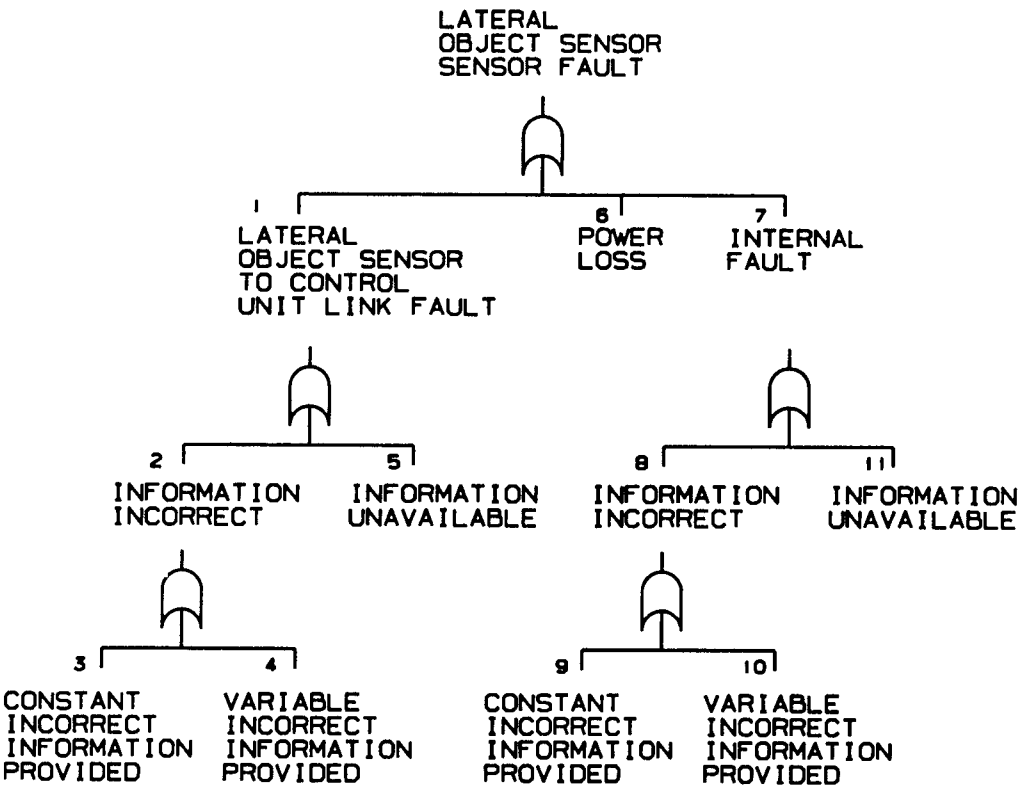
N.2.6

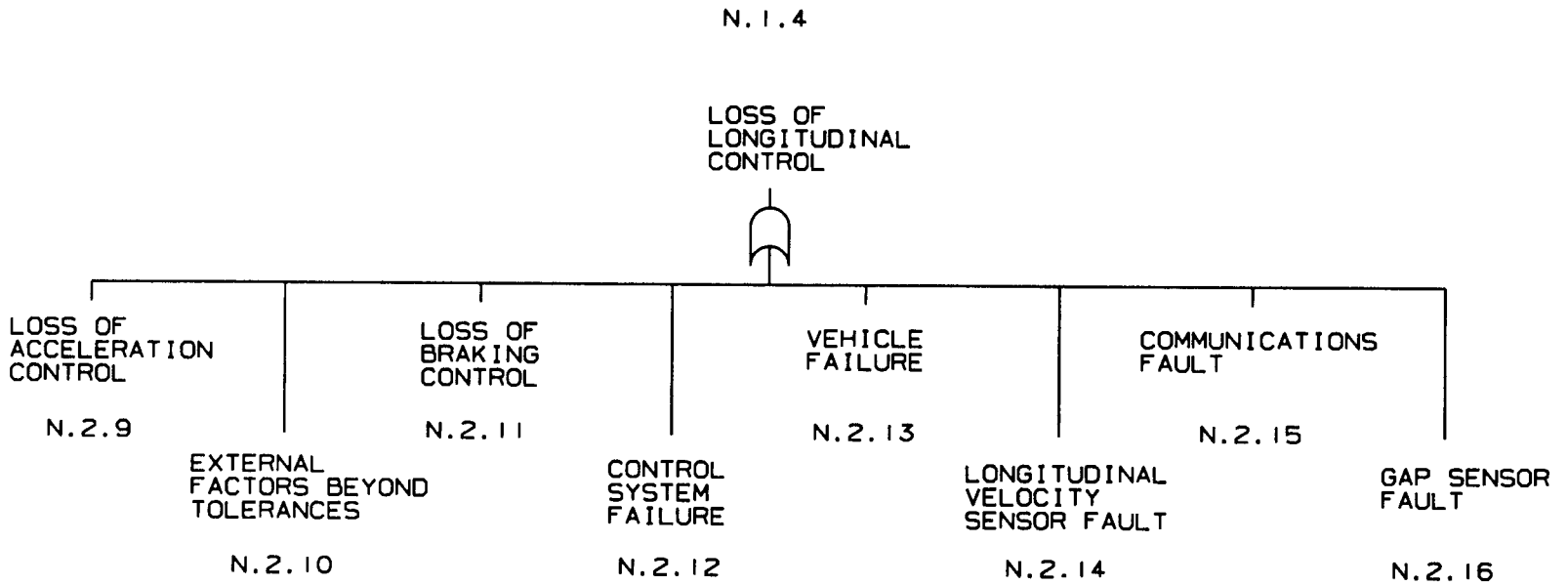

LATERAL ACCELERATION SENSOR FAULT
1
6
7
LATERAL ACCELERATION TO CONTROL UNIT LINK FAULT
POWER LOSS
INTERNAL FAULT
2
5
8
11
ACCELERATION INFORMATION INCORRECT
ACCELERATION INFORMATION UNAVAILABLE
ACCELERATION INFORMATION INCORRECT
ACCELERATION INFORMATION UNAVAILABLE
3
4
9
10
CONSTANT INCORRECT INFORMATION PROVIDED
VARIABLE INCORRECT INFORMATION PROVIDED
CONSTANT INCORRECT INFORMATION PROVIDED
VARIABLE INCORRECT INFORMATION PROVIDED

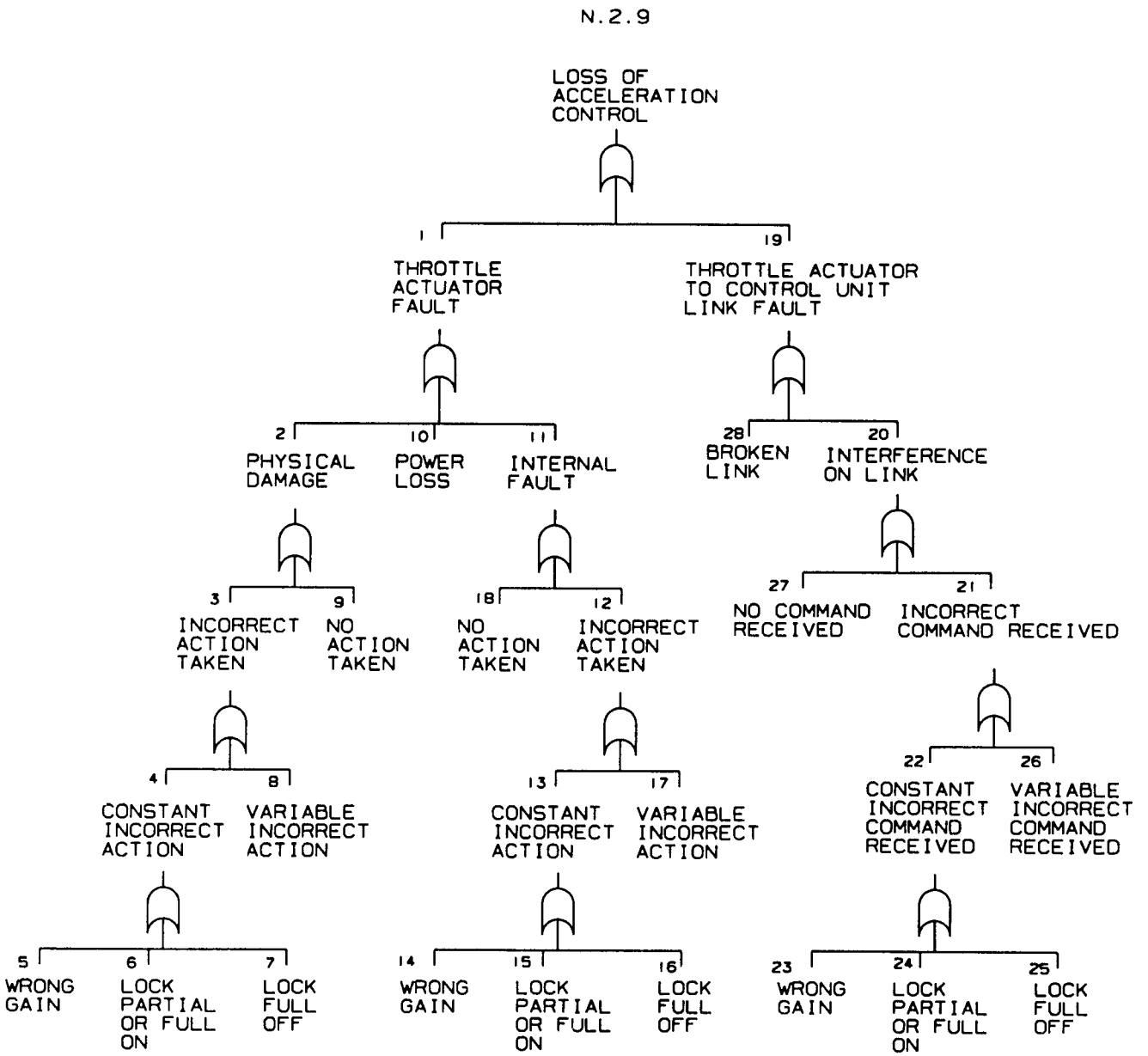
N.2.7

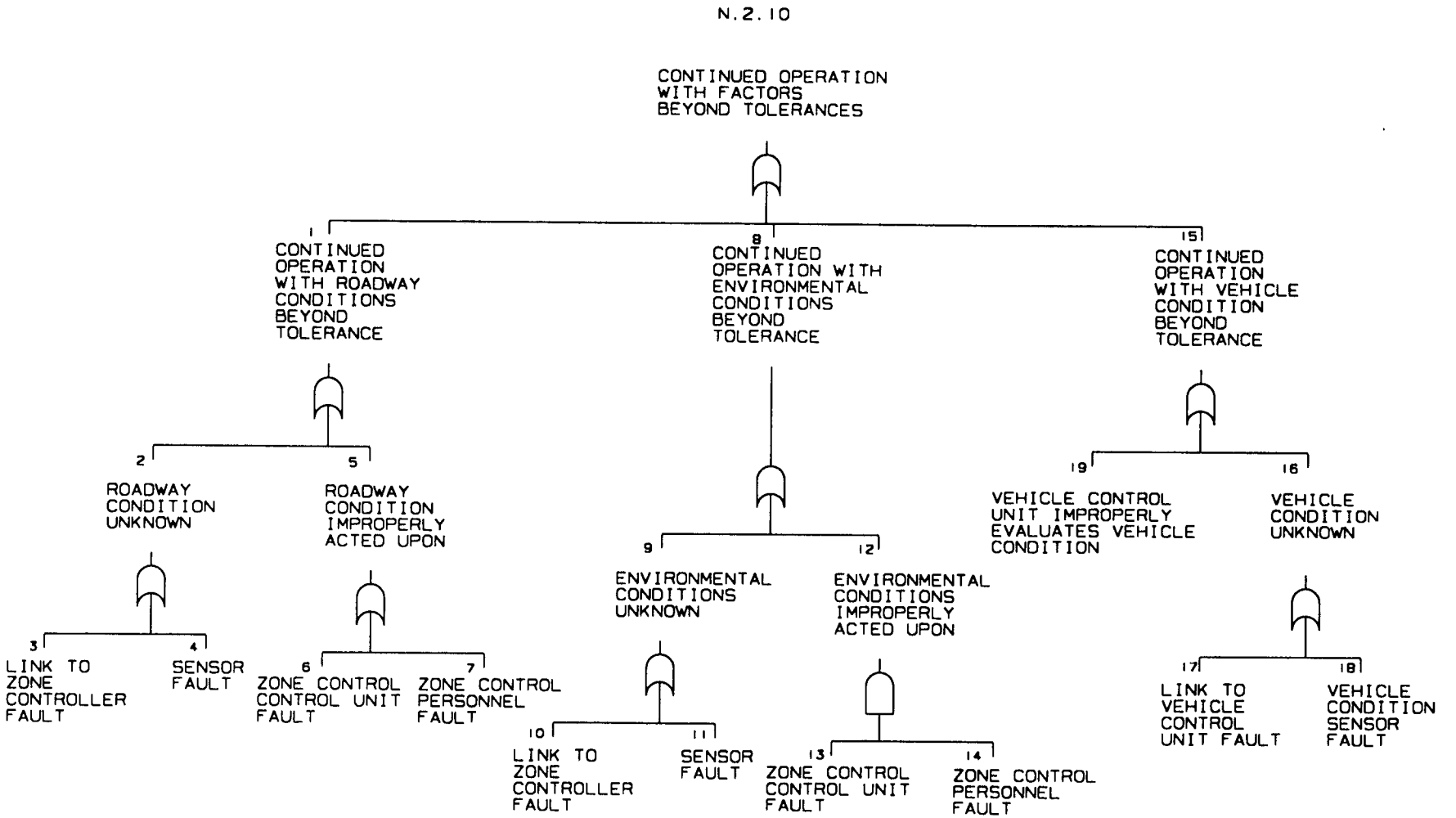

VEHICLE FAILURE
1
2
3
FLAT TIRE
VEHICLE STRUCTURAL FAILURE
LOSS OF PROPULSION

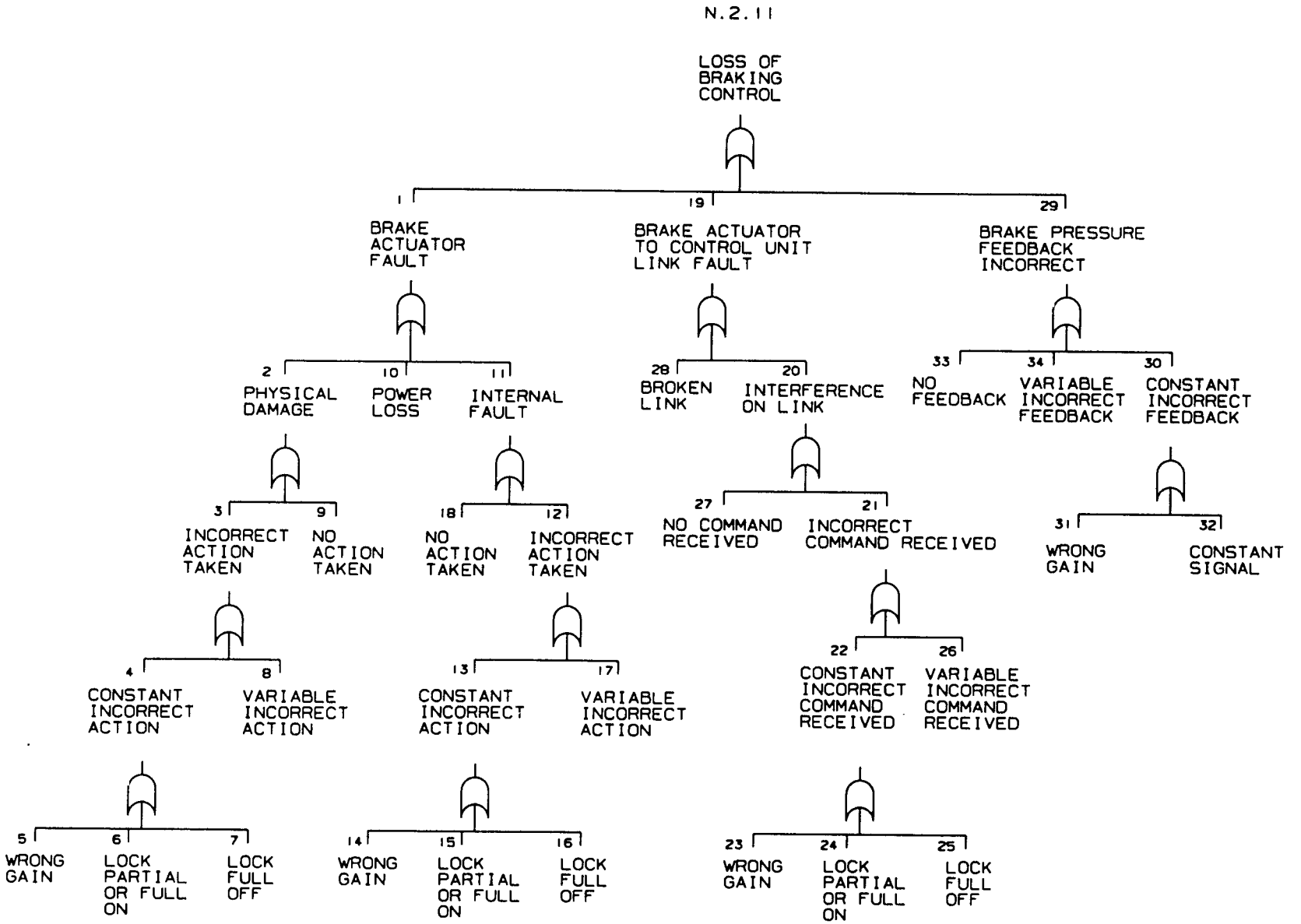
N.2.8

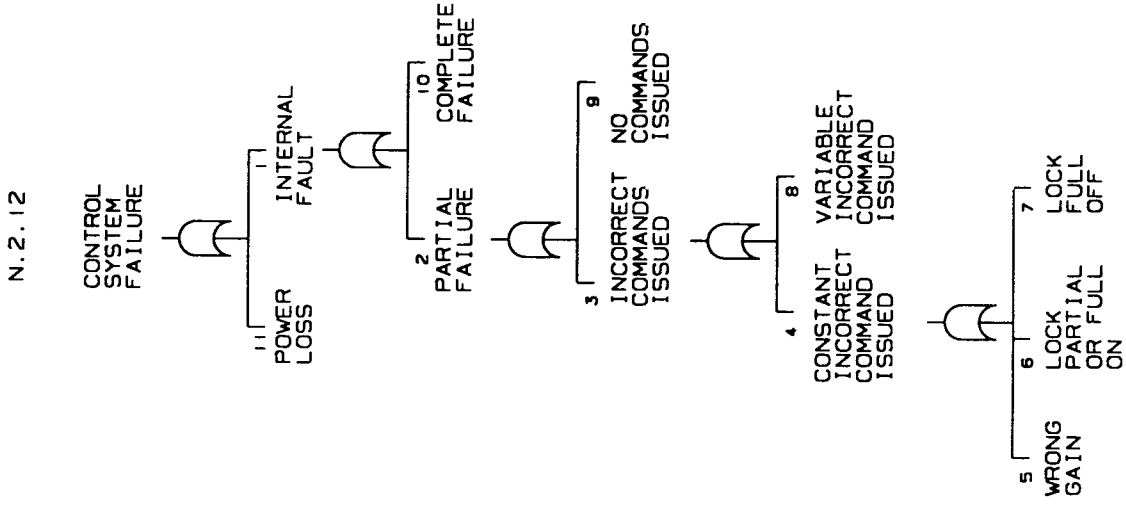

LATERAL
OBJECT SENSOR
SENSOR FAULT
1
LATERAL
OBJECT SENSOR
TO CONTROL
UNIT LINK FAULT
6
POWER
LOSS
7
INTERNAL
FAULT
2
INFORMATION
INCORRECT
5
INFORMATION
UNAVAILABLE
8
INFORMATION
INCORRECT
11
INFORMATION
UNAVAILABLE
3
CONSTANT
INCORRECT
INFORMATION
PROVIDED
4
VARIABLE
INCORRECT
INFORMATION
PROVIDED
9
CONSTANT
INCORRECT
INFORMATION
PROVIDED
10
VARIABLE
INCORRECT
INFORMATION
PROVIDED


N.1.4
LOSS OF LONGITUDINAL CONTROL
LOSS OF ACCELERATION CONTROL
N.2.9
EXTERNAL FACTORS BEYOND TOLERANCES
N.2.10
LOSS OF BRAKING CONTROL
N.2.11
CONTROL SYSTEM FAILURE
N.2.12
VEHICLE FAILURE
N.2.13
LONGITUDINAL VELOCITY SENSOR FAULT
N.2.14
COMMUNICATIONS FAULT
N.2.15
GAP SENSOR FAULT
N.2.16

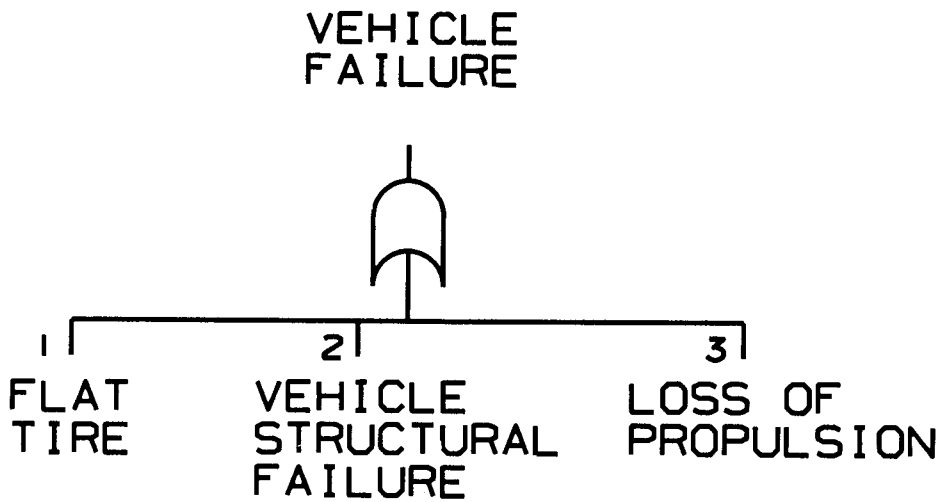

N.2.9
LOSS OF ACCELERATION CONTROL
1
19
THROTTLE ACTUATOR FAULT
THROTTLE ACTUATOR TO CONTROL UNIT LINK FAULT
2
10
11
28
20
PHYSICAL DAMAGE
POWER LOSS
INTERNAL FAULT
BROKEN LINK
INTERFERENCE ON LINK
3
9
18
12
27
21
INCORRECT ACTION TAKEN
NO ACTION TAKEN
NO ACTION TAKEN
INCORRECT ACTION TAKEN
NO COMMAND RECEIVED
INCORRECT COMMAND RECEIVED
4
8
13
17
22
26
CONSTANT INCORRECT ACTION
VARIABLE INCORRECT ACTION
CONSTANT INCORRECT ACTION
VARIABLE INCORRECT ACTION
CONSTANT INCORRECT COMMAND RECEIVED
VARIABLE INCORRECT COMMAND RECEIVED
5
6
7
14
15
16
23
24
25
WRONG GAIN
LOCK PARTIAL OR FULL ON
LOCK FULL OFF
WRONG GAIN
LOCK PARTIAL OR FULL ON
LOCK FULL OFF
WRONG GAIN
LOCK PARTIAL OR FULL ON
LOCK FULL OFF


N.2.10
CONTINUED OPERATION WITH FACTORS BEYOND TOLERANCES
1
CONTINUED OPERATION WITH ROADWAY CONDITIONS BEYOND TOLERANCE
8
CONTINUED OPERATION WITH ENVIRONMENTAL CONDITIONS BEYOND TOLERANCE
15
CONTINUED OPERATION WITH VEHICLE CONDITION BEYOND TOLERANCE
2
ROADWAY CONDITION UNKNOWN
5
ROADWAY CONDITION IMPROPERLY ACTED UPON
9
ENVIRONMENTAL CONDITIONS UNKNOWN
12
ENVIRONMENTAL CONDITIONS IMPROPERLY ACTED UPON
19
VEHICLE CONTROL UNIT IMPROPERLY EVALUATES VEHICLE CONDITION
16
VEHICLE CONDITION UNKNOWN
3
LINK TO ZONE CONTROLLER FAULT
4
SENSOR FAULT
6
ZONE CONTROL CONTROL UNIT FAULT
7
ZONE CONTROL PERSONNEL FAULT
10
LINK TO ZONE CONTROLLER FAULT
11
SENSOR FAULT
13
ZONE CONTROL CONTROL UNIT FAULT
14
ZONE CONTROL PERSONNEL FAULT
17
LINK TO VEHICLE CONTROL UNIT FAULT
18
VEHICLE CONDITION SENSOR FAULT

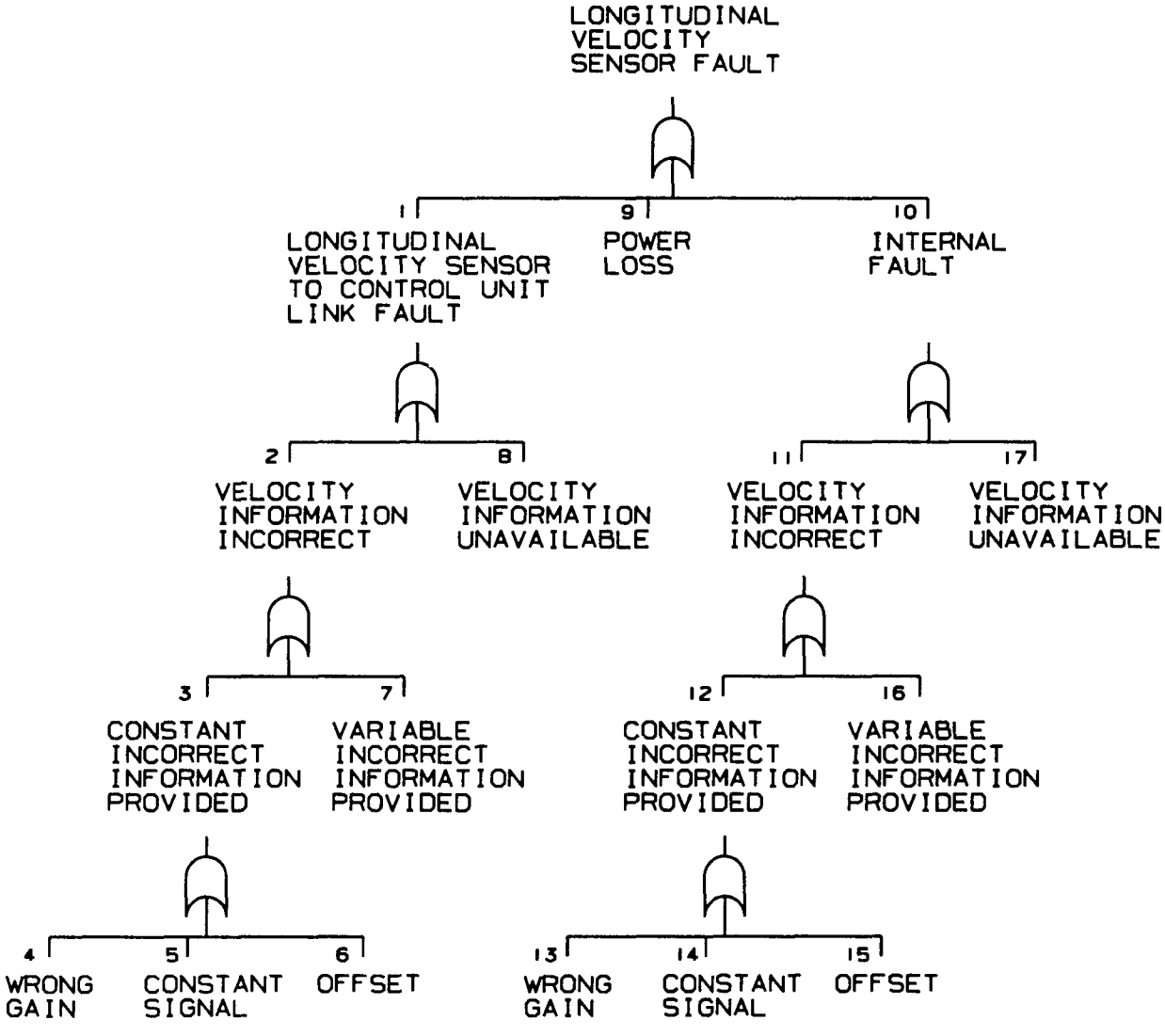

N.2.11
LOSS OF BRAKING CONTROL
1
19
29
BRAKE ACTUATOR FAULT
BRAKE ACTUATOR TO CONTROL UNIT LINK FAULT
BRAKE PRESSURE FEEDBACK INCORRECT
2
10
11
PHYSICAL DAMAGE
POWER LOSS
INTERNAL FAULT
28
20
BROKEN LINK
INTERFERENCE ON LINK
33
34
30
NO FEEDBACK
VARIABLE INCORRECT FEEDBACK
CONSTANT INCORRECT FEEDBACK
3
9
INCORRECT ACTION TAKEN
NO ACTION TAKEN
18
12
NO ACTION TAKEN
INCORRECT ACTION TAKEN
27
21
NO COMMAND RECEIVED
INCORRECT COMMAND RECEIVED
31
32
WRONG GAIN
CONSTANT SIGNAL
4
8
CONSTANT INCORRECT ACTION
VARIABLE INCORRECT ACTION
13
17
CONSTANT INCORRECT ACTION
VARIABLE INCORRECT ACTION
22
26
CONSTANT INCORRECT COMMAND RECEIVED
VARIABLE INCORRECT COMMAND RECEIVED
5
6
7
WRONG GAIN
LOCK PARTIAL OR FULL ON
LOCK FULL OFF
14
15
16
WRONG GAIN
LOCK PARTIAL OR FULL ON
LOCK FULL OFF
23
24
25
WRONG GAIN
LOCK PARTIAL OR FULL ON
LOCK FULL OFF


N.2.12
CONTROL SYSTEM FAILURE
1 INTERNAL FAULT
11 POWER LOSS
2 PARTIAL FAILURE
10 COMPLETE FAILURE
3 INCORRECT COMMANDS ISSUED
9 NO COMMANDS ISSUED
4 CONSTANT INCORRECT COMMAND ISSUED
8 VARIABLE INCORRECT COMMAND ISSUED
5 WRONG GAIN
6 LOCK PARTIAL OR FULL ON
7 LOCK FULL OFF

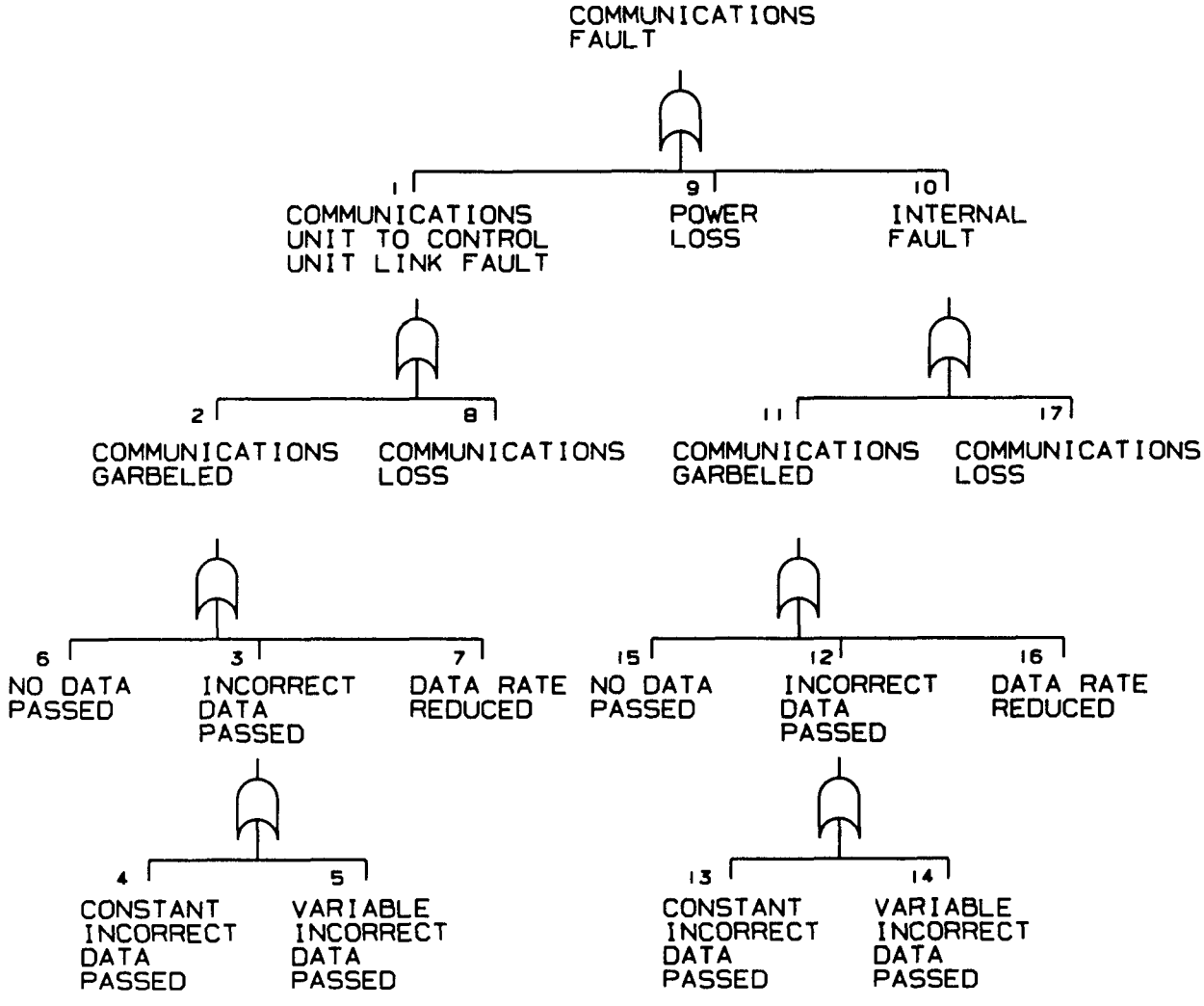
N.2.13


VEHICLE FAILURE
1
2
3
FLAT TIRE
VEHICLE STRUCTURAL FAILURE
LOSS OF PROPULSION

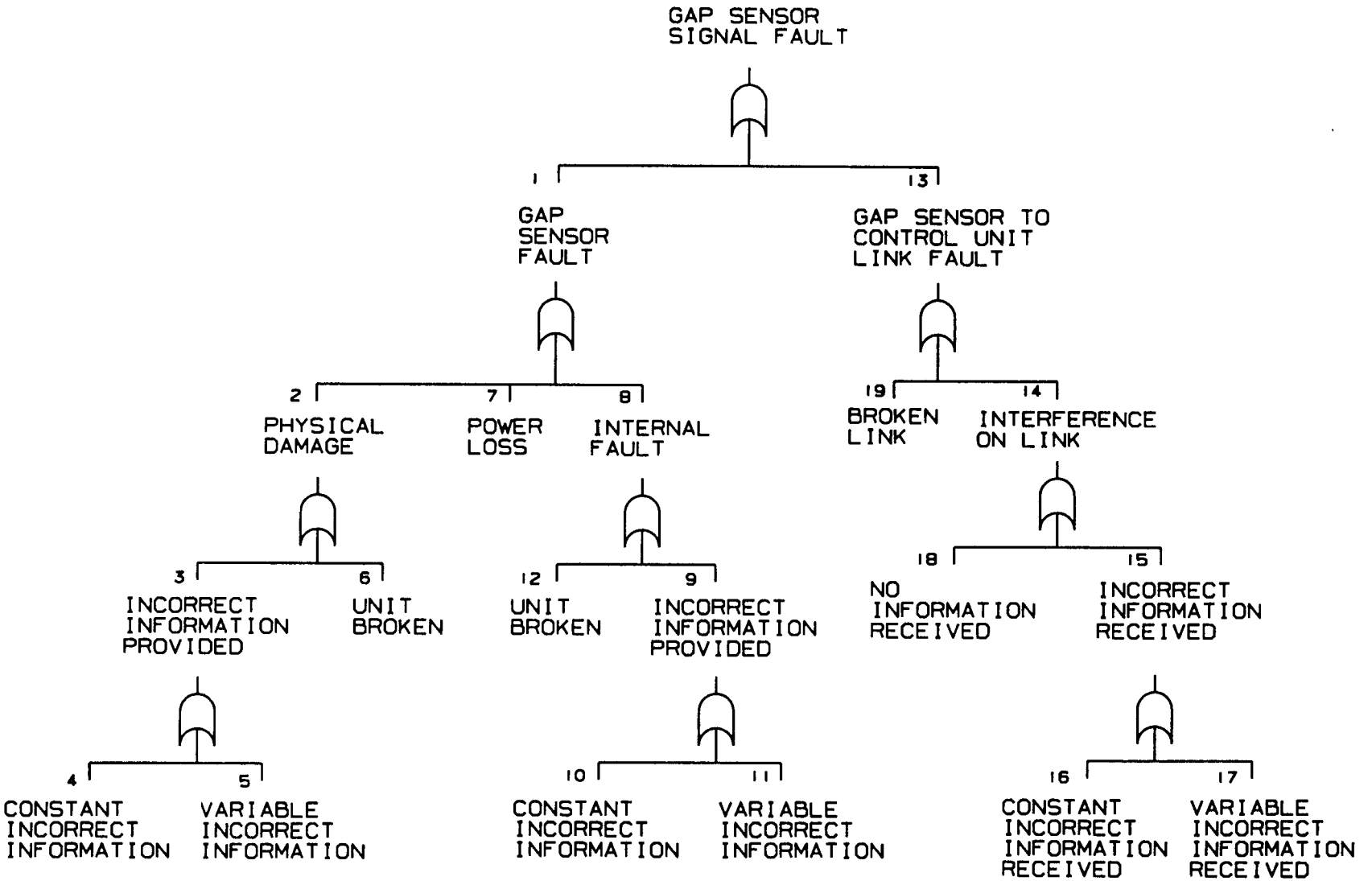
N.2.14


LONGITUDINAL VELOCITY SENSOR FAULT
1
9
10
LONGITUDINAL VELOCITY SENSOR TO CONTROL UNIT LINK FAULT
POWER LOSS
INTERNAL FAULT
2
8
11
17
VELOCITY INFORMATION INCORRECT
VELOCITY INFORMATION UNAVAILABLE
VELOCITY INFORMATION INCORRECT
VELOCITY INFORMATION UNAVAILABLE
3
7
12
16
CONSTANT INCORRECT INFORMATION PROVIDED
VARIABLE INCORRECT INFORMATION PROVIDED
CONSTANT INCORRECT INFORMATION PROVIDED
VARIABLE INCORRECT INFORMATION PROVIDED
4
5
6
13
14
15
WRONG GAIN
CONSTANT SIGNAL
OFFSET
WRONG GAIN
CONSTANT SIGNAL
OFFSET

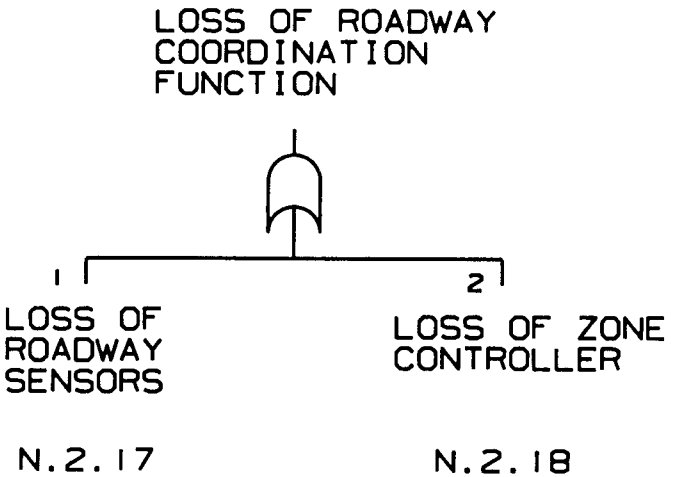
N.2.15


COMMUNICATIONS FAULT
1
COMMUNICATIONS UNIT TO CONTROL UNIT LINK FAULT
9
POWER LOSS
10
INTERNAL FAULT
2
COMMUNICATIONS GARBELED
8
COMMUNICATIONS LOSS
11
COMMUNICATIONS GARBELED
17
COMMUNICATIONS LOSS
6
NO DATA PASSED
3
INCORRECT DATA PASSED
7
DATA RATE REDUCED
15
NO DATA PASSED
12
INCORRECT DATA PASSED
16
DATA RATE REDUCED
4
CONSTANT INCORRECT DATA PASSED
5
VARIABLE INCORRECT DATA PASSED
13
CONSTANT INCORRECT DATA PASSED
14
VARIABLE INCORRECT DATA PASSED

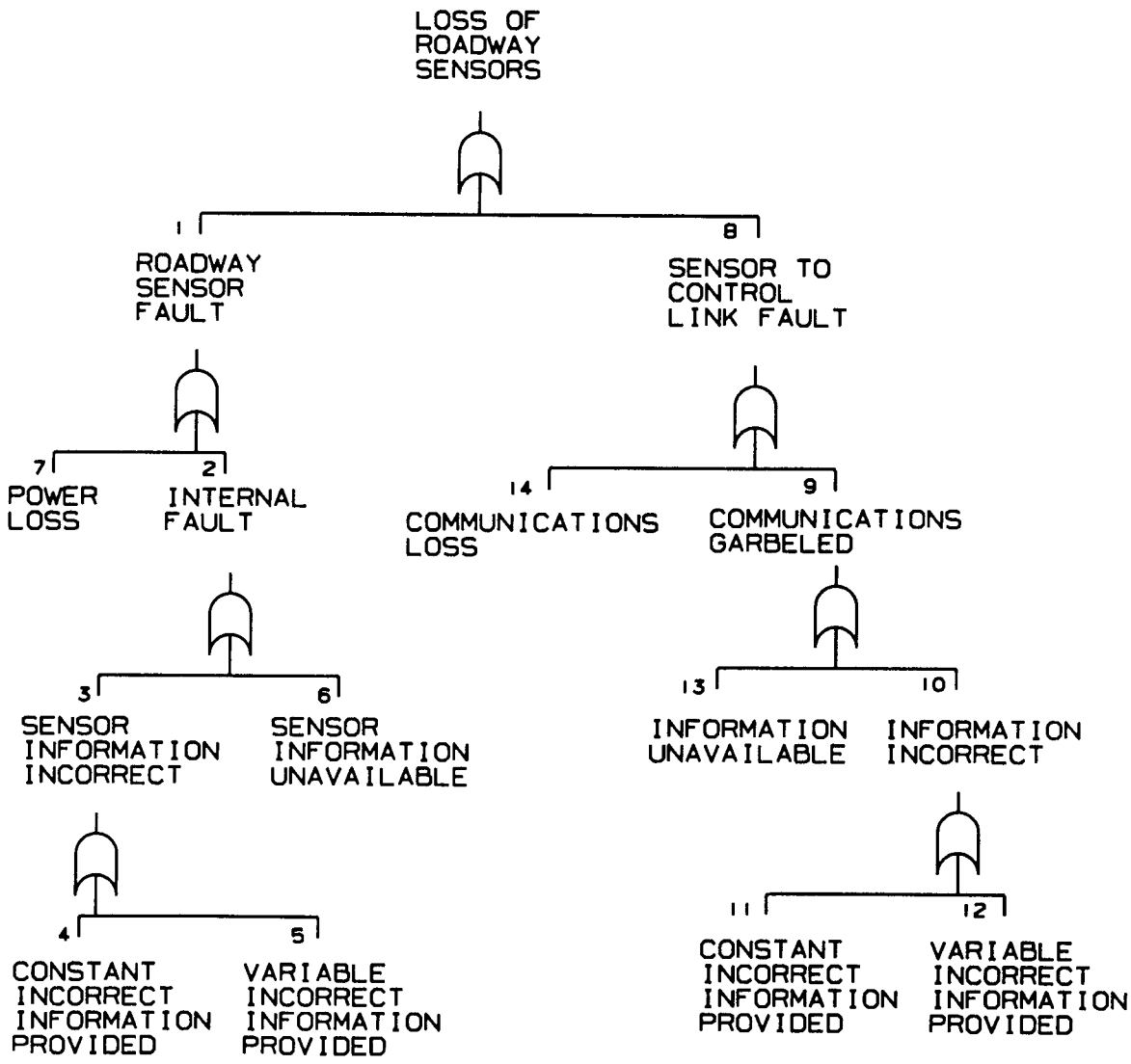
N.2.16


GAP SENSOR SIGNAL FAULT
1
13
GAP SENSOR FAULT
GAP SENSOR TO CONTROL UNIT LINK FAULT
2
7
8
19
14
PHYSICAL DAMAGE
POWER LOSS
INTERNAL FAULT
BROKEN LINK
INTERFERENCE ON LINK
3
6
12
9
18
15
INCORRECT INFORMATION PROVIDED
UNIT BROKEN
UNIT BROKEN
INCORRECT INFORMATION PROVIDED
NO INFORMATION RECEIVED
INCORRECT INFORMATION RECEIVED
4
5
10
11
16
17
CONSTANT INCORRECT INFORMATION
VARIABLE INCORRECT INFORMATION
CONSTANT INCORRECT INFORMATION
VARIABLE INCORRECT INFORMATION
CONSTANT INCORRECT INFORMATION RECEIVED
VARIABLE INCORRECT INFORMATION RECEIVED

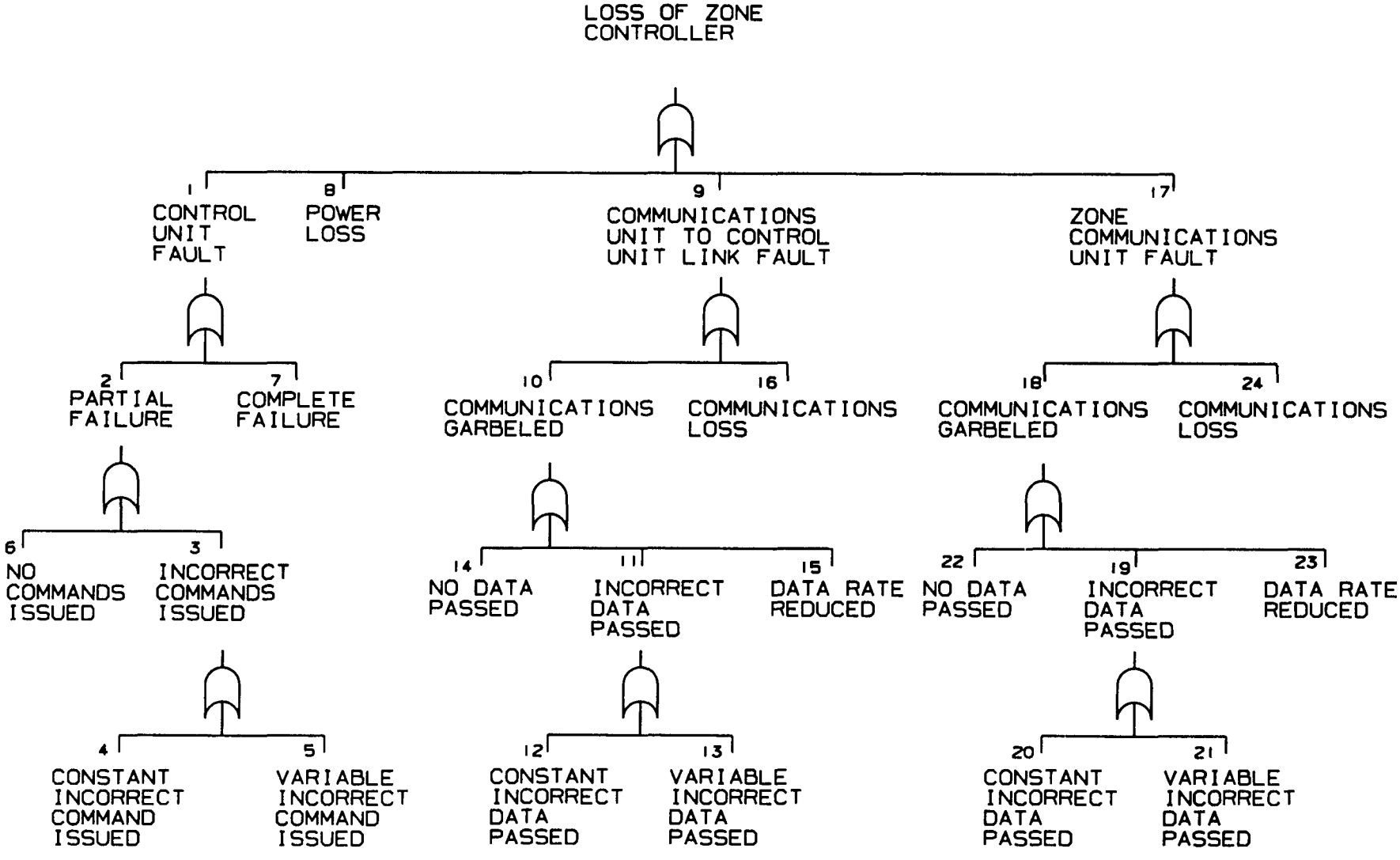
N.1.5


LOSS OF ROADWAY COORDINATION FUNCTION
1
2
LOSS OF ROADWAY SENSORS
LOSS OF ZONE CONTROLLER
N.2.17
N.2.18

N.2.17


LOSS OF ROADWAY SENSORS
1
8
ROADWAY SENSOR FAULT
SENSOR TO CONTROL LINK FAULT
7
2
POWER LOSS
INTERNAL FAULT
14
9
COMMUNICATIONS LOSS
COMMUNICATIONS GARBELED
3
6
13
10
SENSOR INFORMATION INCORRECT
SENSOR INFORMATION UNAVAILABLE
INFORMATION UNAVAILABLE
INFORMATION INCORRECT
4
5
11
12
CONSTANT INCORRECT INFORMATION PROVIDED
VARIABLE INCORRECT INFORMATION PROVIDED
CONSTANT INCORRECT INFORMATION PROVIDED
VARIABLE INCORRECT INFORMATION PROVIDED

N.2.18


LOSS OF ZONE CONTROLLER
1
CONTROL UNIT FAULT
8
POWER LOSS
9
COMMUNICATIONS UNIT TO CONTROL UNIT LINK FAULT
17
ZONE COMMUNICATIONS UNIT FAULT
2
PARTIAL FAILURE
7
COMPLETE FAILURE
10
COMMUNICATIONS GARBELED
16
COMMUNICATIONS LOSS
18
COMMUNICATIONS GARBELED
24
COMMUNICATIONS LOSS
6
NO COMMANDS ISSUED
3
INCORRECT COMMANDS ISSUED
14
NO DATA PASSED
11
INCORRECT DATA PASSED
15
DATA RATE REDUCED
22
NO DATA PASSED
19
INCORRECT DATA PASSED
23
DATA RATE REDUCED
4
CONSTANT INCORRECT COMMAND ISSUED
5
VARIABLE INCORRECT COMMAND ISSUED
12
CONSTANT INCORRECT DATA PASSED
13
VARIABLE INCORRECT DATA PASSED
20
CONSTANT INCORRECT DATA PASSED
21
VARIABLE INCORRECT DATA PASSED

APPENDIX B. ACTION TIMELINES

ID	A. ACTION	B. VEHICLE	C. INFRASTRUCTURE	D. COMMUNICATIONS
1	Enter the highway on a normal entry ramp	Manual Control	None	None
2	Set AHS destination	Driver interacts with AHS in vehicle via AHS input station	None	None
3	Merge into the transition lane	Manual control	None	None
4	Request AHS entry	Manual control, request via pushbutton on steering wheel	Receives AHS entry request, adequate room on AHS for vehicle, vehicle ID confirmed, vehicle status acceptable, vehicle position matches check-in point, destination understood	V/IS - Entry request, vehicle identification, vehicle status, vehicle position, requested destination
5	AHS entry authorized	Manual control, light/tone signals AHS authorization	Accept AHS entry when all AHS entry requirements are met	IS/V - Accept AHS entry
6	AHS entry denied	Manual control, driver must maintain manual control	Failure of any of the items in block C4 and C5	IS/V - Reject AHS entry
7	Transition to automatic control	Driver requests transitions via pushbutton on steering wheel, vehicle monitors post-transition status and reports to IS, light/tone signals AHS control, driver releases steering wheel and pedals	Upon receipt of driver's signal that he is ready to release control of the vehicle, IS assumes control of vehicle, IS evaluates post transition status, IS signals control transfer complete	V/IS - Ready for AHS, post transitio status IS/V - Light & tone on when AHS a control of vehicle
8	Lateral control - lane following	Vehicle follows active guidewire in center of lane	Maintain track of vehicle's position and health	V/IS - Position and status reports
9	Longitudinal control - throttle and brake	Vehicle has on-board gap sensor to measure distance to vehicle or large obstacle ahead, gap maintained via application of throttle and brakes	IS assigns block of roadway to vehicle and will not allow other AHS vehicles into block from adjacent lanes	IS/V - Maximum speed limit
10	Transition lane to AHS lane change	V controls dynamics of lane change, on-board V lateral sensors double check for close range vehicle in destination lane	IS commands instant of lane change, IS assigns block of roadway to vehicle and will not allow other AHS vehicles into block from adjacent lanes	IS/V - Change lane left now V/IS - Emergency override if lateral sensor detect vehicle or obstacle in destination lane
11	AHS lane to AHS lane change	V controls dynamics of lane change, on-board V lateral sensors double check for close range vehicle in destination lane, lane change report	IS commands instant of lane change, IS assigns block of roadway to vehicle and will not allow other AHS vehicles into block from adjacent lanes	IS/V - Change lane, left or right, nov V/IS - Emergency override if lateral sensor detect vehicle or obstacle in destination lane, lane change report
12	Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver hits panic button	IS processes panic stop request and allows/disallows vehicle to slow in lane at maximum AHS rate to a stop, IS commands nearby vehicles to stop behind subject vehicle and to decrease speed in adjacent AHS lanes, zone control contacts driver to inquire about nature of emergency	V/IS - Panic stop maneuver request, emergency explanation IS/V - IS allows or disallows panic s IS alerts nearby vehicles, nature of emergency?
13	Driver desires to exit prior to input destination	Driver requests exit at next exit, hospital area, food stop, rest stop, service stop, or police stop via input on AHS panel	IS determines what exit is appropriate to request and re-routes vehicle to new destination	V/IS - New destination request IS/V - New destination exit informat

14	Vehicle nears destination	Automatic control continued, light/tone alert driver to nearness of destination, AHS panel displays alphanumeric sequence for driver awareness test, driver takes test	IS recognizes destination proximity, generates light/tone to alert driver, generates alphanumeric string for driver awareness test, scores awareness test	IS/V - light/tone signal, alphanumeri sequence V/IS - alphanumeric sequence respo
16	AHS lane to transition lane change	V controls dynamics of lane change, on-board V lateral sensors double check for close range vehicle in destination lane	IS commands instant of lane change based on transition lane vehicle sensor information[1]	IS/V - Change lane right now V/IS - Emergency override if lateral sensor detect vehicle or obstacle
17	Transition to manual control	Driver places hands and feet on wheel and pedals and signals desire to recover manual control in transition lane via switch on steering wheel, driver recovers manual control	IS releases control of vehicle to driver once it has received driver's final ready signal	V/IS - Driver's final ready signal IS/V - Release control to driver
18	Driver fails awareness test	Vehicle continues in AHS lane on automatic control	IS routes vehicle to intervention area	V/IS - None or incorrect series of alphanumeric sequences
19	Merge into manual lane	Manual control	None	None
20	Exit roadway	Manual control	None	None
101	Vehicles in transition lane	None	Sensors in the roadway detect the presence of all vehicles in the transition lane	R/IS - Presence of vehicles in the transition lane
102	Sensors monitor condition of roadway and environment	None	Humans in zone control facilities base decisions about maximum speeds and redirection of traffic on visual information	R/IS - Cameras for general flow and roadway condition monitoring, ice sensors

~~ID~~	A. ACTION	B. VEHICLE	C. INFRASTRUCTURE	D. COMMUNICATIONS
1	Enter the highway on an AHS specific entry ramp (driver implicitly requesting AHS to take control)	Manual control	Vehicle identification confirmed, vehicle status acceptable, vehicle position matches check-in point	V/IS - Vehicle identification, vehicle status, vehicle position
2	AHS entry authorized	Manual control	Adequate room on AHS for vehicle	IS/V - Accept AHS entry
3	AHS entry denied	Manual control, driver must maintain manual control and drive off entry ramp	Failure of any of the items in blocks C1 and C2, command to maintain manual control	IS/V - Reject AHS entry, maintain manual control and exit at reject ramp
4	Transition to automatic control	Light/tone signals AHS control, vehicle monitors post-transition status, driver releases steering wheel and pedals	IS takes control, evaluates post-transition status, alerts driver of transition success	IS/V - Light & tone on after AHS attains control of vehicle V/IS - Post transition status
5	Set AHS destination	Driver interacts with AHS in vehicle via AHS input station	IS understands destination request	V/IS - Destination
6	Merge into AHS lane as singleton	Lane change made under AHS control, lateral sensor act as backup to make sure no collisions	IS merges vehicle into traffic flow from entry ramp (modifying speed of vehicles on mainline if needed)	IS/V - Change lane now IS/Other Vehicles - Modify speed to make gap for merge
7	Form into a platoon	V obeys IS orders with respect to speed and attach, final close-in maneuvering in/near platoon responsibility of vehicle systems	IS commands vehicle to attach at head (becoming new leader by slowing and letting a trailing platoon catch up) or tail (becoming new follower by speeding up to catch a leading platoon) of a platoon	IS/V - new speed command and attach command
8	Lateral control - lane following	Vehicle follows passive markers in center of lane	Maintain track of vehicle position and health	V/IS - Position and health reports
9	Longitudinal control - throttle and brake	Vehicle has on-board headway sensor to measure distance to vehicle or large obstacle ahead, headway maintained via application of throttle and brakes	IS assigns vehicle as platoon follower or leader	IS/V - Maximum speed limit
10	AHS lane to AHS lane change	V controls dynamics of lane change, on-board V lateral sensors double check for close range vehicle in destination lane	IS commands instant of lane change, IS assigns block of roadway to vehicle and will not allow other AHS vehicles into block from adjacent lanes, IS commands speed profiles of vehicles	IS/V - Change lane, left or right, now V/IS - Emergency override if lateral sensor detect vehicle or obstacle IS/Other Vehicles - Modify speed to make gap for merge
11	Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver hits panic button, vehicle slows at maximum allowable AHS rate in lane and stops after IS approval, driver informs sector control of emergency	IS processes and approves panic stop request, identifies and alerts other vehicles affected, sector control contacts driver to inquire nature of emergency	V/IS - Panic stop maneuver request, emergency explanation IS/V - Panic stop approved, nature of emergency IS/Other Vehicles - alerts other vehicles affect of panic stop
12	Driver desires to exit prior to input destination	Driver requests exit at next exit, hospital area, food stop, rest stop, service stop, or police stop via input on AHS panel	IS determines what exit is appropriate to request and re-routes vehicle to new destination	V/IS - New destination request IS/V - New destination
13	Vehicle nears destination	Automatic control continued, light/tone alert driver to nearness of destination, AHS panel	IS recognizes destination proximity, generates light/tone to alert driver, generates	IS/V - light/tone signal, alphanumeric sequence

		displays alphanumeric sequence for driver awareness test, driver takes test	alphanumeric string for driver awareness test, scores awareness test	V/IS - alphanumeric sequence response
14	Vehicle deplatoons	If lead - vehicle accelerates to attain gap between v and platoon, If tail - vehicle decelerates to attain gap between v and platoon, If v in middle - v and back of platoon decelerate to attain gap then v acts as lead above	IS commands deplatoon	IS/V - Deplatoon
15	Merge from AHS lane to exit ramp	V controls dynamics of lane change, on-board V lateral sensors double check for close range vehicle in destination lane	IS commands instant of lane change	IS/V - Change lane, left or right, now V/IS - Emergency override if lateral sensor detect vehicle or obstacle
16	Transition to manual control on exit ramp	Driver places hands and feet on wheel and pedals and signals desire to recover manual control via switch on steering wheel, driver recovers manual control	IS releases control of vehicle to driver once it has received driver's final ready signal	V/IS - Driver's final ready signal IS/V - Release control to driver
17	Driver fails awareness test	Vehicle placed into parking zone next to ramp and police are called	IS commands vehicle park	V/IS - None or incorrect series of alphanumeric sequences IS/V - Park
18	Leave exit ramp	Manual control	None	None
102	Sensors monitor condition of roadway	None	Humans in sector control facilities base decisions about maximum speeds and redirection of traffic on visual information	R/IS - Cameras for general flow and roadway condition monitoring, ice sensors

C 3. ACTION TIMELINE

ID	A. ACTION	B. VEHICLE/PALLET	C. INFRASTRUCTURE	D. COMMUNICATIONS
1	Enter the pallet mate/demate facility and drive into a mating dock	Manual control	IS senses presence of vehicle and pallet, lowers loading gate to allow vehicle onto pallet, illuminates display	IS/P - Illuminate display telling driver to drive onto pallet and await docking
2	Drive onto pallet and lock down	Manual control of vehicle, pallet adjusts wheel locks to vehicle based on sensors in mating dock, driver drives vehicle onto pallet, pallet raises and engages wheel locks once vehicle is on pallet	IS senses vehicle wheel positions	IS/P - Wheel positions
3	Obtain AHS control panel	Driver lowers window to lift AHS control panel (AHSCP) from pole on pallet, brings unit inside vehicle and raises window (wireless connection between pallet and AHS panel), link between AHSCP and pallet confirmed	IS monitors	P/IS - Panel in-use signal, link established between AHSCP and pallet
4	Set AHS destination and transition to AHS control	Driver interacts with AHS in vehicle via AHSCP to set destination	IS recognizes destination, IS signals pallet to move towards AHS roadway under AHS control	P/IS - AHS destination IS/P - Move to AHS roadway
5	Lateral control - lane following	Pallet follows passive markers in center of lane	Maintain track of pallet position and health	P/IS - Position and status reports
6	Longitudinal control - throttle and brake	Pallet has on-board gap sensor to measure distance to vehicle or large obstacle ahead, gap maintained via application of throttle and brakes	IS determines maximum speed limit from roadway conditions	IS/P - Maximum speed limit
7	AHS lane to AHS lane change	P controls dynamics of lane change, on-board P lateral sensors double check for close range vehicle in destination lane	IS recommends lane change based on conditions and requested vehicle destination	IS/P - Change lane, left or right, recommendation P/IS - Lane change complete (part of normal position report)
8	Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver hits panic button	IS processes panic stop request and allows/disallows vehicle to slow in lane at maximum AHS rate to a stop, IS commands nearby vehicles to stop behind subject vehicle and to decrease speed in adjacent AHS lanes, zone control contacts driver to inquire about nature of emergency	P/IS - Panic stop maneuver request, emergency explanation IS/P - IS allows or disallows panic stop, IS alerts nearby vehicles, nature of emergency?
9	Driver desires to exit prior to input destination	Driver requests exit at next exit, hospital area, food stop, rest stop, service stop, or police stop via input on AHS panel	IS determines what exit is appropriate to request and re-routes vehicle to new destination	P/IS - New destination request IS/P - New destination exit information
10	Pallet arrives at destination	Pallet drives into mate/demate facility to an unloading dock under AHS control, driver replaces AHS panel, pallet drops wheel locks, driver manually drives off pallet and out of facility	IS selects/assigns unloading dock, IS senses presence of pallet at commanded unloading dock, IS monitors to see AHS panel is replaced then commands wheel lock drop, monitors to see that vehicle is driven off pallet in reasonable time - calls for human intervention if not, directs pallet to storage, repair, fueling, or other appropriate area	P/IS - Entering demate facility IS/P - Assign unloading dock P/IS - AHS panel returned, vehicle off pallet IS/P - Next assignment

C 3. ACTION TIMELINE

101	Sensors monitor condition of roadway and environment	None	Humans in sector control facilities base decisions about maximum speeds and redirection of traffic on visual information	R/IS - Cameras for general flow and roadway condition monitoring, ice sensors

C 3. ACTION TIMELINE

ID	A. ACTION	B. VEHICLE	C. INFRASTRUCTURE	D. COMMUNICATIONS
1	Enter the highway on a normal entry ramp to manual lane	Manual Control	None	None
2	Set AHS destination	Manual control, driver interacts with AHS in vehicle via AHS input station	None	None
3	Merge into mixed traffic lane	Manual control	None	None
4	Request AHS entry	Manual control, request via pushbutton on steering wheel	Receives AHS entry request, vehicle ID confirmed, vehicle status acceptable, vehicle position matches check-in point, destination understood	V/IS - Entry request, vehicle identification, vehicle status, vehicle position, requested destination
5	AHS entry authorized	Manual control, light/tone signals AHS authorization	Accept AHS entry when all AHS entry requirements are met	IS/V - Accept AHS entry
6	AHS entry denied	Manual control, buzzer signals AHS denied, driver must maintain manual control	Failure of any of the items in block C4 and C5	IS/V - Reject AHS entry
7	Transition to automatic control	Driver requests transition via pushbutton on steering wheel, vehicle monitors post-transition status and report to IS, light/tone signals AHS control, driver releases steering wheel and pedals	Upon receipt of driver's signal that he is ready to release control of the vehicle, IS assumes control of vehicle, IS evaluates post transition status, IS signals control transfer complete	V/IS - Ready for AHS, post transition status IS/V - Light & tone on when AHS has control of vehicle
8	Lateral control - lane following	Vehicle follows passive markers in center of lane	Maintain track of vehicle's position and health	V/IS - Position and status reports
9	Longitudinal control - throttle and brake	Vehicle has on-board headway sensor to measure distance to vehicle or large obstacle ahead, headway maintained via application of throttle and brakes	IS determines maximum speed limit from roadway conditions	IS/V - Maximum speed limit
11	Mixed lane to mixed lane change	V controls dynamics of lane change, V controls moment of lane change based on on-board sensors	IS recommends lane change based on conditions and requested vehicle destination	IS/V - Change lane, left or right, recommendation
12	Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver hits panic button, vehicle slows at maximum allowable AHS rate and stops, V alerts nearby vehicles, driver explains emergency to sector control	IS processes panic stop signal, sector control contacts driver to inquire about nature of emergency	V/IS - Panic stop maneuver signal, emergency explanation V/V - VS alerts nearby vehicles IS/V - Nature of emergency?
13	Driver desires to exit prior to input destination	Driver requests exit at next exit, hospital exit, food stop, rest stop, service stop, or police stop via input on AHS panel	IS determines what exit is appropriate to request and re-routes vehicle to new destination	V/IS - new destination request IS/V - new destination exit information
14	Vehicle nears destination	Automatic control continued, light/tone alert driver to nearness of destination, AHS panel displays alphanumeric sequence for driver awareness test, driver takes test	IS recognizes destination proximity, generates light/tone to alert driver, generates alphanumeric string for driver awareness test, scores awareness test	IS/V - light/tone signal, alphanumeric sequence V/IS - alphanumeric sequence response
16	Transition to manual control	Driver places hands and feet on wheel and pedals and signals desire to recover manual control in rightmost mixed traffic lane via switch on steering wheel, driver recovers	If driver passes awareness test the IS releases control of vehicle to driver once it has received driver's final ready signal	V/IS - Driver's final ready signal IS/V - Release control to driver

C 3. ACTION TIMELINE

		manual control		
17	Driver fails awareness test	Vehicle continues in AHS lane on automatic control	If driver fails awareness test the IS routes vehicle to intervention area	V/IS - None or incorrect series of alphanumeric sequences
18	Merge into manual lane	Manual control	None	None
19	Exit roadway	Manual control	None	None
102	Sensors monitor condition of roadway	None	Humans in sector control facilities base decisions about maximum speeds and redirection of traffic on visual information	R/IS - Cameras for general flow and roadway condition monitoring, ice sensors

C 3. ACTION TIMELINE

APPENDIX C. MALFUNCTION TIMELINES

ID	ACTION	MALFUNCTION	S[1]	US[2]
1	Enter the highway on a normal entry ramp	None defined		
2	Set AHS destination	1. AHS destination not set (driver, vehicle control unit)		X
3	Merge into the transition lane	None defined		
4	Request AHS entry	1. AHS request for entry fails (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		2. Road capacity check fails (roadside sensors, link, zone controller control unit)		X
		3. Vehicle ID fails (vehicle control unit, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		4. Vehicle status fails (vehicle internal sensors, vehicle communications bus, vehicle control unit, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		5. Vehicle position check fails (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		6. AHS destination request fails (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X
		7. AHS accepts destination when no such destination exists (zone controller control unit)	X	
5	AHS entry authorized	1. Driver not aware of authorization (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver)	X	
		2. AHS accepts and authorizes entry with missing, incomplete, or known incorrect check-in information (zone controller unit)		X
		3. AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters (zone controller unit)		X
6	AHS entry denied	1. AHS denies entry to vehicle which has met all check-in requirements (zone controller)	X	
		2. Driver not aware of rejection (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver)		X
7	Transition to automatic control	1. AHS request for transition fails (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X
		2. Transition complete but driver not aware of transition (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver)	X	
		3. Driver does not release steering wheel or get off pedals when AHS takes control even though he is aware of transfer (driver)		
		4. AHS fails to establish control of vehicle but signals driver that it has taken control (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, vehicle actuators)	X	
		5. AHS fails to establish control of vehicle (zone controller control unit, zone controller		X

C 1. MALFUNCTION TIMELINE

		communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, vehicle actuators)		
		6. Zone controller unaware vehicle is under AHS control after AHS takes control (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		7. Zone controller believes vehicle is under AHS control when it is not (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X
				X
8	Lateral control - lane following	1. Wire not functioning (missing, damaged, power loss)		X
		2. Wire not detected (wire sensor, vehicle communications bus, vehicle control unit)		X
		3. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X
		4. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X
		5. Collision (headway sensor, lateral sensors, vehicle communications bus, vehicle control unit, vehicle actuators)		
		6. Loss of steering authority (vehicle control unit, vehicle communications bus, vehicle steering actuators)		X
		7. Vehicle control unit issues improper commands (vehicle control unit)		
		8. Incorrect external sensor information (gap sensor, lateral sensors, vehicle communications bus, vehicle control unit)		X
		9. Incorrect internal status information (steering actuator position sensor, lateral acceleration sensor, vehicle communications bus, vehicle control unit)		X X
		10. Flat tire		
		11. Vehicle structural or systems failure		X
		12. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X
		13. External AHS command prompted by incorrect position data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X X
		14. External AHS command prompted by incorrect vehicle health data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X
				X
8	Lateral control - lane following (continued)	15. AHS command authority lost (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		X
		16. Vehicle unlocks from pallet (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit, wheel		X

C 1. MALFUNCTION TIMELINE

		lock actuators)		
9	Longitudinal control - throttle and brake	1. Loss of acceleration control (throttle actuator, vehicle communications bus, vehicle control system) 2. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 4. Collision (gap sensor, lateral sensors, vehicle communications bus, vehicle control unit, vehicle actuators) 5. Loss of braking control (brake actuator, vehicle communications bus, vehicle control system) 6. Vehicle control unit issues improper commands (vehicle control unit) 7. Flat tire 8. Vehicle structural or systems failure 9. Incorrect external sensor information (gap sensor, lateral sensors, vehicle communications bus, vehicle control unit)		X X X X X X X X X
9	Longitudinal control - throttle and brake (continued)	10. Incorrect internal status information (throttle actuator position sensor, brake actuator position sensor, longitudinal velocity sensor, vehicle communications bus, vehicle control unit) 11. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 12. External AHS command prompted by incorrect position data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 13. External AHS command prompted by incorrect vehicle health data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 14. Vehicle speed limit incorrect (roadside sensors, link, zone controller control unit, sector controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 15. AHS command authority lost (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 16. Vehicle unlocks from pallet (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit, wheel lock actuators)		X X X X X X
10	Transition lane to AHS lane change	1. Lane change command not received (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. AHS commands lane change with destination lane too full (roadside sensors, link, zone controller control unit) 3. Vehicle/obstacle in destination lane not detected (lateral sensors, vehicle	X	 X

C 1. MALFUNCTION TIMELINE

		communications bus, vehicle control unit) 4. Manual driven vehicle merges into subject vehicle - proximity crash. 5. Other vehicle merges too close ahead with too large a closing velocity 6. Other vehicle merges too close behind with too large a closing velocity		X X X X
11	AHS lane to AHS lane change	1. AHS commands lane change with destination lane too full (roadside sensors, link, zone controller control unit) 2. Vehicle/obstacle in destination lane not detected (lateral sensors, vehicle communications bus, vehicle control unit) 3. Lane change command not received (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 4. Lane change report not received (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X X X X
12	Driver perceives emergency situation that may not be detected by on-board or IS sensors	1. Driver activates panic button inappropriately (driver) 2. Driver warning fails (vehicle control unit, vehicle communications bus, vehicle actuators) 3. Other vehicles not alerted (vehicle control unit, vehicle communications bus, vehicle communications unit) 4. Sector control does not contact driver after panic stop (zone controller personnel, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 5. Driver does not inform or misinforms zone control about nature of emergency (driver)	X	 X X X
13	Driver desires to exit prior to input destination	1. Driver's request not/improperly acted upon (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
14	Vehicle nears destination	1. Proximity to destination not recognized (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 2. No driver alert signal (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. No driver awareness test generated (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 4. No driver awareness test response (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 5. Improperly evaluated driver awareness test (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit)	X X X X	 X
16	AHS lane to transition lane change	1. Lane change command not received (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. AHS commands lane change with destination lane too full (roadside sensors, link, zone controller control unit) 3. Vehicle/obstacle in destination lane not detected (lateral sensors, vehicle communications bus, vehicle control unit)	X	 X X

C 1. MALFUNCTION TIMELINE

		4. Manual driven vehicle merges into subject vehicle - proximity crash. 5. Other vehicle merges too close ahead with too large a closing velocity 6. Other vehicle merges too close behind with too large a closing velocity		 X X X
17	Transition to manual control	1. No request signal for manual control (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 2. AHS fails to release control to driver (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Driver fails to take manual control after AHS releases control (driver)	X X	 X
18	Driver fails awareness test	1. Infrastructure wrongly releases control to driver (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. Infrastructure does not route vehicle to intervention area (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X
19	Merge into manual lane	None defined		
20	Exit roadway	None defined		
101	Sensors monitor condition of roadway and environment	1. Conditions warranting operational parameter modification not/improperly acted upon (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X

C 2B. MALFUNCTION TIMELINE

ID	ACTION	MALFUNCTION	S[3]	US[4]
1	Enter the highway on an AHS specific entry ramp (driver implicitly requesting AHS to take control)	1. AHS request for entry fails (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		2. Vehicle ID fails (vehicle control unit, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		3. Vehicle status fails (vehicle internal sensors, vehicle communications bus, vehicle control unit, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		4. Vehicle position check fails (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
2	AHS entry authorized	1. Road capacity check fails (roadside sensors, link, zone controller control unit)		X
		2. AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information (zone controller unit)		X
		3. AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters (zone controller unit)		X
		4. Driver not aware of authorization (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver)	X	
3	AHS entry denied	1. AHS denies entry to vehicle which has met all check-in requirements (sector controller)	X	
		2. Driver not aware of rejection (sector controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver)		X
4	Transition to automatic control	1. AHS request for transition fails (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		2. Transition complete but driver not aware of transition (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver)	X	
		3. Driver does not release steering wheel or get off pedals when AHS takes control even though he is aware of transfer (driver)		
		4. AHS fails to establish control of vehicle but signals driver that it has taken control (sector controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, vehicle actuators)	X	X
		5. AHS fails to establish control of vehicle (sector controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, vehicle actuators)		
		6. Sector controller unaware vehicle is under AHS control after AHS takes control (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
		7. Sector controller believes vehicle is under AHS control when it is not (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X
				X

C 2B. MALFUNCTION TIMELINE

5	Set AHS destination	1. AHS destination request fails (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 2. AHS accepts destination when no such destination exists (sector controller control unit)	X X	
6	Merge into AHS lane as singleton	1. No merge command (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. Gap in mainline traffic not formed (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Vehicle/obstacle in destination lane not detected (lateral sensors, vehicle communications bus, vehicle control unit) 4. Vehicle/obstacle in destination lane detected (lateral sensors, vehicle communications bus, vehicle control unit, roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit)	X X	 X X
7	Form with a platoon	1. No platoon form command (sector controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. Current platoon leader will not relinquish lead (sector controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Platoon parameters improper (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)	X 	 X X
8	Lateral control - lane following	1. Marker (missing, damaged) 2. Markers not detected (marker sensor, vehicle communications bus, vehicle control unit) 3. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)	 	X X X
8	Lateral control - lane following (continued)	4. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 5. Collision (gap sensor, lateral sensors, vehicle communications bus, vehicle control unit, vehicle actuators) 6. Loss of steering authority (vehicle control unit, vehicle communications bus, vehicle steering actuators) 7. Vehicle control unit issues improper commands (vehicle control unit) 8. Incorrect external sensor information (gap sensor, lateral sensors, vehicle communications bus, vehicle control unit) 9. Incorrect internal status information (steering actuator position sensor, lateral acceleration sensor, vehicle communications bus, vehicle control unit) 10. Flat tire 11. Vehicle structural or systems failure 12. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 13. External AHS command prompted by incorrect position data (vehicle position sensor,	 	X X X X X X X X X

C 2B. MALFUNCTION TIMELINE

		vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 14. External AHS command prompted by incorrect vehicle health data (vehicle internal sensors, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 15. AHS command authority lost (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X X
9	Longitudinal control - throttle and brakes	1. Loss of acceleration control (throttle actuator, vehicle communications bus, vehicle control system) 2. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 4. Collision (gap sensor, lateral sensors, vehicle communications bus, vehicle control unit, vehicle actuators) 5. Loss of braking control (brake actuator, vehicle communications bus, vehicle control system) 6. Vehicle control unit issues improper commands (vehicle control unit) 7. Flat tire 8. Vehicle structural or systems failure 9. Incorrect external sensor information (gap sensor, lateral sensors, vehicle communications bus, vehicle control unit) 10. Incorrect internal status information (throttle actuator position sensor, brake actuator position sensor, longitudinal velocity sensor, vehicle communications bus, vehicle control unit) 11. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 12. External AHS command prompted by incorrect position data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 13. External AHS command prompted by incorrect vehicle health data (vehicle internal sensors, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 14. Vehicle speed limit incorrect (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X X X X X X X X X X X

C 2B. MALFUNCTION TIMELINE

9	Longitudinal control - throttle and brakes (continued)	15. Platoon position assignment unknown (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 16. AHS command authority lost (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X
10	AHS lane to AHS lane change - platoon	1. No lane change command (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. Gap in destination lane traffic not formed (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Vehicle/obstacle in destination lane not detected (lateral sensors, vehicle communications bus, vehicle control unit) 4. Vehicle/obstacle in destination lane detected by one or more platoon members (lateral sensors, vehicle communications bus, vehicle control unit, roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit) 5. Platoon actions not coordinated (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X X X X
11	Driver perceives emergency situation that may not be detected by on-board or IS sensors	1. Driver activates panic button inappropriately (driver) 2. Driver warning fails (vehicle control unit, vehicle communications bus, vehicle actuators, vehicle communications unit, zone controller communications unit, zone controller control unit) 3. Other vehicles not alerted (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 4. Sector control does not contact driver after panic stop (zone controller personnel, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 5. Driver does not inform or misinforms zone control about nature of emergency (driver)	X	 X X X X
12	Driver desires to exit prior to input destination	1. Driver's request not/improperly acted upon (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
13	Vehicle nears destination	1. Proximity to destination not recognized (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 2. No driver alert signal (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. No driver awareness test generated (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 4. No driver awareness test response (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 5. Improperly evaluated driver awareness test (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit)	X X X X	 X

C 2B. MALFUNCTION TIMELINE

14	Vehicle deplatoons	1. Deplatoon command not received (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. Vehicle unable to perform deplatoon manuever (vehicle control unit, vehicle communications bus, throttle actuator, brake actuator)	X	 X
15	Merge from AHS lane to exit ramp	1. Lane change command not received (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. AHS commands lane change with destination lane too full (roadside sensors, link, zone controller control unit) 3. Vehicle/obstacle in destination lane not detected (lateral sensors, vehicle communications bus, vehicle control unit)	X	 X X
16	Transition to manual control on exit ramp	1. No request signal for manual control (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 2. AHS fails to release control to driver (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Driver fails to take manual control after AHS releases control (driver)	X X	 X
17	Driver fails awareness test	1. Infrastructure wrongly releases control to driver (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. Infrastructure does not route vehicle to intervention area (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X
18	Leave exit ramp	None defined		
101	Sensors monitor condition of roadway	1. Conditions warranting operational parameter modification not/improperly acted upon (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X

C 3. MALFUNCTION TIMELINE

ID	ACTION	MALFUNCTION	S	US
1	Enter the pallet mate/demate facility and drive into a mating dock	1. Vehicle presence not recognized (mating dock sensors, link to zone controller, zone controller control unit)	X	
		2. Vehicle presence recognized without vehicle present (mating dock sensors, link to zone controller, zone controller control unit)	X	
		3. Pallet presence not recognized (mating dock sensors, link to zone controller, zone controller control unit)	X	
		4. Pallet presence recognized without pallet present (mating dock sensors, link to zone controller, zone controller control unit)		X
		5. Loading gate not lowered (zone controller control unit, link to loading gate actuator, loading gate actuator)	X	
		6. Display telling driver to drive onto pallet not illuminated (zone controller control unit, zone controller communications unit, pallet communications unit, pallet internal communications bus, pallet control unit, pallet display)	X	
2	Drive onto pallet and lock down	1. Wheel locks not adjusted to correct spacing (mating dock sensors, link to zone controller, zone controller control unit, zone controller communications unit, pallet communications unit, pallet internal communications bus, pallet control unit, wheel lock position actuators)		X
		2. Vehicle does not move onto pallet (driver, vehicle manual systems)		
		3. Wheel locks not engaged properly (pallet vehicle sensor, pallet internal communications bus, pallet control unit, pallet wheel lock engagement actuators)	X	X
3	Obtain AHS control panel	1. Driver does not obtain AHS control panel (driver, vehicle window, pallet/AHS panel attachment)	X	
		2. AHS panel does not establish/ looses contact with pallet (AHS panel, pallet communications unit, pallet internal communications bus, pallet control unit)	X	
		3. IS not informed of contact between AHS control panel and pallet (pallet control unit, pallet internal communication bus, pallet communications unit, zone controller communications unit, zone controller control unit)	X	
4	Set AHS destination and transition to AHS control	1. AHS destination not set or not recognized (driver, pallet control unit, pallet internal communication bus, pallet communications unit, zone controller communications unit, zone controller control unit)	X	
		2. Pallet does not move away from dock (zone controller control unit, zone controller communications unit, pallet communications unit, pallet internal communications bus, pallet control unit, pallet propulsion system)	X	
5	Lateral control - lane following	1. Marker (missing, damaged)		X
		2. Markers not detected (marker sensor, pallet communications bus, pallet control unit)		X
		3. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		X
		4. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		X
		5. Collision (headway sensor, lateral sensors, pallet communications bus, pallet control unit, pallet actuators)		
		6. Loss of steering authority (pallet control unit, pallet communications bus, pallet		

C 3. MALFUNCTION TIMELINE

		steering actuators)		X
		7. Pallet control unit issues improper commands (pallet control unit)		
		8. Incorrect external sensor information (headway sensor, lateral obstacle sensors, pallet communications bus, pallet control unit)		X
		9. Incorrect internal status information (steering actuator position sensor, lateral acceleration sensor, pallet communications bus, pallet control unit)		X X X
5	Lateral control - lane following (continued)	10. Flat tire		X
		11. Pallet structural or systems failure		X
		12. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		X
		13. External AHS command prompted by incorrect position data (pallet position sensor, pallet control unit, pallet communications bus, pallet communications unit, zone controller communication unit, zone controller control unit)		X
		14. External AHS command prompted by incorrect pallet health data (pallet internal sensors, pallet control unit, pallet communications bus, pallet communications unit, zone controller communication unit, zone controller control unit)		X
		15. AHS command authority lost (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		
		16. Vehicle unlocks from pallet (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit, wheel lock actuators)		X X
6	Longitudinal control - throttle and brake	1. Loss of acceleration control (throttle actuator, pallet communications bus, pallet control system)		X
		2. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		X
		3. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		X
		4. Collision (headway sensor, lateral sensors, pallet communications bus, pallet control unit, pallet actuators)		X
6	Longitudinal control - throttle and brake (continued)	5. Loss of braking control (brake actuator, pallet communications bus, pallet control system)		X
		6. Pallet control unit issues improper commands (pallet control unit)		X
		7. Flat tire		X
		8. Pallet structural or systems failure		X
		9. Incorrect external sensor information (headway sensor, lateral obstacle sensors, pallet		X

C 3. MALFUNCTION TIMELINE

		communications bus, pallet control unit) 10. Incorrect internal status information (throttle actuator position sensor, brake actuator position sensor, longitudinal velocity sensor, pallet communications bus, pallet control unit) 11. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 12. External AHS command prompted by incorrect position data (pallet position sensor, pallet control unit, pallet communications bus, pallet communications unit, zone controller communication unit, zone controller control unit) 13. External AHS command prompted by incorrect pallet health data (pallet position sensor, pallet control unit, pallet communications bus, pallet communications unit, zone controller communication unit, zone controller control unit) 14. Pallet speed limit incorrect (roadside sensors, link, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 15. AHS command authority lost (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 16. Vehicle unlocks from pallet (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit, wheel lock actuators)		X X X X X X X
7	AHS lane to AHS lane change	1. AHS recommends lane change with adjacent lane too full (roadside sensors, link, zone controller control unit) 2. Pallet/obstacle in destination lane not detected (lateral sensors, pallet communications bus, pallet control unit) 3. Lane change recommendation not received (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 4. Lane change report not received (pallet control unit, pallet communications bus, pallet communications unit, zone controller communication unit, zone controller control unit)		X X X X
8	Driver perceives emergency situation that may not be detected by on-board or IS sensors	1. Driver activates panic button inappropriately (driver) 2. Driver warning fails (pallet control unit, pallet communications bus, pallet actuators) 3. Other pallets not alerted (pallet control unit, pallet communications bus, pallet communications unit) 4. Zone control does not contact driver after panic stop (zone controller personnel, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 5. Driver does not inform or misinforms zone control about nature of emergency (driver)	X	X X X X
9	Driver desires to exit prior to input destination	1. Driver's request not/improperly acted upon (pallet control unit, pallet communications bus, pallet communications unit, zone controller communication unit, zone controller control unit)	X	
10	Pallet arrives at destination	1. AHS control panel not replaced (driver, vehicle window, pallet AHSCP holder) 2. Wheel locks do not disengage (dock sensors, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit, wheel lock actuators)	X X	

C 3. MALFUNCTION TIMELINE

		3. Vehicle does not leave pallet (driver, vehicle systems) 4. Unloading dock not assigned (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit) 5. Pallet presence at unloading dock not sensed (dock sensors, zone controller control unit) 6. Vehicle remains on pallet but is not sensed there (pallet sensors, pallet control unit, pallet communications bus, pallet communications unit, zone controller communication unit, zone controller control unit) 7. Pallet not given new assignment after vehicle exits (zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)	X X X X	X
101	Sensors monitor condition of roadway and environment	1. Conditions warranting operational parameter modification not/improperly acted upon (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, pallet communications unit, pallet communications bus, pallet control unit)		X

C 4. MALFUNCTION TIMELINE

ID	ACTION	MALFUNCTION	S[5]	US[6]
1	Enter the highway on a normal entry ramp to manual lane	None defined		
2	Set AHS destination	1. AHS destination request fails (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 2. AHS accepts destination when no such destination exists (zone controller control unit)	X X	
3	Merge into mixed traffic lane	None defined		
4	Request AHS entry	1. AHS request for entry fails (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 2. Vehicle ID fails (vehicle control unit, vehicle communications unit, zone controller communication unit, zone controller control unit) 3. Vehicle status fails (vehicle internal sensors, vehicle communications bus, vehicle control unit, vehicle communications unit, zone controller communication unit, zone controller control unit) 4. Vehicle position check fails (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X X X X	
5	AHS entry authorized	1. Driver not aware of authorization (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver) 2. AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information (zone controller unit) 3. AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters (zone controller unit)	X	 X X
6	AHS entry denied	1. AHS denies entry to vehicle which has met all check-in requirements (zone controller) 2. Driver not aware of rejection (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver)	X	 X
7	Transition to automatic control	1. AHS request for transition fails (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 2. Transition complete but driver not aware of transition (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, driver) 3. Driver does not release steering wheel or get off pedals when AHS takes control even though he is aware of transfer (driver) 4. AHS fails to establish control of vehicle but signals driver that it has taken control (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, vehicle actuators) 5. AHS fails to establish control of vehicle (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit, vehicle actuators) 6. Zone controller unaware vehicle is under AHS control after AHS takes control (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X X X X	 X

C 1. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

		7. Zone controller believes vehicle is under AHS control when it is not (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X X
8	Lateral control - lane following	1. Marker (missing, damaged)		X
		2. Markers not detected (marker sensor, vehicle communications bus, vehicle control unit)		X
		3. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X
		4. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X
		5. Collision (headway sensor, lateral sensors, vehicle communications bus, vehicle control unit, vehicle actuators)		
		6. Loss of steering authority (vehicle control unit, vehicle communications bus, vehicle steering actuators)		X
		7. Vehicle control unit issues improper commands (vehicle control unit)		
		8. Incorrect external sensor information (lateral obstacle sensors, vehicle communications bus, vehicle control unit)		X
		9. Incorrect internal status information (steering actuator position sensor, lateral acceleration sensor, vehicle communications bus, vehicle control unit)		X X
		10. Flat tire		
		11. Vehicle structural or systems failure		X
		12. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X
		13. External AHS command prompted by incorrect position data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X X
		14. External AHS command prompted by incorrect vehicle health data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)		X
		15. AHS command authority lost (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X
9	Longitudinal control - throttle and brake	1. Loss of acceleration control (throttle actuator, vehicle communications bus, vehicle control system)		X
		2. Operation with out of tolerance roadway conditions (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle		X

C 1. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

		communications bus, vehicle control unit) 3. Operation with out of tolerance environmental conditions (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 4. Collision (headway sensor, lateral sensors, vehicle communications bus, vehicle control unit, vehicle actuators) 5. Loss of braking control (brake actuator, vehicle communications bus, vehicle control system) 6. Vehicle control unit issues improper commands (vehicle control unit) 7. Flat tire 8. Vehicle structural or systems failure 9. Incorrect external sensor information (headway sensor, lateral obstacle sensors, vehicle communications bus, vehicle control unit) 10. Incorrect internal status information (throttle actuator position sensor, brake actuator position sensor, longitudinal velocity sensor, vehicle communications bus, vehicle control unit) 11. Improper external AHS commands (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 12. External AHS command prompted by incorrect position data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 13. External AHS command prompted by incorrect vehicle health data (vehicle position sensor, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit) 14. Vehicle speed limit incorrect (roadside sensors, link, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 15. AHS command authority lost (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X X X X X X X X X X X
11	Mixed lane to mixed lane change	1. AHS recommends lane change with adjacent lane too full (roadside sensors, link, zone controller control unit) 2. Vehicle/obstacle in destination lane not detected (lateral sensors, vehicle communications bus, vehicle control unit) 3. Manual driven vehicle merges into subject vehicle - proximity crash. 4. Other vehicle merges too close ahead with too large a closing velocity 5. Other vehicle merges too close behind with too large a closing velocity		X X X X X
12	Driver perceives emergency situation that may not be detected by on-board or IS sensors	1. Driver activates panic button inappropriately (driver) 2. Driver warning fails (vehicle control unit, vehicle communications bus, vehicle actuators) 3. Other vehicles not alerted (vehicle control unit, vehicle communications bus, vehicle communications unit)	X	 X X

C 1. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

		4. Zone control does not contact driver after panic stop (zone controller personnel, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 5. Driver does not inform or misinforms zone control about nature of emergency (driver)		X X
13	Driver desires to exit prior to input destination	1. Driver's request not/improperly acted upon (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communication unit, zone controller control unit)	X	
14	Vehicle nears destination	1. Proximity to destination not recognized (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 2. No driver alert signal (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. No driver awareness test generated (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 4. No driver awareness test response (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 5. Improperly evaluated driver awareness test (vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit)	X X X X	X
15	Transition to manual control	1. No request signal for manual control (driver, vehicle control unit, vehicle communications bus, vehicle communications unit, zone controller communications unit, zone controller control unit) 2. AHS fails to release control to driver (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 3. Driver fails to take manual control (driver)	X X	X
16	Driver fails awareness test	1. Infrastructure wrongly releases control to driver (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit) 2. Infrastructure does not route vehicle to intervention area (zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X X
17	Merge into manual lane	None defined		
18	Exit roadway	None defined		
101	Sensors monitor condition of roadway	1. Conditions warranting operational parameter modification not/improperly acted upon (roadside sensors, link, zone controller personnel, zone controller control unit, zone controller communications unit, vehicle communications unit, vehicle communications bus, vehicle control unit)		X

C 1. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

APPENDIX D. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION		INFRASTRUCTURE										VEHICLE											
			PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		WIRE SENS		STEER ACT		THRTL ACT		AHS POWER	
			4.7	3.7	4.0	3.3	3.3	3.3	4.7	4.0	4.0	4.0	4.7	1.3	2.0	1.7	3.3	1.3	2.0	2.0	2.3	2.3	2.3	1.3	2.0	2.3
			WIRE		LINK ES-ZC		LINK RS-ZC		COMM		---------		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		VEHCL SYSTM	
			2.3	4.0	1.7	3.7	1.7	3.7	3.3	4.0			3.0	1.7	3.0	1.7	3.7	1.3	3.7	1.7	2.3	1.7	3.3	1.3	2.3	1.0
Set AHS destination	AHS destination not set	2.0											X			X										
Request AHS entry	Road capacity check fails	2.3					X	X	X		X															
	AHS accepts destination when no such destination exists	1.7							X																	
AHS entry authorized	AHS accepts and authorizes entry with missing, incomplete, or known incorrect check-in information	3.0							X																	
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters	3.0							X																	
AHS entry denied	Driver not aware of rejection	2.7							X	X	X		X	X	X	X									X	
Transition to automatic control	AHS request for transition fails	1.7							X	X	X		X	X	X	X									X	
	AHS fails to establish control of vehicle but signals driver that it has taken control	3.0							X	X				X	X	X										
	Zone controller unaware vehicle is under AHS control after AHS takes control	3.7							X	X				X	X	X										
	Zone controller believes vehicle is under AHS control when it is not	2.3							X	X				X	X	X									X	
76 Lateral control - lane following	Wire not functioning	4.0		X							X															
	Wire not detected	3.0													X	X			X						X	
	Operation with out of tolerance roadway conditions	3.3	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	3.3	X		X	X			X	X				X	X	X										
	Collision	3.7	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority	4.0													X	X					X			X	X	X
	Vehicle control unit issues improper commands	3.7														X										
	Incorrect external sensor information	3.0													X	X		X								
	Incorrect internal status information	2.3													X	X	X									
	Flat tire	2.3																						X		
	Vehicle structural or systems failure	3.0																								X
	Improper external AHS commands	3.3	X	X	X	X	X	X	X	X				X	X	X										

C 1. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

	AHS command authority lost	3.7							X	X	X			X	X	X					X	X	X		X	
Longitudinal control - throttle and brake	Loss of acceleration control	2.7													X	X							X		X	X
	Operation with out of tolerance roadway conditions	3.0	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	3.0	X		X	X			X	X				X	X	X										
	Collision	3.7	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control	3.7													X	X						X		X	X	X
	Vehicle control unit issues improper commands	3.0														X										
	Flat tire	2.0																						X		
	Vehicle structural or systems failure	3.0																								X
	Incorrect external sensor information	3.0													X	X		X							X	
	Incorrect internal status information	2.7													X	X	X								X	
	Improper external AHS commands	3.3	X	X	X	X	X	X	X	X				X	X	X										
	Vehicle speed limit incorrect	2.7	X		X	X	X	X	X	X	X			X	X	X										
	AHS command authority lost	3.7							X	X	X			X	X	X					X	X	X		X	
Transition lane to AHS lane change	AHS commands lane change with destination lane too full	3.0					X	X	X	X																
	Vehicle/obstacle in destination lane not detected	4.0													X	X		X							X	
	Manual driven vehicle merges into subject vehicle - proximity crash.	3.7											O													
	Other vehicle merges too close ahead with too large a closing velocity	3.3											O													
	Other vehicle merges too close behind with too large a closing velocity	3.3											O													
AHS lane to AHS lane change	AHS commands lane change with destination lane too full	3.0					X	X	X	X																
	Vehicle/obstacle in destination lane not detected	4.0													X	X		X							X	
	Lane change command not received	1.7							X	X				X	X	X										
	Lane change report not received	2.3							X	X				X	X	X										
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails	3.0											X		X	X						X			X	X
	Other vehicles not alerted	3.3							X	X	X		X	X	X	X									X	
	Sector control does not contact driver after panic stop	2.7	X						X	X	X			X	X	X										
	Driver does not inform or misinforms zone control about nature of emergency	3.0											X													
Vehicle nears destination	Improperly evaluated driver awareness test	3.3							X	X				X	X	X										
AHS lane to transition lane	AHS commands lane change with destination lane too full	3.0					X	X	X	X																

C 1. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

change																										
	Vehicle/obstacle in destination lane not detected	4.0													X	X		X								
	Manual driven vehicle merges into subject vehicle - proximity crash.	3.7											O													
	Other vehicle merges too close ahead with too large a closing velocity	3.3											O													
	Other vehicle merges too close behind with too large a closing velocity	3.7											O													
Transition to manual control	Driver fails to take manual control after AHS releases control	3.7											X													X
Driver fails awareness test	Infrastructure wrongly releases control to driver	3.7							X	X				X	X	X										
	Infrastructure does not route vehicle to intervention area	3.0							X	X	X			X	X	X					X				X	X
Sensors monitor condition of roadway and environment	Conditions warranting operational parameter modification not/improperly acted upon	3.3	X		X	X	X	X	X	X	X			X	X	X										

C 2B. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION		INFRASTRUCTURE										VEHICLE													
			PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		MARKER SENS		STEER ACT		THRTL ACT		AHS POWER	
			4.7	3.7	4.0	3.3	3.3	3.3	4.3	4.0	4.0	4.0	4.7	1.3	2.0	2.3	3.3	2.0	2.3	2.3	2.3	2.3	2.0	2.0	2.0	2.3
			MAG MARK		LINK ES-ZC		LINK RS-ZC		COMM		---------		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		VEHCL SYSTM	
			3.7	3.7	1.7	3.7	1.7	3.7	3.3	4.0			3.0	2.7	3.0	2.3	3.7	2.3	3.3	2.7	2.3	2.7	30.	2.0	2.3	2.0
AHS entry authorized	Road capacity check fails	2.3					X	X	X		X															
	AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information	2.3							X																	
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters	3.3							X																	
AHS entry denied	Driver not aware of rejection	2.7							X	X			X	X	X	X									X	
Transition to automatic control	AHS fails to establish control of vehicle but signals driver that it has taken control	3.0							X	X				X	X	X										
	Zone controller unaware vehicle is under AHS control after AHS takes control	3.7							X	X				X	X	X										
	Zone controller believes vehicle is under AHS control when it is not	2.7							X	X				X	X	X										
Merge into AHS lane as singleton	Gap in mainline traffic not formed	2.0					X	X	X	X	X			X	X	X									X	
	Vehicle/obstacle in destination lane not detected	4.0													X	X		X							X	
Form with a platoon	Current platoon leader will not relinquish lead	1.3													X	X		X				X	X			
	Platoon parameters improper	3.3					X	X	X	X	X			X	X	X		X								
Lateral control - lane following	Marker	2.3		X																						
	Markers not detected	3.3													X	X			X						X	
	Operation with out of tolerance roadway conditions	3.3	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	3.3	X		X	X			X	X				X	X	X										
	Collision	4.0	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority	4.0													X	X					X			X	X	X
	Vehicle control unit issues improper commands	3.3														X										
	Incorrect external sensor information	3.0													X	X		X								
	Incorrect internal status information	2.0													X	X	X									
	Flat tire	2.7																						X		
	Vehicle structural or systems failure	3.3																								X
	Improper external AHS commands	3.3	X	X	X	X	X	X	X	X				X	X	X										
	AHS command authority lost	4.0							X	X	X			X	X	X					X	X	X		X	
Longitudinal control - throttle and brakes	Loss of acceleration control	3.0													X	X							X		X	X
	Operation with out of tolerance roadway conditions	3.0	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	3.3	X		X	X			X	X				X	X	X										

C 2B. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

	Collision	4.0	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control	3.7													X	X						X		X	X	X
	Vehicle control unit issues improper commands	3.7														X										
	Flat tire	2.7																						X		
	Vehicle structural or systems failure	3.0																								X
	Incorrect external sensor information	3.0													X	X		X							X	
	Incorrect internal status information	3.0													X	X	X								X	
	Improper external AHS commands	4.0	X		X	X	X	X	X	X				X	X	X										
	Vehicle speed limit incorrect	2.7	X		X	X	X	X	X	X	X			X	X	X										
	Platoon position assignment unknown	3.7					X	X	X	X	X			X	X	X										
	AHS command authority lost	3.7							X	X	X			X	X	X					X	X	X		X	
AHS lane to AHS lane change - platoon	No lane change command	2.0					X	X	X	X	X			X	X	X										
	Gap in destination lane traffic not formed	2.7					X	X	X	X	X			X	X	X										
	Vehicle/obstacle in destination lane not detected	4.0													X	X		X							X	
	Vehicle/obstacle in destination lane detected by one or more platoon members	3.0					X	X	X	X					X	X		X								
	Platoon actions not coordinated	3.3					X	X	X	X	X			X	X	X									X	
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver activates panic button inappropriately	2.0											X													
	Driver warning fails	3.3											X		X	X						X			X	X
	Other vehicles not alerted	3.7							X	X	X		X	X	X	X									X	
	Zone control does not contact driver after panic stop	2.0	X						X	X	X			X	X	X										
	Driver does not inform or misinforms zone control about nature of emergency	2.3											X													
Driver desires to exit prior to input destination	Driver's request not/improperly acted upon	1.0							X	X	X		X	X	X	X										
Vehicle nears destination	Proximity to destination not recognized	2.0							X	X	X			X	X	X				X						
	No driver alert signal	2.0							X	X	X			X	X	X										
	No driver awareness test generated	2.0							X	X	X			X	X	X										
	No driver awareness test response	2.0							X	X	X		X	X	X	X										
	Improperly evaluated driver awareness test	3.3							X	X				X	X	X										
Vehicle deplatoons	Deplatoon command not received	2.0							X	X	X			X	X	X									X	

C 2B. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

	Vehicle unable to perform deplatoon manuever	2.7													X	X			X	X	X	X	X	X	X
Merge from AHS lane to exit ramp	Lane change command not received	2.0							X	X	X			X	X	X									
	AHS commands lane change with destination lane too full	2.7					X	X	X	X				X	X	X									
	Vehicle/obstacle in destination lane not detected	4.0													X	X		X							
Transition to manual control on exit ramp	No request signal for manual control	2.0											X												
	AHS fails to release control to driver	2.0							X	X				X	X	X					X	X	X			
	Driver fails to take manual control after AHS releases control	3.3											X												
Driver fails awareness test	Infrastructure wrongly releases control to driver	3.7							X	X				X	X	X									
	Infrastructure does not route vehicle to intervention area	2.3							X	X	X			X	X	X					X			X	X
Sensors monitor condition of roadway	Conditions warranting operational parameter modification not/improperly acted upon	3.0	X		X	X	X	X	X	X	X			X	X	X									

C 3. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION		INFRASTRUCTURE										VEHICLE (PALLET)															
			PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		MARKER SENS		STEER ACT		THRTL ACT		AHS POWER	
			4.7	3.7	4.0	3.3	3.3	3.3	4.3	4.0	4.0	4.0	4.7	1.0	2.0	1.7	2.7	1.3	2.0	2.0	2.0	2.3	2.0	1.0	2.0	1.7
			MAG MARK		LINK ES-ZC		LINK RS-ZC		COMM		DOCK SYSTM		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		PALLET SYSTM	
			3.7	3.7	1.7	3.7	1.7	3.7	3.7	4.0	4.3	1.0	2.3	1.7	2.7	1.7	3.7	1.7	3.3	1.3	1.7	1.7	2.7	1.0	2.0	1.0
Enter the pallet mate/demate facility and drive into a mating dock	Pallet presence recognized without pallet present	1.0							X	X		X														
Drive onto pallet and lock down	Wheel locks not adjusted to correct spacing	1.3							X	X	X	X		X	X	X										X
	Wheel locks not engaged properly	3.0																								X
Lateral control - lane following	Marker	3.0		X																						
	Markers not detected	3.3													X	X			X						X	
	Operation with out of tolerance roadway conditions	3.3	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	3.3	X		X	X			X	X				X	X	X										
	Collision	4.0	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority	4.0													X	X					X			X	X	X
	Pallet control unit issues improper commands	3.3														X										
	Incorrect external sensor information	3.0													X	X		X								
	Incorrect internal status information	2.7													X	X	X									
	Flat tire	2.0																						X		
	Pallet structural or systems failure	3.3																								X
	Improper external AHS commands	3.3	X	X	X	X	X	X	X	X				X	X	X										
	AHS command authority lost	3.7						X	X	X				X	X	X					X	X	X		X	
	Vehicle unlocks from pallet	4.0							X	X				X	X	X									X	X
Longitudinal control - throttle and brake	Loss of acceleration control	2.7													X	X							X		X	X
	Operation with out of tolerance roadway conditions	3.0	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	3.7	X		X	X			X	X				X	X	X										
	Collision	4.0	X	X	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control	3.3													X	X						X		X	X	X
	Pallet control unit issues improper commands	3.3														X										

C 3. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

	Flat tire	2.0																						X		
	Pallet structural or systems failure	3.0																								X
	Incorrect external sensor information	3.0													X	X		X								
	Incorrect internal status information	3.0													X	X	X									
	Improper external AHS commands	3.7	X		X	X	X	X	X	X				X	X	X										
	Pallet speed limit incorrect	2.7	X		X	X	X	X	X	X	X			X	X	X										
	AHS command authority lost	3.7							X	X	X			X	X	X					X	X	X		X	
	Vehicle unlocks from pallet	4.0							X	X				X	X	X									X	X
AHS lane to AHS lane change	AHS recommends lane change with adjacent lane too full	2.3					X	X	X	X				X	X	X										
	Pallet/obstacle in destination lane not detected	3.7													X	X		X							X	
	Lane change recommendation not received	1.7							X	X	X			X	X	X									X	
	Lane change report not received	2.3							X	X	X			X	X	X									X	
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails	3.7											X		X	X						X			X	X
	Other pallets not alerted	3.7											X	X	X	X									X	
	Zone control does not contact driver after panic stop	2.0	X																							
	Driver does not inform or misinforms zone control about nature of emergency	2.3											X													
Pallet arrives at destination	Vehicle remains on pallet but is not sensed there	2.7							X		X	X														
Sensors monitor condition of roadway and environment	Conditions warranting operational parameter modification not/improperly acted upon	3.3	X		X	X	X	X	X	X	X			X	X	X										

C 4. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION	INFRASTRUCTURE										VEHICLE													
		PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		MARKER SENS		STEER ACT		THRTL ACT		AHS POWER	
		5.0	4.4	4.0	3.3	3.3	3.7	4.3	4.0	4.0	4.0	5.0	1.3	2.0	1.7	3.3	1.7	2.3	2.3	2.3	2.3	2.0	1.3	2.0	2.3
		MAG MARK		LINK ES-ZC		LINK RS-ZC		COMM		---------		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		VEHCL SYSTM	
		3.7	3.7	1.7	3.7	1.7	3.7	3.3	3.3			3.0	2.0	3.3	2.3	3.7	2.0	3.7	2.0	2.7	2.0	3.3	1.7	2.3	1.7
AHS entry authorized	AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information							X																	
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters							X																	
AHS entry denied	Driver not aware of rejection							X	X			X	X	X	X									X	
Transition to automatic control	AHS fails to establish control of vehicle but signals driver that it has taken control							X	X				X	X	X										
	Zone controller unaware vehicle is under AHS control after AHS takes control							X	X				X	X	X										
	Zone controller believes vehicle is under AHS control when it is not							X	X				X	X	X										
Lateral control - lane following	Unresponsive marker		X																						
	Markers not detected													X	X			X						X	
	Operation with out of tolerance roadway conditions	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	X		X	X			X	X				X	X	X										
	Collision	X	X	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority													X	X					X			X	X	X
	Vehicle control unit issues improper commands														X										
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Flat tire																						X		
	Vehicle structural or systems failure																								X
	Improper external AHS commands	X	X	X	X	X	X	X	X				X	X	X										
	AHS command authority lost							X	X	X			X	X	X					X	X	X		X	
Longitudinal control - throttle and brake	Loss of acceleration control													X	X							X		X	X
	Operation with out of tolerance roadway conditions	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	X		X	X			X	X				X	X	X										
	Collision	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control													X	X						X		X	X	X
	Vehicle control unit issues improper commands														X										
	Flat tire																						X		
	Vehicle structural or systems failure																								X
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Improper external AHS commands	X		X	X	X	X	X	X				X	X	X										

C 4. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

	Vehicle speed limit incorrect		X		X	X	X	X	X	X	X			X	X	X									
	AHS command authority lost								X	X	X			X	X	X					X	X	X		X	
Mixed lane to mixed lane change	AHS recommends lane change with adjacent lane too full						X	X	X	X				X	X	X										
	Vehicle/obstacle in destination lane not detected														X	X		X							X	
	Manual driven vehicle merges into subject vehicle - proximity crash.												O													
	Other vehicle merges too close ahead with too large a closing velocity												O													
	Other vehicle merges too close behind with too large a closing velocity												O													
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails												X		X	X						X			X	X
	Other vehicles not alerted								X	X	X		X	X	X	X									X	
	Zone control does not contact driver after panic stop		X						X	X	X			X	X	X										
	Driver does not inform or misinforms zone control about nature of emergency												X													
Vehicle nears destination	Improperly evaluated driver awareness test								X	X				X	X	X										
Transition to manual control	Driver fails to take manual control after AHS releases control												X													
Driver fails awareness test	Infrastructure wrongly releases control to driver								X	X				X	X	X										
	Infrastructure does not route vehicle to intervention area								X	X	X			X	X	X					X				X	X
Sensors monitor condition of roadway	Conditions warranting operational parameter modification not/improperly acted upon		X		X	X	X	X	X	X	X			X	X	X										

APPENDIX E. POTENTIAL EQUIPMENT MALFUNCTION MANAGEMENT STRATEGIES

Scoring Instructions

The countermeasures described in this appendix are conceived to reduce the probability that a failure will occur. Safety is of primary concern with capacity convenience and cost being of secondary importance. Therefore, these countermeasures have been developed with providing maximum safety under the widest possible conditions in mind.

Score each countermeasure using the numeric rating scale below. All scores from participating team members will be averaged and included in the final report.

Safety

Affect on Safety	Score
Less Safe	-10
No Change	0
Sightly Safer	2
Safer	5
Much Safer	10

Capacity

Affect on Capacity	Score
Less Capacity	-2
No Change	0
More Capacity	2
Much More Capacity	4

Convenience

Affect on Convenience	Score
Less Convenient	-2
No Change	0
More Convenient	2
Much More Convenient	3

Cost

Affect on Cost	Score
Less Cost	3
No Change	0
More Cost	-3
Much More Cost	-6

The levels columns at the left of the table refer to the various levels of the fault trees in appendix A, where these equipment malfunctions are identified. Level A refers to the uppermost level of the subject fault tree page, with each letter level subordinate to the one preceding. The numbers in each column refer to the reference numbers on each fault tree page.

RSC 4. Operationally Oriented Malfunction Management Strategies

ACTION	MALFUNCTION	COUNTERMEASURE	SAF	CAP	CON	CST
AHS entry authorized	AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems	2	0	0	0
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems	2	0	0	0
AHS entry denied	Driver not aware of rejection	Driver training - don't release steering wheel and pedals without positive signal, could be reinforced by periodic tests provided by control unit during normal vehicle entry to AHS	5	0	0	-3
		D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead in transition lane D/I - Alarm sounds to remind driver to assume manual control	5	0	1	-3
Transition to automatic control	AHS fails to establish control of vehicle but signals driver that it has taken control	D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead D/I - Alarm sounds to alert driver to assume manual control	10	0	0	-3
	Zone controller unaware vehicle is under AHS control after AHS takes control	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control adds vehicle to database	2	0	0	0
	Zone controller believes vehicle is under AHS control when it is not	D - Zone control issues command to vehicle and vehicle does not respond D/I - Zone control rechecks vehicle information, if it finds the error the AHS removes track of vehicle from database, if no error is found the zone controller contacts driver to verify vehicle is under manual control, once verified the AHS removes track of vehicle from database	2	2	0	0
Lateral control - lane following	Unresponsive marker	D - Vehicle sensor looses track of road centerline D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the road centerline and is stopping in assigned lane, zone control verifies that other vehicles are experiencing this problem and determines that markers are missing or malfunctioning, lane reverts to manual control driving, zone control releases affected vehicles to manual mode. Response team dispatched to replace/repair markers.	10	-2	2	-3
	Markers not detected	D - Vehicle sensor looses track of road centerline D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the road centerline and is stopping in assigned lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control verifies that other vehicles are not having this problem and determines that the subject vehicle has lost its ability to detect the markers, zone control personnel contact driver for human input, release vehicle control to driver and allow driver to resume full manual control	10	-2	2	-3

Other Malfunctions N.1.1

Other Malfunctions
Normal mode of operation -
These areas monitor the operation of the baseline AHS. In the zone control station, the human personnel serve this function, while in the vehicle this function is served both by the driver and specific vehicle status sensors.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Other Malfunctions					
	1						External Personnel Fault	Background checks, drug screening	4	0	0	-3
		2					Performs Required Task Inadequately	Training and personnel aides (e.g., checklists, computer aided expert system/fuzzy logic)	5	0	0	-2
								Multiple personnel assigned to same duties	6	0	0	-6
		3					Interferes with System Operation	Control system architecture designed to require more than one authorization for changes that significantly impact system operation	5	0	0	-5
	4						Vehicle Status System Fault					
		5					Fail to Detect Vehicle System Fault	Enhanced built-in-test equipment	5	0	2	-3
								Driver input allowed and encouraged	4	0	1	0
								Sensor cross-checks (i.e. infer fault by its effect on vehicle operation or other systems)	4	0	1	-2
		6					Detect Fault in Properly Operating System	Driver input allowed and encouraged	1	0	1	0
								Sensor cross-checks (i.e. infer lack of fault by its lack of effect on vehicle operation or other systems)	2	0	1	-3
	7						Driver					
		8					Performs Required Task Inadequately	Training, with possibly on-line simulations to keep knowledge current	7	0	0	-3
								System designed to prompt driver for input when required	5	0	2	-2
								System designed to failsafe (i.e., go to a more restrictive state in the absence of proper driver inputs)	4	0	1	-2

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
		9					Interferes with System Operation	Driver cannot take control of vehicle while it is under AHS control. Most driver can do is request a panic stop and even this is accomplished by the AHS under AHS control.	6	0	0	-2

Communications Fault Between Vehicle and Roadway N.1.2

Communications Fault Between Vehicle and Roadway
Normal mode of operation -
Establish and maintain a data and voice communications path between the vehicle and the infrastructure

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Communications Fault Between the Vehicle and Roadway					
	1						Communications Garbled	Select a communications mode and protocol with a high resistance to interference, including error checking in the messages	10	0	0	-2
		2					Incorrect Data Passed	Error checking in the message	8	0	0	-1
			3				Constant Incorrect Data Passed	Multiple links	8	0	0	-3
			4				Variable Incorrect Data Passed	Error checking in the messages	8	0	0	-1
		5					No Data Passed	Multiple links	8	0	0	-3
		6					Data Rate Reduced	Error checking in the messages	8	0	0	-1
								Multiple links	8	0	0	-3
	7						Communication Blocked	Multiple links	8	0	0	-3

Lateral Control 1.2.1

Centerline wire tracking sensor
Normal mode of operation -

1. The vehicle maintains track of its lateral position and velocity by reference to a wire burried under the center of the AHS lane.
2. The wire provides an active signal to the vehicle for tracking.
3. The vehicle uses the active signal to track the wire and determine its position along the length of the wire.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Loss of Centerline Tracking	Report to Zone Control	6	0	0	-1
	1						Wire Sensor to Control Unit Link Fault	Multiple Links and a Method to Select the Correct Signal	4	0	0	-3
		2					Incorrect Signal	Multiple Links and a Method to Select the Correct Signal	5	0	0	-3
								Error Correction Incorporated Into Signal	4	0	0	-2
			3				Constant Incorrect Signal	Multiple Links and a Method to Select the Correct Signal	5	0	0	-3
								Error Correction Incorporated Into Signal	4	0	0	-2
			4				Variable Incorrect Signal	Multiple Links and a Method to Select the Correct Signal	5	0	0	-3
								Error Correction Incorporated Into Signal	4	0	0	-2
		5					Loss of Signal	Multiple Links	5	0	0	-3
	6						Wire Sensor Fault	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
		7					Internal Fault	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
			8				Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
				9			Constant Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
				10			Variable Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4

Lateral Control 1.2.1

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
			11				Loss of Signal	Multiple Sensors	7	0	0	-4
		12					Physical Damage	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
								Armor Sensor	6	0	0	-3
		13					Power Loss	Multiple Power Supplies	8	0	0	-4
	14						Wire Signal Fault					
		15					Wire Signal Incorrect	Error Correction Incorporated Into Signal	4	0	0	-2
			16				Incorrect Signal	Error Correction Incorporated Into Signal	4	0	0	-2
				17			Constant Incorrect Signal	Error Correction Incorporated Into Signal	4	0	0	-2
				18			Variable Incorrect Signal	Error Correction Incorporated Into Signal	4	0	0	-2
			19				Loss of Signal	Multiple Wires	8	0	0	-6
		20					Wire Missing	Multiple Wires	8	0	0	-6
		21					Power Loss	Multiple Power Supplies	8	0	0	-4

Lateral Control 1.2.1

Lateral Control 2.2.1, 3.2.1, 4.2.1

Loss of Centerline Marker Tracking
Normal mode of operation -

1. The vehicle maintains track of its lateral position and velocity by reference to a series of magnetic markers buried under the center of the AHS lane.
2. Marker detectors on the vehicles pick up the magnetic information from the markers for tracking purposes.
3. The vehicle uses the markers to track the lane centerline and determine its position on the roadway.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Loss of Centerline Tracking	Report to Zone Control	5	0	0	0
	1						Marker Sensor to Control Unit Link Fault	Multiple Links and a Method to Select the Correct Signal	5	0	0	-3
		2					Incorrect Signal	Multiple Links and a Method to Select the Correct Signal	5	0	0	-3
								Error Correction Incorporated Into Signal	4	0	0	-2
			3				Constant Incorrect Signal	Multiple Links and a Method to Select the Correct Signal	5	0	0	-3
								Error Correction Incorporated Into Signal	4	0	0	-2
			4				Variable Incorrect Signal	Multiple Links and a Method to Select the Correct Signal	5	0	0	-3
								Error Correction Incorporated Into Signal	4	0	0	-2
		5					Loss of Signal	Multiple Links	5	0	0	-3
	6						Marker Sensor Fault	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
		7					Internal Fault	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
			8				Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
				9			Constant Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4

Lateral Control 2.2.1, 3.2.1, 4.2.1

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
				10			Variable Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
			11				Loss of Signal	Multiple Sensors	7	0	0	-4
		12					Physical Damage	Multiple Sensors and a Method to Select the Correct Sensor	8	0	0	-4
								Armor Sensor	5	0	0	-3
			13				Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
				14			Constant Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
				15			Variable Incorrect Signal	Multiple Sensors and a Method to Select the Correct Sensor	7	0	0	-4
			16				Loss of Signal	Multiple Sensors	7	0	0	-4
		17					Power Loss	Multiple Power Supplies	7	0	0	-4
	18						Marker Signal Fault					
		19					Marker Signal Incorrect	Error Correction Incorporated Into Signal	5	0	0	-1
			20				Incorrect Signal	Error Correction Incorporated Into Signal	5	0	0	-1
				21			Constant Incorrect Signal	Error Correction Incorporated Into Signal	5	0	0	-1
				22			Variable Incorrect Signal	Error Correction Incorporated Into Signal	5	0	0	-1
			23				Loss of Signal	Multiple Markers	6	0	0	-6
		24					Marker Missing	Multiple Markers	6	0	0	-6

Lateral Control N.2.2

Continued Operation with Factors Beyond Tolerances
Normal mode of operation -
1. Roadway sensors monitor conditions (rain, fog, debris on road, traffic congestion, etc.) and report to Zone Control.
2. Zone Control automatically adjusts speed limit, gap spacing, and other factors to suit current conditions on roadway, including shutting down road when conditions warrant.
3. Personnel in Zone Control can override the automatic functions of 2 above at their discretion.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Continued Operation with Factors Beyond Tolerances					
	1						Continued Operation with Roadway Conditions Beyond Tolerances	Allow driver to discontinue operation of his AHS vehicle	2	0	0	0
		2					Roadway Condition Unknown	Solicit feedback from vehicle occupants	3	0	0	-1
			3				Link to Zone Controller Fault	High reliability links	4	0	0	-2
								Error correction in link data transmission	4	0	0	-1
								Multiple links	6	0	0	-3
			4				Sensor Fault	High reliability sensors	6	0	0	-2
								Multiple sensors	6	0	0	-4
		5					Roadway Condition Improperly Acted Upon					
			6				Zone Control Control Unit Fault	High reliability control unit	6	0	0	-4
								Multiple control units	10	0	0	-5
			7				Zone Control Personnel Fault	Training and personnel aides (e.g., checklists)	5	0	0	-3
								Multiple personnel assign to same duties	8	0	0	-5
	8						Continued Operation with Environmental Conditions Beyond Tolerances	Allow driver to discontinue operation of his AHS vehicle	3	0	0	0
		9					Environmental Conditions Unknown	Solicit feedback from vehicle occupants	3	0	0	-1

Lateral Control N.2.2

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
			10				Link to Zone Controller Fault	High reliability links	4	0	0	-2
								Error correction in link data transmission	4	0	0	-1
								Multiple links	6	0	0	-3
			11				Sensor Fault	High reliability sensors	6	0	0	-2
								Multiple sensors	6	0	0	-4
		12					Environmental Conditions Improperly Acted Upon					
			13				Zone Control Control Unit Fault	High reliability control unit	7	0	0	-3
								Multiple control units	10	0	0	-5
			14				Zone Control Personnel Fault	Training and personnel aides (e.g., checklists)	5	0	0	-3
								Multiple personnel assign to same duties	8	0	0	-5
	15						Continued Operation with Vehicle Condition Beyond Tolerances	Allow driver to discontinue operation of his AHS vehicle	2	0	0	-1
		16					Vehicle Condition Unknown	Solicit feedback from vehicle occupants	3	0	2	-2
			17				Link to Control Unit Fault	High reliability links	4	0	0	-2
								Error correction in link data transmission	4	0	0	-1
								Multiple links	6	0	0	-3
			18				Vehicle Condition Sensor Fault	High reliability sensors	8	0	0	-4
								Multiple sensors	8	0	0	-5
		19					Vehicle Control Unit Improperly Evaluates Vehicle Condition	High reliability control unit	3	0	0	-2
								Multiple control units	6	0	0	-4

Lateral Control N.2.2

Lateral Control N.2.3

Steering

Normal mode of operation

1. A signal is sent to the steering actuator commanding front wheel angular orientation based on maneuver requirements.
2. The steering actuator positions the wheels at the commanded angular orientation.
3. Items 1 and 2 are continually repeated throughout the automated portion of the trip.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Loss of Steering Authority	Alert Zone Control to warn other nearby vehicles	6	0	0	-1
	1						Steering Actuator Fault	Backup Actuator	8	0	1	-4
		2					Physical Damage	Better Protect Actuator (Armor, guards, etc.)	4	0	0	-2
								Backup Actuator	8	0	1	-4
			3				Incorrect Action Taken					
				4			Constant Incorrect Action Taken					
					5		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	5	0	0	-2
					6		Locked in Position	Design actuator so that it cannot lock in a position	7	0	0	0
								Multiple actuators with ability to disconnect each from system	8	0	0	-4
					7		Free	Backup Actuator	8	0	1	-4
				8			Variable Incorrect Action Taken					
			9				No Action Taken (Steering actuator does not respond to control system inputs)	Backup Actuator	8	0	1	-4
		10					Power Loss	Alternative Power Source	8	0	0	-4
		11					Internal Fault	High Reliability	4	0	0	-2

Lateral Control N.2.3

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
								Backup Actuator	8	0	1	-4
			12				Incorrect Action Taken					
				13			Constant Incorrect Action Taken					
					14		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	5	0	0	-2
					15		Locked in Position	Design actuator so that it cannot lock in a position	7	0	0	0
								Multiple actuators with ability to disconnect each from system	8	0	0	-4
					16		Free	Backup Actuator	8	0	1	-4
				17			Variable Incorrect Action Taken					
			18				No Action Taken (Steering actuator does not respond to control system inputs)	Backup Actuator	8	0	1	-4
	19						Steering Actuator to Control Unit Link Fault	Backup or Dual links	8	0	1	-3
		20					Interference on Link	Dual links, both must agree to make steering change	7	0	0	-3
			21				Incorrect Command Received	Error checking incorporated into steering position command signal	4	0	0	-1
				22			Constant Incorrect Command Received					
					23		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit				
					24		Locked in Position	Stop in AHS lane, alert zone control, await assistance	4	-2	0	-2
				25			Variable Incorrect Command Received					
			26				No Command Received	Backup or Dual links	8	0	1	-4

Lateral Control N.2.3

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
		27					Broken Link	Backup or Dual links	8	0	1	-4

Lateral Control N.2.3

Lateral Control N.2.4

Control System
Normal mode of operation -

1. The control system determines the desired direction of vehicle travel
2. The control system accepts inputs from the Zone Controller and from vehicle sensors that influence its determination concerning the desired direction of vehicle travel at a particular time.
3. The control system commands the steering actuator to match actual to desired direction of vehicle travel.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Control System Failure	Backup or Multiple Control Units	10	0	1	-4
	1						Internal Fault	High Reliability	7	0	0	-2
								Backup or Multiple Control Units	10	0	1	-4
		2					Partial Failure	Backup or Multiple Control Units	10	0	1	-4
			3				Incorrect commands Issued					
				4			Constant Incorrect Command Issued					
					5		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	3	0	0	-1
					6		Locked in Position(command sent to keep steering actuator in a single position)	Backup or Multiple Control Units	10	0	1	-4
				7			Variable Incorrect Command Issued	Backup or Multiple Control Units	10	0	1	-4
			8				No Commands Issued	Backup or Multiple Control Units	10	0	1	-4
		9					Complete Failure	Backup or Multiple Control Units	10	0	1	-4
	10						Power Loss	Backup or Dual Power Source	7	0	0	-4

Lateral Control N.2.3

Lateral Control N.2.5

Communications
Normal mode of operation -
1. Communication unit passes messages to/from vehicle to other vehicles or Zone Controller.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Communications Fault					
	1						Communications Unit to Control Unit Link Fault	Multiple Links	5	0	0	-3
		2					Communications Garbled	Select a communications mode and protocol with a high resistance to interference, including error checking in the messages	5	0	0	-1
			3				Incorrect Data Passed	Error checking in the messages	4	0	0	-1
				4			Constant Incorrect Data Passed	Multiple Links	5	0	0	-3
				5			Variable Incorrect Data Passed	Error checking in the messages	4	0	0	-1
			6				No Data Passed	Multiple Links	5	0	0	-3
			7				Data Rate Reduced	Error checking in the messages	4	0	0	-1
								Multiple Links	4	0	0	-3
		8					Communications Loss	Multiple Links	5	0	0	-3
	9						Power Loss	Multiple Power Sources	7	0	1	-4
	10						Internal Fault	Multiple Communications Units	8	0	1	-4
		11					Communications Garbled	Select a communications mode and protocol with a high resistance to interference, including error checking in the messages	5	0	0	-1
			12				Incorrect Data Passed	Error checking in the messages	4	0	0	-1

Lateral Control N.2.5

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
				13			Constant Incorrect Data Passed	Multiple Communications Units	8	0	1	-4
				14			Variable Incorrect Data Passed	Error checking in the messages	4	0	0	-1
			15				No Data Passed	Multiple Communications Units	8	0	1	-4
			16				Data Rate Reduced	Error checking in the messages	3	0	0	-1
								Multiple Links	3	0	0	-2
		17					Communications Loss	Multiple Communications Units	8	0	1	-4

Lateral Control N.2.5

Lateral Control N.2.7

Vehicle Systems
Normal mode of operation -
1. Systems required for normal vehicle operation

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Vehicle Failure	Report to Zone Control	5	0	0	0
	1						Flat Tire	Run Flat Tires	5	0	2	-4
								Maintain/Recover longitudinal and lateral control, move to breakdown lane	3	0	0	-1
								Improve reliability via periodic inspections to eliminate bad tires	2	0	-2	-1
	2						Vehicle Structural Failure	Improve reliability via periodic inspections to eliminate vehicles likely to suffer structural failures	6	0	-2	-3
	3						Loss of Propulsion	Move to breakdown lane	3	0	0	0

Lateral Control N.2.8

Lateral Object Sensor
Normal mode of operation -

1. Lateral object sensors scan to sides of vehicle to determine target bearing, range, and range rate.
2. Information is provided to control system.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Lateral Object Sensor Fault					
	1						Lateral Object Sensor to Control Unit Link Fault	Backup or Multiple Links	5	0	0	-3
		2					Information Incorrect					
			3				Constant Incorrect Information Provided					
			4				Variable Information Provided	Backup or Multiple Links	5	0	0	-3
		5					Information Unavailable	Backup or Multiple Links	5	0	0	-3
	6						Power Loss	Backup or Dual Power Supplies	7	0	0	-4
	7						Internal Fault	Backup or Dual Sensors	8	0	0	-4
		8					Information Incorrect					
			9				Constant Incorrect Information Provided					
			10				Variable Incorrect Information Provided	Backup or Dual Sensors	6	0	0	-4
		11					Information Unavailable	Backup or Dual Sensors	6	0	0	-4

Lateral Control N.2.5

Longitudinal Control N.2.9

Digital throttle position actuator.
Normal mode of operation -

1. The control system desires to have the vehicle moving at a particular speed,
2. Throttle position vs. speed under standard conditions (level road, no wind, etc.) is known by the control system,
3. The control system commands throttle position and looks for feedback that it was attained,
4. The control system compares actual vehicle speed to desired vehicle speed,
5. The control system commands the throttle position actuator is to increase or decrease its position by n steps,
6. Repeat 4 and 5 until actual vehicle speed matches desired vehicle speed.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Loss of Acceleration Control	Alert Zone Control to warn other nearby vehicles	3	0	0	0
	1						Throttle Actuator Fault	Backup Actuator	6	0	1	-3
		2					Physical Damage	Better Protect Actuator (Armor, guards, etc.)	3	0	0	-1
								Backup Actuator	6	0	1	-3
			3				Incorrect Action Taken					
				4			Constant Incorrect Action Taken					
					5		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	3	0	0	-1
					6		Locked Partial or Full On	If speed is too high - modulate brakes to control speed. move to breakdown lane and shut off engine	4	0	0	-2
								If speed is too low - move to breakdown lane and leave AHS at next exit	2	0	0	-2
					7		Locked Full Off	Move to breakdown lane and leave at next exit	2	0	0	-2
				8			Variable Incorrect Action Taken	Move to breakdown lane and shut off engine, modulate brakes if necessary to control excess speed	3	0	0	-2

Longitudinal Control N.2.9

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
			9				No Action Taken (Throttle actuator does not respond to control system inputs)	Backup Actuator	6	0	1	-3
		10					Power Loss	Alternative Power Source	6	0	1	-4
		11					Internal Fault	High Reliability	5	0	0	-3
								Backup Actuator	6	0	1	-3
			12				Incorrect Action Taken					
				13			Constant Incorrect Action Taken					
					14		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	3	0	0	-1
					15		Locked Partial or Full On	If speed is too high - modulate brakes to control speed, move to breakdown lane and shut off engine	4	0	0	-2
								If speed is too low - move to breakdown lane and leave AHS at next exit	2	0	0	-2
					16		Locked Full Off	Move to breakdown lane and leave at next exit	2	0	0	-2
				17			Variable Incorrect Action Taken	Move to breakdown lane and shut off engine, modulate brakes if necessary to control excess speed	3	0	0	-2
			18				No Action Taken	Backup Actuator	6	0	1	-3
	19						Throttle Actuator to Control Unit Link Fault	Backup or Dual links	4	0	0	-2
		20					Interference on Link	Dual links, both must agree to make throttle change	4	0	0	-2
			21				Incorrect Command Received	Error checking incorporated into throttle position command signal	4	0	0	-1
				22			Constant Incorrect Command Received					

Longitudinal Control N.2.9

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
					23		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	3	0	0	-1
					24		Locked Partial or Full On	If speed is too high - modulate brakes to control speed, move to breakdown lane and shut off engine	4	0	0	-2
								If speed is too low - move to breakdown lane and leave AHS at next exit	2	0	0	-2
					25		Locked Full Off	Move to breakdown lane and leave at next exit	2	0	0	-2
				26			Variable Incorrect Command Received	Error checking incorporated into throttle position command signal	4	0	0	-1
								Move to breakdown lane and shut off engine, modulate brakes if necessary to control excess speed	3	0	0	-2
			27				No Command Received	Backup or Dual links	4	0	0	-2
		28					Broken Link	Backup or Dual links	4	0	0	-2
	29						Throttle Position Feedback Incorrect					
		30					Constant Incorrect Feedback					
			31				Wrong Gain					
			32				Sensor Locked Into Place					
		33					Variable Incorrect Feedback					

Longitudinal Control N.2.9

Longitudinal Control N.2.10

Continued Operation with Factors Beyond Tolerances
Normal mode of operation -

1. Roadway sensors monitor conditions (rain, fog, debris on road, traffic congestion, etc.) and report to Zone Control.
2. Zone Control automatically adjusts speed limit, gap spacing, and other factors to suit current conditions on roadway, including shutting down road when conditions warrant.
3. Personnel in Zone Control can override the automatic functions of 2 above at their discretion.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Continued Operation with Factors Beyond Tolerances					
	1						Continued Operation with Roadway Conditions Beyond Tolerances	Allow driver to discontinue operation	2	0	0	0
		2					Roadway Condition Unknown	Solicit feedback from vehicle occupants	3	0	0	-1
			3				Link to Zone Controller Fault	High reliability links	4	0	0	-2
								Error correction in link data transmission	4	0	0	-1
								Multiple links	6	0	0	-3
			4				Sensor Fault	High reliability sensors	6	0	0	-2
								Multiple sensors	6	0	0	-4
		5					Roadway Condition Improperly Acted Upon					
			6				Zone Control Control Unit Fault	High reliability control unit	4	0	0	-3
								Multiple control units	6	0	0	-4
			7				Zone Control Personnel Fault	Training and personnel aides (e.g., checklists)	4	0	0	-1
								Multiple personnel assign to same duties	7	0	1	-4

Longitudinal Control N.2.9

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
	8						Continued Operation with Environmental Conditions Beyond Tolerances	Allow driver to discontinue operation	2	0	0	0
		9					Environmental Conditions Unknown	Solicit feedback from vehicle occupants	3	0	0	-1
			10				Link to Zone Controller Fault	High reliability links	4	0	0	-2
								Error correction in link data transmission	4	0	0	-1
								Multiple links	6	0	0	-3
			11				Sensor Fault	High reliability sensors	6	0	0	-2
								Multiple sensors	6	0	0	-4
		12					Environmental Conditions Improperly Acted Upon					
			13				Zone Control Control Unit Fault	High reliability control unit	4	0	0	-3
								Multiple control units	6	0	0	-4
			14				Zone Control Personnel Fault	Training and personnel aides (e.g., checklists)	4	0	0	-1
								Multiple personnel assign to same duties	7	0	1	-4
	15						Continued Operation with Vehicle Condition Beyond Tolerances	Allow driver to discontinue operation	2	0	0	0
		16					Vehicle Condition Unknown	Solicit feedback from vehicle occupants	3	0	0	-1
			17				Link to Control Unit Fault	High reliability links	4	0	0	-2
								Error correction in link data transmission	4	0	0	-1
								Multiple links	6	0	0	-3
			18				Vehicle Condition Sensor Fault	High reliability sensors	6	0	0	-2
								Multiple sensors	6	0	0	-4

Longitudinal Control N.2.9

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
		19					Vehicle Control Unit Improperly Evaluates Vehicle Condition	High reliability control unit	4	0	0	-3
								Multiple control units	6	0	0	-4

Longitudinal Control N.2.9

Longitudinal Control N.2.11

Digital brake position actuator.
Normal mode of operation, stopping or slowing vehicle -

1. The control system desires to stop the vehicle at a particular rate,
2. Brake actuator position vs. braking rate under standard conditions (level road, no wind, etc.) is known by the control system,
3. The control system commands brake actuator position and looks for feedback that it was attained,
4. The control system compares actual rate of vehicle speed decrease to desired rate of vehicle speed decrease,
5. The control system commands the brake position actuator to increase or decrease its position by n steps,
6. Repeat 4 and 5 until the actual rate of vehicle speed decrease matches the desired rate of vehicle speed decrease.

Normal mode of operation, controlling vehicle speed on downgrades -

1. The control system desires to have the vehicle moving at a particular speed,
2. Throttle position is commanded at idle and speed is still greater than desired,
3. The control system commands brake actuator position and looks for feedback that it was attained,
4. The control system compares actual vehicle speed to desired vehicle speed,
5. The control system commands the brake position actuator to increase or decrease its position by n steps,
6. Repeat 4 and 5 until actual vehicle speed matches desired vehicle speed.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Loss of Braking Control	Alert Zone Control to warn other nearby vehicles	3	0	0	0
	1						Brake Actuator Fault	Backup Actuator	7	0	1	-3
		2					Physical Damage	Better Protect Actuator (Armor, guards, etc.)	4	0	0	-2
								Backup Actuator	7	0	1	-3
			3				Incorrect Action Taken					
				4			Constant Incorrect Action Taken					
					5		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	2	0	0	0

Longitudinal Control N.2.11

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
					6		Locked Partial or Full On	Move to breakdown lane and stop (if sufficient power is available)	4	0	0	-1
					7		Locked Full Off	Move to breakdown lane and shut off engine, modulate throttle if necessary to control excess speed	4	0	0	-1
				8			Variable Incorrect Action Taken	Move to breakdown lane and shut off engine, modulate throttle if necessary to control excess speed	4	0	0	-1
			9				No Action Taken (Brake actuator does not respond to control system inputs)	Backup Actuator	7	0	1	-3
		10					Power Loss	Alternative Power Source	6	0	1	-3
		11					Internal Fault	High Reliability	4	0	0	-2
								Backup Actuator	7	0	0	-4
			12				Incorrect Action Taken					
				13			Constant Incorrect Action Taken					
					14		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	2	0	0	0
					15		Locked Partial or Full On	Move to breakdown lane and stop (if sufficient power is available)	4	0	0	-1
					16		Locked Full Off	Move to breakdown lane and leave at next exit	4	0	0	-1
				17			Variable Incorrect Action Taken	Move to breakdown lane and shut off engine, modulate throttle if necessary to control excess speed	4	0	0	-1
			18				No Action Taken	Backup Actuator	7	0	1	-3
	19						Brake Actuator to Control Unit Link Fault	Backup or Dual links	6	0	0	-3
		20					Interference on Link	Dual links, both must agree to make brake change	5	0	0	-3

Longitudinal Control N.2.11

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
			21				Incorrect Command Received	Error checking incorporated into brake position command signal	6	0	0	-1
				22			Constant Incorrect Command Received					
					23		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	2	0	0	0
					24		Locked Partial or Full On	Move to breakdown lane and stop (if sufficient power is available)	4	0	0	-1
					25		Locked Full Off	Move to breakdown lane and shut off engine, modulate throttle if necessary to control excess speed	4	0	0	-1
				26			Variable Incorrect Command Received	Error checking incorporated into brake position command signal	4	0	0	-1
								Move to breakdown lane and shut off engine, modulate throttle if necessary to control excess speed	7	0	1	-3
			27				No Command Received	Backup or Dual links	6	0	0	-3
		28					Broken Link	Backup or Dual links	5	0	0	-3

Longitudinal Control N.2.11

Longitudinal Control N.2.12

Control System, Longitudinal Control
Normal mode of operation -

1. The control system determines the desired speed and rate of change of speed of the vehicle.
2. The control system accepts inputs from the Zone Controller and from vehicle sensors that influence its determination concerning the desired vehicle speed at a particular time.
3. The control system commands the throttle and brake actuators to match actual to desired speed or rate of change of speed.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Control System Failure	Backup or Multiple Control Units	10	0	1	-4
	1						Internal Fault	High Reliability	7	0	0	-2
								Backup or Multiple Control Units	10	0	1	-4
		2					Partial Failure	Backup or Multiple Control Units	10	0	1	-4
			3				Incorrect commands Issued					
				4			Constant Incorrect Command Issued					
					5		Wrong Gain	Identify wrong gain, calculate gain correction, apply gain correction in control unit	3	0	0	-1
					6		Lock Partial or Full On	Move to breakdown lane and stop, modulate other longitudinal actuator to control speed if necessary	10	0	1	-4
					7		Lock Full Off	Move to breakdown lane and stop, modulate other longitudinal actuator to control speed if necessary	10	0	1	-4
				8			Variable Incorrect Command Issued	Move to breakdown lane and stop, modulate other longitudinal actuator to control speed if necessary	10	0	1	-4
			9				No Commands Issued	Backup or Multiple Control Units	10	0	1	-4
		10					Complete Failure	Backup or Multiple Control Units	10	0	1	-4
	11						Power Loss	Backup or Dual Power Source	7	0	0	-4

Longitudinal Control N.2.11

Longitudinal Control N.2.13

Vehicle Systems
Normal mode of operation -
1. Systems required for normal vehicle operation, not associated with AHS

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Vehicle Failure	Report to Zone Control	5	0	0	0
	1						Flat Tire	Run Flat Tires	5	0	2	-4
								Maintain/Recover longitudinal and lateral control, move to breakdown lane	3	0	0	-1
								Improve reliability via periodic inspections to eliminate bad tires	2	0	-2	-1
	2						Vehicle Structural Failure	Improve reliability via periodic inspections to eliminate vehicles likely to suffer structural failures	6	0	-2	-3
	3						Loss of Propulsion	Move to breakdown lane	3	0	0	0

Longitudinal Control N.2.14

Longitudinal Velocity Sensor
Normal mode of operation -
1. Velocity sensor is same one that drives the speedometer.
2. Velocity sensor provides information about vehicle speed to control system.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Longitudinal Velocity Sensor Fault					
	1						Longitudinal Velocity Sensor to Control Unit Link Fault	Backup or Dual Links	4	0	0	-3
								Use Redundant Information (derive speed from time between markers, or rate of change of position)	3	0	0	-1
		2					Velocity Information Incorrect					
			3				Constant Incorrect Velocity Information					
				4			Wrong Gain	Identify failed link, identify wrong gain, calculate gain correction apply gain correction in control unit	2	0	0	0
				5			Constant Signal	Identify failed link, ignore failed sensor	2	0	0	0
				6			Offset	Identify failed link, identify offset, calculate offset correction, apply offset correction in control unit	2	0	0	0
			7				Variable Incorrect Velocity Information	Backup or Dual Links	4	0	1	-3
		8					Velocity Information Unavailable	Backup or Dual Links	4	0	1	-3
	9						Power Loss	Backup or Dual Power Supplies	7	0	1	-4
	10						Internal Fault	Backup or Dual Sensors	6	0	1	-3
								Use Redundant Information (derive speed from time between markers, or rate of change of position)	6	0	1	-1
		11					Velocity Information Incorrect					

Longitudinal Control N.2.14

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
			12				Constant Incorrect Velocity Information					
				13			Wrong Gain	Identify failed sensor, identify wrong gain, calculate gain correction apply gain correction in control unit	2	0	0	0
				14			Constant Signal	Identify failed sensor, ignore failed sensor	2	0	0	0
				15			Offset	Identify failed sensor, identify offset, calculate offset correction, apply offset correction in control unit	2	0	0	0
			16				Variable Incorrect Velocity Information	Backup or Dual Sensors	4	0	1	-3
		17					Velocity Information Unavailable	Backup or Dual Sensors	4	0	1	-3

Longitudinal Control N.2.15

Communications
Normal mode of operation -
1. Communication unit passes messages to/from vehicle to other vehicles or Zone Controller.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Communications Fault					
	1						Communications Unit to Control Unit Link Fault	Multiple Links	5	0	0	-3
		2					Communications Garbled	Select a communications mode and protocol with a high resistance to interference, including error checking in the messages	5	0	0	-1
			3				Incorrect Data Passed	Error checking in the messages	4	0	0	-1
				4			Constant Incorrect Data Passed	Multiple Links	5	0	0	-3
				5			Variable Incorrect Data Passed	Error checking in the messages	4	0	0	-1
			6				No Data Passed	Multiple Links	5	0	0	-3
			7				Data Rate Reduced	Error checking in the messages	4	0	0	-1
								Multiple Links	4	0	0	-3
		8					Communications Loss	Multiple Links	5	0	0	-3
	9						Power Loss	Multiple Power Sources	7	0	1	-4
	10						Internal Fault	Multiple Communications Units	8	0	1	-4
		11					Communications Garbled	Select a communications mode and protocol with a high resistance to interference, including error checking in the messages	5	0	0	-1
			12				Incorrect Data Passed	Error checking in the messages	4	0	0	-1

Longitudinal Control N.2.15

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
				13			Constant Incorrect Data Passed	Multiple Communications Units	8	0	1	-4
				14			Variable Incorrect Data Passed	Error checking in the messages	4	0	0	-1
			15				No Data Passed	Multiple Communications Units	8	0	1	-4
			16				Data Rate Reduced	Error checking in the messages	3	0	0	-1
								Multiple Links	3	0	0	-2
		17					Communications Loss	Multiple Communications Units	8	0	1	-4

Longitudinal Control N.2.15

Longitudinal Control N.2.16

Gap Sensor
Normal mode of operation -

1. Gap sensor provides target tag (e.g., target 1, target 2, etc.), target range, and target bearing (information frequently updated) to control unit for targets ahead of vehicle.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Gap Sensor Signal Fault	Alert Zone Control	5	0	0	-1
	1						Gap Sensor Fault					
		2					Physical Damage	Multiple Sensors - need to identify incorrect information	7	0	1	-4
								Armor Sensors	4	0	0	-2
								Excess Initial Capacity	3	0	0	-2
			3				Incorrect Information Provided	Multiple Sensors - need to identify incorrect information	7	0	1	-4
				4			Constant Incorrect Information					
				5			Variable Incorrect Information					
			6				Unit Broken	Multiple Sensors - need to identify incorrect information	7	0	1	-4
		7					Power Loss	Multiple Power Sources	7	0	1	-4
		8					Internal Fault	Multiple Sensors - need to identify incorrect information	7	0	1	-4
								Excess Initial Capacity	3	0	0	-2
			9				Incorrect Information Provided	Multiple Sensors - need to identify incorrect information	7	0	1	-4
				10			Constant Incorrect Information					
				11			Variable Incorrect Information					

Longitudinal Control N.2.16

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
			12				Unit Broken	Multiple Sensors - need to identify incorrect information	7	0	1	-4
	13						Gap Sensor to Control Unit Link Fault					
		14					Interference on Link	Multiple Links - need to identify incorrect information	5	0	0	-3
								Better Isolation of the link from interference	2	0	0	-1
			15				Incorrect Information Received	Multiple Links - need to identify incorrect information	5	0	0	-3
				16			Constant Incorrect Information Received					
				17			Variable Incorrect Information Received					
			18				No Information Received	Multiple Links - need to identify incorrect information	5	0	0	-3
		19					Broken Link	Multiple Links - need to identify incorrect information	5	0	0	-3

Longitudinal Control N.2.16

Roadway Coordination N.2.17

Loss of Roadway Sensors
Normal mode of operation -
1. Roadway sensors monitor conditions (rain, fog, debris on road, traffic congestion, etc.) and report to Zone Control.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Loss of Roadway Sensors	Report to Zone Control	5	0	0	-1
	1						Roadway Sensor Fault					
		2					Internal Fault	High reliability design/construction	4	0	0	-2
								Multiple or backup sensors	6	0	1	-4
			3				Sensor Information Incorrect	High reliability design/construction	4	0	0	-2
								Multiple or backup sensors	6	0	1	-4
								Error detection built-in test in sensor	4	0	0	-2
				4			Constant Incorrect Information Provided	Multiple or backup sensors	6	0	1	-4
								Recalibrate sensor using redundent information if available	4	0	0	-1
								Use redundent information provided by other sensors if available	5	0	0	-1
								Operate w/o information	-8	0	0	0
				5			Variable Incorrect Information Provided	Multiple or backup sensors	6	0	1	-4
								Use redundent information provided by other sensors if available	5	0	0	-1
								Operate w/o information	-8	0	0	0
								Filter information to extract useable information if possible	2	0	0	-2

Roadway Coordination N.2.17

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
			6				Sensor Information Unavailable	Multiple or backup sensors	6	0	1	-4
								Use redundent information provided by other sensors if available	5	0	0	-1
								Operate w/o information	-8	0	0	0
		7					Power Loss	High reliability design/construction	4	0	0	-2
								Multiple or backup power source	6	0	1	-4
	8						Sensor to Control Unit Link Fault	High reliability design/construction	4	0	0	-2
								Multiple or backup links	6	0	1	-4
								Error correction provided in data stream	3	0	0	-1
		9					Communications Garbled					
			10				Information Incorrect					
				11			Constant Incorrect Information Provided	High reliability design/construction	4	0	0	-2
								Multiple or backup links	6	0	1	-4
								Error correction provided in data stream	3	0	0	-1
				12			Variable Incorrect Information Provided	Multiple or backup links	6	0	1	-4
								Error correction provided in data stream	3	0	0	-1
								Operate w/o information	-8	0	0	0
								Filter information to extract useable information if possible	2	0	0	-2
			13				Information Unavailable	Multiple or backup links	6	0	1	-4
								Use redundent information provided by other sensors if available	5	0	0	-1

Roadway Coordination N.2.17

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
								Operate w/o information	-8	0	0	0
		14					Communications Loss	Multiple or backup links	6	0	1	-4
								Use redundent information provided by other sensors if available	5	0	0	-1
								Operate w/o information	-8	0	0	0

Roadway Coordination N.2.18

Loss of Zone Controller
Normal mode of operation -

1. Zone controller receives information from roadway sensors and vehicles and sends messages to coordinate vehicle movements and positions.

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
0							Loss of Zone Controller	If communication is lost between the vehicle and zone controller, the vehicle will send a message to nearby vehicles inquiring whether they still have communication, if the answer is yes, the vehicle will coordinate with nearby vehicles to attain the breakdown lane as soon as practical, if the answer is no, the vehicle will automatically brake to a halt in the AHS lane along with all other AHS vehicles	8	1	0	-3
	1						Control Unit Fault					
		2					Partial Failure					
			3				Incorrect Commands Issued					
				4			Constant Incorrect Command Issued	High reliability unit	4	0	0	-2
								Multiple control units	8	0	1	-4
								Error detection built-in test	4	0	0	-1
				5			Variable Incorrect Command Issued	High reliability unit	4	0	0	-2
								Multiple control units	8	0	1	-4
								Error detection built-in test	4	0	0	-1
			6				No Commands Issued	Require a command to be issued periodically to make sure that the zone control to vehicle control communications path is operational. This command should be of a nature that requires some computation on the part of the zone controller	3	0	0	0

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
		7					Complete Failure	High reliability unit	4	0	0	-2
								Multiple control units	8	0	1	-4
	8						Power Loss	Multiple power sources with failure detection on each	8	1	1	-4
	9						Communications Unit to Control Unit Link Fault					
		10					Communications Garbled					
			11				Incorrect Data Passed					
				12			Constant Incorrect Data Passed	High reliability link	4	0	0	-2
								Multiple links	8	0	1	-4
								Error detection and correction in message	4	0	0	-1
				13			Variable Incorrect Data Passed	High reliability link	4	0	0	-2
								Multiple links	8	0	1	-4
								Error detection and correction in message	4	0	0	-1
			14				No Data Passed	High reliability link	4	0	0	-2
								Multiple links	8	0	1	-4
			15				Data Rate Reduced	Operate in a mode that can accept the reduced data rate	2	0	0	-1
		16					Communications Loss	High reliability link	4	0	0	-2
								Multiple links	8	0	1	-4
	17						Zone Communications Unit Fault					
		18					Communications Garbled					
			19				Incorrect Data Passed					

LEVEL							FAILURE	COUNTERMEASURE	SAF	CAP	CON	CST
A	B	C	D	E	F	G						
				20			Constant Incorrect Data Passed	High reliability unit	4	0	0	-2
								Multiple control units	8	0	1	-4
								Error detection built-in test	4	0	0	-1
				21			Variable Incorrect Data Passed	High reliability unit	4	0	0	-2
								Multiple control units	8	0	1	-4
								Error detection built-in test	4	0	0	-1
			22				No Data Passed	High reliability unit	4	0	0	-2
								Multiple units	8	0	1	-4
			23				Data Rate Reduced	Operate in a mode that can accept the reduced data rate	2	0	0	-1
		24					Communications Loss	High reliability unit	4	0	0	-2
								Multiple units	8	0	1	-4

Scoring Instructions

The countermeasures described in this appendix are conceived to reduce the consequences of a failure, given that the failure has already occurred. Safety is of primary concern with capacity convenience and cost being of secondary importance. Therefore, these countermeasures have been developed with providing maximum safety under the widest possible conditions in mind.

The countermeasures are described as two parts. The first part is labeled D - , and describes how the AHS can detect the failure. The second part of the countermeasure is labeled D/I - , and describes the decision and implementation of a course of action to reduce the severity of the consequences of the failure.

Score each countermeasure using the numeric rating scale below. All scores from participating team members will be averaged and included in the final report.

Safety

Affect on Safety	Score
Less Safe	-10
No Change	0
Slightly Safer	2
Safer	5
Much Safer	10

Capacity

Affect on Capacity	Score
Less Capacity	-2
No Change	0
More Capacity	2
Much More Capacity	4

Convenience

Affect on Convenience	Score
Less Convenient	-2
No Change	0
More Convenient	2
Much More Convenient	3

Cost

Affect on Cost	Score
Less Cost	3
No Change	0
More Cost	-3
Much More Cost	-6

APPENDIX F. POTENTIAL OPERATIONAL MALFUNCTION MANAGEMENT STRATEGIES

ACTION	MALFUNCTION	COUNTERMEASURE	SAF	CAP	CON	CST
Set AHS destination	AHS destination not set	D - Periodic recheck of destination reveals no destination set D/I - Zone control asks driver to set destination, if driver sets destination zone control verifies destination exists and allows vehicle to continue, if driver does not set destination, zone control starts check out procedure, if driver refuses to participate in check out procedure, zone control moves vehicle to shoulder and stops vehicle to await authorities				
Request AHS entry	Road capacity check fails	D- Driver sees that AHS lane is full after AHS has accepted vehicle for entry, or driver sees that AHS is open after AHS has rejected vehicle because lane is full D/I - Driver contacts zone control to ask for capacity recheck, zone control rechecks road capacity and reissues command to vehicle, driver can abort attempt to enter AHS				
	AHS accepts destination when no such destination exists	D - Periodic recheck of destination reveals mistake D/I - Zone control asks driver to set destination, if driver sets destination zone control verifies destination exists and allows vehicle to continue, if driver does not set destination, zone control starts check out procedure, if driver refuses to participate in check out procedure, zone control moves vehicle to shoulder and stops vehicle to await authorities				
AHS entry authorized	AHS accepts and authorizes entry with missing, incomplete, or known incorrect check-in information	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems				
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems				
AHS entry denied	Driver not aware of rejection	Driver training - don't release steering wheel and pedals without positive signal, could be reinforced by periodic tests provided by control unit during normal vehicle entry to AHS				
		D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead in transition lane D/I - Alarm sounds to remind driver to assume manual control				
Transition to automatic control	AHS request for transition fails	D - Driver pushes button to request AHS take control but no signal responds, wheel and pedals remain under manual control D/I - Driver makes another request, after several failures the vehicle control unit informs driver that some failure has occurred and advises he seek vehicle maintenance				
	AHS fails to establish control of vehicle but signals driver that it has taken control	D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead in transition lane D/I - Alarm sounds to alert driver to assume manual control				
	Zone controller unaware vehicle is under AHS control after AHS takes control	D - Driver notices that vehicle remains in transition lane too long with control functions unavailable to driver D/I - Driver informs zone control, zone control releases vehicle to manual control, driver can initiate request to come back under AHS control or remain in manual mode				
	Zone controller believes vehicle is under AHS control when it is not	D - Zone control issues command to transition to AHS lane and vehicle does not respond D/I - Zone control rechecks vehicle information, if it finds the error the AHS removes track of vehicle from database, if no error is found the zone controller contacts driver to verify vehicle is under manual control, once verified the AHS removes track of vehicle from database				
Lateral control - lane following	Wire not functioning	D - Vehicle sensor looses track of wire position D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the wire and is stopping in AHS lane, zone control verifies that wire is not functioning, AHS lane reverts to manual control driving, zone control releases affected vehicles to manual mode				
	Wire not detected	D - Vehicle sensor looses track of wire position D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the wire and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control verifies that wire is functioning and personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				

RSC 1. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

Collision	D - Vehicle status sensors indicate collision has occurred D/I - Vehicle attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other vehicles as appropriate - Zone control personnel contact driver and request human input, response team dispatched if required, otherwise vehicle moves to shoulder under automated or manual control to await authorities				
Loss of steering authority	D - Vehicle moves away from wire without AHS command D/I - If condition exceeds set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has lost steering authority and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched				
Vehicle control unit issues improper commands	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
	D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
Incorrect external sensor information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
	D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
Incorrect internal status information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
	D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
Flat tire	D - Vehicle status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clears a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane and act as though loss of steering authority has occurred				
Vehicle structural or systems failure	D - Vehicle status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has suffered unknown failure and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched				
Improper external AHS commands	D - Vehicle control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a merge into the AHS lane to the left where there is no such lane) D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
	D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
AHS command authority lost	D - Vehicle looses contact with zone control, or vehicle does not properly respond to zone control commands D/I - Vehicle comes to a stop in the assigned lane at normal AHS braking rate. Vehicle contacts other vehicles to determine if contact with zone control has been lost by them also. If other vehicles have also lost contact, all vehicles revert to manual control after a set period of time. If other vehicles still have contact, relay is set up through another vehicle in contact and zone control moves subject vehicle to a safe state. Order of preference: under				

RSC 1. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		manual control in manual lane, stopped on shoulder. Zone control personnel take action as appropriate.				
Longitudinal control - throttle and brake	Loss of acceleration control	D - Vehicle speed does not equal set speed in absence of acceleration commands D/I - If vehicle is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if vehicle is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; allow to manually drive along shoulder to next exit				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				
	Collision	D - Vehicle status sensors indicate collision has occurred D/I - Vehicle attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other vehicles as appropriate - Zone control personnel contact driver and request human input, response team dispatched if required, otherwise vehicle moves to shoulder under automated or manual control to await authorities				
	Loss of braking control	D - Vehicle speed does not equal set speed in absence of acceleration commands D/I - If vehicle is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if vehicle is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; allowed to manually drive along shoulder to next exit				
	Vehicle control unit issues improper commands	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Flat tire	D - Vehicle status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane and act as though loss of steering authority has occurred				
	Vehicle structural or systems failure	D - Vehicle status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has suffered unknown failure and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane or shoulder, driver instructed to manually move to transition lane and resume full manual control or move to shoulder, if driver cannot steer, emergency response team is dispatched				
	Incorrect external sensor information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect internal status information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Improper external AHS commands	D - Vehicle control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a faster speed even though there is a vehicle under AHS control ahead at set gap) D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button.				

RSC 1. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Vehicle speed limit incorrect	D - Driver detects that his unconstrained AHS vehicle is traveling at a different speed than other unconstrained AHS vehicles (unconstrained means that the vehicle is free to travel at the set speed limit, i.e., not following behind another AHS vehicle at the set gap) D/I - Driver alerts zone control personnel, zone control verbally verify set speed limit with driver, if different than reading on speedometer zone control places vehicle in a safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. If stopped on shoulder or in AHS lane, zone control takes action as necessary. Zone control checks other vehicles for set speed limit.				
		D - Roadway sensors detect unconstrained AHS vehicle traveling at other than speed limit D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate. Zone control checks other vehicles for set speed limit.				
	AHS command authority lost	D - Vehicle looses contact with zone control, or vehicle does not properly respond to zone control commands D/I - Vehicle comes to a stop in the assigned lane at normal AHS braking rate. Vehicle contacts other vehicles to determine if contact with zone control has been lost by them also. If other vehicles have also lost contact, all vehicles revert to manual control after a set period of time. If other vehicles still have contact, relay is set up through another vehicle in contact and zone control moves subject vehicle to a safe state. Order of preference: under manual control in manual lane, stopped on shoulder. Zone control personnel take action as appropriate.				
Transition lane to AHS lane change	AHS commands lane change with destination lane too full	D - Vehicle lateral sensors show vehicles in destination lane and insufficient gap to merge safely D/I - Vehicle does not make merge. Vehicle alerts zone control to problem. Zone control unit and/or personnel try to determine why lane change command was given with destination lane too full. Zone control takes action as appropriate.				
	Vehicle/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane.				
		D - Driver alerts zone control that there is a vehicle in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies vehicle in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the vehicle can proceed. Otherwise, zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects vehicle in destination lane, driver hits panic button D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Manual driven vehicle merges into subject vehicle - proximity crash.	D - Lateral sensors detect target vehicle merging into subject vehicle D/I - Most of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention (sound horn, flash lights). Probably does not warrant special attention drawing devices because this should be a very infrequent occurrence as manually driven vehicles are not allowed in the AHS lane.				
	Other vehicle merges too close ahead with too large a closing velocity	D - Gap sensor detects target vehicle merging ahead of subject vehicle D/I - If the target vehicle is moving more slowly than the subject vehicle, the subject vehicle will brake. However, if the distance target vehicle is detected is too close and the closing velocity too great, a collision will occur. Most of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention (sound horn, flash lights). Probably does not warrant special attention drawing devices because this should be a very infrequent occurrence as manually driven vehicles are not allowed in the AHS lane.				
	Other vehicle merges too close behind with too large a closing velocity	D - If detection occurs at all it is from the driver of the subject vehicle or possibly roadway sensors. D/I - If the target vehicle is moving more rapidly than the subject vehicle, the subject vehicle will accelerate if it does not violate the gap parameters. However, if the distance target vehicle is detected is too close and the closing velocity too great, a collision will occur. Many of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention (sound horn, flash lights). Probably does not warrant special attention drawing devices because this should be a very infrequent occurrence as manually driven vehicles are not allowed in the AHS lane.				
AHS lane to AHS lane change	AHS commands lane change with destination lane too full	D - Vehicle lateral sensors show vehicles in destination lane and insufficient gap to merge safely D/I - Vehicle does not make merge. Vehicle alerts zone control to problem. Zone control unit and/or personnel try to determine why lane change command was given with destination lane too full. Zone control takes action as appropriate.				

RSC 1. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

	Vehicle/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane.				
		D - Driver alerts zone control that there is a vehicle in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies vehicle in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the vehicle can proceed. Otherwise, zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects vehicle in destination lane, driver hits panic button D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Lane change command not received					
	Lane change report not received					
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the vehicle's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial vehicle's warning. These vehicle's panic stop would be dealt with in the same way as the initial vehicle's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Other vehicles not alerted	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the vehicle's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial vehicle's warning. These vehicle's panic stop would be dealt with in the same way as the initial vehicle's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Sector control does not contact driver after panic stop	D - Driver does not hear from zone control after a panic stop. D/I - Driver can call zone control directly. If vehicle cannot directly reach zone control, a relay through another vehicle can be tried. If vehicle communications is totally out, zone control can contact a nearby affected vehicle and ask their view of the situation.				
Vehicle nears destination	Driver does not inform or misinforms zone control about nature of emergency Improperly evaluated driver awareness test	D - Driver's conversation with zone control relayed to nearby vehicles that are affected by the emergency stop. D/I - Other drivers hear the misinformation passed and break in to inform the zone control of the right information. Any such emergency stop made in on an urban AHS is likely to involve multiple vehicles, thus the truth should be able to substantially outvote any misinformation. D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
AHS lane to transition lane change	AHS commands lane change with destination lane too full	D - Vehicle lateral sensors show vehicles in destination lane and insufficient gap to merge safely D/I - Vehicle does not make merge. Vehicle alerts zone control to problem. Zone control unit and/or personnel try to determine why lane change command was given with destination lane too full. Zone control takes action as appropriate.				
	Vehicle/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane.				
		D - Driver alerts zone control that there is a vehicle in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies vehicle in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the vehicle can proceed. Otherwise, zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects vehicle in destination lane, driver hits panic button D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared				

RSC 1. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Manual driven vehicle merges into subject vehicle - proximity crash.	D - Lateral sensors detect target vehicle merging into subject vehicle D/I - Most of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention (sound horn, flash lights). Probably does not warrant special attention drawing devices because this should be a very infrequent occurrence as manually driven vehicles are not allowed in the AHS lane.				
	Other vehicle merges too close ahead with too large a closing velocity	D - Gap sensor detects target vehicle merging ahead of subject vehicle D/I - If the target vehicle is moving more slowly than the subject vehicle, the subject vehicle will brake. However, if the distance target vehicle is detected is too close and the closing velocity too great, a collision will occur. Most of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention (sound horn, flash lights). Probably does not warrant special attention drawing devices because this should be a very infrequent occurrence as manually driven vehicles are not allowed in the AHS lane.				
	Other vehicle merges too close behind with too large a closing velocity	D - If detection occurs at all it is from the driver of the subject vehicle or possibly roadway sensors. D/I - If the target vehicle is moving more rapidly than the subject vehicle, the subject vehicle will accelerate if it does not violate the gap parameters. However, if the distance target vehicle is detected is too close and the closing velocity too great, a collision will occur. Many of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention (sound horn, flash lights). Probably does not warrant special attention drawing devices because this should be a very infrequent occurrence as manually driven vehicles are not allowed in the AHS lane.				
Transition to manual control	Driver fails to take manual control after AHS releases control	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
Driver fails awareness test	Infrastructure wrongly releases control to driver	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
	Infrastructure does not route vehicle to intervention area	D - None required for this countermeasure D/I - Construct exit ramp such that unless the driver takes positive action to avoid it, the vehicle will land in an area that has a barrier net to stop the vehicle and a disturbance sensor on the net to alert the zone control that this incident has occurred.				
Sensors monitor condition of roadway and environment	Conditions warranting operational parameter modification not/improperly acted upon	D - Driver notices that roadway and/or environmental conditions appear to warrant change in operational parameters (e.g., speed limit, following distance, etc.) D/I - Driver contacts zone control to indicate belief that conditions appear to warrant change in operational parameters, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				

RSC 2B. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

ACTION	MALFUNCTION	COUNTERMEASURE	SAF	CAP	CON	CST
AHS entry authorized	Road capacity check fails	D- Driver sees that AHS lane is full after AHS has accepted vehicle for entry, or driver sees that AHS is open after AHS has rejected vehicle because lane is full D/I - Driver contacts zone control to ask for capacity recheck, zone control rechecks road capacity and reissues command to vehicle, driver can abort attempt to enter AHS				
	AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems				
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems				
AHS entry denied	Driver not aware of rejection	Driver training - don't release steering wheel and pedals without positive signal, could be reinforced by periodic tests provided by control unit during normal vehicle entry to AHS				
		D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead in transition lane D/I - Alarm sounds to remind driver to assume manual control				
Transition to automatic control	AHS fails to establish control of vehicle but signals driver that it has taken control	D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead in transition lane D/I - Alarm sounds to alert driver to assume manual control				
	Zone controller unaware vehicle is under AHS control after AHS takes control	D - Driver notices that vehicle remains in transition lane too long with control functions unavailable to driver D/I - Driver informs zone control, zone control releases vehicle to manual control, driver can initiate request to come back under AHS control or remain in manual mode				
	Zone controller believes vehicle is under AHS control when it is not	D - Zone control issues command to transition to AHS lane and vehicle does not respond D/I - Zone control rechecks vehicle information, if it finds the error the AHS removes track of vehicle from database, if no error is found the zone controller contacts driver to verify vehicle is under manual control, once verified the AHS removes track of vehicle from database				
Merge into AHS lane as singleton	Gap in mainline traffic not formed	D - Vehicle's lateral sensors detect vehicle(s) in destination lane D/I - Vehicle detecting target will not change lanes. Zone control notified of problem.				
	Vehicle/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane.				
		D - Driver alerts zone control that there is a vehicle in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies vehicle in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the vehicle can proceed. Otherwise, zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects vehicle in destination lane, driver hits panic button D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
Form with a platoon	Current platoon leader will not relinquish lead	D -				
	Platoon parameters improper					
Lateral control - lane following	Marker	D - Vehicle sensor looses track of road centerline D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the road centerline and is stopping in AHS lane, zone control verifies that other vehicles are experiencing this problen and determines that markers are missing or malfunctioning, AHS lane reverts to manual control driving, zone control releases affected vehicles to manual mode. Response team dispatched to replace/repair markers.				
	Markers not detected	D - Vehicle sensor looses track of road centerline D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the road centerline and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control verifies that other vehicles are not having this problem and				

RSC 2B. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		determines that the subject vehicle has lost its ability to detect the markers, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				
	Collision	D - Vehicle status sensors indicate collision has occurred D/I - Vehicle attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other vehicles as appropriate - Zone control personnel contact driver and request human input, response team dispatched if required, otherwise vehicle moves to shoulder under automated or manual control to await authorities				
	Loss of steering authority	D - Vehicle moves away from markers without AHS command D/I - If condition exceeds set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has lost steering authority and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched				
	Vehicle control unit issues improper commands	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect external sensor information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect internal status information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Flat tire	D - Vehicle status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clears a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane and act as though loss of steering authority has occurred				
	Vehicle structural or systems failure	D - Vehicle status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has suffered unknown failure and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched				
	Improper external AHS commands	D - Vehicle control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a merge into the AHS lane to the left where there is no such lane) D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS				

RSC 2B. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	AHS command authority lost	D - Vehicle looses contact with zone control, or vehicle does not properly respond to zone control commands D/I - Vehicle comes to a stop in the assigned lane at normal AHS braking rate. Vehicle contacts other vehicles to determine if contact with zone control has been lost by them also. If other vehicles have also lost contact, all vehicles revert to manual control after a set period of time. If other vehicles still have contact, relay is set up through another vehicle in contact and zone control moves subject vehicle to a safe state. Order of preference: under manual control in manual lane, stopped on shoulder. Zone control personnel take action as appropriate.				
Longitudinal control - throttle and brakes	Loss of acceleration control	D - Vehicle speed does not equal set speed in absence of acceleration commands D/I - If vehicle is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if vehicle is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; allow to manually drive along shoulder to next exit				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				
	Collision	D - Vehicle status sensors indicate collision has occurred D/I - Vehicle attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other vehicles as appropriate - Zone control personnel contact driver and request human input, response team dispatched if required, otherwise vehicle moves to shoulder under automated or manual control to await authorities				
	Loss of braking control	D - Vehicle speed does not equal set speed in absence of acceleration commands D/I - If vehicle is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if vehicle is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; allowed to manually drive along shoulder to next exit				
	Vehicle control unit issues improper commands	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Flat tire	D - Vehicle status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane and act as though loss of steering authority has occurred				
	Vehicle structural or systems failure	D - Vehicle status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has suffered unknown failure and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane or shoulder, driver instructed to manually move to transition lane and resume full manual control or move to shoulder, if driver cannot steer, emergency response team is dispatched				
	Incorrect external sensor information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect internal status information	D - Roadway sensors detect that vehicle is not following proper course				

RSC 2B. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Improper external AHS commands	D - Vehicle control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a faster speed even though there is a vehicle under AHS control ahead at set gap) D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Vehicle speed limit incorrect	D - Driver detects that his unconstrained AHS vehicle is traveling at a different speed than other unconstrained AHS vehicles (unconstrained means that the vehicle is free to travel at the set speed limit, i.e., not following behind another AHS vehicle at the set gap) D/I - Driver alerts zone control personnel, zone control verbally verify set speed limit with driver, if different than reading on speedometer zone control places vehicle in a safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. If stopped on shoulder or in AHS lane, zone control takes action as necessary. Zone control checks other vehicles for set speed limit.				
		D - Roadway sensors detect unconstrained AHS vehicle traveling at other than speed limit D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate. Zone control checks other vehicles for set speed limit.				
	Platoon position assignment unknown	D - Zone control notices a single vehicle traveling without trying to join a platoon (without a platoon position assignment, head or tail, vehicle does not know whether to accelerate and join platoon ahead or decelerate and join platoon behind) D/I - Zone control retransmits platoon position assignement, if no response zone control personnel contact driver to evaluate situation and take appropriate action				
	AHS command authority lost	D - Vehicle looses contact with zone control, or vehicle does not properly respond to zone control commands D/I - Vehicle comes to a stop in the assigned lane at normal AHS braking rate. Vehicle contacts other vehicles to determine if contact with zone control has been lost by them also. If other vehicles have also lost contact, all vehicles revert to manual control after a set period of time. If other vehicles still have contact, relay is set up through another vehicle in contact and zone control moves subject vehicle to a safe state. Order of preference: under manual control in manual lane, stopped on shoulder. Zone control personnel take action as appropriate.				
AHS lane to AHS lane change - platoon	No lane change command	D - Zone control expecting a lane change and no such action is forthcomming D/I - Zone control reissues lane change command, if no response zone control will try to ascertain and correct the problem or at least identify and isolate the offending vehicle.				
	Gap in destination lane traffic not formed	D - One or more vehicle's lateral sensors in lane changing platoon detect vehicle(s) in destination lane D/I - Vehicle detecting target will not change lanes and will contact others in platoon to prevent their changing of lanes. This will occur before any vehicles move to change lanes.				
	Vehicle/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Vehicle control system seeks to stabilize vehicle tracking on centerline and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane.				
		D - Driver alerts zone control that there is a vehicle in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies vehicle in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the vehicle can proceed. Otherwise, zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects vehicle in destination lane, driver hits panic button D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				

RSC 2B. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

	Vehicle/obstacle in destination lane detected by one or more platoon members	D - One or more vehicle's lateral sensors in lane changing platoon detect vehicle(s) in destination lane D/I - Vehicle detecting target will not change lanes and will contact others in platoon to prevent their changing of lanes. This will occur before any vehicles move to change lanes.				
	Platoon actions not coordinated	D - One or more vehicle(s) actions do not fit in with the actions of the rest of the platoon members. Detection method depends on actions taken (e.g., vehicle trying to change lanes out of the middle of a platoon could be detected by the other platoon members and/or the roadway sensors). D/I - Once a vehicle has formed as part of a platoon, the control laws should be written so cannot take an independent action without agreement from the other platoon members. However, if a malfunction occurs that causes a vehicle to act without the agreement of other platoon members, the action of other platoon members would depend on the action of the subject vehicle. For example, a vehicle that was leaving the platoon would be allowed to do so and a vehicle that moved forward to bump the vehicle ahead (in the absense of a pertubation) would be deplatooned as soon as possible. The common thread with any of these malfunctions is that the zone control would be alerted and could take appropriate actions.				
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver activates panic button inappropriately	D - Appropriateness of panic button activation is determined by the zone control personnel who contact the driver after an activation to discuss the reason for the activation D/I - Depending how inappropriate the panic button activation was, the vehicle will be moved from the AHS, the driver will be fined, the driver's AHS privlidges will be suspended/revoked, possible jail time for repeat inappropriate activations or inappropriate activations that cause property damage or injury				
	Driver warning fails	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the vehicle's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial vehicle's warning. These vehicle's panic stop would be dealt with in the same way as the initial vehicle's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Other vehicles not alerted	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the vehicle's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial vehicle's warning. These vehicle's panic stop would be dealt with in the same way as the initial vehicle's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Zone control does not contact driver after panic stop	D - Driver does not hear from zone control after a panic stop. D/I - Driver can call zone control directly. If vehicle cannot directly reach zone control, a relay through another vehicle can be tried. If vehicle communications is totally out, zone control can contact a nearby affected vehicle and ask their view of the situation.				
	Driver does not inform or misinforms zone control about nature of emergency	D - Driver's conversation with zone control relayed to nearby vehicles that are affected by the emergency stop. D/I - Other drivers hear the misinformation passed and break in to inform the zone control of the right information. Any such emergency stop made in on an urban AHS is likely to involve multiple vehicles, thus the truth should be able to substantially outvote any misinformation.				
Driver desires to exit prior to input destination	Driver's request not/improperly acted upon					
Vehicle nears destination	Proximity to destination not recognized	D - Driver notices that he is nearing exit but there is no indication from the AHS at the time that the driver is acustomed to receiving an alert D/I - Driver requests to be let off AHS at the next exit (push of a button rather than voice communication with zone control)				
		D - Driver notices that he is nearing exit but there is no indication from the AHS at the time that the driver is acustomed to receiving an alert D/I - Driver informs AHS that his destination is approaching rapidly and no alert has sounded, zone control rechecks destination and corrects problem if sufficient time remains available, otherwise vehicle is let off at next exit (requires voice communication with zone control)				
	No driver alert signal	D - Driver notices that he is nearing exit but there is no indication from the AHS at the time that the driver is acustomed to receiving an alert D/I - Driver requests to be let off AHS at the next exit (push of a button rather than voice communication with zone control)				
		D - Driver notices that he is nearing exit but there is no indication from the AHS at the time that the driver is acustomed to receiving an alert D/I - Driver informs AHS that his destination is approaching rapidly and no alert has sounded, zone control rechecks destination and corrects problem if sufficient time remains available, otherwise vehicle is let off at next exit (requires voice communication with zone control)				
	No driver awareness test generated	D - Driver notices that he is nearing exit but there is no indication from the AHS at the time that the driver is acustomed to receiving a driver awareness test D/I - Driver requests to be let off AHS at the next exit (push of a button rather than voice communication with zone control)				
		D - Driver notices that he is nearing exit but there is no indication from the AHS at the time that the driver is acustomed to receiving a driver awareness test D/I - Driver informs AHS that his destination is approaching rapidly and no driver awareness test has been received, zone control rechecks destination and corrects problem if sufficient time remains available, otherwise vehicle is let off at next exit (requires voice communication with zone control)				
	No driver awareness test response	D - Zone controol is expecting a driver awareness test response and one is not forthcomming D/I - Second driver awareness test is generated and sent to vehicle, if still no response, zone control personnel contact driver to evaluate situation and take appropriate action				
	Improperly evaluated driver awareness test	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment				

RSC 2B. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		(weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
Vehicle deplatoons	Deplatoon command not received	D - Zone control notes that vehicle is not performing deplatoon manuever D/I - Zone control reissues deplatoon command, if no response zone control personnel contact driver to evaluate the situation and take appropriate action				
		D - Driver notices that deplatoon manuever was not undertaken at the appropriate time D/I - Driver requests to be let off AHS at the next exit (push of a button rather than voice communication with zone control)				
	Vehicle unable to perform deplatoon manuever					
Merge from AHS lane to exit ramp	Lane change command not received					
	AHS commands lane change with destination lane too full	D - Vehicle lateral sensors show vehicles in destination lane and insufficient gap to merge safely D/I - Vehicle does not make merge. Vehicle alerts zone control to problem. Zone control unit and/or personnel try to determine why lane change command was given with destination lane too full. Zone control takes action as appropriate.				
	Vehicle/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane.				
		D - Driver alerts zone control that there is a vehicle in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies vehicle in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the vehicle can proceed. Otherwise, zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects vehicle in destination lane, driver hits panic button D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
Transition to manual control on exit ramp	No request signal for manual control	D - Zone control expects request for manual control and one is not forthcomming D/I - Zone control sends alert to driver to remind him to request manual control, if still no response zone control personnel contact driver to evaluate situation and take appropriate action				
	AHS fails to release control to driver	D - When the vehicle moves to a section of road that has no markers, the vehicle will come to a stop and inform zone control D/I - Zone control personnel can then manually intervene to correct situation				
		D - Driver notes that he does not have manual control when he expects to have manual control D/I - Driver hits panic button - since vehicles on exit ramp behind driver may be under manual control this could cause an accident - therefore, panic button should be disabled during this phase of the journey				
	Driver fails to take manual control after AHS releases control	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
Driver fails awareness test	Infrastructure wrongly releases control to driver	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
	Infrastructure does not route vehicle to intervention area	D - None required for this countermeasure D/I - Construct exit ramp such that unless the driver takes positive action to avoid it, the vehicle will land in an area that has a barrier net to stop the vehicle and a disturbance sensor on the net to alert the zone control that this incident has occurred.				
Sensors monitor condition of roadway	Conditions warranting operational parameter modification not/improperly acted upon	D - Driver notices that roadway and/or environmental conditions appear to warrant change in operational parameters (e.g., speed limit, following distance, etc.) D/I - Driver contacts zone control to indicate belief that conditions appear to warrant change in operational parameters, zone control takes appropriate action, driver can request immediate release from AHS - AHS would move vehicle to transition lane and release control to driver as in a normal check-out transition				

RSC 3. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

ACTION	MALFUNCTION	COUNTERMEASURE	SAF	CAP	CON	CST
Enter the pallet mate/demate facility and drive into a mating dock	Pallet presence recognized without pallet present	D - Driver sees that no pallet is present D/I - Driver contacts mate/demate facility personnel to alert them that a problem exists.				
Drive onto pallet and lock down	Wheel locks not adjusted to correct spacing	D - Driver either sees that wheel locks are not properly adjusted or feels it as he drives onto pallet D/I - Driver contacts mate/demate facility personnel to alert them that a problem exists.				
	Wheel locks not engaged properly	D - Per AHS driver training, driver tries to gently accelerate after AHS panel indicates his vehicle is locked to the pallet. The driver feels the movement indicating that one or more wheels locks are not properly engaged. D/I - Driver contacts mate/demate facility personnel to alert them that a problem exists.				
Lateral control - lane following	Marker	D - Pallet sensor looses track of road centerline D/I - Immediate braking of vehicle to a stop and inform zone control that pallet has lost track of the road centerline and is stopping in AHS lane, zone control verifies that other pallets are experiencing this problem and determines that markers are missing or malfunctioning, pallets moved to adjacent AHS lane or if none exists all pallets stopped on AHS roadway. Response team dispatched to replace/repair markers.				
	Markers not detected	D - Pallet sensor looses track of road centerline D/I - Immediate braking of pallet to a stop and inform zone control that pallet has lost track of the road centerline and is stopping in AHS lane, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control verifies that other pallets are not having this problem and determines that the subject pallet has lost its ability to detect the markers, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team (this and subsequent operational MMS for this RSC assume that the driver has a very limited manual movement control over pallet function - just enought to move the pallet at 2-3 mph and steer it without very fine control - maybe a go/stop button on the AHS panel and a thumbwheel to control steering. Also, driver can unload his vehicle from the pallet under emergency conditions.))				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request release from AHS at next exit				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request release from AHS at next exit				
	Collision	D - Pallet status sensors indicate collision has occurred D/I - Pallet attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other pallets as appropriate - Zone control personnel contact driver and request human input, response team dispatched if required, otherwise pallet moves to shoulder under automated or manual control to await authorities				
	Loss of steering authority	D - Pallet moves away from markers without AHS command D/I - If condition exceeds set tolerance, immediate braking of pallet to a stop and inform zone control that pallet has lost steering authority and is stopping in AHS lane, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched				
	Pallet control unit issues improper commands	D - Roadway sensors detect that pallet is not following proper course D/I - Zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button. D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect external sensor information	D - Roadway sensors detect that pallet is not following proper course D/I - Zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button. D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver				

RSC 3. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		is fined if he does not have good reason for stopping.				
	Incorrect internal status information	D - Roadway sensors detect that pallet is not following proper course D/I - Zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button. D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Flat tire	D - Pallet status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Pallet control system seeks to stabilize pallet tracking on wire and slows pallet, pallet informs zone control of situation, if stable tracking at lower speed is achieved, zone control clears a path to the shoulder and moves pallet to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake pallet to stop in AHS lane and act as though loss of steering authority has occurred				
	Pallet structural or systems failure	D - Pallet status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of pallet to a stop and inform zone control that pallet has suffered unknown failure and is stopping in AHS lane, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched.				
	Improper external AHS commands	D - Pallet control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a merge into the AHS lane to the left where there is no such lane) D/I - Zone control commands pallet to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button. D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	AHS command authority lost	D - Pallet looses contact with zone control, or pallet does not properly respond to zone control commands D/I - Pallet comes to a stop in the assigned lane at normal AHS braking rate. Pallet contacts other pallets to determine if contact with zone control has been lost by them also. If other pallets have also lost contact, all pallets revert to manual control after a set period of time. If other pallets still have contact, relay is set up through another pallet in contact and zone control moves subject pallet to a safe state stopped on shoulder. Zone control personnel take action as appropriate.				
	Vehicle unlocks from pallet	D - Pallet sensors indicate vehicle is free to move in wheel locks D/I - If one sensor indicates unlocked, limit maneuvering to low Gs and exit at next pallet mate/demate facility for inspection. If more than one sensor indicates unlocked, pull to shoulder, stop, and await response team.				
Longitudinal control - throttle and brake	Loss of acceleration control	D - Pallet speed does not equal set speed in absence of acceleration commands D/I - If pallet is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if pallet is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; await response team				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request release from AHS at next exit				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request release from AHS at next exit				
	Collision	D - Pallet status sensors indicate collision has occurred D/I - Pallet attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other pallets as appropriate - Zone control personnel contact driver and request human input, response team dispatched if required, otherwise pallet moves to shoulder under automated or manual control to await authorities				
	Loss of braking control	D - Pallet speed does not equal set speed in absence of acceleration commands D/I - If pallet is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if pallet is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; await response team				
	Pallet control unit issues improper commands	D - Roadway sensors detect that pallet is not following proper course D/I - Zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button.				

RSC 3. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Flat tire	D - Pallet status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Pallet control system seeks to stabilize pallet tracking on wire and slows pallet, pallet informs zone control of situation, if stable tracking at lower speed is achieved, zone control clears a path to the shoulder and moves pallet to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake pallet to stop in AHS lane and act as though loss of steering authority has occurred				
	Pallet structural or systems failure	D - Pallet status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of pallet to a stop and inform zone control that pallet has suffered unknown failure and is stopping in AHS lane, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched.				
	Incorrect external sensor information	D - Roadway sensors detect that pallet is not following proper course D/I - Zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button. D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect internal status information	D - Roadway sensors detect that pallet is not following proper course D/I - Zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button. D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Improper external AHS commands	D - Pallet control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a merge into the AHS lane to the left where there is no such lane) D/I - Zone control commands pallet to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that pallet is not following reasonable course, driver hits panic button. D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Pallet speed limit incorrect	D - Driver detects that his unconstrained AHS pallet is traveling at a different speed than other unconstrained AHS pallets (unconstrained means that the pallet is free to travel at the set speed limit, i.e., not following behind another AHS pallet at the set gap) D/I - Driver alerts zone control personnel, zone control verbally verify set speed limit with driver, if different than reading on speedometer zone control places pallet in a safe state. Order of preference: stopped on shoulder, stopped in AHS lane. If stopped on shoulder or in AHS lane, zone control takes action as necessary. Zone control checks other pallets for set speed limit.				
		D - Roadway sensors detect unconstrained AHS pallet traveling at other than speed limit D/I - Zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate. Zone control checks other pallets for set speed limit.				
	AHS command authority lost	D - Pallet looses contact with zone control, or pallet does not properly respond to zone control commands D/I - Pallet comes to a stop in the assigned lane at normal AHS braking rate. Pallet contacts other pallets to determine if contact with zone control has been lost by them also. If other pallets have also lost contact, all pallets revert to manual control after a set period of time. If other pallets still have contact, relay is set up through another pallet in contact and zone control moves subject pallet to a safe state stopped on shoulder. Zone control personnel take action as appropriate.				
	Vehicle unlocks from pallet	D - Pallet sensors indicate vehicle is free to move in wheel locks D/I - If one sensor indicates unlocked, limit maneuvering to low Gs and exit at next pallet mate/demate facility for inspection. If more than one sensor indicates unlocked, pull to shoulder, stop, and await response team.				
AHS lane to AHS lane	AHS recommends lane change with adjacent lane	D - Pallet's lateral sensors detect pallet(s) in destination lane				

RSC 3. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

change	too full	D/I - Pallet detecting target will not change lanes. Pallet contacts zone control to inform it of this problem.				
	Pallet/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Pallet control system seeks to stabilize pallet tracking on centerline and slows pallet, pallet informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves pallet to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake pallet to stop in AHS lane.				
		D - Driver alerts zone control that there is a pallet in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies pallet in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the pallet can proceed. Otherwise, zone control commands pallet to safe state. Order of preference: stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects pallet in destination lane, driver hits panic button D/I - Immediate braking of pallet to a stop and inform zone control that pallet is stopping in AHS lane at drivers command, zone control alerts other pallets to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to shoulder, driver instructed to manually move to shoulder and await response team, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Lane change recommendation not received					
	Lane change report not received					
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the pallet's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial pallet's warning. These pallet's panic stop would be dealt with in the same way as the initial pallet's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Other pallets not alerted	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the pallet's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial pallet's warning. These pallet's panic stop would be dealt with in the same way as the initial pallet's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Zone control does not contact driver after panic stop	D - Driver does not hear from zone control after a panic stop. D/I - Driver can call zone control directly. If pallet cannot directly reach zone control, a relay through another pallet can be tried. If pallet communications is totally out, zone control can contact a nearby affected pallet and ask their view of the situation.				
	Driver does not inform or misinforms zone control about nature of emergency	D - Driver's conversation with zone control relayed to nearby pallets that are affected by the emergency stop. D/I - Other drivers hear the misinformation passed and break in to inform the zone control of the right information. Any such emergency stop made in on an urban AHS is likely to involve multiple pallets, thus the truth should be able to substantially outvote any misinformation.				
Pallet arrives at destination	Pallet remains on pallet but is not sensed there	D - Driver notices movement of pallet away from dock at end of trip with his vehicle still on it. D/I - Driver retrieves AHS panel and communicates problem to pallet mate/demate facility personnel. Facility control center has ability to stop pallet movement and direct it back to dock to allow vehicle exit.				
Sensors monitor condition of roadway and environment	Conditions warranting operational parameter modification not/improperly acted upon	D - Driver notices that roadway and/or environmental conditions appear to warrent modification of AHS operating parameters D/I - Driver contacts zone control to indicate belief that roadway and/or environmental conditions appear to warrent modification of AHS operating parameters, zone control takes appropriate action, driver can request release from AHS at next exit				

RSC 4. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

ACTION	MALFUNCTION	COUNTERMEASURE	SAF	CAP	CON	CST
AHS entry authorized	AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems				
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control asks driver for non-critical information or takes appropriate action including moving vehicle to shoulder or removing vehicle from AHS for more critical problems				
AHS entry denied	Driver not aware of rejection	Driver training - don't release steering wheel and pedals without positive signal, could be reinforced by periodic tests provided by control unit during normal vehicle entry to AHS				
		D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead in transition lane D/I - Alarm sounds to remind driver to assume manual control				
Transition to automatic control	AHS fails to establish control of vehicle but signals driver that it has taken control	D - Vehicle moves away from lane centerline without command from AHS or closes too close to vehicle ahead D/I - Alarm sounds to alert driver to assume manual control				
	Zone controller unaware vehicle is under AHS control after AHS takes control	D - Periodic recheck of vehicle information reveals mistake D/I - Zone control adds vehicle to database				
	Zone controller believes vehicle is under AHS control when it is not	D - Zone control issues command to vehicle and vehicle does not respond D/I - Zone control rechecks vehicle information, if it finds the error the AHS removes track of vehicle from database, if no error is found the zone controller contacts driver to verify vehicle is under manual control, once verified the AHS removes track of vehicle from database				
Lateral control - lane following	Unresponsive marker	D - Vehicle sensor looses track of road centerline D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the road centerline and is stopping in assigned lane, zone control verifies that other vehicles are experiencing this problem and determines that markers are missing or malfunctioning, lane reverts to manual control driving, zone control releases affected vehicles to manual mode. Response team dispatched to replace/repair markers.				
	Markers not detected	D - Vehicle sensor looses track of road centerline D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle has lost track of the road centerline and is stopping in assigned lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control verifies that other vehicles are not having this problem and determines that the subject vehicle has lost its ability to detect the markers, zone control personnel contact driver for human input, release vehicle control to driver and allow driver to resume full manual control				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would allow driver to resume full manual control				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would allow driver to resume full manual control				
	Collision	D - Vehicle status sensors indicate collision has occurred D/I - Vehicle attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other vehicles as appropriate - Zone control personnel contact driver and request human input, response team dispatched if required, otherwise vehicle moves to shoulder under automated or manual control to await authorities				
	Loss of steering authority	D - Vehicle moves away from markers without AHS command D/I - If condition exceeds set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has lost steering authority and is stopping in assigned lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver and allow driver to resume full manual control, if driver cannot steer, emergency response team is dispatched				
	Vehicle control unit issues improper commands	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control, stopped on shoulder, stopped in assigned lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate. Normally driver allowed to proceed under manual control.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in assigned lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver and allow driver to resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect external sensor information	D - Roadway sensors detect that vehicle is not following proper course				

RSC 4. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		D/I - Zone control commands vehicle to safe state. Order of preference: under manual control, stopped on shoulder, stopped in assigned lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate. Normally driver allowed to proceed under manual control.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in assigned lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input,release steering control to driver and allow driver to resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Incorrect internal status information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control, stopped on shoulder, stopped in assigned lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate. Normally driver allowed to proceed under manual control.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in assigned lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input,release steering control to driver and allow driver to resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Flat tire	D - Vehicle status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Vehicle control system seeks to stabilize vehicle tracking on lane centerline and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clears a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in assigned lane and allow driver to resume manual control.				
	Vehicle structural or systems failure	D - Vehicle status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has suffered unknown failure and is stopping in assigned lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who moves to shoulder and awaits emergency response team.				
	Improper external AHS commands	D - Vehicle control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a merge into the lane to the left where there is no such lane) D/I - Zone control commands vehicle to safe state. Order of preference: under manual control, stopped on shoulder, stopped in lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control.)				
		D/I - Vehicle stops at normal AHS braking rate and informs zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control - however not as fast a brake rate as above.)				
	AHS command authority lost	D - Vehicle looses contact with zone control, or vehicle does not properly respond to zone control commands D/I - Vehicle comes to a stop in the assigned lane at normal AHS braking rate. Vehicle contacts other vehicles to determine if contact with zone control has been lost by them also. If other vehicles have also lost contact, all vehicles revert to manual control after a set period of time. If other vehicles still have contact, relay is set up through another vehicle in contact and zone control moves subject vehicle to a safe state. Order of preference: under manual control, stopped on shoulder. Zone control personnel take action as appropriate.				
Longitudinal control - throttle and brake	Loss of acceleration control	D - Vehicle speed does not equal set speed in absence of acceleration commands D/I - If vehicle is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if vehicle is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; allow to manually drive along shoulder to next exit				
	Operation with out of tolerance roadway conditions	D - Driver notices that roadway conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the roadway conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would release control to driver as in a normal check-out transition				
	Operation with out of tolerance environmental conditions	D - Driver notices that environmental conditions appear out of tolerance D/I - Driver contacts zone control to indicate belief that the environmental conditions are out of tolerance, zone control takes appropriate action, driver can request immediate release from AHS - AHS would release control to driver as in a normal check-out transition				
	Collision	D - Vehicle status sensors indicate collision has occurred D/I - Vehicle attempts to come to a stop as quickly as possible and in lane if possible and informs zone controller of collision, confirm position, and describe severity (peak accelerations), zone controller stops/slows/reroutes other vehicles as appropriate - Zone control personnel contact driver and				

RSC 4. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		request human input, response team dispatched if required, otherwise vehicle moves to shoulder under automated or manual control to await authorities				
	Loss of braking control	D - Vehicle speed does not equal set speed in absence of acceleration commands D/I - If vehicle is too fast - shut off engine, inform zone control, zone control clears path to shoulder, coast to shoulder; if vehicle is too slow, inform zone control, zone control clears path to shoulder, move to shoulder; allowed to manually drive along shoulder to next exit				
	Vehicle control unit issues improper commands	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control.)				
		D/I - Vehicle stops at normal AHS braking rate and informs zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control - however not as fast a brake rate as above.)				
	Flat tire	D - Vehicle status sensors show lack of pressure in one or more tires combined with some disturbance associated with tracking lane centerline D/I - Vehicle control system seeks to stabilize vehicle tracking on wire and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, driver allowed to change tire or response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane and act as though loss of steering authority has occurred				
	Vehicle structural or systems failure	D - Vehicle status sensors show significant deviation from desired conditions D/I - If conditions exceed set tolerance, immediate braking of vehicle to a stop and inform zone control that vehicle has suffered unknown failure and is stopping in AHS lane, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane or shoulder, driver instructed to manually move to transition lane and resume full manual control or move to shoulder, if driver cannot steer, emergency response team is dispatched				
	Incorrect external sensor information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control.)				
		D/I - Vehicle stops at normal AHS braking rate and informs zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control - however not as fast a brake rate as above.)				
	Incorrect internal status information	D - Roadway sensors detect that vehicle is not following proper course D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D/I - Vehicle stops at normal AHS braking rate and informs zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control - however not as fast a brake rate as above.)				
	Improper external AHS commands	D - Vehicle control unit and sensors detect that external AHS commands are improper (e.g., zone control commands a faster speed even though there is a vehicle under AHS control ahead at set gap) D/I - Zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate.				
		D - Driver detects that vehicle is not following reasonable course, driver hits panic button. D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control.)				
		D/I - Vehicle stops at normal AHS braking rate and informs zone control that vehicle is stopping in lane at drivers command, zone control alerts other				

RSC 4. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver who resumes full manual control, if driver cannot resume normal manual control, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping. (May be counterproductive since not all vehicles in lane are under AHS control - however not as fast a brake rate as above.)				
	Vehicle speed limit incorrect	D - Driver detects that his unconstrained AHS vehicle is traveling at a different speed than other unconstrained AHS vehicles (unconstrained means that the vehicle is free to travel at the set speed limit, i.e., not following behind another AHS vehicle at the set gap) D/I - Driver alerts zone control personnel, zone control verbally verify set speed limit with driver, if different than reading on speedometer zone control places vehicle in a safe state. Order of preference: under manual control, stopped on shoulder, stopped in AHS lane. If stopped on shoulder or in AHS lane, zone control takes action as necessary. Zone control checks other vehicles for set speed limit.				
		D - Roadway sensors detect unconstrained AHS vehicle traveling at other than speed limit D/I - Zone control commands vehicle to safe state. Order of preference: under manual control, stopped on shoulder, stopped in AHS lane. Zone control personnel contact driver, alert him to problem, and take necessary action as appropriate. Zone control checks other vehicles for set speed limit.				
	AHS command authority lost	D - Vehicle looses contact with zone control, or vehicle does not properly respond to zone control commands D/I - Vehicle comes to a stop in the assigned lane at normal AHS braking rate. Vehicle contacts other vehicles to determine if contact with zone control has been lost by them also. If other vehicles have also lost contact, all vehicles revert to manual control after a set period of time. If other vehicles still have contact, relay is set up through another vehicle in contact and zone control moves subject vehicle to a safe state. Order of preference: under manual control, stopped on shoulder. Zone control personnel take action as appropriate.				
Mixed lane to mixed lane change	AHS recommends lane change with adjacent lane too full	D - Vehicle's lateral sensors detect vehicle(s) in destination lane D/I - Vehicle detecting target will not change lanes.				
	Vehicle/obstacle in destination lane not detected	D - Collision or violent evasive action required. D/I - Vehicle control system seeks to stabilize vehicle tracking on centerline and slows vehicle, vehicle informs zone control of situation, if stable tracking at lower speed is achieved, zone control clear a path to the shoulder and moves vehicle to shoulder and stops, zone control personnel contract driver for human input, response team dispatched as appropriate; if stable tracking at lower speed is not achieved, brake vehicle to stop in AHS lane.				
		D - Driver alerts zone control that there is a vehicle in the destination lane and driver will not allow lane change (Two possibilities for driver input: A restrictive AHS, in which the driver can prevent some AHS actions by use of a button - if the driver does not prevent the action, the action will happen. A permissive AHS, in which the driver must authorized some AHS actions by the use of a button - if the driver does not authorize the action, the action will not happen.) D/I - Zone control verifies vehicle in destination lane, attempts to determine cause for wrong lane change command. If zone control can find and fix the fault the vehicle can proceed. Otherwise, zone control commands vehicle to safe state. Order of preference: under manual control in manual lane, stopped on shoulder, stopped in AHS lane. Zone control personnel take necessary action as appropriate.				
		D - Driver detects vehicle in destination lane, driver hits panic button D/I - Immediate braking of vehicle to a stop and inform zone control that vehicle is stopping in AHS lane at drivers command, zone control alerts other vehicles to stop/slow/reroute as appropriate, zone control personnel contact driver for human input, release steering control to driver after path is cleared to transition lane, driver instructed to manually move to transition lane and resume full manual control, if driver cannot steer, emergency response team is dispatched. Driver is fined if he does not have good reason for stopping.				
	Manual driven vehicle merges into subject vehicle - proximity crash.	D - Lateral sensors detect target vehicle merging into subject vehicle D/I - Most of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention. Probably warrants special attention drawing devices because this is a mixed traffic scenario.				
	Other vehicle merges too close ahead with too large a closing velocity	D - Gap sensor detects target vehicle merging ahead of subject vehicle D/I - If the target vehicle is moving more slowly than the subject vehicle, the subject vehicle will brake. However, if the distance target vehicle is detected is too close and the closing velocity too great, a collision will occur. Most of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention. Probably warrants special attention drawing devices because this is a mixed traffic scenario.				
	Other vehicle merges too close behind with too large a closing velocity	D - If detection occurs at all it is from the driver of the subject vehicle or possibly roadway sensors. D/I - If the target vehicle is moving more rapidly than the subject vehicle, the subject vehicle will accelerate if it does not violate the gap parameters. However, if the distance target vehicle is detected is too close and the closing velocity too great, a collision will occur. Many of these accidents are the result of the target vehicle driver not seeing the subject vehicle. The subject vehicle should do something to draw the target vehicle driver's attention. Probably warrants special attention drawing devices because this is a mixed traffic scenario.				
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the vehicle's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial vehicle's warning. These vehicle's panic stop would be dealt with in the same way as the initial vehicle's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Other vehicles not alerted	D - None required for this countermeasure D/I - In addition to informing the zone control, the driver's request for a panic stop will also sound the vehicle's horn and flash its lights to visually alert nearby drivers. These nearby drivers can also request a panic stop if they feel the need to do so based on the initial vehicle's warning. These vehicle's panic stop would be dealt with in the same way as the initial vehicle's panic stop. (May be counterproductive by spreading panic to all nearby drivers.)				
	Zone control does not contact driver after panic stop	D - Driver does not hear from zone control after a panic stop.				

RSC 4. OPERATIONALLY ORIENTED MALFUNCTION MANAGEMENT STRATEGIES

		D/I - Driver can call zone control directly. If vehicle cannot directly reach zone control, a relay through another vehicle can be tried. If vehicle communications is totally out, zone control can contact a nearby affected vehicle and ask their view of the situation.				
	Driver does not inform or misinforms zone control about nature of emergency	D - Driver's conversation with zone control relayed to nearby vehicles that are affected by the emergency stop. D/I - Other drivers hear the misinformation passed and break in to inform the zone control of the right information. Any such emergency stop made in on an urban AHS is likely to involve multiple vehicles, thus the truth should be able to substantially outvote any misinformation.				
Vehicle nears destination	Improperly evaluated driver awareness test	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
Transition to manual control	Driver fails to take manual control after AHS releases control	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
Driver fails awareness test	Infrastructure wrongly releases control to driver	D - Vehicle sensors and control unit can observe driver behavior for some period after release of control to driver for signs of driver impairment (weaving in or across lanes, inability to maintain speed, etc.). D/I - During this observation period, if the control unit senses driver impairment, control can be retaken by AHS and vehicle routed to nearest intervention area.				
	Infrastructure does not route vehicle to intervention area	D - None required for this countermeasure D/I - Construct exit ramp such that unless the driver takes positive action to avoid it, the vehicle will land in an area that has a barrier net to stop the vehicle and a disturbance sensor on the net to alert the zone control that this incident has occurred.				
Sensors monitor condition of roadway	Conditions warranting operational parameter modification not/improperly acted upon	D - Driver notices that roadway and/or environmental conditions appear to warrant change in operational parameters (e.g., speed limit, following distance, etc.) D/I - Driver contacts zone control to indicate belief that conditions appear to warrant change in operational parameters, zone control takes appropriate action, driver can request immediate release from AHS - AHS would release control to driver as in a normal check-out transition				

APPENDIX G. SERIOUSNESS OF MALFUNCTIONS USING SELECTED MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION	INFRASTRUCTURE										VEHICLE													
		PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		WIRE SENS		STEER ACT		THRTL ACT		AHS POWER	
		WIRE		LINK ES-ZC		LINK RS-ZC		COMM		---------		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		VEHCL SYSTM	
Set AHS destination	AHS destination not set											X			X										
Request AHS entry	Road capacity check fails					X	X	X		X															
	AHS accepts destination when no such destination exists							X																	
AHS entry authorized	AHS accepts and authorizes entry with missing, incomplete, or known incorrect check-in information							X																	
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters							X																	
AHS entry denied	Driver not aware of rejection							X	X	X		X	X	X	X									X	
Transition to automatic control	AHS request for transition fails							X	X	X		X	X	X	X									X	
	AHS fails to establish control of vehicle but signals driver that it has taken control							X	X				X	X	X										
	Zone controller unaware vehicle is under AHS control after AHS takes control							X	X				X	X	X										
	Zone controller believes vehicle is under AHS control when it is not							X	X				X	X	X									X	
Lateral control - lane following	Wire not functioning			X						X															
	Wire not detected													X	X			X						X	
	Operation with out of tolerance roadway conditions		X			X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions		X		X	X		X	X				X	X	X										
	Collision		X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority													X	X					X			X	X	X
	Vehicle control unit issues improper commands														X										
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Flat tire																						X		
	Vehicle structural or systems failure																								X
	Improper external AHS commands		X	X	X	X	X	X	X				X	X	X										
	AHS command authority lost							X	X	X			X	X	X					X	X	X		X	
Longitudinal control - throttle and brake	Loss of acceleration control													X	X							X		X	X
	Operation with out of tolerance roadway conditions		X			X	X	X	X				X	X	X										

RSC 1. SERIOUSNESS OF MALFUNCTIONS WITH SELECTED MALFUNCTION MANAGEMENT STRATEGY

	Operation with out of tolerance environmental conditions		X		X	X			X	X				X	X	X										
	Collision		X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control														X	X						X		X	X	X
	Vehicle control unit issues improper commands															X										
	Flat tire																							X		
	Vehicle structural or systems failure																									X
	Incorrect external sensor information														X	X		X							X	
	Incorrect internal status information														X	X	X								X	
	Improper external AHS commands		X	X	X	X	X	X	X	X				X	X	X										
	Vehicle speed limit incorrect		X		X	X	X	X	X	X	X			X	X	X										
	AHS command authority lost								X	X	X			X	X	X					X	X	X		X	
Transition lane to AHS lane change	AHS commands lane change with destination lane too full						X	X	X	X																
	Vehicle/obstacle in destination lane not detected														X	X		X							X	
	Manual driven vehicle merges into subject vehicle - proximity crash.												O													
	Other vehicle merges too close ahead with too large a closing velocity												O													
	Other vehicle merges too close behind with too large a closing velocity												O													
AHS lane to AHS lane change	AHS commands lane change with destination lane too full						X	X	X	X																
	Vehicle/obstacle in destination lane not detected														X	X		X							X	
	Lane change command not received								X	X				X	X	X										
	Lane change report not received								X	X				X	X	X										
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails												X		X	X						X			X	X
	Other vehicles not alerted								X	X	X		X	X	X	X									X	
	Sector control does not contact driver after panic stop		X						X	X	X			X	X	X										
	Driver does not inform or misinforms zone control about nature of emergency												X													
Vehicle nears destination	Improperly evaluated driver awareness test								X	X				X	X	X										
AHS lane to transition lane change	AHS commands lane change with destination lane too full						X	X	X	X																
	Vehicle/obstacle in destination lane not detected														X	X		X								
	Manual driven vehicle merges into subject vehicle - proximity crash.												O													
	Other vehicle merges too close ahead with too large a closing velocity												O													
	Other vehicle merges too close behind with too large a closing velocity												O													
Transition to manual control	Driver fails to take manual control after AHS releases control												X													X
Driver fails awareness test	Infrastructure wrongly releases control to driver								X	X				X	X	X										
	Infrastructure does not route vehicle to								X	X	X			X	X	X					X				X	X

RSC 1. SERIOUSNESS OF MALFUNCTIONS WITH SELECTED MALFUNCTION MANAGEMENT STRATEGY

	intervention area																								
Sensors monitor condition of roadway and environment	Conditions warranting operational parameter modification not/improperly acted upon		X		X	X	X	X	X	X	X			X	X	X									

RSC 2B. SERIOUSNESS OF MALFUNCTIONS WITH SELECTED MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION	INFRASTRUCTURE										VEHICLE (PALLET)													
		PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		MARKER SENS		STEER ACT		THRTL ACT		AHS POWER	
		MAG MARK		LINK ES-ZC		LINK RS-ZC		COMM		---------		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		PALLET SYSTM	
AHS entry authorized	Road capacity check fails					X	X	X		X															
	AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information							X																	
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters							X																	
AHS entry denied	Driver not aware of rejection							X	X			X	X	X	X									X	
Transition to automatic control	AHS fails to establish control of vehicle but signals driver that it has taken control							X	X				X	X	X										
	Zone controller unaware vehicle is under AHS control after AHS takes control							X	X				X	X	X										
	Zone controller believes vehicle is under AHS control when it is not							X	X				X	X	X										
Merge into AHS lane as singleton	Gap in mainline traffic not formed					X	X	X	X	X			X	X	X									X	
	Vehicle/obstacle in destination lane not detected													X	X		X							X	
Form with a platoon	Current platoon leader will not relinquish lead													X	X		X				X	X			
	Platoon parameters improper					X	X	X	X	X			X	X	X		X								
Lateral control - lane following	Marker		X																						
	Markers not detected													X	X			X						X	
	Operation with out of tolerance roadway conditions		X			X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions		X		X			X	X				X	X	X										
	Collision		X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority													X	X					X			X	X	X
	Vehicle control unit issues improper commands														X										
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Flat tire																						X		
	Vehicle structural or systems failure																								X
	Improper external AHS commands		X	X	X	X	X	X	X				X	X	X										
	AHS command authority lost							X	X	X			X	X	X					X	X	X		X	
Longitudinal control - throttle and brakes	Loss of acceleration control													X	X							X		X	X
	Operation with out of tolerance roadway conditions		X			X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions		X		X	X		X	X				X	X	X										

RSC 2B. SERIOUSNESS OF MALFUNCTIONS WITH SELECTED MALFUNCTION MANAGEMENT STRATEGY

	Collision		X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control														X	X						X		X	X	X
	Vehicle control unit issues improper commands															X										
	Flat tire																							X		
	Vehicle structural or systems failure																									X
	Incorrect external sensor information														X	X		X							X	
	Incorrect internal status information														X	X	X								X	
	Improper external AHS commands		X		X	X	X	X	X	X				X	X	X										
	Vehicle speed limit incorrect		X		X	X	X	X	X	X	X			X	X	X										
	Platoon position assignment unknown						X	X	X	X	X			X	X	X										
	AHS command authority lost								X	X	X			X	X	X					X	X	X		X	
AHS lane to AHS lane change - platoon	No lane change command						X	X	X	X	X			X	X	X										
	Gap in destination lane traffic not formed						X	X	X	X	X			X	X	X										
	Vehicle/obstacle in destination lane not detected														X	X		X							X	
	Vehicle/obstacle in destination lane detected by one or more platoon members						X	X	X	X					X	X		X								
	Platoon actions not coordinated						X	X	X	X	X			X	X	X									X	
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver activates panic button inappropriately												X													
	Driver warning fails												X		X	X						X			X	X
	Other vehicles not alerted								X	X	X		X	X	X	X									X	
	Zone control does not contact driver after panic stop		X						X	X	X			X	X	X										
	Driver does not inform or misinforms zone control about nature of emergency												X													
Driver desires to exit prior to input destination	Driver's request not/improperly acted upon								X	X	X		X	X	X	X										
Vehicle nears destination	Proximity to destination not recognized								X	X	X			X	X	X				X						
	No driver alert signal								X	X	X			X	X	X										
	No driver awareness test generated								X	X	X			X	X	X										
	No driver awareness test response								X	X	X		X	X	X	X										
	Improperly evaluated driver awareness test								X	X				X	X	X										
Vehicle deplatoons	Deplatoon command not received								X	X	X			X	X	X									X	
	Vehicle unable to perform deplatoon manuever														X	X			X	X	X	X	X	X	X	X
Merge from AHS lane to exit ramp	Lane change command not received								X	X	X			X	X	X										
	AHS commands lane change with destination lane too full						X	X	X	X				X	X	X										
	Vehicle/obstacle in destination lane not detected														X	X		X								
Transition to manual control on exit ramp	No request signal for manual control												X													
	AHS fails to release control to driver								X	X				X	X	X					X	X	X			
	Driver fails to take manual control after AHS												X													

RSC 2B. SERIOUSNESS OF MALFUNCTIONS WITH SELECTED MALFUNCTION MANAGEMENT STRATEGY

	releases control																								
Driver fails awareness test	Infrastructure wrongly releases control to driver								X	X				X	X	X									
	Infrastructure does not route vehicle to intervention area								X	X	X			X	X	X					X			X	X
Sensors monitor condition of roadway	Conditions warranting operational parameter modification not/improperly acted upon		X		X	X	X	X	X	X	X			X	X	X									

RSC 3. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION	INFRASTRUCTURE										VEHICLE (PALLET)													
		PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		MARKER SENS		STEER ACT		THRTL ACT		AHS POWER	
		MAG MARK		LINK ES-ZC		LINK RS-ZC		COMM		DOCK SYSTM		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		PALLET SYSTM	
Enter the pallet mate/demate facility and drive into a mating dock	Pallet presence recognized without pallet present							X	X		X														
Drive onto pallet and lock down	Wheel locks not adjusted to correct spacing							X	X	X	X		X	X	X										X
	Wheel locks not engaged properly																								X
Lateral control - lane following	Marker		X																						
	Markers not detected													X	X			X						X	
	Operation with out of tolerance roadway conditions	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	X		X	X			X	X				X	X	X										
	Collision	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority													X	X					X			X	X	X
	Pallet control unit issues improper commands														X										
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Flat tire																						X		
	Pallet structural or systems failure																								X
	Improper external AHS commands	X	X	X	X	X	X	X	X				X	X	X										
	AHS command authority lost						X	X	X				X	X	X					X	X	X		X	
	Vehicle unlocks from pallet							X	X				X	X	X									X	X
Longitudinal control - throttle and brake	Loss of acceleration control													X	X							X		X	X
	Operation with out of tolerance roadway conditions	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	X		X	X			X	X				X	X	X										
	Collision	X	X	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control													X	X						X		X	X	X
	Pallet control unit issues improper commands														X										
	Flat tire																						X		
	Pallet structural or systems failure																								X
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Improper external AHS commands	X		X	X	X	X	X	X				X	X	X										
	Pallet speed limit incorrect	X		X	X	X	X	X	X	X			X	X	X										
	AHS command authority lost							X	X	X			X	X	X					X	X	X		X	
	Vehicle unlocks from pallet							X	X				X	X	X									X	X

RSC 3. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

AHS lane to AHS lane change	AHS recommends lane change with adjacent lane too full						X	X	X	X				X	X	X									X	
	Pallet/obstacle in destination lane not detected														X	X		X							X	
	Lane change recommendation not received								X	X	X			X	X	X									X	
	Lane change report not received								X	X	X			X	X	X									X	
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails												X		X	X						X			X	X
	Other pallets not alerted												X	X	X	X									X	
	Zone control does not contact driver after panic stop		X																							
	Driver does not inform or misinforms zone control about nature of emergency												X													
Pallet arrives at destination	Vehicle remains on pallet but is not sensed there								X		X	X														
Sensors monitor condition of roadway and environment	Conditions warranting operational parameter modification not/improperly acted upon		X		X	X	X	X	X	X	X			X	X	X										

RSC 4. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

ACTION	MALFUNCTION	INFRASTRUCTURE										VEHICLE													
		PRSNL		ENVNT SENS		ROAD SENS		ZONE CNTRL		AHS POWER		DRVR		INTNL BUS		STATUS SENS		MARKER SENS		STEER ACT		THRTL ACT		AHS POWER	
		MAG MARK		LINK ES-ZC		LINK RS-ZC		COMM		---------		COMM		VEHCL CNTRL		EXTRNL SENS		POSITN SENS		BRAKE ACT		TIRES		VEHCL SYSTM	
AHS entry authorized	AHS accepts and authorizes entry with missing, incomplete, or know incorrect check-in information							X																	
	AHS accepts and authorizes entry with known vehicle and/or roadway unsuitable parameters							X																	
AHS entry denied	Driver not aware of rejection							X	X			X	X	X	X									X	
Transition to automatic control	AHS fails to establish control of vehicle but signals driver that it has taken control							X	X				X	X	X										
	Zone controller unaware vehicle is under AHS control after AHS takes control							X	X				X	X	X										
	Zone controller believes vehicle is under AHS control when it is not							X	X				X	X	X										
Lateral control - lane following	Unresponsive marker		X																						
	Markers not detected													X	X			X						X	
	Operation with out of tolerance roadway conditions	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	X		X	X			X	X				X	X	X										
	Collision	X	X	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of steering authority													X	X					X			X	X	X
	Vehicle control unit issues improper commands														X										
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Flat tire																						X		
	Vehicle structural or systems failure																								X
	Improper external AHS commands	X	X	X	X	X	X	X	X				X	X	X										
	AHS command authority lost							X	X	X			X	X	X					X	X	X		X	
Longitudinal control - throttle and brake	Loss of acceleration control													X	X							X		X	X
	Operation with out of tolerance roadway conditions	X				X	X	X	X				X	X	X										
	Operation with out of tolerance environmental conditions	X		X	X			X	X				X	X	X										
	Collision	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
	Loss of braking control													X	X						X		X	X	X
	Vehicle control unit issues improper commands														X										
	Flat tire																						X		
	Vehicle structural or systems failure																								X
	Incorrect external sensor information													X	X		X								
	Incorrect internal status information													X	X	X									
	Improper external AHS commands	X		X	X	X	X	X	X				X	X	X										
	Vehicle speed limit incorrect	X		X	X	X	X	X	X	X			X	X	X										

RSC 4. SERIOUSNESS OF MALFUNCTIONS IN ABSENCE OF MALFUNCTION MANAGEMENT STRATEGY

	AHS command authority lost								X	X	X			X	X	X					X	X	X		X	
Mixed lane to mixed lane change	AHS recommends lane change with adjacent lane too full						X	X	X	X				X	X	X										
	Vehicle/obstacle in destination lane not detected														X	X		X							X	
	Manual driven vehicle merges into subject vehicle - proximity crash.												O													
	Other vehicle merges too close ahead with too large a closing velocity												O													
	Other vehicle merges too close behind with too large a closing velocity												O													
Driver perceives emergency situation that may not be detected by on-board or IS sensors	Driver warning fails												X		X	X						X			X	X
	Other vehicles not alerted								X	X	X		X	X	X	X									X	
	Zone control does not contact driver after panic stop		X						X	X	X			X	X	X										
	Driver does not inform or misinforms zone control about nature of emergency												X													
Vehicle nears destination	Improperly evaluated driver awareness test								X	X				X	X	X										
Transition to manual control	Driver fails to take manual control after AHS releases control												X													
Driver fails awareness test	Infrastructure wrongly releases control to driver								X	X				X	X	X										
	Infrastructure does not route vehicle to intervention area								X	X	X			X	X	X					X				X	X
Sensors monitor condition of roadway	Conditions warranting operational parameter modification not/improperly acted upon		X		X	X	X	X	X	X	X			X	X	X										