Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Malfunction Management and Analysis

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-95-096
March 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.

1. Report No.
FHWA-RD-95-XXX

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
Precursor Systems Analyses Of Automated Highway System

Final Report
Malfunction Management and Analysis
Volume 5

5. Report Date

6. Performing Organization Code

7. Author(s) M. McGowan, T. Franks, W. Schineller, M. Shannon

8. Performing Organization Report No.

9. Performing Organization Name and Address
Raytheon Company
Missile Systems Division
50 Apple Hill Drive
Tewksbury, Ma 01876

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTFH61-93-C-00196

12. Sponsoring Agency Name and Address
The Federal Highway Administration
400 Seventh Street, S.W.
Washington, D.C. 20590

13. Type of Report and Period Covered
Final Report
Sept 1993 - Feb 1995

14. Sponsoring Agency Code

15. Supplementary Notes
Contracting Officer's Technical Representative (CTOR) - J. Richard Bishop (HSR-12)

16. Abstract

This document is the draft final report of the Automated Highway System. The activities of Malfunction Management and Analysis are reported on in this document. This document type is resource materials.

This volume is the fifth in a series. There are nine other volumes in the series.

FHWA-RD-95-XXX	Volume 1	Executive Summary
FHWA-RD-95-XXX	Volume 2	Automated Check In
FHWA-RD-95-XXX	Volume 3	Automated Check Out
FHWA-RD-95-XXX	Volume 4	Lateral and Longitudinal Control
FHWA-RD-95-XXX	Volume 5	Malfunction Management and Analysis
FHWA-RD-95-XXX	Volume 6	Commercial Vehicle and Transit AHS Analysis
FHWA-RD-95-XXX	Volume 7	Entry/Exit Implementation
FHWA-RD-95-XXX	Volume 8	Vehicle Operational Analysis
FHWA-RD-95-XXX	Volume 9	AHS Safety Issues
FHWA-RD-95-XXX	Volume 10	Knowledge Based Systems and Learning Methods

17. Key Words
Automated Highway System, Check in, Check out, Lateral and Longitudinal Control, Malfunction Management, Entry/Exit, Safety, Commercial, Transit Knowledge Based Systems

18. Distribution Statement
No restrictions. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 39	22. Price

Table Of Contents

List Of Figures

List Of Tables

LIST OF ABBREVIATIONS

AASHTO	American Association of State Highway and Transportation Officials
ABS	anti-lock brake system
AHS	Automated Highway System
AI	Artificial Intelligence
AICC	Autonomous Intelligent Cruise Control
AICC	Adaptive Intelligent Cruise Control
ALK	automatic lane keeping
ANSI	American National Standards Institute
APTS	Advanced Public Transportation System
ASR	anti wheel spin regulation
ASTM	American Society for Testing and Materials
ATIS	Advanced Traveler Information System
ATMS	Advanced Traffic Management System
AVCS	Advanced Vehicle Control Systems
AVI	automated vehicle identification
AVL	automated vehicle location
BAA	Broad Agency Announcement
CICC	cooperative intelligent cruise control
CLT	crossing left turn
CVO	Commercial Vehicle Operations
CVSA	Commercial Vehicle Safety Alliance
DOT	Department of Transportation
EIA	Electronics Industry Association
EMS	emergency medical services
ERSC	Evolutionary Representative System Configuration
ETC	electronic toll collection
EVM	emergency vehicle management
FARS	Fatal Accident Reporting System
FFBD	functioal flow block diagram
FHWA	Federal Highway Administration
FLIR	forward looking infrared radar
FMEA	failure modes and effects analysis
FTA	Federal Transit Administration
GES	General Estimates System
GPS	Global Positioning Satellite navigation system
HAR	Highway Advisory Radio
HAZMAT	hazardous materials
HDS	headway detection system
HOV	high occupancy vehicle
HUD	head-up display
ICAS	intersection collision avoidance system
ICC	intelligent cruise control
IEEE	Institute of Electrical and Electronics Engineers
ISTEA	Intermodal Surface Transportation Efficiency Act
ITE	Institute of Transportation Engineers
IVHS	Intelligent Vehicle Highway System
LCM	lane change / merge collisions
LED	light-emitting diode display
LORAN	Land-based Radio Navigation System
MCSAP	Motor Carrier Safety Assistance Program
MOE	measure of effectiveness
NAB	National Association of Broadcasters
NEC	Northeast corridor

NEMA	National Electrical Manufacturer Association
NHTSA	National Highway Traffic Safety Administration
PATH	Program for Advanced Transit and Highways (California)
PCD	personal communication device
PDS	proximity detection system
PPT	personalized public transit
PRT	perception reaction time
PSA	precursor systems analyses
PSAP	public safety answering point
PSS	Public Safety Services
PTS	public travel security
RECA	rear end collision avoidance
RECW	rear end collision warning
RL	reinforcement learning
RSC	representative system configuration
RSPA	Research and Special Programs Administration
RTTASC	real-time traffic-adaptive signal control
SAE	Society of Automotive Engineers
SCP	straight crossing path
SHMS	speed headway maintanence system
SOV	single occupancy vehicle
SRVD	single vehicle roadway departure
TCS	traction control system
TDM	travel demand management
TIA	Telecommunications Industry Association
TMC	traffic management center
TMS	tire monitor system
VMS	variable message sign
VMT	vehicle miles traveled
VRC	vehicle-to-roadside communication

1.0 EXECUTIVE SUMMARY

An objective of the Automated Highway System (AHS) is a system that will be accident-free in the absence of malfunctions. The purpose of the malfunction management and analysis effort was to identify strategies for managing AHS malfunctions, and to identify issues and risks associated with implementing these strategies. In addition measures of effectiveness have been identified which could be used to evaluate and to optimize various malfunction management strategies.

A through understanding of the system's normal operation must be developed as the starting point for malfunction management and analysis. This can be accomplished by using the system engineering approach of functional analysis to develop a framework of the systems normal sequence of operations. Functional analysis presents the interactions between the various functions and can also be used for developing timelines for the occurrence of the various functions.

The next step is to develop a set of operating conditions for the system which defines normal operations. A system as complex as an AHS is not like an assembly line, a conveyor belt, or even a railroad where objects move along a set path. Even these less complex systems are complicated. An example is the luggage conveyor system at the new Denver airport and the widely reported difficulties it has encountered. In a system as complex as the AHS, normal operations will not be described by discrete values but rather a range of values (i.e., the one sigma value of a normal distribution) in which operations can occur. The definition of the normal operating conditions then allows the question of what is a malfunction and when does it occur to be answered.

The end product of the functional analysis assists in answering the questions concerning malfunction identification. It accommodates two approaches. One considers a loss in functionality of an operational requirement and the other component failure within a particular system element.

Once malfunctions have been identified the next step is to evaluate the impact on the system in order to prioritize the response. Two key attribute to consider are the likelihood of occurrence and the severity of impact on normal operations given its occurrence. For AHS applications, a malfunctions severity might be measured according to its impact on safety, system throughput, and user comfort.

It is advantageous to assemble multiple response options to a particular malfunction. Operational flexibility in a particular system design depends on the ability of the system to adapt to the situation. Each of these responses to a particular malfunction could have a different implementation time for restoring normal system operation or other performance measures such as user cost, system cost, likelihood of successful implementation, and severity of impact on safety, system efficiency, and user comfort. The system designer must not only consider the final results of the malfunction management strategy but also the transient effects of a particular response after a malfunction outweighing the benefits to the system given the response's successful implementation.

The following are the key findings of the malfunction analysis task.   A complete set of malfunction management strategies will balance the desire to have the system perform without failing with the need to respond to failure when it inevitably occurs, within the constraints imposed by safety, system efficiency, user comfort, and cost.

A complete evaluation of malfunction management options includes cost/benefit tradeoffs between the preventative reduction in the probability of malfunction occurence and the responsive reduction in the severity of the malfunction given its occurrence.

The time criticality and potential severity of certain malfunctions preclude dependence on system responses once the malfunction occurs. In these instances the malfunction management strategy must rely on built in redundancies either in the vehicle or roadway infrastructure.

Reliance on the driver (perceptions, capabilities, predictability, and accountability) for malfunction prevention, detection, diagnosis, and execution of management tasks is a risk/challenge.

Certain malfunctions do not lend themselves to a straight forward methodological breakdown. The complexity of the AHS assures that malfunction management will be a continuously evolving process.

The transient effects of a particular management response may outweigh the benefits gained by its implementation.

2.0 INTRODUCTION FOR ACTIVITY AREA

This section of the report provides a description of the activity, the purpose of this effort, a listing of the issues addressed, an overview of the overall approach, and a summary of the guiding assumptions.

2.1 Description Of Activity Area

The Malfunction Management and Analysis activity was to describe requirements and strategies for safely handling and managing malfunctions, to estimate the consequences of these malfunctions and the malfunction strategies by identifying measures of effectiveness and to define alternative ways in which malfunctions can be detected.

2.2 Purpose Of This Effort-Specific Focus

Although perfect safety has always been, and will continue to be, a primary goal of transportation technology, the fact is that no transportation system has yet achieved it. The AHS will certainly strive to reach that goal. However, as in any system, things can go wrong or unanticipated events can occur. The purpose of this effort is to define a methodology for identifying potential malfunction and then identify measures of effectiveness (MOEs) which can be used in evaluating and selecting the optimum response. The goal of any malfunction management strategy is to prevent malfunctions from occurring and when they do occur to mitigate their effects.

2.3 Issues Addressed

The Malfunction Management and Analysis issues addressed in this activity area were:

- Functional analysis to define normal operations.
- Identification and categorization of potential malfunctions.
- Investigation of malfunction detection techniques.
- Definition of MOEs to rate malfunction severity.
- Definition of MOEs to rate malfunction responses.
- Development of malfunction management strategies.

2.4 Overall Approach For This Activity Area

The overall approach was to first define a methodology which would permit the determination of normal operations in an AHS. This first step provides an effective framework to define, comprehend, and analyze complex system designs. Next a method for detecting malfunctions is identified. Once identified, an assessment of the severity of the malfunction must be conducted considering MOEs. Finally, malfunction management strategies are discussed which not only consider the final outcome but also the effects of the transient responses on the system

2.5 Guiding Assumptions - Origins and Rationale

The key guiding assumption was that the AHS is to be collision free in the absence of malfunctions as specified by the Broad Agency Announcement (BAA) for the Precursor Systems Analyses (PSA) of AHS.[1] Additionally, for users of the system to be at ease, the system must not only **be** safe, it must **appear** safe. Conversely, the appearance of safety must always mean that, intrinsically, the system actually is safe.

Other assumptions were:

- Operation in a freeway type of roadway was assumed.
- The AHS will operate in a wide range of weather conditions.
- Only instrumented vehicles will be allowed to operate on instrumented roadways

3.0 EVOLUTIONARY REPRESENTATIVE SYSTEMS CONFIGURATIONS (ERSC)

Initial analysis concluded that the PSA could best contribute to the AHS effort by focusing its investigation on determining the degree to which an evolutionary approach could best meet the AHS challenge by investigating five Evolutionary Representative System Configurations (ERSC). The approach was to build upon current and planned capability using technology which is available in the near term to define an AHS system, to provide the earliest significant performance, to determine how far such a system could go in meeting the growing requirements, and then to identify more advanced technologies, as required, to meet the tougher challenges downstream. The first three ERSCs are envisioned to be single automated lanes, while ERSCs four and five would have multiple lanes. Figure 1 provides an overview of the key characteristics of each ERSC. This approach is explained in detail in Volume One of this series of reports.

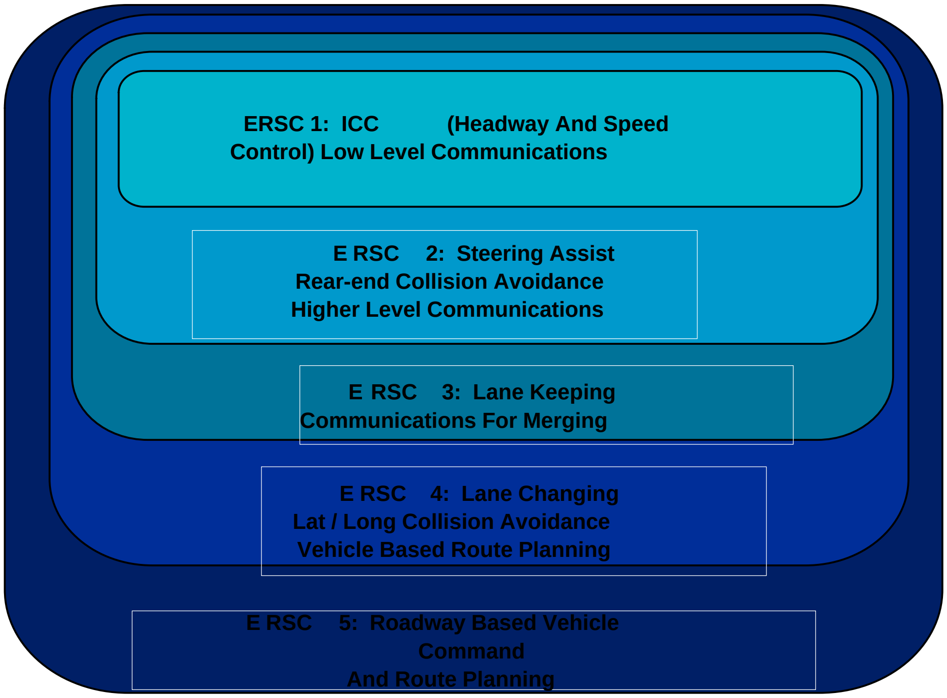

ERSC 1: ICC (Headway And Speed Control) Low Level Communications
E RSC 2: Steering Assist
Rear-end Collision Avoidance
Higher Level Communications
E RSC 3: Lane Keeping
Communications For Merging
E RSC 4: Lane Changing
Lat / Long Collision Avoidance
Vehicle Based Route Planning
E RSC 5: Roadway Based Vehicle Command
And Route Planning

Figure 1 Evolutionary Representative System Configurations

4.0 TECHNICAL DISCUSSIONS OF EACH STEP

When developing concepts for the eventual physical realization of a system that promises to have many interrelated functions, a top level systems engineering approach can help organize otherwise potentially unwieldy tasks into more manageable components. The AHS, with complex vehicle-vehicle, vehicle-roadway, and vehicle-driver interactions, is certainly a system concept with many interrelated functions. Therefore, it is appropriate to apply a top level systems engineering perspective to the malfunction management and analysis task during the PSA contract phase of the AHS program.

The complete systems engineering process leads to a well defined and optimally balanced system design. It does not produce the actual system itself. Rather, it produces the set of documentation necessary to fully describe the system to be developed and produced. To ensure their influence on the system design, the process provides for the timely and appropriate integration of mainstream disciplines of system design engineering with engineering specialties such as reliability, maintainability, human factors, safety, environmental assessment, and producibility .

Malfunction management, like other engineering specialties, must be adaptively integrated into the context of the overall systems engineering process. For every different system design, it is important to appropriately account for the issues, risks, and concerns raised as result of malfunction management analysis throughout the concept development process.

Figure 2 highlights the malfunction management study methodology. The first step in our process then was to describe how the system engineering approach is used to determine the normal operations for the AHS. We then describe how the functional analysis assists with the malfunction identification process. Once the normal system operation and potential malfunctions are known, malfunction detection techniques are identified. MOEs are then defined which can be applied to the malfunction to determine its severity and also to evaluate the various responses. Finally, malfunction management strategies are defined to mitigate the effect of the malfunction on the system. Particular attention is paid to the effects of transient responses on the system.

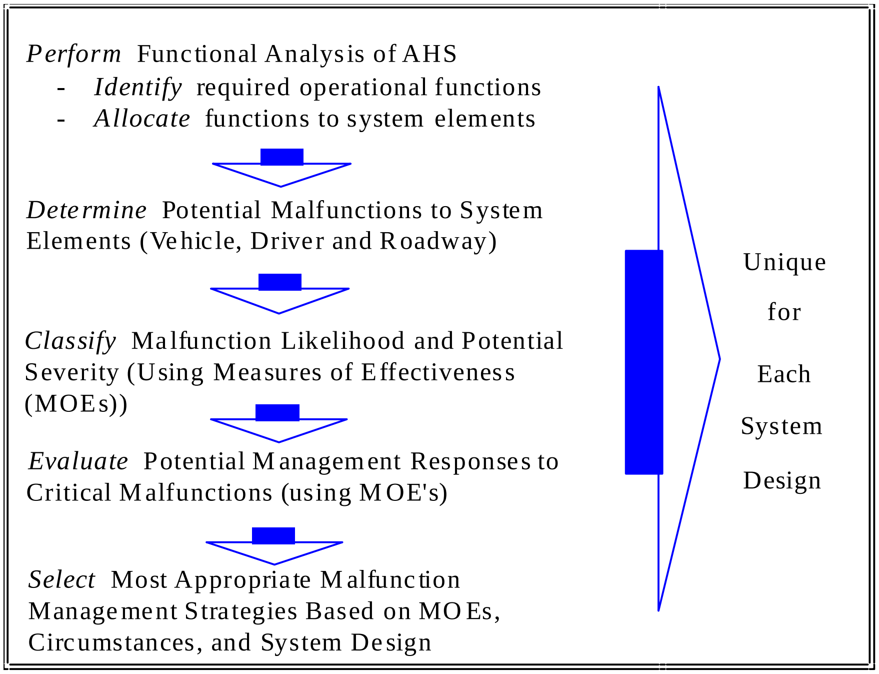

Perform Functional Analysis of AHS
- *Identify* required operational functions
- *Allocate* functions to system elements
Determine Potential Malfunctions to System Elements (Vehicle, Driver and Roadway)
Classify Malfunction Likelihood and Potential Severity (Using Measures of Effectiveness (MOEs))
Evaluate Potential Management Responses to Critical Malfunctions (using MOE's)
Select Most Appropriate Malfunction Management Strategies Based on MOEs, Circumstances, and System Design
Unique for Each System Design

Figure 2 Malfunction Management and Analysis - Study Methodology

4.1 Develop Operational and Physical Description of Normal AHS Operations

A necessary starting point for the malfunction management and analysis of an automated highway system (AHS) is a thorough understanding of what can be referred to as the system's "normal operations". Before malfunctions can be considered, there must be a clearly defined framework in place to determine what the system can do and how this gets done while operating under benign conditions. Without a framework established to define normal system operations, questions such as "What is a malfunction?" and "When is it a malfunction?" are often difficult to consider. These questions often depend on an answer to the broader question, "What are normal operations?".

From a systems engineering perspective, an understanding of normal operations requires knowledge about how each operational function is physically implemented within specific system elements. A process known as functional analysis helps to establish this level of understanding.

As a first step in the systems engineering process, functional analysis defines a baseline set of functions and performance requirements which must be met in order to adequately accomplish the system's operational goals. It is useful for developing and refining requirements for equipment, software, personnel, and operational procedures that are necessary to complete the development and deployment of the system. Functional analysis is a two step process: it begins with the identification of top level operational functions, and it ends with the allocation of these functions to lower level elements within the system.

An example of a top level function required for AHS travel under benign operating conditions might be "class 3 vehicles traveling at a rate of 25 meters per second on AASHTO standard roadways are required to stop within a distance of 100 meters upon receipt of signal". The division of responsibility for this function might be shared between subsystem elements from the vehicle and roadway.

Functional analysis iteratively identifies and deconstructs primary system performance requirements into increasingly detailed functions. System design flexibility is reduced as more operational requirements are allocated to elements in a particular design configuration. It can be thought of as adding constraints to a concept so that a boundless range of design options is reduced to a more realistic, workable system representation with which to perform a next series of evaluations.

The functional analysis process helps to produce a well-defined operational and physical description of the system that is uniformly complete. To a given level of detail, it results in a clear mapping between operational functions of the system and the physical elements or combinations of physical elements that are responsible for performing them. Below this given level of detail, the mapping may not be unique. Since there may be several potential way for different subsystem elements to satisfy the same higher level system requirement, it may be possible to consider several lower level design options.

A follow-on, feedback step in this systems engineering process verifies that a synthesis of lower level system elements is capable of meeting the allocated functional requirements. Functional synthesis complements the functional analysis process to yield an improved and more robust description of system operations and the system elements that perform those operations. While functional analysis seeks out elements to perform operational functions, functional synthesis seeks out operational functions that can be performed by system elements. Though verification of normal operations through functional synthesis is beyond the scope of the PSA, it is mentioned here for completeness, and because it resembles the process of constructing malfunction management responses.

For a system such as AHS, there are reasons to anticipate a wide potential variation in performance related parameters for the driver, vehicle, and roadway elements. Variation in user demand, and in the operational, environmental, and maintenance status of AHS will compound the range of normal operating conditions. Therefore, AHS will be assured to have a rather broad, and far from absolute definition of normal operations.

There is considerable variation in the population of drivers that utilize today's highways. Driver motor skills, vision, reaction time, compliance, ability to reason, familiarity with surrounding environment, and mood can be expected to vary between drivers and even within the same driver over time.   Driver performance can experience significant changes over days and years. Drivers may suffer sensory loss, develop more cautious or aggressive driving natures, be mentally or dexterously affected by medical prescription drugs, be affected by emotions, etc.

The nation's highways have an established precedence of being very accommodating and accepting of this driver diversity. Typically, it is up to the individual driver to assess his or her fitness to perform the necessary functions for travel on today's roadways. Most drivers bring only a little training (that may be required to be officially licensed vehicle operator) and various degrees of 'on the road' experience to their driving tasks.

There is considerable variation in the fleet of passenger, commercial, transit, maintenance, and incident response vehicles that travel today's highways. For passenger vehicles and trucks, this variation represents a long developed free market response to diverse consumer needs (including perceived needs generated from advertiser influence, etc.). These needs are composed of interrelated and often opposing factors such as availability, affordability, utility, fuel economy, performance, appearance, maintainability, safety, passenger capacity, goods capacity, and popularity.

Vehicle performance specifications can experience significant changes between model years. For a particular model, performance status over time introduces another contributor to vehicle variation on today's roads. Vehicles may get damaged as a result of collisions, be subject to aftermarket modifications, receive different levels of maintenance service, and experience normal wear during its lifetime which can all effect its operational performance. A wide variation in vehicle types implies a wide variation in operational parameters. Indeed, acceleration, braking, steering, and communications parameters on today's roads are diverse.

There is considerable variation in the network of roads that serve as today's highways. They vary by number of lanes, frequency of entry/access facilities, method of toll payment (if any), surface material, surface conditions, level of use, user population (e.g., urban, rural, commuters, vacationers, commercial users), geographic topography (e.g., need for steep gradients, narrow turns, elevated sections, bridges, tunnels, etc.), and environmental conditions.

Many higher level operational functions of an AHS cannot be easily categorized as exclusively driver, vehicle, or roadway functions. A fourth broad category, specified as interdependent functions, captures those functions which are performed by a combination of driver, vehicle, and roadway elements. As an example, the traditional operational function "vehicle must maintain traction with road surface" is realized through interrelated functions between roadway and vehicle. These interdependent functions could make up a significant portion of new AHS functions as reassigned traditional driver functions are shared between newly automated vehicle and roadway functions.

The range of variation in a system's operational conditions can be divided into three categories:

- *Desirable* conditions exist when all system requirements are met or exceeded,
- *Uncertain* conditions exist when system performance resides somewhere between *Desirable* and *Unacceptable*, and
- *Unacceptable* conditions exist when serious performance degradations result from a loss in system functionality.

Desirable conditions *never* require malfunction management responses, and unacceptable conditions *always* require malfunction management responses. A system typically operates between these extremes - in a region which can be referred to as normal operations in the absence of a malfunction. It can be difficult to assess when deviations from desirable performance should be tolerated and when they should be dealt with through malfunction management strategies.

Differentiating between a malfunction and a tolerable deviation within normal operations is not always straightforward. For instance, depending on the scope of the definition for normal system operations, an AHS condition such as "two inches of snow accumulation on road surface" may be considered either a malfunction to the system or just an infrequent, yet normal occurrence.

Similarly, the system response to this event such as "reduce vehicle speeds to 40 miles per hour" may then fall into the category of a malfunction management response or just another normal system function. However, another event such as "degraded communications between vehicles", which may be more clearly understood as a malfunction, may utilize the identical system response ("reduce vehicle speeds to 40 miles per hour") to alleviate the adverse condition. In this second case the response is more clearly understood to be a malfunction management strategy.

Typically, larger scale malfunctions don't spontaneously happen. Usually a sequence of adverse occurrences propagates over time until some aspect of overall system performance is sufficiently degraded below an acceptable level. Thus, another dimension to the definition of a malfunction occurrence is the moment in time which establishes that a change in conditions or a malfunction has occurred. For instance a hypothetical sequence of events on today's roads might be:

1. sharp-edged debris falls off moving truck;
2. vehicle runs over debris in roadway;
3. debris damages a tire and creates leak;
4. under pressurized tire reduces vehicle's lateral control response;
5. driver is unable to maintain vehicle's position in lane;
6. lane departure occurs and vehicle veers into guardrail;

One could argue that the threshold crossing from normal operations to a malfunction occurred at any one of these steps. With proper detection resources in place, a malfunction response at any prior stage could prevent the next, more severe occurrence from happening (e.g., at step two, the driver could have detected and steered around debris; at step four, a controlled vehicle stop in lane or in breakdown lane could be performed).

It is not possible to quantify overall system performance for normal operations during the PSA. The ERSC descriptions do not lead to a sufficient quantitative characterization of performance related functions. Models to accommodate the simulation of various AHS environments and operational conditions do not presently exist. Thus, rating a malfunction's impact on normal operations is limited to the use of system-level MOEs with subjective / qualitative resolution.

4.2 Functional Analysis Assist with Malfunction Identification Process

The end product of a functional analysis process can assist with malfunction identification. It accommodates two approaches to discriminate malfunctions from normal operations:

Approach 1. Consider a loss in functionality of an operational requirement. Trace this loss to a potential underlying failure in a particular system element that could lead to this operational loss. This failure is a malfunction.

Approach 2. Consider a component failure within a particular system element. Evaluate whether a propagation of this failure has the potential to create or contribute to a loss in functionality of an operational requirement. If it does, then this failure is a malfunction.

Obviously, the functional analysis process for identifying malfunctions can only be as focused as the system requirements used in each assessment. Softer system requirements that tolerate a wider range of normal operations will tend to make this identification process more subjective and less certain.

The first approach is preferred at this stage of the AHS program since it is more biased towards the information presently available. It follows the top-down system decomposition approach. Operational functions are allocated to system elements just as operational malfunctions are evaluated for potential underlying physical malfunction. Notions of AHS operational functions and requirements are more prevalent in the AHS community than physical descriptions of a candidate system. Currently, there is neither a set of operational requirements or a physical system description available that could be considered to completely describe normal operations for AHS.

4.3 Malfunction Detection and Diagnosis

Detection is part of the malfunction management timeline. The earlier a malfunction is detected, and the closer to the root cause, the better the chance for success of a malfunction management strategy.

Some malfunctions are easier to detect than others. Traditional diagnostics can be designed into the system (at a cost) to check many individual components. These can pinpoint many malfunctions quickly; for example, a drop in oil pressure indicating an engine failure in this vehicle. However, it may not be technically feasible or cost-effective to monitor every sub-component, particularly in earlier ERSCs, when fewer functions are fully automated. For example, in ERSC1 a headway maintenance system could be implemented which is not fully self-diagnostic. To monitor malfunctions in such subsystems, a malfunction management strategy should incorporate secondary "non-diagnostic" detection means. Secondary malfunction detection could be achieved by observing unexpected, abnormal operational behavior and inferring a malfunction. Secondary detection also provides redundancy to normal diagnostic tests.

In general, the element on which a given system is installed is expected to have primary responsibility for detecting malfunctions to that system. For example, each vehicle has primary responsibility for monitoring the status of all its on-board systems. Drivers are responsible for themselves. In some cases, however, an element may not be able to best monitor itself. For example, vehicles traveling on the roadway are in the best position to detect missing magnetic nails. Malfunction management could assign vehicles the responsibility to report this to the roadway, which would in turn initiate a response.

The bottom line is that for every function designed into the system, malfunction management requires that some element be assigned primary responsibility for detecting malfunctions.

Based on their criticality, reliability, and technical feasibility issues, functions cannot and need not have the same frequency for detecting failures. The three categories of detection frequency of continuous monitoring, diagnostic tests and scheduled inspection are now discussed.

Wherever technically feasible and cost-effective, it is desirable to continuously monitor individual components of each subsystem. Continuous monitoring can be accomplished through Built-In Test (BIT) and should be focused on safety-critical items. Continuous monitoring can be performed for many vehicle functions even during travel on non-AHS roads. This simplifies check-in procedures for ensuring the vehicle fitness before entering the AHS, and is best for detecting malfunctions early on the malfunction management timeline before serious degradation occurs. Brake pads are an example of a component that can be continuously monitored.

Diagnostic tests can be programmed into the system to occur at particular times. Some vehicle tests could be performed at ignition, while others could be performed during non-AHS travel, at check-in, at regular intervals during AHS travel, or at check-out. Some aspects of the roadway may be tested with a special probe vehicle during off peak usage hours. Diagnostic tests involve consistency checks on outputs using known input sets. They apply not only to hardware and software based systems on the vehicle and roadway, but also to the driver. The driver could be put through tests to verify his/her readiness to perform manual functions. The required frequency of such tests would have to be determined during the system design process.

Regularly scheduled inspections of subsystems at each element level are valuable for detecting minor malfunctions even before they degrade into malfunctions that could cause operational deviations. Inspections apply to drivers in the form of license renewals, as well as to vehicles and the roadway. The frequency at which various subsystems are inspected should be determined in terms of miles traveled or time as a function of how they wear, the severity of potential malfunctions, and cost.

Observation of operational deviations can be indicative of malfunctions that were not directly detected by diagnostic means. Depending on the malfunction, one element, such as the driver, may be able to perform secondary detections of malfunctions in another element, such as another vehicle. Secondary detections of malfunctions can serve as a redundant back-up to primary detection methods. Secondary detection considerations for each element are discussed in the next three sections.

Malfunction management strategies in earlier ERSCs can include the driver as a secondary means for observing many kinds of operational deviations. To the extent that the driver is involved, the system design must have a way of utilizing information he/she can provide. Communications would have to be designed accordingly. For example, the driver might observe another vehicle tailgating behind him, perhaps because the following vehicle's headway maintenance is not operating properly (out of calibration or disengaged). This information could be communicated back to the following vehicle or to the roadway, which could attempt to diagnose and respond to the malfunction.

Vehicle sensors may be designed to look for unexpected behavior by other vehicles or even by their own driver, and then the vehicle could communicate this to other system elements.

Particularly in later ERSCs, when it assumes more control, the roadway can play an important role in detecting malfunctions. Each traffic control centers could compare its own model of the road (a prediction based on the commands it issues) with the picture of the traffic situation it receives (from drivers and vehicles). Discrepancies between the expected and actual traffic picture could flag possible malfunctions requiring further diagnosis and response.

4.3.1 Diagnosis of Malfunctions

The wrong response to a malfunction can have an adverse impact on system operation. To avoid creating a worse situation, diagnosis of a malfunction should be as accurate as possible before the system reacts. Diagnosis can occur prior to and during a malfunction response. This section outlines the steps of the diagnosis process that are necessary for selecting the appropriate response.

The first step of diagnosis is to verify that a malfunction actually exists. Verification of a malfunction can be attempted by repeating the test which detected it, or more preferably, performing an independent test.

The element responsible for the malfunction needs to be identified so that the response can focus on the problem and minimize impact on the rest of the system. For example, if a malfunction is detected when a group of vehicles is observed to be slowing to a halt, those vehicles are probably not <u>all</u> malfunctioning. More likely, the vehicle in front is experiencing a malfunction, or perhaps there is a problem with the roadway itself. Proper identification of the element responsible might mean the difference between commanding a single vehicle into the breakdown lane or bringing all vehicles to a stop.

Next the severity of the degradation must be assessed. When an element suffers a malfunction, it could result in minor or major degradation from normal operation. In the case of a minor degradation to an element, like the roadway being wet, the response need not have a major impact on system operation; commanded speed for all vehicles could be reduced and gap increased somewhat. In the case of a major degradation, like a refrigerator falling off the back of a truck, more drastic measures might be taken, such as shutting down a lane and rerouting all traffic. Additional situational information, such as traffic density, is also an important part of the diagnosis.

The diagnosis should first specify the level of the elemental degradation (i.e., what happened). For example, if a headlamp failed on a vehicle, the diagnosis should indicate this, and furthermore whether just one or all headlamps were out. Similarly, in developing the management strategy for any malfunction, thought should be given to what additional information about the status of the element is useful.

The diagnosis should also specify relevant information about the operational situation. By the situation, we mean the environment, traffic density, etc. To extend the failed headlamp example, the diagnosis should indicate something about visibility. If the diagnosis was that a vehicle had two failed headlamps, but that it was daylight with good visibility, this would influence the selection of an appropriate response.

Detection discrimination between different elemental malfunctions that result in the same loss in operational functionality may be a challenge. Two completely different malfunctions may "look" the same operationally for a period of time. Methods of diagnosis must recognize this gray area, and strike a balance between being overcautious and undercautious.

4.4 Measures of Effectiveness (MOEs) to Identify Malfunctions and Classify Their Severity

In the systems engineering approach, malfunction occurrences are first identified by noting the potential ability of a failure in a system element to sufficiently degrade normal operations. Then they are classified by the severity of that impact. When malfunction severity is situationally dependent, and the differentiating information is unavailable, a conservative, worst case impact on normal operations should be assumed.

Since malfunctions can degrade normal operations in many ways, it is necessary to utilize a crosscutting set of measures of effectiveness (MOEs) that reflect this broad scope. However, it is also desirable to limit the malfunction severity rating categories. This allows systems designers to remain focused on how key measures of system performance are degraded in the presence of a malfunction.

The utility of MOEs during the PSA is to help identify likely problem areas and risks in the AHS program, and to demonstrate a system engineering based approach to malfunction management. It has been subjectively determined that each MOE be defined on a scale with five ratings (ratings A through E). A malfunction is assigned one of these ratings or it is determined that the malfunction has no bearing on this particular MOE (rating N/A for not applicable). Such a scale is sufficient for highlighting the more critical areas of normal operations/malfunction management at this stage in the AHS program, and a scale with any further resolution might unnecessarily imply detailed knowledge about system performance that is unavailable at this time.

The MOE ratings are geared for use while in the presence of a malfunction to a system element. Ratings are specified for a typical vehicle or driver. For the roadway, a specific segment, rather than the entire system should be considered as the element. This element is assumed to have been contributing to normal operations in some way prior to the malfunction. Ratings on each MOE scale have been biased towards the perceived normal operating regions of AHS, i.e., they have more resolution in the regions where normal AHS operations and most minor malfunctions will occur. It may be necessary to qualify a particular malfunction rating with relevant AHS operational circumstances at time of and in vicinity of its occurrence.

The following MOE classifies malfunction likelihood of occurrence to a system element:

- malfunction likelihood of occurrence (described in Section 4.4.1).

The following MOEs classify malfunction severity:

- malfunction impact on safety (described in Section 4.4.2),
- malfunction impact on system efficiency (described in Section 4.4.3), and

- malfunction impact on user comfort (described in Section 4.4.4).

4.4.1 Malfunction Likelihood of Occurrence

This MOE rates malfunction likelihood to a particular system element at a specified point in time. This scale is biased towards unlikely occurrences. Element age and wear are assumed to be independent of this MOE. If the element is expected to be periodically inspected, serviced, and/or calibrated, then it is assumed that the rating represents an averaged value over this time interval.

Table 1 Malfunction Likelihood of Occurrence

Rating	Criteria
A = Very Rare	Element designed and built to highest achievable reliability. It can be expected that this element will not fail. Driver task that is natural and trivial to all drivers.
B = Improbable	Failure unlikely. History of similar designs shows very few failures. Driver task requires simple, routine interpretation and execution.
C = Remote	Few failures likely to occur, but possible. Driver task requires moderate, but typically routine interpretation and execution.
D = Occasional	Some failures likely to occur. Driver task requires moderate interpretation and execution of potentially unfamiliar tasks.
E = Probable	Failures typically occur several times. Driver task requires skilled interpretation and execution of potentially unfamiliar tasks.
N/A=Not Applicable	Not a malfunction likelihood of occurrence issue.

4.4.2 Malfunction Impact on Safety

This MOE rates a malfunction's potential impact on actual (not perceived) safety. This scale is biased towards pre-accident safety conditions. There is no attempt to explicitly account for the level of property damage and injuries sustained from a malfunction which may result from an accident.

Unsafe conditions include: a driver, vehicle, or roadway who is not well informed of upcoming events, a driver who is incapable of performing routine tasks, a vehicle operating with safety-related instrumentation anomaly, a vehicle operating with unstable dynamics and control, a road surface with unexpected anomaly, a roadway with safety-related instrumentation anomaly, collisions resulting in property damage, and collisions resulting in personal injuries.

Table 2 Malfunction Impact on Safety

Rating	Criteria
A = Slight	Negligible to slight effect on vehicle or safety.
B = Moderate	Moderate effect on vehicle or safety.
C = Major	Vehicle performance severely affected, but drivable and safe. Roadway function impaired. Driver slow to respond to requests. Vehicle-based malfunction response sufficient, but may desire system level malfunction response .
D = Severe	Gradual vehicle failure, potentially safety related. Vehicle able to stop without mishap, but safe. Roadway inoperable. Driver not responding to requests. System level malfunction response necessary.
E = Critical	Potentially hazardous failure. Safety related, sudden failure in vehicle or roadway. Driver overriding system functions. System level malfunction response necessary.
N/A=Not Applicable	Not related to safety.

4.4.3 Malfunction Impact on System Efficiency

This MOE is concerned with system efficiency issues such as traffic flow performance and roadway accessibility. It rates a system's ability to provide travel needs to AHS users. This scale is biased towards system operating conditions at near capacity levels.

Although performance values are used here to distinguish between ratings, it should be noted that these values are subjective, and not based on any simulation of AHS conditions. A particular malfunction may impact a subset of these somewhat related system efficiency parameters:

a) percent reduction in desired travel (free flow) speed,
b) percent reduction from maximum traffic density,
c) number of AHS travel lanes unavailable,
d) percent reduction from maximum entry/exit access rate.

A half value [.5] suffix for parameter c) indicates that the breakdown lane exists, but is unavailable for travel (or occupied).

Table 3 Malfunction Impact on System Efficiency

Rating	Criteria
A = Slight	a. Reduces desired travel speed by 2 % b. Reduces maximum traffic density by 2 % c. Reduces number of travel lanes by 0 d. Reduces maximum entry/exit access rate by 2 %
B = Moderate	a. Reduces desired travel speed by 5 % b. Reduces maximum traffic density by 5 % c. Reduces number of travel lanes by 0.5 d. Reduces maximum entry/exit access rate by 5 %
C = Major	a. Reduces desired travel speed by 20 % b. Reduces maximum traffic density by 20 % c. Reduces number of travel lanes by 1.0 d. Reduces maximum entry/exit access rate by 20 %
D = Severe	a. Reduces desired travel speed by 50 % b. Reduces maximum traffic density by 50 % c. Reduces number of travel lanes by 2.0 d. Reduces maximum entry/exit access rate by 50 %
E = Critical	a. Reduces desired travel speed by 100 % b. Reduces maximum traffic density by 100 % c. Reduces number of travel lanes by ALL d. Reduces maximum entry/exit access rate by 100 %
N/A=Not Applicable	Not related to system effectiveness.

4.4.4 Malfunction Impact on User Comfort

This MOE rates a typical driver's personal comfort level in the presence of a malfunction. User comfort level while traveling on AHS should not be mistaken for user acceptance, which may depend on cost, utility, and other issues not directly related to user comfort. Human factors are only subjectively accounted for. Actual driver skills, and issues such as driver acclimation, learning, etc., are not explicitly accounted for. Drivers' perceptions do not necessarily match reality, but in this case it's the perceptions that matter. For instance, perceived system safety is a user comfort issue.

Table 4 Malfunction Impact on User Comfort

Rating	Criteria
A = Slight	Tolerant. Minor system perturbations. Meets travel needs.
B = Moderate	Annoyed. Uncomfortable perceptions, unexpected occurrences.
C = Major	Aggravated. System unexpectedly requests user participation. System does not provide travel needs of user
D = Severe	Hostile. User may attempt to manually override system.
E = Critical	Traumatic. User in physical turmoil, becomes unglued, unlikely to use system again, and likely to be vigorously outspoken against its further development.
N/A=Not Applicable	Not related to user acceptance.

4.4.5 Secondary MOEs to Identify and Classify Malfunctions

Certain malfunctions may be more effectively classified with a more extensive list of MOEs. However, it is sufficient for this study to limit identification and classification of malfunctions to issues concerning malfunction likelihood, and impact on safety, system effectiveness, and user comfort.

Other system-level MOEs are useful for evaluating normal operations in the AHS program, but they play more of a secondary role in the analysis of malfunctions. MOEs in this category include cost, environmental impact, legal liability, and human factors feasibility. Malfunctions that have more than minimal impact on these secondary MOEs can be addressed for overall user acceptance on a case by case basis.

4.5 Components of Complete Malfunction Management Strategy

A complete malfunction management strategy includes malfunction prevention, detection, and response. Timeliness is also a critical factor that involves all components.

4.5.1 Malfunction Management Timeline

Incidents on the highway are seldom the result of a single, instantaneous malfunction. In many cases, severe incidents can be traced to a sequence of malfunctions which were either not noticed, or ignored until too late. Quite often malfunctions could have been prevented, or at least detected and responded to at an earlier stage, but cost or some other issue stood in the way.

In general, the longer the system is permitted to operate with malfunctions present, the greater the risk: both likelihood of occurrence and severity of the consequences tend to increase with time. Of course, some malfunctions may be allowed to persist longer than others with little or no risk. Thus, the notion of a *timeline* associated with each potential malfunction is introduced.

The malfunction management timeline starts with *prevention*, before a loss in operational functionality actually occurs. Malfunction prevention is discussed in the next section. The timeline extends through when the malfunction actually begins to occur. At this point, the *detection* process clock continues to run until the malfunction is identified by the system. Detection was addressed in Section 4.3. After detection, an appropriate *response* to the malfunction may be initiated along the timeline. A successful response prevents a chain reaction of more serious, higher level malfunctions from occurring. A good malfunction management strategy doesn't necessarily detect and respond to every low level malfunction, but does ensure that higher order malfunctions are detected and responded to at some point along the timeline before a serious incident occurs.

An overly preventative system design may have more upfront costs. It is generally more costly to design and build a system which attempts to catch every low-level malfunction. On the other hand, risk is generally greater when operating at the response end of the timeline, allowing higher level malfunctions to occur and persist before reacting. This may lead to more operational costs. Thus, the best system design results from a tradeoff in prevention and response costs. The most beneficial malfunction management cost allocation is one that minimizes the overall risk of severe malfunctions.

4.5.2 Malfunction Prevention

An obvious malfunction management strategy is to prevent a malfunction from occurring, as cost allows. AHS concepts involve three basic elements: 1) the roadway, 2) the vehicle, and 3) the driver. Just as the types of malfunctions which may occur within each of these elements differ, so do the prevention policies available to each element.

In an evolutionary approach, the roadway gradually assumes control of malfunction management as the AHS matures. Roadway malfunctions can be prevented through enforcement, reliability, redundancy, and maintenance.

In early ERSCs, when the driver is still involved, the roadway's ability to prevent many potential malfunctions is largely indirect, through enforcement of "rules of the road". Stricter enforcement helps keep unfit drivers and vehicles off the road, and ensures that drivers carry out commands issued by the roadway.

Roadway systems must always be designed to be highly reliable. As the number and complexity of roadway subsystem elements increases with each ERSC, so does the potential for serious malfunctions by the roadway, and reliability becomes increasingly critical.

Redundancy in the system design is an effective way of preventing many roadway malfunctions when possible. Redundant systems perform the same function independently, so that the failure of one does not result in a malfunction of the overall system (as long as the parallel system continues to operate). For example, the lane keeping function might depend on magnetic nails in the roadway which individual vehicles will sense (magnetically). In case one or more nails become undetectable, the system design may employ a redundant, vision-based system to perform lane keeping. As another example, roadside communication might be deployed so that multiple transmitters/receivers provide redundant, overlapping coverage of every position on the road.

Proper road maintenance is also a key to prevention. More frequent maintenance will tend to reduce the risk of malfunctions, but again, cost is a limiting factor.

Each vehicle on the highway adds more potential for malfunctions to the system. Malfunction prevention from the vehicle side is achieved largely through building high reliability into each vehicle, using as much redundancy in on-board systems as is feasible, and adhering to a program of regularly scheduled maintenance.

Maintenance is especially critical for each vehicle, since many components cannot be made highly reliable, or backed up with redundant systems (e.g. steering). Even more than with the roadway, normal operation causes some vehicle parts to degrade over time. Some degradation is gradual (tire and brake wear), while in other cases, components fail with little or no warning. Another example are sensor lenses, which would have to be kept clean, just like a windshield today.

Since vehicle maintenance responsibility (costs) will probably be assumed by vehicle owners, whose car care habits vary greatly, enforcement of vehicle standards by the roadway, as mentioned previously, will be very critical.

The driver retains a fair amount of control of the vehicle until later ERSCs. Even in the later ERSCs, he/she is not entirely without responsibility for the vehicle. In the early ERSCs, the driver is depended on to perform such basic functions as lateral control, and even in the mature AHS envisioned for ERSC5, he/she is still somewhat involved in check-in (providing trip data) and check-out (re-assuming control of the vehicle when exiting onto non-AHS roads). Failure to perform driver responsibilities constitutes a malfunction. Therefore, driver education, training, and certification will be necessary for prevention in any malfunction management strategy.

4.5.3 Malfunction Responses: Managing Risk While Restoring Normal Operations

Once a malfunction has been detected and diagnosed, the system can select and implement an appropriate malfunction response.

Malfunction responses are sets of actions constructed from system element functions and they can be separated into two categories:

- *immediate responses* and
- *supplemental responses* .

In the presence of a malfunction, immediate responses are performed relatively promptly to alleviate current risk and instability to the system. Their implementation results in a system that has transitioned from an unacceptable state to either normal operations (a desirable state) or to some tolerable, yet still degraded state. If immediate responses do not reestablish normal operations, then additional supplemental responses are performed. In some cases, an overall malfunction response strategy may require immediate and supplemental responses while, for others, immediate responses may be sufficient.

The two primary considerations for selecting an appropriate malfunction response are:

- a response's ability to ultimately restore normal operations , and
- a response's ability to minimize adverse transient effects during its implementation.

Transient effects of a malfunction response account for system performance between initial malfunction diagnosis and some time later after the immediate response has been implemented. To assist in the assessment of candidate malfunction response strategies, MOEs are necessary to rate the transient effects and end result of a response. (See flow in Figure 3.)

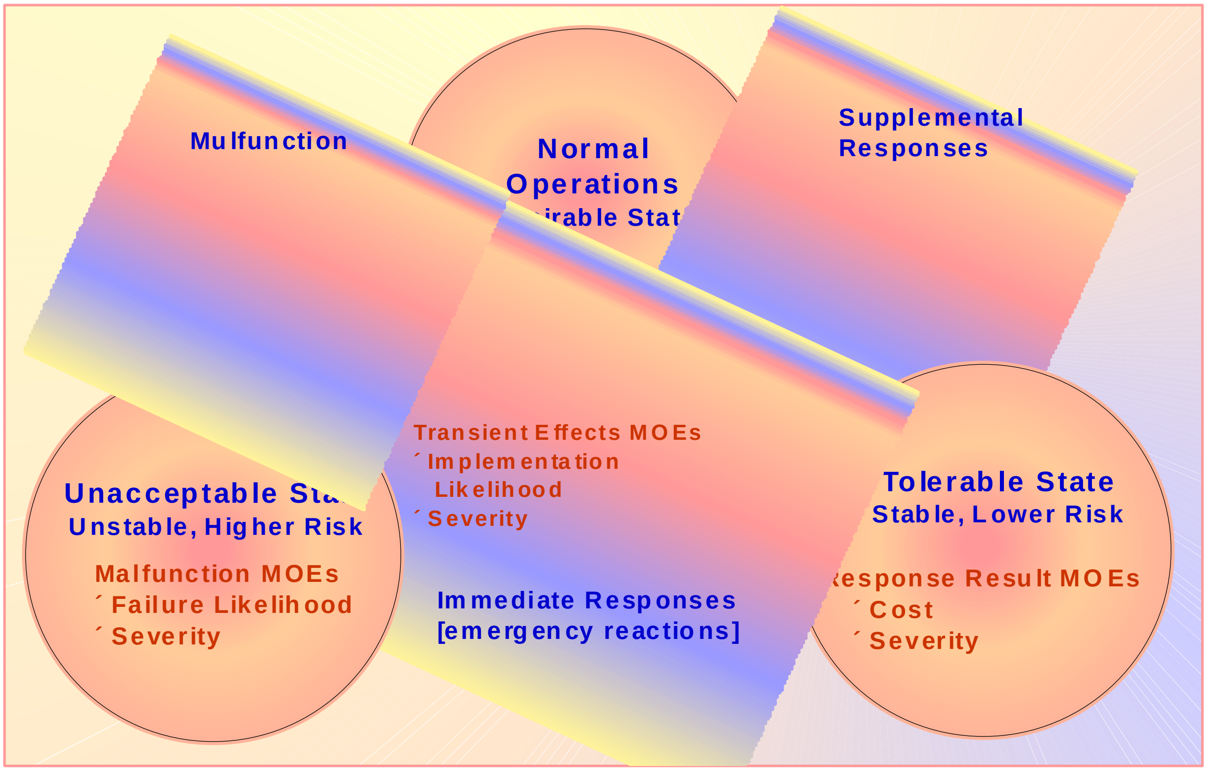


Figure 3 Malfunction Response Dynamics

As more automated instrumentation is introduced as the ERSCs evolve, and operational requirements are reassigned to different elements in the evolving system design, malfunction response options can be expected to differ between ERSCs. In a gradual evolutionary development and deployment scenario, malfunction management strategies should also be expected to evolve gradually. Many functions that have not changed significantly can probably rely on prior malfunction management strategies. It is also possible that certain functions that have not changed may indirectly benefit from evolution. This is possible if improved malfunction management strategies can be realized through access to improvements elsewhere in the system. Malfunction strategies will need to be developed for newly introduced system functionality. In this case, some of the response options may be new, while some may be available from prior designs.

It may be more cost effective for one ERSC to develop prevention and early detection resources into the system design so that the operational malfunction in question never occurs. Due to the limited functionality within the system elements, this preventative option may not be technically feasible in an earlier ERSC. Therefore, this ERSC would need to emphasize and fund response techniques to this operational malfunction.

Depending on the level of instrumentation available in a particular evolutionary state, the roadway may control a vehicle directly or request a driver to execute vehicle commands. In early ERSCs, various aspects of malfunction management may depend on driver participation. When appropriate or necessary, drivers may be expected to participate in prevention, detection, diagnosis, response selection, and response execution aspects of various malfunction management strategies. This introduces concerns about driver compliance to perform critical or even routine aspects of early AHS travel.

The first step in determining malfunction responses is to construct or synthesize candidate malfunction responses. These can be either immediate responses which minimize the transient effects while reducing risk due to malfunction or supplemental responses to reestablish normal operations.

Malfunction responses are sets of actions performed by system elements. Each system element (vehicle, driver, roadway) has specific functionality. At the time a malfunction is detected and diagnosed, each element may have lost or degraded capability to perform one or more of its normal functions. The options available to the system when constructing a malfunction response are thus limited by the system's remaining functionality.

It is advantageous to assemble multiple response options to a particular malfunction. Operational flexibility in a particular system design depends on the ability of system to adapt to the situation. Thus, all feasible response options to a malfunction should be considered for evaluation.

Possible driver responses vary according to his/her physical and mental state, and according to the allowed driver functionality in a particular ERSC. In earlier ERSCs, drivers may be required to play a more significant role in malfunction management. Compliance is a major concern for driver responses.

Vehicle responses include acceleration, deceleration, maneuvers, and communication. The state of a vehicle and its surrounding environment may restrict the vehicle functionality. For example, when the fuel is low, a vehicle may not be able to proceed three extra exits ahead. Vehicle response options differ from ERSC to ERSC.

The roadway will have more response options in later ERSCs when it has more information available and more direct control over vehicles. In earlier ERSCs, it may only be able to issue a command for a lower speed, whereas in later ERSCs it can slow down vehicles directly and steer them away from incidents.

In the presence of a malfunction, immediate responses are performed relatively promptly to alleviate current risk and instability to the system. Their implementation results in a system that has transitioned from an unacceptable state to either normal operations (a desirable state) or to some improved, tolerable, yet still degraded state.

Each of several different immediate responses could produce equally *safe* outcomes, but have different effects on system efficiency, user comfort, and implementation cost MOEs. While it is desirable for an immediate response to minimize adverse transient effects, it should also avoid putting the system in a state where it is more difficult to restore normal operations. Thus, malfunction management strategy goes beyond selecting an immediate response which simply keeps the system safe. For instance, a center median or a right shoulder breakdown lane may be equally suitable locations for temporarily storing a malfunctioning vehicle. Routing the vehicle to either location might be considered as equally attractive immediate responses.   However, this vehicle may be more easily serviced from the breakdown lane in a response to restore normal operations. Therefore, routing this vehicle into the breakdown lane is the better immediate response.

For some malfunctions, it may be necessary for an immediate response to include *emergency reactions* to prevent a serious consequence. For instance, if a vehicle experiences a sudden tire blowout, that event may automatically trigger the vehicle to execute an immediate controlled stop in order to reduce the risk of an accident. In addition, this emergency reaction may include a simultaneous notification to the driver that the vehicle is performing a controlled stop, and that no participation is required from the driver.

Certain malfunctions might potentially severely impact the stability of vehicle dynamics and control. If the decision time criticality (for detection and diagnosis) of these malfunctions may require a response that is based on redundancy of this function in the vehicle.

When compared to supplemental responses, immediate responses to malfunctions can be more time critical, shorter term solutions. They can range from requesting a *driver* to bring vehicle to a full stop and then immediately exit the system under manual control, to a *vehicle* automatically routing vehicle around an in lane obstruction, to a *roadway* giving travel priority to an emergency medical response vehicle.

It is important to quickly, accurately, and reliably diagnose those malfunctions that may require time critical reactions as part of their overall malfunction response. Malfunction management will require that the AHS system have excellent models of itself, and computer resources capable to quickly evaluate current situations and near term consequences. In the absence of complete information from the diagnosis, the models should be conservative and substitute worst case parameters.

While in the process of transitioning from an unacceptable state with a high risk of severe incident to a tolerable state with reduced risk, an immediate response may introduce factors which adversely impact system performance. Malfunction responses in a system as complex as AHS cannot be guaranteed to be isolated from the rest of the system. However, favorable immediate response candidates avoid any likelihood of introducing additional risk to the system.

For example, a favorable end result may be realized from a response that removes a malfunctioning vehicle from the automated lane. However, this response may depend on the driver to perform this exiting maneuver, especially in early evolutionary stages. Depending on the surrounding conditions, different drivers cannot be expected to comply with this request in the same way. Thus transient effects should reflect the system performance risks associated with this potential noncompliance.

While an immediate response attempts to minimize the *likelihood* of an adverse impact on system operations, it is also important to factor in an immediate response's ability to reduce the *severity* of a that impact should it occur anyway.

The system needs to have a model of itself, based on the diagnosis, and quickly form a prediction of how severe the possible effects of responses under consideration could be. Could this response result in this vehicle being hit from behind, or does it have the potential to cause an accident across several lanes? The former of these two scenarios might result in some damage to two vehicles, with a negligible effect on the rest of the system, while the latter could create serious damage and shut down several lanes for a period of time.

If immediate responses do not reestablish normal operations, then additional supplemental responses may be required. Supplemental responses to malfunctions are typically more routine, longer term solutions compared to immediate responses. They can range from a *driver* traveling manually to the next access point before entering the AHS (due to a malfunctioning entry/check-in facility), to a *vehicle* which is stopped in a breakdown lane automatically paging for towing service, to a *roadway* disseminating information about an incident to upstream traffic before uninformed drivers attempt to alter their travel plans in a way that is adverse to the system.

Some supplemental responses may be more passive if the system is gradually returning to normal operations on its own. An immediate response to an incident may residually reduce system efficiency for a period of time under peak usage hours, but the system will be functioning normally as soon as traffic volume reduces during off peak hours.
Also, the system may temporarily alter the speed and headway parameters of vehicles in response to adverse weather. The system will return to normal operations as the adverse weather conditions dissipate. The immediate response may reduce system efficiency, while the supplemental response depends more on the weather than on system actions.

4.5.4 Selection of Best Malfunction Management Response Strategies

The systems engineering approach emphasizes the impact of malfunctions and their management on overall normal operations. In this context, malfunction management is a high level, crosscutting discipline. Overall system performance related measures of effectiveness (MOEs) are used to assess a malfunction's impact on normal operations. Similarly, the MOEs necessary to rate the worthiness of a particular malfunction response can be based on examining these same measures from a different perspective.

Unmanaged malfunction severity is measured by its impact on safety, system efficiency, and user comfort. These same MOE categories are now used to assess a malfunction response's ability to restore normal operations. Malfunction likelihood of occurrence is not a factor in rating malfunction responses. However, two additional performance measures are introduced to rate malfunction responses: the cost to implement a malfunction response and the likelihood of a successfully implementing that response. Malfunction responses are assessed by two criteria: transient effects on the system caused by a response and the result of a response. The malfunction response MOEs are summarized below.

The primary MOEs used to assess the results of a malfunction response are:

- malfunction response impact on safety,
- malfunction response impact on system efficiency,
- malfunction response impact on user comfort, and .
- malfunction response impact on user or system cost.

It is desirable to categorize malfunction management responses according to how promptly and completely they restore normal operations, or at least some acceptable level of system performance. For AHS applications, a malfunction management response might be measured according to system performance measures such as user cost, system cost, likelihood of successful implementation, and severity of impact on safety, system efficiency, and user comfort.

Malfunction responses were separated into two categories: immediate responses and supplemental responses. The ratings here focus on the immediate response portion of a malfunction response. It is meant to be independent of the transient effect of response ratings. It is a measure of how close the current state of the system is to normal operations. Immediate malfunction responses that return the system to normal operations are desirable, and will be rated highly in that category. The implementation cost of the response (either by the user or the system) is a relevant MOE for an immediate response. For some malfunctions, an immediate response is all that is necessary. However, for those responses that require, supplemental responses, any additional costs associated with those supplemental responses is added to the rating for overall implementation cost. Since supplemental responses are meant to restore normal operations with little implementation risk, they are not rated for implementation success likelihood or result of response effectiveness.

It is important to keep in mind that an immediate malfunction response must be rated on more than just that response's ability to return the system to normal operations. For instance, the benefits associated with a response that restores normal operations may be outweighed by the unacceptably high transient effect safety risks experienced during its implementation.

Severity of impact on normal operations is measured for both malfunctions and their responses by the same MOEs with the same rating scales. They both are defined with respect to a normal operations benchmark. The ratings of SLIGHT, MODERATE, MAJOR, SEVERE, and CRITICAL have the same meaning in both instances, however, the operating conditions that illustrate their meaning may be different. For example, user comfort may receive a MODERATE rating when the driver is first notified of a minor vehicle malfunction unrelated to vehicle dynamics and control. The result of a malfunction response that places the vehicle in the breakdown lane may receive the same MODERATE user comfort rating.

The MOE of malfunction response impact on system rates actual (not perceived) safety after an immediate malfunction response has been performed. The same ratings that defined malfunction impact on safety in Table 2 can be used here. This scale is biased towards pre-accident safety conditions. Less than a highest rating implies that the system has not returned to normal operations.

The MOE of malfunction response impact on system efficiency is concerned with system efficiency issues such as traffic flow performance and roadway accessibility after the completion of a malfunction response. The same ratings that defined malfunction impact on system efficiency in Table 3 can be used here. In addition to the four suggested categories to rate malfunctions (i.e., impact on travel speed, traffic density, travel lanes, and entry/exit access), it may be insightful to consider a malfunction response's impact on system efficiency via the time duration needed to complete the malfunction response.

The MOE of malfunction response impact on user comfort rates a typical driver's personal comfort level after a malfunction response has been performed. The same ratings that defined malfunction impact on user comfort in Table 4 can be used here. Additional considerations to rate user comfort in a malfunction response include: a change in driver functional responsibility/participation required and any change to a user's travel plans.

The MOE of malfunction response implementation cost (to user or system) rates the cost of a implementing a particular malfunction response. If the response is composed of immediate and supplemental responses, then it represents the combined cost.

Table 5 Malfunction Response Implementation Cost (to User or System)

Effect	**Criteria**
A = Slight	Negligible cost to individual user, consistent with non-AHS costs. No or negligible cost to system
B = Moderate	User may consider AHS utility before paying additional expense $ / mile installation cost; $ / mile operational cost
C = Major	Cost will limit AHS market penetration to 85 % of potential users $$ / mile installation cost; $$ / mile operational cost Reduces funding of other transportation programs.
D = Severe	Cost will limit AHS market penetration to 50 % of potential users $$$ / mile installation cost; $$$ / mile operational cost Reduces funding of other taxpayer funded programs
E = Critical	Affordable only to commercial, transit, fleet, and 10 % of general population. $$$$ / mile installation cost; $$$$ / mile operational cost Political opposition to this level of funding would be strong
N/A=Not Applicable	Not related to cost

There could be other secondary MOEs to evaluate a malfunction response. A potentially relevant MOE for malfunction response analysis relates to environmental issues. For instance, a response to a roadway malfunction that results in a system slowdown or shutdown for an extended period may result in increased vehicle emissions from heavy traffic in this vicinity. Air quality may degrade below acceptable levels. However, in this particular example, it is expected that the system efficiency MOE provides enough correlation to air quality so that environmental issues do not have to be separately rated. In other words, a response that results in major delays would be rejected due to system efficiency long before air quality issues became a concern.

The primary MOEs used to assess transient effects of malfunction responses are:

- likelihood of successful implementation
  (or rated below as the likelihood of failing to implement response),
- transient effects on safety,
- transient effects on system efficiency, and
- transient effects on user comfort.

The risks associated with the transient effects of a malfunction response cannot be overlooked. The system is operating with less than full functionality, and until an appropriate response is successfully performed that puts the system in a more stable, lower risk state, the system is potentially hazardous. Due to the anticipated short duration of an initial malfunction response, safety may play a more significant role in measuring the transient effects of impact on severity than system efficiency or user comfort. The likelihood of being able to transition the system from a high risk to lower risk state in the presence of a malfunction is also a very important measure. For instance, the system may request that a malfunctioning vehicle pull over into the breakdown lane at a time when it is already occupied (e.g., full of snow) or when no breakdown lane is available.

The MOE of transient effects of malfunction response on safety rates safety related transient effects while an immediate malfunction response is being performed. The same ratings that defined malfunction impact on safety in Table 2 can be used here.

The MOE of transient effects of malfunction response on system efficiency is concerned with system efficiency transient effects while an immediate malfunction response is being performed. The same ratings that defined malfunction impact on system efficiency in Table 3 can be used here.

The MOE of transient effects of malfunction response on user comfort rates transient effects of user comfort while an immediate malfunction response is being performed. The same ratings that defined malfunction impact on user comfort in Table 4 can be used here.

For the sake of consistency in the ratings, where A is desirable and E is not, the transient effect MOE referred to as "likelihood of successfully implementing malfunction response" is reworded as "likelihood of failing to implement malfunction response". The meaning is the same. The likelihood of failing to implement malfunction response rates the transient effect of the system's ability to perform a selected malfunction response. Table 6 presents the rating criteria for this MOE. Situational factors such as traffic density or driver compliance may impact the likelihood of failing to implement the preferred response. This scale is biased towards unlikely occurrences, i.e., it should be expected that most responses can be performed.

Table 6 Likelihood of Failing to Implement Malfunction Response

Rating	Criteria
A = Very Rare	Under automated control within single vehicle or roadway element. Response execution is independent of surroundings. Driver task that is natural and trivial to all drivers.
B = Improbable	Under automated control within several system elements. Response execution has little to do with surroundings. Driver task requires simple, routine interpretation and execution.
C = Remote	Response includes an interaction with several system elements. Response execution is rarely sensitive to surroundings. Driver task requires moderate, but typically routine interpretation and execution.
D = Occasional	Response includes moderate sequence of interactions with several system elements. Response execution is occasionally sensitive to surroundings. Driver task requires moderate interpretation and execution of potentially unfamiliar tasks.
E = Probable	Response includes complex interactions with multiple system elements. Response execution is highly sensitive to surroundings. Undesirable driver task requires skilled interpretation and execution of potentially unfamiliar tasks.
N/A=Not Applicable	Not a likelihood of failing to implement malfunction response issue.

4.6 Application of Malfunction Management Strategy

The ERSCs developed during the PSA can be used to illustrate malfunction management strategies for longitudinal and lateral control.

An overview of the malfunction response selection process as applied to the ERSCs is given in figure 4. A general understanding of a particular ERSC is developed from the description found in Volume 1 (executive summary) of this report. A top level functional analysis of operational functions establishes driver, vehicle, and roadway contributions to these operational functions. Malfunctions to these contributing elements are postulated and evaluated for potential impact on the system's normal operations. Malfunction response options are then developed and evaluated for their ability to improve the state of the system in the presence of a malfunction. Selection of the most appropriate response to a malfunction may depend on situational considerations. If no favorable assessments can be realized for a particular adverse malfunction, then a system redesign with potentially increased costs may be necessary.

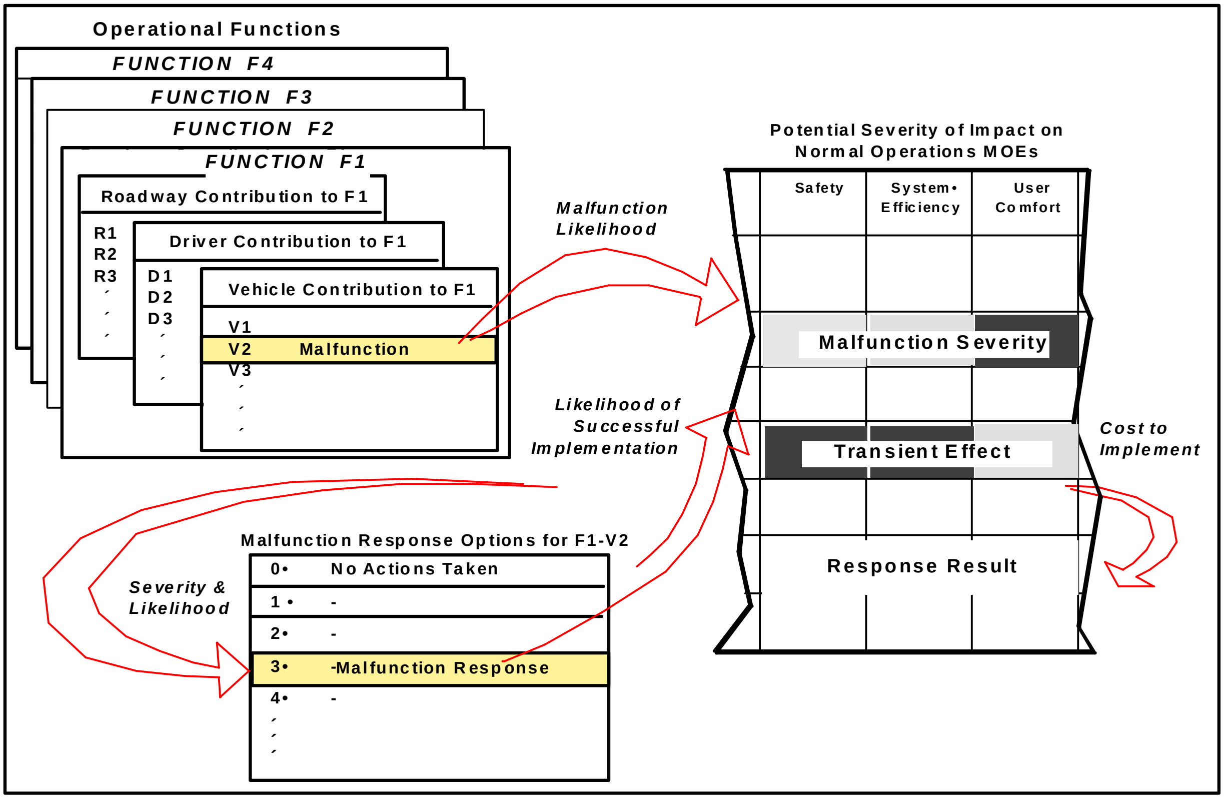


Figure 4 Malfunction Response Selection Process

4.6.1 Malfunction Analysis of Longitudinal Control

Malfunctions associated with newly automated functions which contribute to automated longitudinal control in ERSC1 are analyzed. Figure 5 pictorially presents the newly automated communication paths postulated for normal operations longitudinal control.

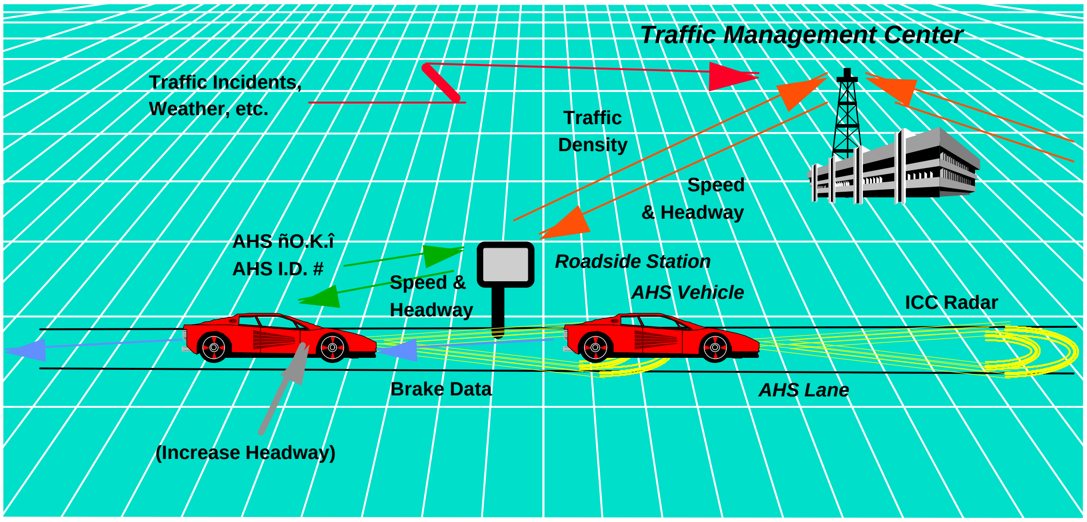
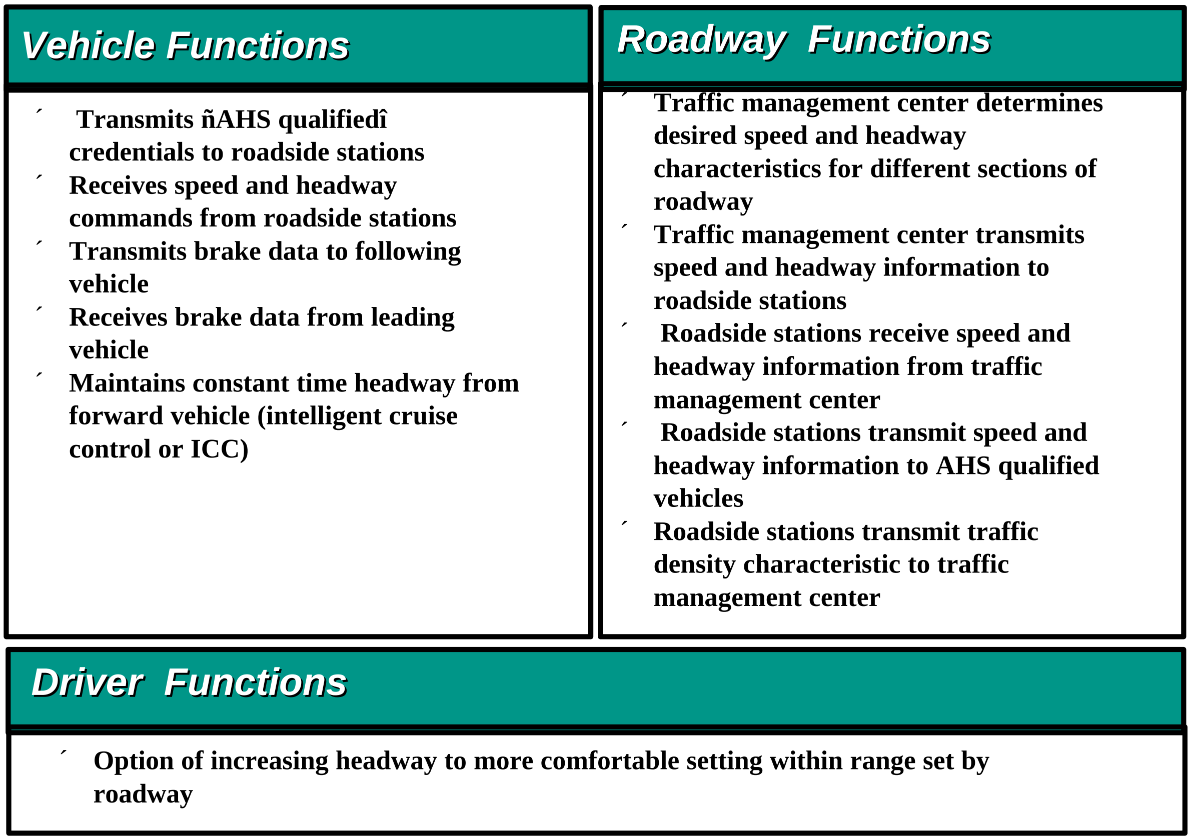


Figure 5 Communication Paths for Longitudinal Control in ERSC1

4.6.1.1 Description of Normal Operations and Operational Functions

The system functionality available for longitudinal control of vehicles in ERSC1 is described in Volume 1 (Executive Summary) and Volume 4 (Lateral and Longitudinal Control Analysis) of this report. In ERSC1, longitudinal control is a semiautomated function. An intelligent cruise control device (ICC) in the vehicle maintains automated control of vehicle speed and headway as dictated by roadway commands. The driver is still responsible for obstacle detection and avoidance, emergency stops, and lateral control. Only a single travel lane is anticipated for this configuration. Figure 6 describes individual functions residing in the roadway, vehicle, and driver elements of the system.

Under normal operations, the ICC maintains a constant time headway policy from any forward vehicle. It receives commands from the roadway, it receives brake data from the forward vehicle, and it uses sensors to measure the forward vehicle's longitudinal motion.



Vehicle Functions

- **Transmits ñAHS qualifiedî credentials to roadside stations**
- **Receives speed and headway commands from roadside stations**
- **Transmits brake data to following vehicle**
- **Receives brake data from leading vehicle**
- **Maintains constant time headway from forward vehicle (intelligent cruise control or ICC)**

Roadway Functions

- **Traffic management center determines desired speed and headway characteristics for different sections of roadway**
- **Traffic management center transmits speed and headway information to roadside stations**
- **Roadside stations receive speed and headway information from traffic management center**
- **Roadside stations transmit speed and headway information to AHS qualified vehicles**
- **Roadside stations transmit traffic density characteristic to traffic management center**

Driver Functions

- **Option of increasing headway to more comfortable setting within range set by roadway**

Figure 6 *Normal Operations* for Longitudinal Control (Speed and Headway Maintenance) in ERSC1

The traffic management center (TMC) synthesizes traffic density and entry demand information with environmental and incident information to arrive at speed and headway settings for the different sections of the roadway. The TMC transmits speed and headway settings to each roadway section.

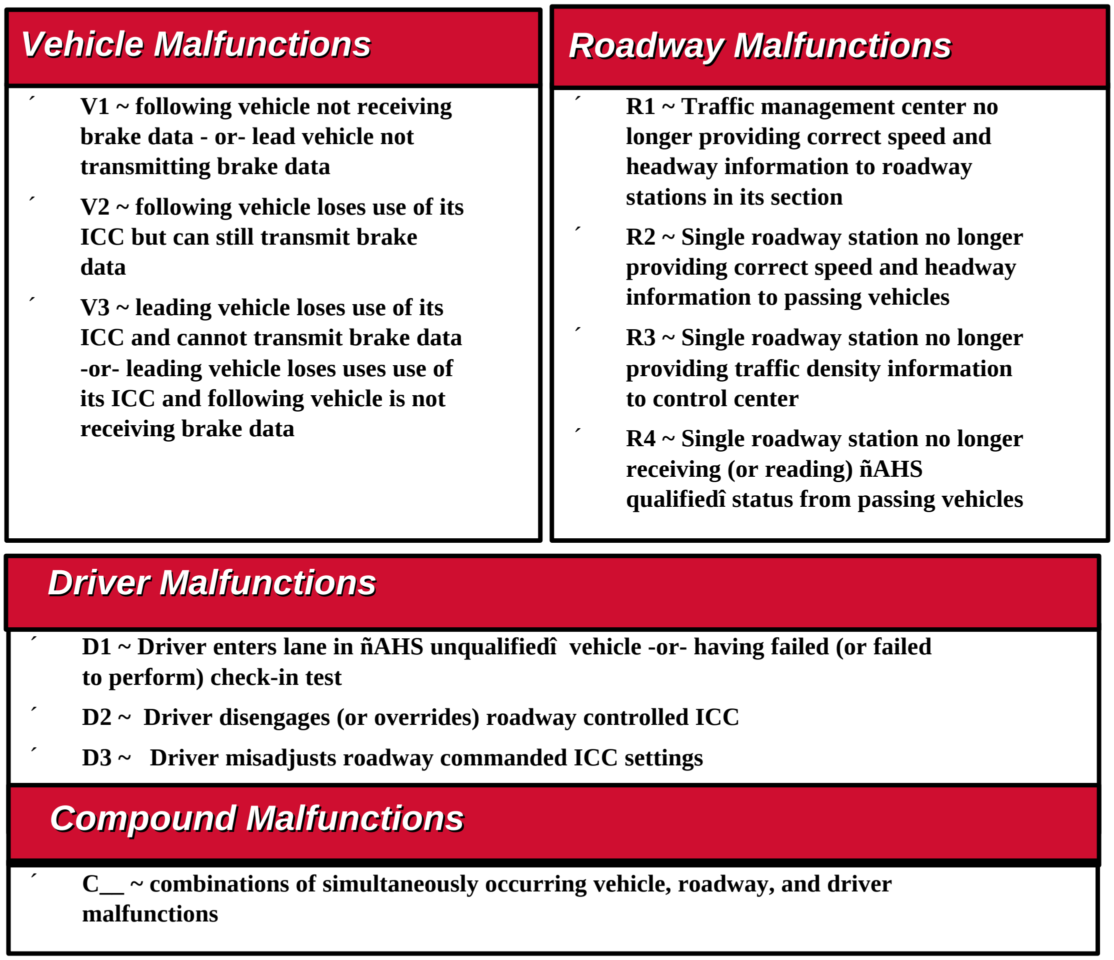
Roadside monitor stations (RMS) along each section of road interpret the information sent from the TMC and send speed and headway inputs directly to the ICCs of passing vehicles. The distance between stations is a function of desired traffic flow control and may be more frequent at or near entry and exit nodes.

The vehicle's ICC receives speed and headway inputs from the roadway (the RMS). The vehicle can fine tune the headway setting if brake data is available from the forward vehicle. The ICC then maintains this constant time headway from the forward vehicle if it is traveling at less than or equal to the desired speed. The headway is maintained by sensing the forward vehicle's acceleration/deceleration and receiving brake data from the forward vehicle.

The driver may be given the option to slightly increase the headway to a more comfortable heading within a range sent by the roadway to the ICC. Slight variations of headway will not disrupt the efficiency of the system (this will be present anyway given the differences in vehicle capabilities and availability of brake data). The driver will typically not be able to modify the speed setting (except for emergencies). A lower speed may be a more comfortable setting for some drivers, but since all upstream traffic in the single automated lane would be constrained by this speed, speed adjustments are assumed to not be allowed.

4.6.1.2 Potential Mulfunctions

Figure 7 highlights several possible malfunctions for each of the vehicle, roadway, and driver components of the system that could impact longitudinal control.



Vehicle Malfunctions

- V1 ~ following vehicle not receiving brake data - or- lead vehicle not transmitting brake data
- V2 ~ following vehicle loses use of its ICC but can still transmit brake data
- V3 ~ leading vehicle loses use of its ICC and cannot transmit brake data -or- leading vehicle loses uses use of its ICC and following vehicle is not receiving brake data

Roadway Malfunctions

- R1 ~ Traffic management center no longer providing correct speed and headway information to roadway stations in its section
- R2 ~ Single roadway station no longer providing correct speed and headway information to passing vehicles
- R3 ~ Single roadway station no longer providing traffic density information to control center
- R4 ~ Single roadway station no longer receiving (or reading) ñAHS qualifiedî status from passing vehicles

Driver Malfunctions

- D1 ~ Driver enters lane in ñAHS unqualifiedî vehicle -or- having failed (or failed to perform) check-in test
- D2 ~ Driver disengages (or overrides) roadway controlled ICC
- D3 ~ Driver misadjusts roadway commanded ICC settings

Compound Malfunctions

- C__ ~ combinations of simultaneously occurring vehicle, roadway, and driver malfunctions

Figure 7 *Potential Malfunctions* for Longitudinal Control in ERSC1

Figure 8 rates the malfunction likelihood and potential severity for the malfunctions described in Figure 7. They are categorized as vehicle, roadway, and driver malfunctions. An interpretation of the MOE rating scales is provided in Section 4.4.

	Potential Effect On Normal			
ERSC1 Malfunctions to Longitudinal Control	Safety	System Efficiency	User Comfort	Malfunction Likihood
Vehicle				
V1 ~ Brake data	C	A	A	C
V2 ~ ICC failure	E	C	A	B
V3 ~ V1 + V2	E	C	A	A
Roadway				
R1 ~ CC to stations	E	E	C	A
R2 ~ Station to vehicle	C	C	A	B
R3 ~ Station to TMC	A	B	A	C
R4 ~ Vehicle to station	B	A	A	B
Driver Malfunctions				
D1 ~ No ICC (non AHS or failed	E	C	A	B
D2 ~ Disengages	E	C	A	C
D3 ~ Misadjusts	C	C	A	D

Severity or Cost:	A Slight	B Moderate	C Major	D Severe	E Critical
Likelihood:	A Very rare	B Improbabl	C Remote	D Occassional	E Probable

Figure 8 *Potential Malfunction Impact* on Longitudinal Control in ERSC1

A brief description of *potential impact on normal operations, potential severity of result if unmanaged, malfunction likelihood, detection methods, and response options* for each of these malfunctions is now discussed. An assessment of these response options is given in Section 4.5.3 and 4.5.4.

VEHICLE MALFUNCTIONS

V1 ~ Following vehicle not receiving brake data
-or- lead vehicle not transmitting brake data

Potential impact on normal operations:

- Vehicle travels with unsafe headway (spacing). ICC still operational, so no impact on system efficiency. Driver may be unaware of malfunction, so user comfort remains high.

Potential severity of result if unmanaged:

- Collision if emergency braking required while vehicle at unsafe headway

Malfunction likelihood:

- Remote. For example, high reliability in line-of-sight transmitting and receiving communication components, but only one component needs to fail or be blocked by some obstruction (dirt, etc.).

Detection:

- Following vehicle does not receive data from forward vehicle
- Forward vehicle display reports transmitter malfunction.

Responses:

- Following vehicle ICC increases headway behind forward vehicle
- Following vehicle continues with same speed and headway

V2 ~ Following vehicle loses use of its ICC but can still transmit brake data.

Potential impact on normal operations:

- Vehicle travels with unregulated headway (spacing). Lack of ICC control, so system efficiency degraded. Driver may be unaware of malfunction, so user comfort remains high.

Potential severity of result if unmanaged:

- Collision if emergency braking required while vehicle at unsafe headway

Malfunction likelihood:

- Improbable. Criticality of ICC component results in high possible reliability. May be rarely effected by environmental interference.

Detection - for vehicle following failed vehicle:

- RMS detects vehicle without "AHS qualified" capability and informs following vehicle (transmission to ICC, warning light to driver)
- Following vehicle ICC senses erratic velocity/acceleration profile of failed leading vehicle now under manual longitudinal control (application of knowledge based systems)
- Failed vehicle communicates loss of ICC to following vehicle (would not want to rely on presence of vehicle to vehicle communication - see situation V3)

Detection - for failed vehicle:

- In vehicle display reports ICC malfunction and loss of "AHS qualified" status to driver
- Driver detects ICC malfunctioning (or using out of bounds speed and/or headway values) and manually overrides. Loss of "AHS qualified" status is reported to driver.

Response - for vehicle following failed vehicle:

- ICC significantly increases headway behind vehicle 2 and may enter into a "soft" following mode to avoid fluctuations due to manual driver in forward vehicle

Response - for failed vehicle:

- Driver assumes longitudinal control responsibilities and should increase distance from forward vehicle. Driver must exit automated lane
  a) as soon as safe exit can be performed in a continuous entry/exit configuration
  b) at the next exit ramp in a dedicated entry/exit configuration.

V3 ~ leading vehicle loses use of its ICC and cannot transmit brake data -or- leading vehicle loses ICC and following vehicle is not receiving brake data

Potential impact on normal operations:

- Vehicle travels with unregulated headway (spacing). Lack of ICC control, so system efficiency degraded. Driver may be unaware of malfunction, so user comfort remains high.

Potential severity of result if unmanaged:

- Collision if emergency braking required while vehicle at unsafe headway

Malfunction likelihood:

- Very Rare. Simultaneous malfunctions must occur.

Detection - for vehicle following failed vehicle:

- Same techniques as in V1 & V2 (except failed vehicle can not inform following vehicle of ICC failure)

Detection - for failed vehicle:

- Same techniques as in V1 and V2

Response - for vehicle following failed vehicle:

- Same as V2

Response - for failed vehicle:

- Same as V2

ROADWAY MALFUNCTIONS

R1 ~ Traffic management center (TMC) no longer providing correct speed and headway information to roadside monitor station (RMS) in its section.

Potential impact on normal operations:

- No way for vehicles to get correct information in this section of road. Multiple vehicles travel with incorrect speed and headway. Unacceptably severe safety and system efficiency concerns. If driver is unaware, user comfort remains high. Otherwise, very worrisome.

Potential severity of result if unmanaged:

- Multiple collisions if emergency braking required while vehicles at unsafe headways

Malfunction likelihood:

- Very Rare. TMC transmitters will likely have reliability equivalent to commercial radio stations. System may operate so that each RMS has access to two independent TMCs for redundant coverage.

Detection:

- RMS does not receive communication of speed and headway information from the TMC, or initial check of received information shows it to be out of bounds for AHS operations. In addition the TMC would use other lines of communication to inform affected stations of the problem.

Response:

- RMS would revert to default settings. These settings could consider time of day, permit more driver adjusting, and be station dependent (e.g., stations near entry and exit points would transmit different speed and headway commands than stations in between nodes). These settings would not result in as efficient of a system but would result in a safe system. A determination in an emergency like this has to be made as to whether the roadway can actually aid in system efficiency and safety and what additional responsibility if any should be given to the driver. In the most extreme case the automated lane would return to what is essentially a manual lane with driver aids.

R2 ~ Single RMS no longer providing correct speed and headway information to passing vehicles.

Potential impact on normal operations:

- RMS not transmitting up to date recommended values.

Potential severity of result if unmanaged:

- Multiple collisions if emergency braking required while vehicles at unsafe headways

Malfunction likelihood:

- Moderate. There are expected to be many RMSs along AHS roadways. Their close proximity to the roadside, exposure to environment, continuous use, etc. may yield an occasional failure.

Detection - for vehicles:

- Vehicles do not receive speed and headway inputs from the roadway or an initial check of received inputs show them to be out of bounds for AHS operations.

Detection - for roadway:

- Station diagnostic equipment detects transmitter malfunction.

Response - for vehicles:

- If no new inputs or errant inputs then the vehicles maintain current speed and headway, and await receipt of new instructions at next RMS.

Response - for roadway:

- RMS informs TMC of its malfunctioning state. If roadway diagnostics does not reveal the problem for some reason then a routine inspection will or a passing vehicle may call it in.

R3 ~ Single RMS no longer providing traffic density information to TMC

Non critical malfunction -

- Traffic flow control only slightly degraded by less efficient use of speed and headway settings and no safety concern. Maintenance crew dispatched to station after TMC stops receiving transmissions

R4 ~ Single RMS no longer receiving "AHS qualified" status from passing vehicles.

Non critical malfunction -

- Roadway detection and enforcement of non compliant vehicles in the automated lane requires a slightly longer time. A potential safety concern since unsafe speed and/or headway may be maintained for a longer time, however distance between RMSs is relatively small and detection will occur at RMS. Reliable manufacturing of the stations with prompt repair after malfunctioning should be sufficient.

DRIVER MALFUNCTIONS

D1 ~ Driver enters lane in "AHS unqualified" vehicle -or- having failed (or failed to have performed) check-in test

Detection - for vehicle:

- Vehicle will not be operating with "AHS qualified" status

Detection - for driver:

- If the driver is not aware that the vehicle is traveling in the automated lane without currently being "AHS qualified" (in vehicle display will show this but driver may not be paying attention) the roadway will alert the driver after passing a station (e.g., could be something as basic as flashing red lights).

Detection - for roadway:

- Roadway station does not receive "AHS qualified" signal from the vehicle

Response - for driver:

- Driver must exit the automated lane immediately or be subject to prosecution

Response - for roadway:

- Responsible for enforcing the requirement that the vehicle leave the auto lane.

D2 ~ Driver disengages (or overrides) roadway controlled ICC

Detection - for vehicle:

- Vehicle's ICC has changed modes to accept driver and not roadway commands

Detection - for driver:

- In vehicle display warns driver to re-engage roadway controlled ICC mode or "AHS qualified" status will be revoked

Detection - for roadway:

- Roadway station does not receive "AHS qualified" signal from the vehicle

Response - for vehicle:

- "AHS qualified" status is revoked

Response - for driver:

- Driver must re-engage roadway controlled ICC mode immediately or exit the automated lane

Response - for roadway:

- Responsible for enforcing the requirement that the vehicle leave the auto lane if its ICC is no longer accepting roadway commands

D3 ~ Driver misadjusts roadway commanded ICC settings.

Detection - for vehicle:

- Vehicle determines that its current speed or headway is out of the legal bounds currently being sent by the roadway

Detection - for driver:

- In vehicle display warns driver to readjust the ICC settings or "AHS qualified" status will be revoked

Detection - for roadway:

- Roadway station does not receive "AHS qualified" signal from the vehicle

Response - for vehicle:

- ICC may not allow driver to change settings outside of roadway limits without the driver disengaging from roadway controlled ICC mode (see D2) to avoid accidental misadjustments

Response - for driver:

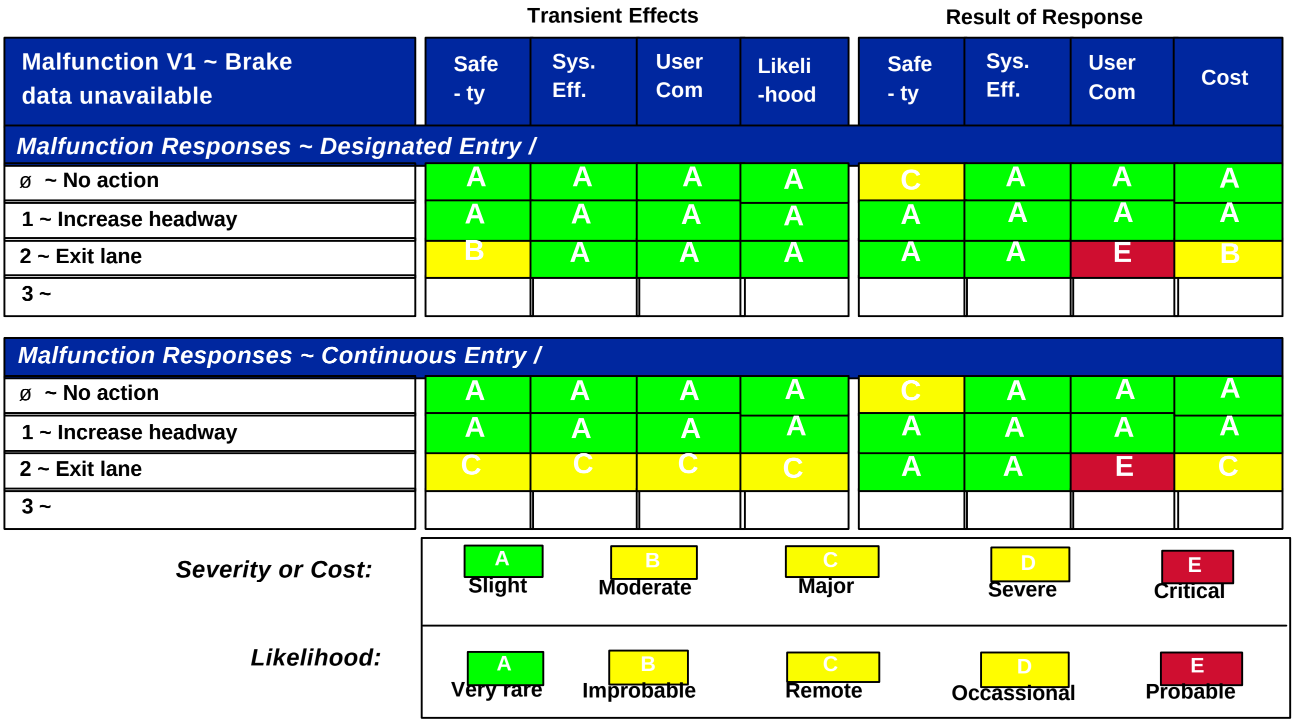
- Driver must readjust ICC settings to be within the roadway commanded limits or leave the auto lane

Response - for roadway:

- Responsible for enforcing the requirement that the vehicle leave the auto lane if its ICC is being misused

4.6.1.3 Assessment of Malfunction Response Options (Transient Effects and Response Results)

Figure 9 highlights the relative effectiveness of several potential response options to a longitudinal control malfunction (brake data unavailable) in the partially automated ERSC1. The same response options are rated under two different operating situations. In one case, the malfunction occurs in a facility with designated entry/exit points, i.e., AHS access occurs at specific points along the roadway. The other case is a malfunction on a facility with continuous entry/exit points so that transitions between AHS and non-AHS lanes can occur anywhere along the roadway.



	Transient Effects				Result of Response			
Malfunction V1 ~ Brake data unavailable	Safe - ty	Sys. Eff.	User Com	Likeli -hood	Safe - ty	Sys. Eff.	User Com	Cost
Malfunction Responses ~ Designated Entry /								
ø ~ No action	A	A	A	A	C	A	A	A
1 ~ Increase headway	A	A	A	A	A	A	A	A
2 ~ Exit lane	B	A	A	A	A	A	E	B
3 ~								
Malfunction Responses ~ Continuous Entry /								
ø ~ No action	A	A	A	A	C	A	A	A
1 ~ Increase headway	A	A	A	A	A	A	A	A
2 ~ Exit lane	C	C	C	C	A	A	E	C
3 ~								

	A	B	C	D	E
Severity or Cost:	Slight	Moderate	Major	Severe	Critical
Likelihood:	Very rare	Improbable	Remote	Occassional	Probable

Figure 9 ***Potential Malfunction Responses*** **for Longitudinal Control** ***Malfunction V1*** **in ERSC1**

Response option _ (no action)

Transient effects and response results in a facility with designated entry/exit access points

- When braking capability of leading vehicle is unknown, it is possible that it could brake in a shorter distance than the following vehicle. If an emergency braking situation arises, the leading vehicle could stop before the following vehicle comes to a complete stop, and an accident would result.

Transient effects and response results in a facility with continuous entry/exit access points

- Same as in designated entry/exit access point case. No difference due to roadway configuration.

Response option 1 (increase headway)

Transient effects and response results in a facility with designated entry/exit access points

- When braking capability of leading vehicle is unknown, increasing headway to some default safe value should be a sufficient response to this malfunction. It restores safety. Since vehicle travel speeds should be about the same, the added gap between two vehicles (not all vehicles) will have an inconsequential impact on system efficiency. Also, cost is minimal since response is generated with existing system functionality. There are no significant transient effects from this response.

Transient effects and response results in a facility with continuous entry/exit access points

- Same as in designated entry/exit access point case. No difference due to roadway configuration.

Response option 2 (exit lane)

Transient effects and response results in a facility with designated entry/exit access points

- This response results in the restoration of safety and system efficiency, but it is inconvenient to the user who must exit. There may be an associated system cost to monitor/enforce vehicle departure from facility. In a designated facility, safety may be a concern if decision occurs near an exit facility and the response time is minimal.

Transient effects and response results in a facility with continuous entry/exit access points

- Same results as for designated case except that cost may be still higher due to more difficult verification/enforcement in facility where vehicles access to system does not occur at specific check points. Vehicle could exit and then reenter a short while later. There are more transient response concerns in a continuous entry/exit facility. Vehicle/driver may attempt to exit, but cannot find a suitable gap in the manual lanes. Vehicle may try to speed up, slow down, or loiter in lane while trying to exit.

Figure 10 highlights the relative effectiveness of several potential response options to a longitudinal control malfunction (ICC failure) in the partially automated ERSC1. The same response options are rated under two different operating situations. In one case, the malfunction occurs in a facility with designated entry/exit points, i.e., AHS access occurs at specific points along the roadway. The other case is a malfunction on a facility with continuous entry/exit points so that transitions between AHS and non-AHS lanes can occur anywhere along the roadway.

Malfunction V2 ~ ICC Failure	Transient Effects				Result of Response			
	Safe - ty	Sys. Eff.	User Com	Likeli -hood	Safe - ty	Sys. Eff.	User Com	Cost
Malfunction Responses ~ Designated Entry / Exit								
ø ~ No action	A	A	A	A	E	C	A	A
1 ~ Increase headway	A	A	A	A	C	C	A	A
2 ~ Exit lane	B	A	A	A	A	A	E	B
3 ~								
Malfunction Responses ~ Continuous Entry / Exit								
ø ~ No action	A	A	A	A	E	C	A	A
1 ~ Increase headway	A	A	A	A	C	C	A	A
2 ~ Exit lane	C	C	C	C	A	A	E	C
3 ~								

Severity or Cost:	A Slight	B Moderate	C Major	D Severe	E Critical
Likelihood:	A Very rare	B Improbable	C Remote	D Occassional	E Probable

Figure 10 ***Potential Malfunction Responses*** **for Longitudinal Control** ***Malfunction V2*** **in ERSC1**

Response option _ (no action)

Transient effects and response results in a facility with designated entry/exit access points

- ICC operation is critical to safe efficient operation. User comfort may be satisfied if failure has not resulted in noticeable vehicle dynamics deviations.

Transient effects and response results in a facility with continuous entry/exit access points

- Same as in designated entry/exit access point case. No difference due to roadway configuration.

Response option 1 (increase headway)

Transient effects and response results in a facility with designated entry/exit access points

- Increasing headway to some default safe value is an insufficient response to this malfunction. While safe clearance to malfunctioning vehicle improves safety, vehicle is still a hazard to itself. Also, cost is minimal since response is generated with existing system functionality. There are no significant transient effects from this response.

Transient effects and response results in a facility with continuous entry/exit access points

- Same as in designated entry/exit access point case. No difference due to roadway configuration.

Response option 2 (exit lane)

Transient effects and response results in a facility with designated entry/exit access points

- This response results in the restoration of safety and system efficiency, but it is inconvenient to the user who must exit. There may be an associated system cost to monitor/enforce vehicle departure from facility. In a designated facility, safety may be a concern if decision occurs near an exit facility and the response time is minimal.

Transient effects and response results in a facility with continuous entry/exit access points

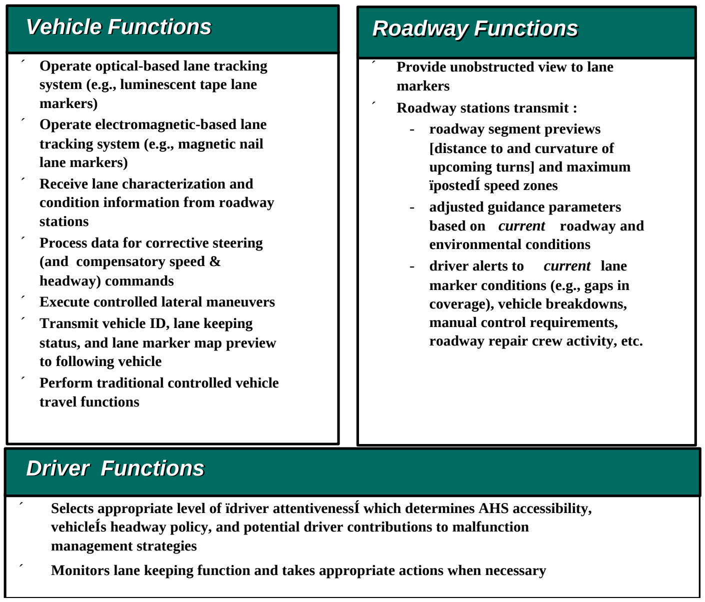
- Same results as for designated case except that cost may be still higher due to more difficult verification/enforcement in facility where vehicles access to system does not occur at specific check points. Vehicle could exit and then reenter a short while later. There are more transient response concerns in a continuous entry/exit facility. Vehicle/driver may attempt to exit, but cannot find a suitable gap in the manual lanes. Vehicle may try to speed up, slow down, or loiter in lane while trying to exit.

4.6.2 Malfunction Analysis of Lateral Control in ERSC3

Malfunctions associated with newly automated functions which contribute to automated lateral control in ERSC3 are analyzed in the following subsections.

4.6.2.1 Description of Normal Operations and Operational Functions

The system functionality available for lateral control (lane keeping) of vehicles in ERSC3 is described in Volume 1 (Executive Summary) and Volume 4 (Lateral and Longitudinal Control Analysis) of this report. In ERSC3, lateral control is an automated function. Lane keeping is a time critical function: a complete loss in its functionality results in a highly unacceptable state due to safety concerns. For this reason, redundancy is built into the design. Two independent systems track the vehicle in the lane: a system which is guided by magnetic nails embedded in the road, and another completely independent system which optically senses lane markers. Only a single travel lane is anticipated for this configuration. Figure 11 describes how individual operational functions are allocated to the roadway, vehicle, and driver elements of the system.



Vehicle Functions

´ Operate optical-based lane tracking system (e.g., luminescent tape lane markers)

´ Operate electromagnetic-based lane tracking system (e.g., magnetic nail lane markers)

´ Receive lane characterization and condition information from roadway stations

´ Process data for corrective steering (and compensatory speed & headway) commands

´ Execute controlled lateral maneuvers

´ Transmit vehicle ID, lane keeping status, and lane marker map preview to following vehicle

´ Perform traditional controlled vehicle travel functions

Roadway Functions

´ Provide unobstructed view to lane markers

´ Roadway stations transmit :

- roadway segment previews [distance to and curvature of upcoming turns] and maximum ïpostedÍ speed zones
- adjusted guidance parameters based on *current* roadway and environmental conditions
- driver alerts to *current* lane marker conditions (e.g., gaps in coverage), vehicle breakdowns, manual control requirements, roadway repair crew activity, etc.

Driver Functions

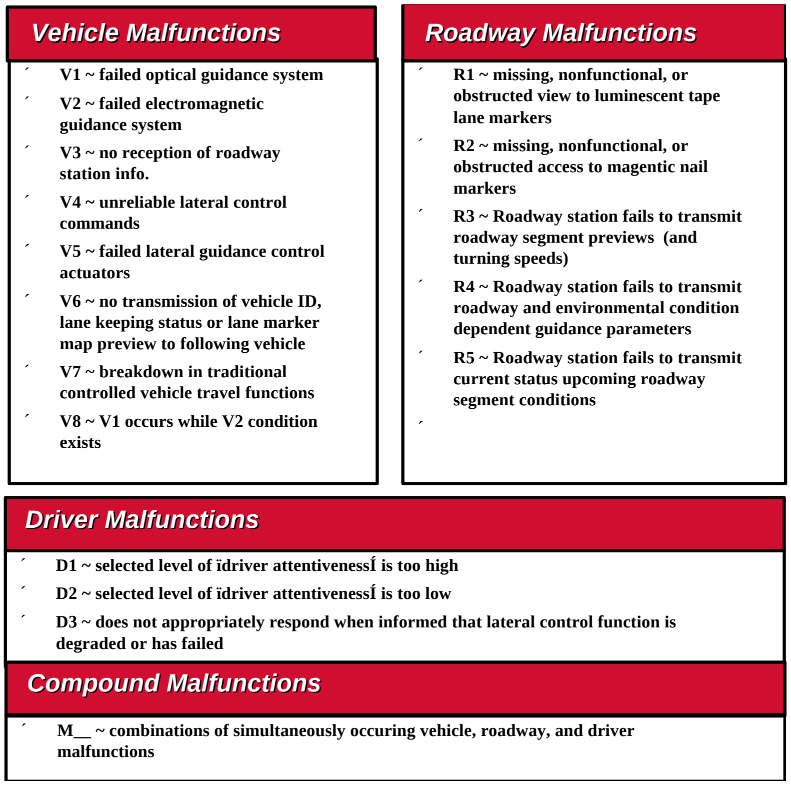
´ Selects appropriate level of ïdriver attentivenessÍ which determines AHS accessibility, vehicleÍs headway policy, and potential driver contributions to malfunction management strategies

´ Monitors lane keeping function and takes appropriate actions when necessary

Figure 11 *Normal Operations* for Lateral Control (Lane Keeping) in ERSC3

4.6.2.2 Potential Malfunctions

Figure 12 highlights several possible malfunctions for each of the vehicle, roadway, and driver components of the system that could impact lateral control in ERSC3.



Vehicle Malfunctions

- **V1 ~ failed optical guidance system**
- **V2 ~ failed electromagnetic guidance system**
- **V3 ~ no reception of roadway station info.**
- **V4 ~ unreliable lateral control commands**
- **V5 ~ failed lateral guidance control actuators**
- **V6 ~ no transmission of vehicle ID, lane keeping status or lane marker map preview to following vehicle**
- **V7 ~ breakdown in traditional controlled vehicle travel functions**
- **V8 ~ V1 occurs while V2 condition exists**

Roadway Malfunctions

- **R1 ~ missing, nonfunctional, or obstructed view to luminescent tape lane markers**
- **R2 ~ missing, nonfunctional, or obstructed access to magentic nail markers**
- **R3 ~ Roadway station fails to transmit roadway segment previews (and turning speeds)**
- **R4 ~ Roadway station fails to transmit roadway and environmental condition dependent guidance parameters**
- **R5 ~ Roadway station fails to transmit current status upcoming roadway segment conditions**

Driver Malfunctions

- **D1 ~ selected level of ïdriver attentivenessÍ is too high**
- **D2 ~ selected level of ïdriver attentivenessÍ is too low**
- **D3 ~ does not appropriately respond when informed that lateral control function is degraded or has failed**

Compound Malfunctions

- **M__ ~ combinations of simultaneously occuring vehicle, roadway, and driver malfunctions**

Figure 12 *Potential Malfunctions* for Lateral Control in ERSC3

Figure 13 rates the malfunction likelihood and potential severity for the malfunctions described in Figure 12. They are categorized as vehicle, roadway, and driver malfunctions. An interpretation of the MOE rating scales is provided in Section 4.4.

Potential Effect On Normal Operations

ERSC3 Malfunctions to Lateral Guidance Control	Safety	System Efficiency	User Comfort	Malfunction Likelihood
Vehicle Malfunctions				
V1 ~ optical guidance system	B	A	B	A
V2 ~ E-mag guidance system	B	A	B	A
V3 ~ no roadway station info.	C	A	C	B
V4 ~ lateral guidance controller	E	E	E	A
V5 ~ lateral control actuators	E	E	E	A
V6 ~ commo to following vehicle	D	B	C	A
V7 ~ mechanical functions	E	E	E	A
V8 ~ V1 while V2 exists	E	E	E	A
Roadway Malfunctions				
R1 ~ optical tape lane markers	B	B	A	C
R2 ~ magnetic lane markers	B	B	A	B
R3 ~ roadway segment preview	C	B	B	A
R4 ~ roadway & envr. conditions	C	C	C	B
R5 ~ driver alerts	D	C	D	C
Driver Malfunctions				
D1 ~ ïattentivenessÍ too high	D	A	D	D
D2 ~ ïattentivenessÍ too low	A	B	C	C
D3 ~ no response to request	E	E	E	A

Severity or Cost:	A Slight	B Moderate	C Major	D Severe	E Critical
Likelihood:	A Very rare	B Improbable	C Remote	D Occassional	E Probable

Figure 13 ***Potential Malfunction Impact*** **on Lateral Control in ERSC3**

4.6.2.3 Assessment of Malfunction Response Options to Lateral Control Malfunctions in ERSC3 (Transient Effects and Response Results)

Figure 14 highlights the relative effectiveness of several potential response options to a lateral guidance control malfunction in the partially automated ERSC3. In this case, the postulated malfunction addressed is to the optical guidance system in the vehicle which tracks lane reference markers and is responsible for lane keeping in this ERSC. Lane keeping is a time critical function: a complete loss in its functionality results in a highly unacceptable state due to safety concerns. For this reason, redundancy is built into the design. It is assumed that the other postulated lane keeping system (vehicle tracking magnetic nails imbedded in road surface) is fully functional at the time of the optical system failure.

	Transient Effects				Result of Response			
Malfunction V1 ~ failed optical guidance system	Safety	Sys. Eff.	User Com	Likelihood	Safety	Sys. Eff.	User Com	Cost
Malfunction Management Strategies								
ø ~ No action	B	A	B	C	E	C	C	A
1 ~ Stop vehicle & tow	B	E	E	C	A	A	E	B
2 ~ Redundant component	B	A	B	B	A	A	A	C
3 ~ Manual steering (ERSC1)	D	C	D	C	B	C	D	A
4 ~ Exit automated lane	C	B	B	C	A	A	E	A
5 ~ Automated reduced speed	A	C	C	A	B	E	E	A
6 ~								

Severity or Cost:	A Slight	B Moderate	C Major	D Severe	E Critical
Likelihood:	A Very rare	B Improbable	C Remote	D Occassional	E Probable

Figure 14 ***Potential Malfunction Responses*** **for Lateral Control** ***Malfunction V1*** **in ERSC3**

Response option _ (no action)

Response result:

- Response option _ (no action) may result in a system could otherwise operate quite benignly with the magnetic tracking system for an indefinite period of time. However, the system is unacceptably dependent on a single lane keeping system, and there would be serious safety concerns if the vehicle's magnetic nail tracking system failed or if the nail markers were somehow obstructed from the tracking system.

Transient effect:

- There would be few immediate serious transient effects from this non response, except that knowledge of the malfunction may make some drivers engage in undesirable responses.

Response option 1 (stop vehicle and tow)

Response result:

- Response option 1 (stop vehicle and tow) prevents the malfunction from causing a safety concern and eventually removes the problem from the system. The response result restores normal operations to the system at the expense of inconveniencing the malfunctioning vehicle's passengers (travel plans not satisfied) and the minor system cost of dispatching a tow truck to the scene.

Transient effect:

- While the response result may be an acceptable option, the transient effects of this response in a heavy traffic environment may be intolerable. ERSC3 is depicted as a single lane configuration. A stopped vehicle in the lane for any significant time would critically impact system efficiency and the user comfort of many. Such a disturbance to the system could introduce safety concerns unrelated to the original malfunction.

Response option 2 (switch over to redundant component)

Response result:

- Response option 2 (switch over to redundant component) which restores full normal operations is a desirable option as long as it is not overly costly to the vehicle design.

Transient effect:

- There may be some transient effects concerns. Likelihood of successful implementation of this response may be a minor concern if is possible that same failure could exist in backup part. The actual switch over to the backup component could introduce minor transients with user comfort and safety.

Response option 3 (manual steering, like falling back to ERSC1)

Response result:

- The end result of response option 3 (manual steering, like falling back to ERSC1) is a single vehicle performing manual lane keeping in a system otherwise occupied by vehicles under automated lane keeping control. This requires the driver to perform a function that he or she had not planned on, but still allows them to realize their travel needs. Sufficient safety should be gained with an altered speed and headway policy for this vehicle, and this could adversely impact system performance if the current ERSC3 travel conditions allowed for fast travel at high traffic densities.

Transient effect:

- This response has severe safety concerns in the transient response of implementing the strategy. The transient effects of this response are a concern because the driver may not be immediately fit to respond to the system request to resume manual control. This issue and the uncertainty of driver compliance rates this a severe user comfort concern. Also, safety is a severe concern here. Under normal check-out operations, transition to manual control happens at planned times and locations known to the system and driver. In this case, the notice could be rather sudden, and after transition the vehicle stays in the lane.

Response option 4 (exit automated lane)

Response result:

- Response option 4 (exit automated lane) yields similar results as response option 1. In this case though, it is less costly to the system for the vehicle/driver to exit without further assistance from the roadway. User comfort is still unacceptable due to unsatisfied travel plans.

Transient effect:

- The transient effects associated with executing this response may be tolerable. If the vehicle/driver can exit relatively promptly under their own control, safety risk (which grows with time in this case) should not be too serious. This response is considered to be less time critical than response option 3, so user comfort and system efficiency impact during the transition are expected to be tolerable. There may be a concern with the vehicle/driver compliance or ability to exit the system on a short notice. For instance, traffic congestion at exit may prevent or delay the response's implementation.

Response option 5 (automated reduction in vehicle speed)

Response result:

- Response option 5 (automated reduction in vehicle speed) may restore safety to the system if speed is sufficiently reduced to make reliance on the magnetic system alone is more reliable and tolerable (e.g., if a missed track occurs, there is sufficient reaction time to bring vehicle to immediate stop).

Transient effect:

- However, in a single lane deployment, this results in an unacceptable impact on system efficiency, user comfort, and the comfort of any unlucky user who managed to get stuck behind this nuisance.

5.0 CONCLUSION

The following key findings and conclusions have been reached concerning AHS Malfunction Management and Analysis.

- A complete set of malfunction management strategies will balance the desire to have the system perform without failing with the need to respond to failure when it inevitably occurs, within the constraints imposed by safety, system efficiency, user comfort, and cost.

- A complete evaluation of malfunction management options includes cost/benefit tradeoffs between the preventative reduction in the probability of malfunction occurence and the responsive reduction in the severity of the malfunction given its occurrence.

- The time criticality and potential severity of certain malfunctions preclude dependence on system responses once the malfunction occurs. In these instances the malfunction management strategy must rely on built in redundancies either in the vehicle or roadway infrastructure.

- Reliance on the driver (perceptions, capabilities, predictability, and accountability) for malfunction prevention, detection, diagnosis, and execution of management tasks is a risk/challenge.

- Certain malfunctions do not lend themselves to a straight forward methodological breakdown. The complexity of the AHS assures that malfunction management will be a continuously evolving process.

- The transient effects of a particular management response may outweigh the benefits gained by its implementation.

- The systems engineering approach of functional analysis provides a complete framework around which to define the normal operations of an AHS.

- The best method for identifying a malfunction is for the identification process to occur as close to the source as possible. This is beneficial in that it increases the probability of detection and diagnosis while reducing the time from when the event occurs to when it is detected.

- Based on their criticality and reliability, functions need not have the same frequency for detecting failures (polling). Continuous monitoring can be accomplished through the use of built in test (BIT). Diagnostic tests can be programmed into the system to occur at appropriate or opportune times such as engine start up. Regular inspections of subsystems can also be scheduled. Additionally, observations of operational deviations can be indicative of malfunctions that were not directly detected by diagnostic means. For instance, a vehicle's malfunctioning speed controller could be observed by the driver, another vehicle, or even the roadway.

- The appropriate MOEs to evaluate the merit of individual managing strategies are safety, efficiency of the system, user comfort, and cost. Safety should include a reduction in the likelihood of an accident and a reduction in the severity of an accident (personal injury and property damage). The system efficiency must include the reduction in the likelihood of disruption to the system and a reduction in the effects on the system given a disruption. User comfort rates the desirability of the service provided from the perpective of a typical potential system user. Cost includes the additional cost required to implement the strategy considering both vehicle and infrastructure. This last factor could impact other areas such as market penetration. Other secondary MOEs exist, but many are less quantifiable and result from improvements concerning the primary MOEs (i.e., improved system efficiency also results in improved air quality and user desirability). Further, caution must be exercised when developing the MOEs that sight of the key parameters effecting the system is not lost and that so many MOEs are involved that decision making becomes cumbersome.

- The final step is the development of strategies to mitigate malfunctions. Situational factors must be considered in order to select the most appropriate malfunction management response. Certain malfunctions may have several feasible response options. No single malfunction management response to a particular malfunction may be the most appropriate under all conditions. Situational factors such as the local roadway configuration, incident response vehicle availability, traffic and weather conditions, driver capability, etc., may weigh more heavily into a more optimal, adaptive response selection decision process. Therefore, appropriate information about these factors must be made available at the point where the decision is made.

- In addition to considering the situation in which the malfunction occurs, the transient effects of a particular management response may outweigh the benefits to be gained by its implementation.