Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

AHS PSA Contract Overview

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-96-047
January 1996

FOREWORD

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

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

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

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

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

NOTICE

Technical Report Documentation Page

1. Report No. FHWA-RD-96-047	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS AHS PSA Contract Overview		5. Report Date January 1996 6. Performing Organization Code
7. Author(s) R. Aikawa, L. Clare		8. Performing Organization Report No.
9. Performing Organization Name and Address Rockwell International 3370 Miraloma Ave. Anaheim, CA 92803-3150		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFH61-93-C-00201
12. Sponsoring Agency Name and Address Federal Highway Administration Turner-Fairbank Highway Research Center 6300 Georgetown Pike, HSR-10 McLean, Virginia 22101		13. Type of Report and Period Covered Final Report 9/93 - 11/94 Resource Materials 14. Sponsoring Agency Code
15. Supplementary Notes Contracting Officer's Technical Representative (COTR) – J. Richard Bishop		

16. Abstract

This report documents the three Rockwell Precursor Systems Analyses of automated Highway Systems tasks of Lateral and Longitudinal Control Analysis, Malfunction Management and analysis, and Vehicle Operations analysis.

The overall goal of the Lateral and Longitudinal control analysis task included performing system operational analyses in terms of safety and capacity and identifying issues and risks regarding the fundamental operations and maneuvers of vehicle control in a fully automated highway environment.

The overall goal of the Malfunction Management and Analysis task included defining the boundaries of an AHS, establishing functional requirements, and suggesting potential configuration. then developing operational sequences through which functions are executed and identifying allocated subsystems were performed. Metrics to gauge severity levels of malfunctions were developed and used to asses malfunctions. similarities and differences between malfunctions and system configurations were examined to develop strategies to mitigate or avoid malfunctions and to raise issues and risks involved with the AHS.

The overall goal of the Vehicle Operations Analysis task was to identify issues and risks associated with a fully automated AHS vehicle. the primary issues that were addressed were related to vehicle-infrastructure functional decomposition, performance requirements, fail-safety and criticality, communications, self-monitoring and self-diagnosis technology, and overall vehicle management

17. Key Words Automated Highway Systems Intelligent Vehicle Highway System		18. Distribution Statement No restrictions. This document is available to the public through the National Technical Information Services, Springfield, Virginia 22161.	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 36	22. Price

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

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

Table of Contents

List of Figures

List of Tables

1. EXECUTIVE SUMMARY OF ALL ACTIVITY AREAS

This report documents the three Rockwell Precursor Systems Analyses of Automated Highway Systems tasks of Lateral and Longitudinal Control Analysis, Malfunction Management and Analysis, and Vehicle Operations Analysis.

The development of the Automated Highway System (AHS) is recognized as a major component in the Intelligent Vehicle/Highway Systems (IVHS) framework. This component will have a broad impact on the highway system in terms of improved safety and reduced congestion. It will provide for reduced emissions while increasing traffic flow. Trip time will be decreased as a result of coordinated, efficient traffic integration and higher safe speeds.

The AHS will require advanced sensing, processing, and actuation developments to be successful. A thorough analysis of these elements of AHS must be conducted to identify the system requirements and the issues and risks inherent in its development and implementation.

1.1 LATERAL AND LONGITUDINAL CONTROL ANALYSIS

The overall goal of this task included performing system operational analyses in terms of safety and capacity and identifying issues and risks regarding the fundamental operations and maneuvers of vehicle control in a fully automated highway environment.

1.1.1 Approach

To insure practical and meaningful results of the analysis, a four step approach was adopted. These four steps are: (1) define system configurations on the basis of the PSA AHS requirements provided in the BAA guidelines, (2) define basic vehicle operations and maneuvers required for the defined system configurations, (3) perform generic analysis on each operation and maneuver, and (4) identify issues and risks from the analyses. The detailed system configurations are described in terms of four Representative Systems Configurations (RSCs). The basic operations and maneuvers required, thus studied in the report, are: headway maintenance including safety formulation; lane change maneuver including lane holding, lane entry/exit, and roadway entry/exit; platoon formation, obstacle avoidance, and automated traffic stream stability.

1.1.2 Results and Issues

<u>Headway Maintenance</u>

Safety distance between two vehicles depends upon many deterministic as well as random factors, e.g., vehicle velocities, brake capabilities, road condition, tires, and weather. Safety distance may be able to be established adaptively in real time, if we know what constitutes safety apriori.

Safety distance can be defined according to two basic principles: no impact and limited impact. No impact principle states that the safety distance is the minimum distance required at which the rear vehicle will not impact the front vehicle when it decelerates suddenly. The limited impact principle states that the safety distance is the maximum distance required at which the impact energy is under a certain threshold when the front vehicle decelerates suddenly.

Lane Change Maneuver

An intuitively robust, but inefficient, lane change maneuver process seems to be possible if gap making in the receiving lane and speed matching are both done by slowing down the pertinent vehicles.

While the efficiency of a lane change maneuver can be optimized, given a particular traffic condition, the optimization is often accomplished at the expense of system robustness. The trade off between efficiency and robustness requires careful analysis, tuning, and tests in the future.

A transition lane between automated and manual lanes seems to be necessary to warrant a fully automated lane change maneuver from auto to manual, assuming only automated vehicles are allowed in the transition lane.

Platoon Formation

There does not appear to be a compelling rationale for having the front platoon actively participate in the merging of two platoons. An active front platoon would imply system complexity beyond AICC with information simultaneously flowing both forward and backward between the platoons. This would create two-way dynamic coupling that could be generally undesirable.

It is important to distinguish between nominal merge conditions, which would apply to the majority of platoon formations, and special cases, which will occur relatively rarely (emergency and failure cases). Platoon formation will always be an optional activity performed for traffic flow efficiency and not specifically to enhance safety. Thus, aborting a platoon merge probably will be the correct strategy for many, if not most, off-nominal conditions. The nominal merge control design should not be compromised to allow platoon formation under off-nominal conditions where the maneuver could and should be aborted.

The nominal merge maneuver should be addressed as a constrained trajectory optimization problem, if a relevant cost function is identified. A minimum time maneuver is a possibility, but not a compelling one, since elapsed times for a merge maneuver will be much shorter than useful platoon "half-lives". Thus, minimum time maneuvers are primarily of interest as reference maneuvers. Maximizing safety and passenger comfort is much more important.

Obstacle Avoidance

Currently the most important question concerning AHS obstacle avoidance is the discrete control strategy for determining if a vehicle should maneuver around an obstacle or simply remain in its current lane and brake .

The basic discrete lane change decision algorithm can be based on comparison of estimates of the expected costs of: (1) remaining in the lane and possibly impacting the object or, (2) maneuvering around the obstacle and possibly colliding with a vehicle in an adjacent lane.

The key uncertainties in the lane change decision problem, both for analysis and real-time systems, are the statistical distributions of the properties of the population of random objects that can be expected to appear on highways. The object properties of interest, in order of decreasing importance, are size, density, and effective structural stiffness. Relevant statistical data is not readily available.

The lane change decision problem for an automatic system is fundamentally the same as that for a human driver. However, in addition to simply detecting an object in the roadway, human drivers apparently apply, with various degrees of competence, subtle identification schemes to predict the danger of impacting the object. These probably involve cues from size, shape, color, and motion compared to a "knowledge-base" of likely highway objects. Achieving this capability in sensor processing for an automatic system can be expected to be a major challenge and a critical path in AHS development.

The primary need for future research in this area is better characterization of the population of random objects that can be expected to appear on highways (AHS highways in particular). Statistical distributions of (in order of decreasing importance) size, density, and effective stiffness should be obtained. Reasonable empirical data could probably be obtained from state highway departments and highway patrols.

Stream Stability

There is a general consensus that if communications links are provided so that each vehicle in a platoon obtains continuous information regarding the motion of the lead vehicle, then stability of the platoon can be sustained indefinitely. The issue is the impact on the safety of the platoon in the event of sudden failure of the communications system.

It has been found that the effect on the traffic flow of vehicles entering and exiting the AHS effects must be accounted for in deriving the potential flow capacity increase benefits of an AHS, as well as used in any on-ramp flow control (to ensure the system is not overloaded).

The AHS, like any road traffic system, is representative of a complex dynamic system, in which many entities interact asynchronously based on local information and nonlinear rules of operation. Analysis and prediction in such systems are generally intractable, much like predicting the weather (which can be chaotic in the sense of sensitive dependence on initial conditions). Newly emerging concepts in the field of complex systems theory will need to be applied to bound the problem of performance evaluation, and ensure stable conditions will prevail.

It seems clear that in the AHS, the coupling among vehicles will necessarily be increased. Thus, when an incident occurs, the effects will be much more widespread both in the number affected and the spatial extent. While one approach is to emphasize the rapid removal of problems, we feel that at least concurrent with this must be a careful design that ensures that the AHS is not too brittle, wherein every small disturbance is felt by every vehicle in a large region.

1.2 MALFUNCTION MANAGEMENT AND ANALYSIS

The overall goal of this task included defining the boundaries of an AHS, establishing functional requirements, and suggesting potential configuration. Then developing operational sequences through which functions are executed and identifying allocated subsystems were performed. Metrics to gauge severity levels of malfunctions were developed and used to assess malfunctions. Similarities and differences between malfunctions and system configurations were examined to develop strategies to mitigate or avoid malfunctions and to raise issues and risks involved with the AHS.

1.2.1 Approach

A six-step approach was used to perform this analysis. These six tasks were arranged to maximize the timing of the effort and what information is required before beginning the next task. In addition, the utilization of Statemate is indicated in the shaded boxes. The requirements analysis effort was conducted prior to the actual tasks of this study. Following, tasks 1, 2, and 3 were performed in parallel since there is little interrelationship between them with task 1 to define measures of effectiveness, task 2 to define AHS operations and modes of operation, and task 3 to formulate major system categories for malfunction breakdown. Task 4 requires the analysis to be performed after the completion of the prior three tasks evaluating AHS operation severity. Task 5 requires analysis from task 4 to apply malfunction management strategies for deriving issues and risks and analyze options to alleviate. Task 6 is the documentation of the final.

1.2.2 Results and Issues

Check-in Phase Malfunctions

For a check-in phase malfunction due to a coordination planning failure that goes undetected, the consequences can be severe. If the configuration is infrastructure-weighted (IW), then the link must be closed off dictating the need for a "Stop" operational function. Similarly, if the configuration is vehicle-weighted (VW), then the vehicle must be stopped and a "Stop" operational function is needed. Thus, an additional "Stop" operational function will be added.

Speed Control Malfunctions

Given a malfunction initiated by the exclusively vehicle elemental functions of "Speed regulation command", "Braking regulation command", "Actuation", or "Information link between the regulation layer and the physical layer" and the "Spacing regulation" and "Longitudinal position regulation" malfunctions initiated by a "Sensing" failure for a VW configuration, a conservative transition from these operational functions would be to a "Stop" operational function. The assumption is that any one of the failures would be detected through some type of self diagnosis and that a redundant component would be enabled. The problem with continuing the mission is that the redundant component might also fail; hence, immediate removal of the vehicle from the AHS is required. The conservative approach says that allowing the vehicle to debark at the next available exit might not be soon enough and that the "Stop operational function must be immediately enabled. The link is closed until the vehicle can either debark in a manual mode or is towed away.

The less conservative approach initiates an immediate transition to debark at the next available exit using the existing operational functions. For the "Spacing regulation" and "Longitudinal position regulation" malfunction initiated by a "Sensing" failure for an IW configuration, the sensing might be a roadway sensor. Thus, the logical transition would be to close the link with the malfunctioning sensor with an immediate "Stop" operational function within the link to minimize safety impacts.

Steering Control Malfunctions

Similar to the speed control malfunctions, the steering control malfunctions conservative approach would be to initiate transition to a "Stop" operational function and close the affected link until the vehicle can either debark in a manual mode or is towed away.

The malfunctions that can be IW initiated are initiated by the IW configuration "Sensing" failure and the "Steering for lane-changing" operational function initiated by the IW configuration "Lane assignment" failure. Again, similar to the speed control malfunctions, the logical transition would be to close the link with the malfunctioning roadway sensor or roadway processor with an immediate "Stop" operational function within the link to minimize safety impacts.

Coordination Malfunction

The operational function affected is "Maneuvering coordination management" and is distinguished by the IW and VW configurations. In either case, the logical transition would be to allow AHS operation without maneuver coordination, i.e. remain on the AHS as a free agent vehicle.

Check-out Phase Malfunctions

The operational function affected is the "Normal transition from automatic to human control" and is initiated by failures in the "Normal maneuver coordination planning", "Human-machine interface", "Information link between the coordination layer and the regulation layer", "Information link between the regulation layer and the physical layer", "Manually maneuver vehicle", and "Provide information". As this operational function takes place after the vehicle enters the exit area or transition lane, the major concern is the driver interface and driver condition. The exception is for the unrestricted-entry (UE) configuration where no transition lane exists and thus severe safety impacts can occur with coordination related failures. For all the situations, the logical transition would be to a "Stop" operational function immediately. The impact on those configurations with a transition lane would be minimal, with the UE configuration suffering from link closure.

Representative System Configuration

Examination of the number of high safety and efficiency severity levels assessed by the RSCs was performed. The examination provided indications of the differences between the four RSCs. While it may be premature to draw too much from these differences, some distinct characteristics emerge.

- The IW UE RSC is undoubtedly the most risky system with re spect to likelihood for malfunctions.
- Barrier+transition-lane (BT) is the safest regardless of IW or VW.
- The VW UE RSC becomes high risk due to the uncertainty surrounding the exit. If this could be resolved, it would indeed become the most promising and least expensive RSC.
- The VW RSCs are more efficient that the IW RSCs.

AHS malfunctions were examined in context of operational functions, the four RSCs of an AHS, and the elemental functions and their allocated subsystems. Following are issues identified and addressed in this study for each of these three areas.

Issue #1 - "Check-in" Phase Coordination Planning Malfunction Detection Might Impact AHS Design.

During an AHS "check-in," a malfunction due to coordination planning failure can occur and go undetected. If it is detected and if the configuration is IW, then an entire link would most likely be closed down. If the configuration is VW, then the vehicle must be stopped and an operational "Stop" function would be implemented and in either configuration, the malfunction effects can be eventually mitigated. However, the issue is with the detection of the malfunction.

An effective method of detecting this malfunction would be an extension of current traffic surveillance systems. As this was evaluated as a malfunction with high safety severity for all four configurations, it is highly likely that this malfunction and its mitigation must be addressed by any AHS design. If such a capability were to be developed, how and when should it be addressed by those building an AHS and what type of interface with it have with other roadside and vehicle detection mechanisms?

Issue #2 - Speed and Steering Control Malfunctions and Trade-offs Exist Between Safety and Efficiency.

It is inevitable that a speed or steering control malfunction will occur. The cause of this malfunction ranges from actuator failure to speed regulation software error, i.e. a hardware stops working completely to an intermittent glitch. Due to the timing requirements for speed and steering control, detection methods might not provide enough fidelity. Thus, malfunction management strategies might rely upon Monte Carlo-type statistical results based upon simulations. One strategy is to hardwire a braking capability and apply full braking.

Defining malfunction strategies based upon probability of occurrence is straightforward. The difficulty would be in any required trade-offs between safety and efficiency. While one naturally wants always to prioritize safety, continuous stopping will certainty dissuade the most avid AHS user. Thus, a better definition of safety and efficiency requirements become necessary for detailing malfunction management strategies.

Issue #3 - Resolving "Check-out" Phase Could Make or Break an AHS.

The resolving of many of the perceived risks of "check-out" through technology development, rather than malfunction management strategies, can cast positive light on AHS, specifically the VW UE configuration. As the VW UE configuration appears to be the least costly in terms of infrastructure costs, it appears to be the easiest concept to sell. Thus, to best promote an AHS, emphasis should be placed upon the resolving of the "check-out" risks specifically the operation of the transition from automatic to human control with potential failures such as proper manual vehicle maneuvering or driver capability testing.

Issue #4 - Automobile Software Development Standardization Needs to be Established.

Nearly 1/3 of the expected high safety severity level malfunctions are expected to arise with software related origins. Of these, most are listed as vehicle based, i.e., most probably due to a vehicle processor fail ure and/or embedded software error, and a few are listed as infrastructure based, i.e., most probably due to a roadside processor failure and/or software error. The area of software error in general has proven itself difficult to manage, with safety critical vehicle processor embedded software of high concern. The current Department of Transportation and Federal Highway Administration attitude would appear to be a conservative approach to the software issue leveraging off the continuing improvements and advances in software without direct investment, along with revelations from studies undertaken in other industries. On the basis of review of software and safety status, software development, emerging standardization efforts, legislative aspects, and perspectives from other in dustries, it is recommended that the issue of automobile software development standardization be examined by the federal government. Issues to be addressed include the extent of involvement, i.e., should the software impacts to AHS only or automotive in general be analyzed, and gaining the detailed "lessons learned" from other industries.

Issue #5 - Driver Training Issues Need to be Addressed as Part of System Development, not Hindsight.

Physical layer elemental functions with high safety and efficiency severity levels for IW and VW configurations allocated to the driver input include "Manually maneuver vehicle" and "Provide information". As these two functions are critical to entering and exiting the AHS, the driver is critical as evidenced by its definition as a major system of the AHS. Yet too often even if the human is an integral part of a system, the design does not consider human design constraints or requirements, rather human operational constraints or requirements result.

For the successful implementation of AHS, the driver and driver training issues must be considered as part of the system development. Just as technology assessment and infusion are considered for the design, driver training and expected driver changes must be considered, i.e., work to simulate driver reactions and incorporate human factors requirements should be extended to simulate how driver reactions can and are going to change and design for the incorporation of these changes.

1.3 VEHICLE OPERATIONS ANALYSIS

The overall goal of this task was to identify issues and risks associated with a fully automated AHS vehicle.

Specifically, this task had four primary objectives:

1. What new vehicle subsystems are required to meet the functional requirements of AHS including sensors, processing, and vehicle to vehicle communications and vehicle to infrastructure communications?

2. What subsystems have reliability issues that can have a significant impact on AHS operation and safety?

3. Can the reliability of these subsystems be improved through new design or redundancy?

4. Is it sufficient to perform subsystem checkout at start up or will a self monitoring self diagnosis system offer greatly improved safety and fail-soft capability? Will additional subsystem sensors be required?

1.3.1 Approach

The study started with the functional requirements task. Significant emphasis was placed on understanding the vehicle functional requirements and on understanding the implications of various schemes for vehicle-infrastructure functional decomposition. This effort formed the basis for the next step which was to analyze the fail-safety and criticality of the key vehicle functions and to identify those which must be considered the most safety critical for an AHS vehicle.

Six Representative System Configurations (RSC) were defined representing different approaches to partitioning required AHS functions between the infrastructure and vehicle. From these six RSCs three were determined to represent the most promising approaches to vehicle-infrastructure partitioning.

Twenty-one Operational Functions were defined which cover all AHS operations. From these sixteen operational functions three were selected for detailed criticality analysis. Safety critical paths were defined for each of the three key operational functions. The key safety critical functions were then analyzed in terms of possible technology implementations and the potential benefits of self-monitoring and self-diagnosis technologies for predicting impending failures as a means of improving fail-safety.

The Communications task included the communications and information processing requirements to perform each of the critical AHS functions. In addition to defining the communications requirements, this task provided insights into the various vehicle-infrastructure functional decomposition approaches. This analysis illuminated communications and processing differences between the six RSCs and helped to identify potential issues with several of the RSCs.

1.3.2 Results and Issues

The following observations and conclusions have been derived from this study:

1. Because of the significant communications requirements between the coordination and Regulation layer for the Maneuver planning function, it appears that the maneuver planning function of the Coordination layer should be done on the vehicle. This allows the coordination-regulation communications to be intra vehicle instead of infrastructure-vehicle communications.

Additional analysis must be done to examine other issues related to performing the coordination function on the vehicle. Stability must be examined within the context of specific algorithm approaches across expected operating regimes. System level performance evaluation will require treatment of the AHS as a complex adaptive system whose behavior is determined by the interaction among semi-autonomous individual entities that communicate largely asynchronously and employ limited information bases.

2. Because of the information processing requirements, it appears that the Link Layer should be performed by the infrastructure rather than the vehicle. Additional analyses are required to examine in more detail specific optimization algorithms and the associated processing requirements.

3. The communication function is critical for control of strings of vehicles based on the spacing distance control. Autonomous or time headway control approaches are more robust to losses of communication. With spacing control, the absence of communication does not guarantee us attenuation of errors down a string of vehicles. The errors in tracking can be reduced through accurate estimators. If spacing control methods are used the communication control is critical.

4. The noise experienced in a platoon is a percentage of the target spacing. Hence spacing errors will be larger at larger target spacings. Vehicles following at larger spacing, albeit safer, will not necessarily result in the best form of control. Low gain controllers must be designed to

ensure that small variations in spacing errors do not translate into high control effort and actuator saturation.

5. The effect of actuator limitations was studied but it was found that throttle actuators at least as fast as 150 ms are fast enough for the frequency and type of maneuvers that can be expected in automatic vehicle control on highways. Brake actuators slower than 150 ms can lead to poor tracking performance during high jerk deceleration maneuvers.

6. The closing rate function is by far the most important function for longitudinal control. Performance is greatly degraded in the absence of closing rate information. In addition, if the communications are not working, potentially hazardous situations can arise due to large lags in acceleration tracking. The degradation of performance without closing rate and communication information is true regardless of the control approach used. The closing rate function is safety critical.

7. Self-diagnosis and self-monitoring technology can have significant benefit to improving the safety of AHS. Additional study is needed to determine the best technology approach and whether it is best to have a centralized self monitoring elemental function or to have a distributed monitoring capability with each element performing its own diagnostics.

2. INTRODUCTION

2.1 SUMMARY DESCRIPTION OF ACTIVITY AREAS ADDRESSED

2.1.1 Lateral and Longitudinal Control Analysis

The overall goal of this task included performing system operational analyses in terms of safety and capacity and identifying issues and risks regarding the fundamental operations and maneuvers of vehicle control in a fully automated highway environment. The basic operations and maneuvers required for the Representative Systems Configurations (RSCs) presented in this analysis are: headway maintenance including safety formulation; lane change maneuver including lane holding, lane entry/exit, and roadway entry/exit; platoon formulation; obstacle avoidance; and automated traffic stream stability.

2.1.2 Malfunction Management and Analysis

The overall goal of this task included defining the boundaries of an AHS, establishing functional requirements, and suggesting potential configuration. Then developing operational sequences through which functions are executed and identifying allocated subsystems were performed. Metrics to gauge severity levels of malfunctions were developed and used to assess malfunctions. Similarities and differences between malfunctions and system configurations were examined to develop strategies to mitigate or avoid malfunctions and to raise issues and risks involved with the AHS.

This analysis defined the boundaries of the system before analyzing its malfunctions. Once functional requirements were established, potential configurations were suggested upon which we performed initial analyses. Operational sequences were developed through which the functions are executed and identified subsystems which have been allocated functions. As with understanding the functionality of the system, it was of equal importance to understand the malfunctions of the system. Metrics were defined to gauge the severity of the malfunctions in terms of their effect on goals of the system. This analysis was performed understanding the relationship of these malfunctions to the operational configurations we assumed and the context in which the malfunction occurred, i.e. when during an operational sequence did the malfunction occur and what was the system configuration. Similarities and differences between malfunctions and system configurations were investigated, then offered strategies that helped to mitigate or avoid these malfunctions and raised issues and risks involved with the malfunctions and the strategies.

Confidence in the analysis was established through the usage of a Computer Aided Software Engineering (CASE) tool, Statemate. Its modeling capability of both functional and behavior aspects of a system along with its structured analysis foundation provides a means to verify functional requirements. In addition, modeling of Statemate was performed in enough detail to execute two functions and examine the behavior of the particular functions in a specific scenario. While the Statemate model for effective simulation is still youthful for an overall quantitative assessment, i.e. only those states relevant to the two functions are modeled with algorithms of sufficient fidelity, creating the model was invaluable and provided guidance in our analyses.

2.1.3 Vehicle Operations Analysis

The overall goal of this task was to identify issues and risks associated with a fully automated AHS vehicle.

The primary issues that were addressed were related to vehicle-infrastructure functional decomposition, performance requirements, fail-safety and criticality, communications, self-monitoring and self-diagnosis technology, and overall vehicle management. Specifically, this task had five primary objectives:

1. What new vehicle subsystems are required to meet the functional requirements of AHS including sensors, processing, and vehicle to vehicle communications and vehicle to infrastructure communications?

2. What subsystems have reliability issues that can have a significant impact on AHS operation and safety?

3. Can the reliability of these subsystems be improved through new design or redundancy?

4. Is it sufficient to perform subsystem checkout at start up or will a self monitoring self diagnosis system offer greatly improved safety and fail-soft capability? Will additional subsystem sensors be required?

2.2 ISSUES ADDRESSED BY ACTIVITY AREA

Following are tables 1, 2, and 3 listing issues identified as compiled by the MITRE Corporation. As indicated in the referenced document, this table is used to provide an indication of the issues addressed in this study relative to other studies in that task area.

Table 1. Lateral and Longitudinal Control Analysis Issues Matrix.

Issue	Description
Required vehicle maneuvers	Yes. Lane change, headway maintenance, obstacle avoidance
Platoon maneuvers	Yes, platoon formation
Stream stability	Yes. Investigating impacts of AHS maneuvers on stability of the traffic stream
High level control system requirements	Yes
Safety requirements	Yes, safety vs. capacity tradeoff (for all key maneuvers
Synchronous vs. asynchronous behavior	Yes

Table 2. Malfunction Management and Analysis Issues Matrix.

Issue	Description
Identification and categorization of potential malfunctions	Yes. Major subsystems and their potential malfunctions are identified. A CASE tool, Statemate, was used to model the system and help identify malfunctions.
Definition of MOEs	Yes. The key parameters of safety and efficiency are defined.
Development of malfunction management strategies.	Yes. Strategies are developed based upon malfunction severity levels and RSCs.

Table 3. Vehicle Operations Analysis Issues Matrix.

Issue	Description
Functional decomposition	Yes
Reliability and accuracy	Yes. Top level performance and reliability requirements
Vehicle control	Yes. Safety-criticality analysis
Vehicle and driver status	Special emphasis on self-diagnostics and interaction with malfunction management
Communication	Yes. Top level communication architecture. Survey communication alternatives

2.3 OVERALL APPROACH/METHODOLOGY ACROSS ALL ACTIVITY AREAS

2.3.1 Longitudinal and Lateral Control Analysis

To insure practical and meaningful results of the analysis, a four step approach was adopted. These four steps are: (1) define system configurations on the basis of the PSA AHS requirements provided in the BAA guidelines, (2) define basic vehicle operations and maneuvers required for the defined system configurations, (3) perform generic analysis on each operation and maneuver, and (4) identify issues and risks from the analyses. The detailed system configurations are described in the next chapter, Representative Systems Configurations (RSC). The basic operations and maneuvers required for the RSCs, thus studied in the report, are: headway maintenance including safety formulation; lane change maneuver including lane holding, lane entry/exit, and roadway entry/exit; platoon formation, obstacle avoidance, and automated traffic stream stability.

2.3.2 Malfunction Management and Analysis

Figure 1 illustrates the six-step (tasks) approach used to perform this analysis.

These six tasks are arranged to show the timing of the effort and what information is required before beginning the next task. In addition, the utilization of Statemate is indicated in the shaded boxes. The requirements analysis effort was conducted prior to the actual tasks of this study. Task 1 is to define measures of effectiveness. Measures of effectiveness are defined to provide a foundation for the evaluation of the malfunctions. Both safety and efficiency (throughput) are described in terms of their impact due to the malfunction. Task 2 is to define AHS operations and modes of operation. Rather than focus on each of the functions performed on an AHS, a system-wide or operational viewpoint of the AHS was adopted. It is in context of these operations relative to the RSCs that the malfunctions are examined. Task 3 is to formulate major system categories for malfunction breakdown. Evaluation of malfunctions demands an understanding of what subsystem malfunctioned. Thus, for each of the RSCs, allocations of AHS functions to major subsystems were made. Based upon these allocations, evaluation of malfunctions conjectured are made. Task 4 is to evaluate AHS operation severity. Given the completion of tasks 1, 2, and 3, an evaluation of AHS malfunctions can be performed. An operational function malfunction is assumed for each RSC. Based on which elemental function and thus which major subsystem might have failed, an evaluation of the impact of the malfunction using the MOEs is performed. Task 5 is to apply malfunction management strategies for deriving issues and risks and analyze options to alleviate risks. The results of task 4 are compiled and analyzed. Understanding of the significance of the various RSCs, the major subsystems, and operational functions, provides the foundation for development of mitigation strategies. Task 6 is the documentation of the final report.

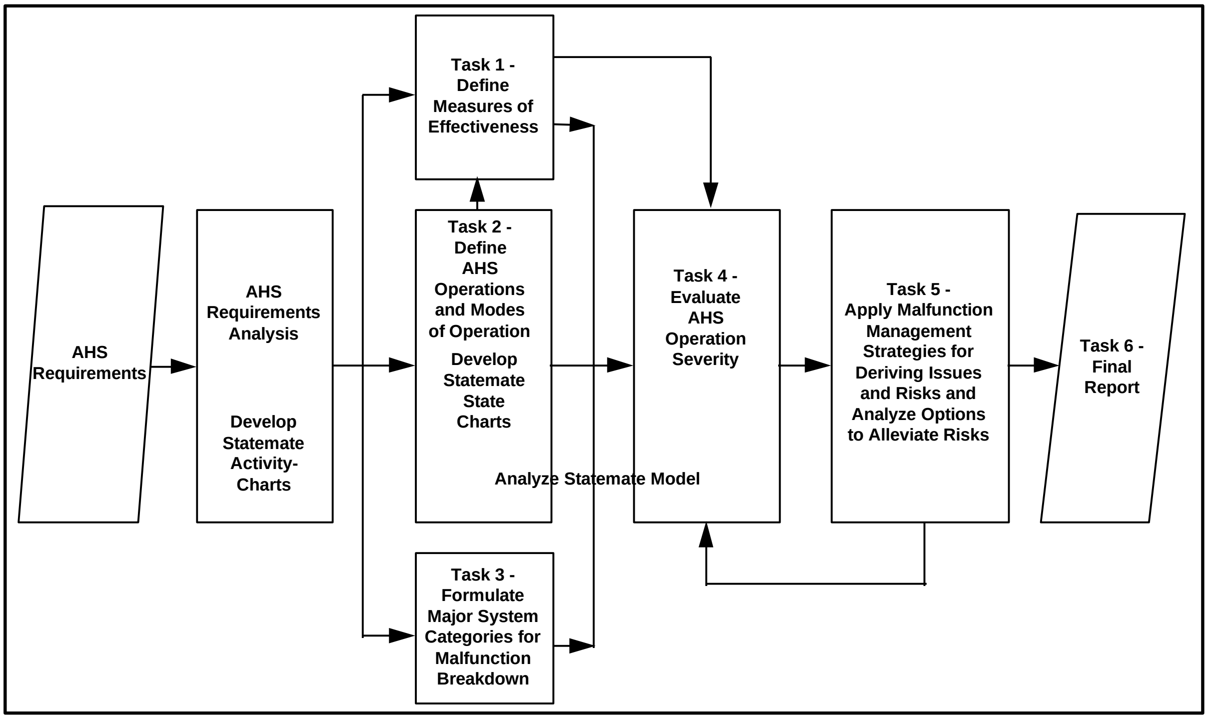

Figure 1. Malfunction Management and Analysis Study Flow

2.3.3 Vehicle Operations Analysis

Figure 2 presents an overview of the entire Rockwell Vehicle Operational Analysis effort and illustrates the relationship between the various tasks.

The study started with the functional requirements task. Significant emphasis was placed on understanding the vehicle functional requirements and on understanding the implications of various schemes for vehicle-infrastructure functional decomposition. This effort formed the basis for the next step which was to analyze the fail-safety and criticality of the key vehicle functions and to identify those which must be considered the most safety critical for an AHS vehicle.

Six Representative System Configurations (RSC) were defined representing different approaches to partitioning required AHS functions between the infrastructure and vehicle. From these six RSCs three were determined to represent the most promising approaches to vehicle-infrastructure partitioning.

Twenty-one Operational Functions were defined which cover all AHS operations. From these sixteen operational functions three were selected for detailed criticality analysis. Safety critical paths were defined for each of the three key operational functions. The key safety critical functions were then analyzed in terms of possible technology implementations and the potential benefits of self-monitoring and self-diagnosis technologies for predicting impending failures as a means of improving fail-safety.

The Communications task included the communications and information processing requirements to perform each of the critical AHS functions. In addition to defining the communications requirements, this task provided insights into the various vehicle-infrastructure functional decomposition approaches. This analysis illuminated communications and processing differences between the six RSCs and helped to identify potential issues with several of the RSCs.

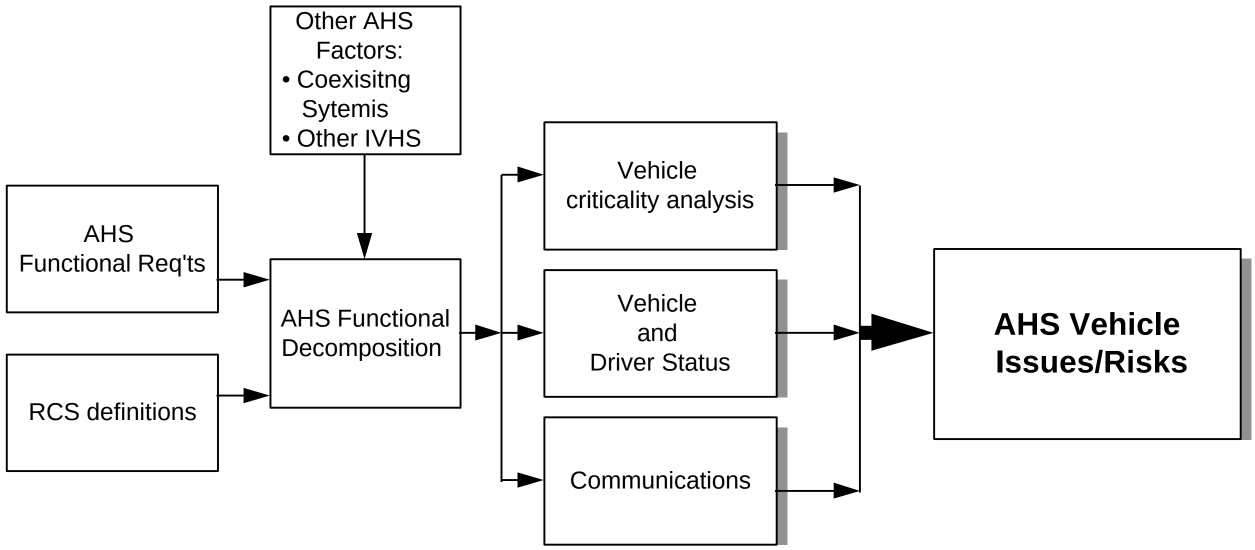

Figure 2. Vehicle Operations Analysis Study Flow

2.4 GUIDING ASSUMPTIONS

2.4.1 Lateral and Longitudinal Control Analysis

All of the various maneuvers that are possibly needed in an AHS can be decomposed into one or a combination of three basic maneuvers: speed change, longitudinal displacement, and lateral displacement.

The speed change maneuver is invoked when a free agent or the lead vehicle of a platoon is commanded, by either the infrastructure or other vehicles, to follow a certain desired velocity trajectory with or without constraints, e.g., vehicles approaching an exit or entry. The desired velocity is reached through the use of throttle control and braking control. It is possible that the desired velocity may not be reached within a time constraint, if any, for those vehicles with insufficient acceleration and/or brake capability from certain initial velocities. The key parameters associated with this maneuver are acceleration and brake capabilities including the tire rolling resistance, initial vehicle velocity, commanded velocity, and constraints, like time and/or distance.

The longitudinal displacement maneuver is invoked when (1) a vehicle needs to keep a minimum safe distance from the vehicle ahead, so that collision is prevented should the lead vehicle decelerate rapidly, or (2) a vehicle decides to platoon with another vehicle, or (3) a vehicle intends to change lanes, where longitudinal displacement maneuver is usually accompanied by lateral maneuver, or (4) a vehicle needs to make room in its own lane to accommodate another vehicle's maneuver. Time and/or distance constraints may be imposed to any one of the above situations. Regardless of which situation it may be, longitudinal displacement, like the speed change maneuver, is accomplished by throttle and brake control. The key parameters associated with this maneuver are acceleration and brake capabilities including tire rolling resistance, initial vehicle longitudinal position, commanded desirable displacement, and time and/or distance constraint.

The lateral displacement maneuver is invoked when (1) a vehicle needs to stay within its lane boundary (lane holding), or (2) a vehicle wishes to change lanes, or (3) a vehicle is trying to avoid an obstacle along its scheduled path. This maneuver is always performed simultaneously with non-zero vehicle longitudinal movement and it is accomplished by wheel steering, whereby a lateral force in the required direction is generated. The key parameters associated with this maneuver are the steering angle, the acceleration and brake capabilities including tire rolling resistance, initial vehicle lateral position, commanded lateral position, and time and/or distance constraints.

2.4.2 Malfunction Management and Analysis

The Department of Transportation established the AHS program in direct response to the Intermodal Surface Transportation Efficiency Act of 1991, Part B, Section 6054(b): "The Secretary (of Transportation) shall develop an automated highway and vehicle prototype from which future fully automated intelligent vehicle-highway sys tems can be developed...". In defining AHS, the term "fully automated intelligent vehicle-highway system" is in terpreted to mean a system that evolves from today's roads, provides fully automated "hands-off" operation at better levels of performance than today's roadways in terms of safety, efficiency, and operator comfort, and allows equipped vehicles to operate in both urban and rural areas on highways that are both instrumented and not instru mented.

These goals are achieved through the performance of a wide range of functions, including traffic management, route planning, route guidance, vehicle maneuver coordination, automated vehicle control, and driver interface. The first step in performing this malfunction management analysis task is to define the functional requirements of an AHS while at the same time developing operational concepts that are feasible and able to meet the defined requirements.

2.4.3 Vehicle Operations Analysis

The study was performed with the following general guidelines and assumptions:

1. All RSCs implement a fully automated AHS. The study did not examine evolutionary concepts or concepts that did not provide a fully automated AHS.

2. The functional decomposition was to be technology independent. Those aspects of the analysis that examined functional decomposition, functional requirements, and criticality of functions did this in a technology independent way.

3. AHS could evolve in small steps through technology improvements without modifications to the functional decomposition or functional requirements.

3. REPRESENTATIVE SYSTEMS CONFIGURATIONS (RSCs)

Four Representative System Configurations (RSC) were identified that exemplify the contrasting features of the AHS characteristics. These four RSCs were developed from a framework built upon the distinguishing characteristics of instrumentation distribution, traffic synchronization, infrastructure impact, and operating speed. Contrasting features were identified within each characteristic in order to fully understand and represent the characteristics in the RSCs.

3.1 INSTRUMENTATION DISTRIBUTION

The spectrum of instrumentation distributions is characterized by the two fundamentally different system configurations of an infrastructure-weighted instrumentation distribution and a vehicle-weighted instrumentation distribution.

The infrastructure-weighted configuration provides for the majority of the instrumentation to be hosted as part of the infrastructure. Vehicle position sensing and processing is performed by the infrastructure, as are commands directing vehicle kinematics. This configuration does not mandate a particular design with specific sensors and locations. In fact, this configuration is open to combinations of sensor types and can support vehicle platooning.

The vehicle-weighted configuration provides for autonomous vehicles with nearly all the sensors and instrumentation mounted on the vehicle. Platoons are formed and broken apart through negotiation between neighboring vehicles. The only command information from the infrastructure are traffic speed and reroute commands.

3.2 TRAFFIC SYNCHRONIZATION

There are basically two traffic synchronization mechanizations: individual vehicle or platoon provided control. These two mechanizations are tightly tied to the instrumentation distribution configurations. The infrastructure-weighted configuration is highly synchronous in that all maneuvers of individual vehicles or platoons are controlled through the infrastructure-based system. The vehicle-weighted configuration is largely autonomous with only occasional infrastructure-based commands.

3.3 INFRASTRUCTURE IMPACT

Three factors affect the degree of infrastructure modification or addition. Safety considerations prompt infrastructure modifications such as lanes isolated by barriers. The need for such modification is based upon reliability and/or fail-safety of the equipment, and constraints placed on traffic, roadway geometry, operating speeds, and other safety influences.

Operational concepts also influence the need for infrastructure modifications or additions. Concepts such as off-freeway platoon formations and platoons formed on the freeway in a platoon lane or a transition lane affect the need for an off-freeway "marshaling yard" or a transitional lane.

The third factor is the growth in freeway traffic. As the lane capacity is increased, the need to increase on and off ramp capacity as well as the surface street network feeding them increases. This aspect is not specifically addressed in this report.

Given these factors with focus upon safety, two mechanizations are examined: a barrier+transition and an unrestricted-entry mechanization. The barrier+transition mechanization assumes that safety will require physical barriers around the dedicated and instrumented lanes. This mechanization represents a roadway system assumed to have one or more dedicated lanes separated by safety barriers. The lanes would have periodic openings between multiple safety-lanes for moving back and forth between them. A transition lane would exist between the safety-lanes and normal traffic. The transition lane has no barriers between it and the normal traffic. The rationale for a transition lane is to alleviate the problem of aligning all the gaps to enter and leave the lane that could create entry and exit difficulties.

A contrasting mechanization is the unrestricted-entry mechanization that eliminates the safety barriers separating the dedicated lanes from the transition and normal traffic lanes of the barrier+transition mechanization. This removal of safety barriers is based upon the assumption that adequate safety can be achieved without the barriers. Without the safety barriers, entry and exit are simplified such that a transition lane is not needed.

3.4 OPERATING SPEED

Several considerations are provided regarding the implications of permitting higher speeds in an AHS as compared to today's traffic. The speed differential between normal traffic and a high speed AHS could be dangerously severe. This implies a need for dedicated high-speed lanes. In addition, the higher speed on the AHS itself increases the severity of accidents favoring physical barriers to eliminate angular collisions.

The higher speeds imply greater distances traveled prior to or during maneuvers. This implies the need for faster reaction capabilities, including longer range sensors, faster processing, and tighter vehicle control.

Finally, higher speeds will increase the maximum efficiency of the AHS lanes. These considerations suggest that the barrier+transition mechanization can be the basis for a high speed system. At normal speeds, the barrier+transition mechanization is less cost-effective than the unrestricted-entry mechanization as it requires the safety barriers and transition lane. The trade off is to convert one of the dedicated lanes of the barrier+transition mechanization into a high speed lane.

3.5 REPRESENTATIVE SYSTEM CONFIGURATIONS SUMMARY

In summary, two sets of complementary mechanizations, four RSCs, are proposed. These combinations are provided in table 4. These four RSCs will be examined extensively as we perform this analysis.

Table 4. Representative System Configuration Characteristics Mapping.

	AHS Characteristics			
Selected RSCs	**Infrastructure Impact**	**Traffic Synchronization**	**Instrumentation Distribution**	**Operating Speed**
IWSM-BT	High	High	High	High Infrastructure
IWSM-UE	Moderate	Moderate	Moderate	Moderate Infrastructure
VWAM-BT	High	Moderate	Moderate	High Vehicle
VWAM-UE	Low	Low	High	Moderate Vehicle
Legend:	IWSM	Infrastructure Weighted Synchronous Mechanization		
	VWAM	Vehicle Weighted Autonomous Mechanization		
	BT	Barrier + Transition Lane Guard Mechanization		
	UE	Unrestricted-Entry Lane Mechanization		

3.6 INSTRUMENTATION REFINEMENTS FOR VEHICLE OPERATIONS ANALYSIS

To accomplish the vehicle operations analysis it was necessary to define additional RSCs that reflect a more detailed decomposition of the instrumentation distribution between the vehicle and the infrastructure. Within that context, a description of six RSCs is defined in terms of the AHS control layers and the associated elemental functions.

The six RSCs are illustrated in figure 3. In the figure, the numbering of the RSCs is purely arbitrary and does not represent an evolutionary ordering or rank ordering of the RSCs. Each RSC has been conceived to be able to perform all of the required functions of a fully automated AHS. The various RSCs illustrate potential functional partitions between the infrastructure and vehicle. RSC #1 is predominately infrastructure weighted and RSC #6 is predominately vehicle weighted. Some functions such as the regulation layer and the actuation functions of the physical layer will always be contained within the vehicle. Also, some of the Net layer functions will always be accomplished by the infrastructure. The remaining functions can be reasonably partitioned between the infrastructure and the vehicle as illustrated.

Moving from RSC #1 each subsequent RSC represents a portion of the control functions shifted from the infrastructure to the vehicle. RSC #2 represents a functional partitioning where some of the coordination layer control functions such as maneuver coordination planning are performed on the vehicle rather then by the infrastructure.

RSC #3 continues with some of the Link layer control functions partitioned to the vehicle. RSC #3 represents a system with even more vehicle autonomy then RSC #2 with both maneuver planning and lane assignment and vehicle parameter monitoring performed by the vehicle. This RSC has significantly reduced communication requirements between the vehicle and the infrastructure compared to RSC #1, but adds the complexity of a self organizing system with many elements capable of making decisions.

RSC #4 illustrates a functional partitioning with all of the coordination layer control functions performed on the vehicle. RSC #4 allows the entry/exit permission function to be made by the vehicle. This requires a complete and reliable self diagnosis/self monitoring system within the vehicle.

Continuing with RSC #5, the partitioning now includes all of the Link layer control functions performed by the vehicle. RSC #5 assumes the vehicle receives all information necessary to make decisions for incident management and establishing vehicle priorities.

And finally, the functional partitioning for RSC #6 includes some of the Link layer control functions performed by the vehicle. RSC #6 assumes the vehicles can effectively plan the individual vehicle routes.

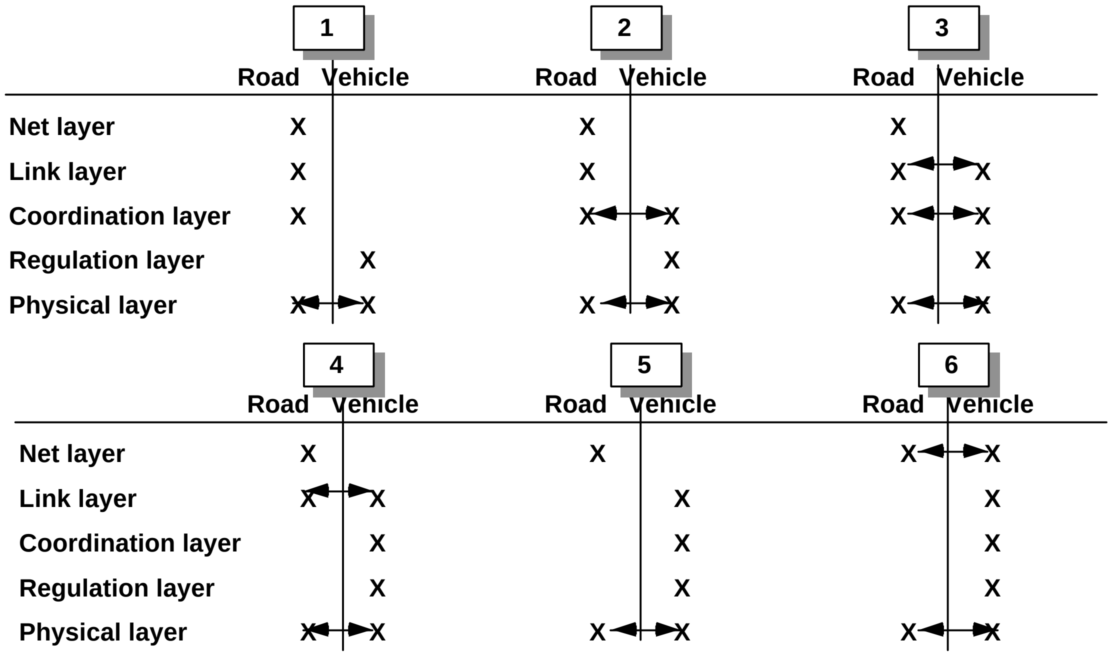

Figure 3. Functional Partitioning Between Vehicle and Infrastructure

4. HIGHLIGHTS OF THE TECHNICAL DISCUSSIONS OF EACH ACTIVITY AREA

4.1 KEY FINDINGS

4.1.1 Longitudinal and Lateral Control Analysis

Rockwell has performed precursor analyses in the area of AHS lateral and longitudinal control analyses in terms of primarily four maneuvers (headway maintenance, lane change, platoon formation and obstacle avoidance), and stream stability. As stated earlier in Section 1, the purpose of this effort is to identify issues and risks for future AHS researchers. In lieu of that, the most important conclusion resulting from these analyses is that there are ***no show stoppers*** at this stage of the program. However, there are many issues that remain unresolved and which necessitate further investigation. The major conclusions and recommendations are summarized below:

Headway Maintenance Maneuvers

Headway Maintenance Maneuvers issues and risks identified are summarized below. Note that issues and risks are not necessarily concerns of the feasibility of the idea of AHS as the remedy for the next century's transportation problems but they are simply some technical subjects that ought to be thoroughly investigated in the future.

1. Safety distance between two vehicles depends upon many deterministic as well as random factors, e.g., velocity, road surface condition, tires, and weather. Should the safety distance be established upon the worst scenario (e.g., brick wall stop) or on a probability basis?

2. Can the safety distance between vehicles be preset realistically? If not, how do we establish it adaptively in real time?

3. To standardize longitudinal control systems of automated vehicles, the following requirements need to be defined: ride comfort, the mobility of vehicles in an AHS, the nominal gap, the maximum tolerable gap variation, the maximum tolerable impact energy for platooning.

Analysis of Lane Change Maneuvers

Lane Change Maneuver (LCM) issues and risks identified are summarized below. The issues and risks are subjects for future studies.

1. While the efficiency of an LCM can be optimized given a particular traffic condition, the optimization is often accomplished at the expense of system robustness. The trade off between efficiency and robustness requires careful analysis, tuning, and tests in the future.

2. How much and when should the driver be given control of the vehicle to perform an LCM from an automated lane to a manual lane, and vice versa in the DE mechanization?

3. How do we estimate the necessary lead time to initiate an LCM which is constrained by the location and length of the opening of a physical barrier between an automated and transition lane as in a BT mechanization?

4. Since lateral and longitudinal control systems are always operated simultaneously, and they are usually designed and analyzed separately, the possibility of adverse cross-axis interactions should be minimized to ensure the total system integrity. For example, the minimization of the effect of weight shift between front and rear tires on lateral maneuverability when the vehicle is accelerating longitudinally.

5. What is the effect of LCM on lane keeping? Biasing the vehicle's reference lateral position to, perhaps, the center line of the receiving lane?

Platoon Formation Task and Maneuver

There does not appear to be a compelling rationale for having the front platoon actively participate in the merge of two platoons. An active front platoon would imply system complexity beyond AICC with information simultaneously flowing both forward and rearward between the platoons. This would create two-way dynamic coupling that could be generally undesirable.

With a passive front platoon, merge involves only *inter*-platoon, not *intra*-platoon, dynamics. Consequently only the dynamics and control of the lead vehicle of the rear platoon need be treated explicitly.

It is important to distinguish between nominal merge conditions that would apply to the majority of platoon formations and special cases that will occur relatively rarely (emergency and failure cases). Platoon formation will always be an optional activity performed for traffic flow efficiency and not specifically to enhance safety. Thus aborting a platoon merge probably will be the correct strategy for many, if not most, off-nominal conditions. *The nominal merge control design should not be compromised to allow platoon formation under off-nominal conditions where the maneuver could and should be aborted*.

If the front platoon speed is much lower than the speed limit, or if it is decelerating rapidly, or if a third vehicle intrudes between the platoons, an off-nominal condition is indicated and platoon formation should not be initiated. This is particularly true without two-way inter-platoon communication. Further, the front platoon cannot accelerate significantly for long or the speed limit would be exceeded. Thus merging with an accelerating (or decelerating) front platoon should not be a system design issue.

Acceleration and jerk limits for platoon merges will be imposed for passenger comfort rather than safety and traffic flow. Thus these limits will likely be set by manufacturers (rather than the Government).

The nominal merge maneuver could be addressed as a constrained trajectory optimization problem, if a relevant cost function could be identified. A minimum time maneuver is a possibility, but not a compelling one since elapsed times for a merge maneuver will be much shorter than useful platoon "half-lives". Thus minimum time maneuvers are primarily of interest as reference maneuvers. Maximizing safety and passenger comfort is much more important.

Obstacle Avoidance Maneuvers

Currently the most important question concerning AHS obstacle avoidance is the discrete control strategy for determining if a vehicle should maneuver around an obstacle or simply remain in its current lane and brake .

The basic discrete lane change decision algorithm can be based on comparison of estimates of the expected costs of: (1) remaining in the lane and possibly impacting the object or, (2) maneuvering around the obstacle and possibly colliding with a vehicle in an adjacent lane.

The key uncertainties in the lane change decision problem, both for analysis and real-time systems, are the statistical distributions of the properties of the population of random objects that can be expected to appear on highways. The object properties of interest, in order of decreasing importance, are size, density, and effective structural stiffness. Relevant statistical data is not readily available.

The lane change decision problem for an automatic system is fundamentally the same as that for a human driver. However, in addition to simply detecting an object in the roadway, human drivers apparently apply, with various degrees of competence, subtle identification schemes to predict the danger of impacting the object. These probably involve cues from size, shape, color, and motion compared to a "knowledge-base" of likely highway objects. Achieving this capability in sensor processing for an automatic system can be expected to be a major challenge and a critical path in AHS development.

Even if an automated lane change decision capability can be developed and shown to equal or exceed human capability in tests, accidents with an automated system are probably more likely to result in lawsuits. This follows simply because of the "deeper pockets" of a system manufacturer compared to those of an individual driver.

The most sensitive object factor is size. Increased object size increases collision severity in the "no lane change" case by increasing object mass. It increases severity in the "lane change" case by increasing the expected relative velocity with respect to adjacent vehicles.

The most sensitive vehicle factor is the limit deceleration capability, but it effects only the "no lane change" case to a first approximation. Increasing the limit reduces the severity of "no lane change" accidents by decreasing the object impact speed. In lane changes some reduction in accident severity is achieved by increasing the effective side stiffness of the vehicle.

All of the AHS system parameters (lane speed, longitudinal vehicle separation, lane width, object detection range, and system effective time delay) are potentially significant. Reduction in longitudinal vehicle spacing and reduction in lane width from current nominals, possibilities that have been proposed as benefits from AHS and vehicle platooning, could have serious adverse impacts on the obstacle avoidance problem.

The primary need for future research in this area is better characterization of the population of random objects that can be expected to appear on highways (AHS highways in particular). Statistical distributions of (in order of decreasing importance) size, density, and effective stiffness should be obtained. Reasonable empirical data could probably be obtained from state highway departments and highway patrols.

When improved object statistics are available, the analytical procedure reported here should be refined to predict the variances of accident severity as well as expected severity. The lane change accident probabilities should also be refined. Ultimately the lane change model should be based on a vehicle dynamic simulation (which are currently available). However this step should be postponed, until a refined version of the closed form probabilistic model reported here has been thoroughly examined.

The problem of detecting and characterizing random roadway objects with machine systems should be studied as a distinct problem. This should begin with a study of human driver behavior and technique for object detection and classification. This could be done with integrated driver-in-the-loop simulation and field experiments. This effort can build on relevant technology developments for similar applications. New technologies in the area of artificial intelligence, machine vision, etc. should be examined. Developments could find application in collision warning systems (especially for night and foul weather) before AHS is operational.

Stream Stability

Perturbation amplification in strings of automated vehicles. There is a general consensus that if communications links are provided so that each vehicle in a platoon obtains continuous information regarding the motion of the lead vehicle, then stability of the platoon can be sustained indefinitely. There is an issue of the safety of the platoon in the event of sudden failure of the communications system, however, this does not appear to be insurmountable and back-up control algorithms have been designed. There is an issue of the cost of the communications system, including the use of the spectral bandwidth needed. It is not generally agreed that a longitudinal control system can be designed without the aid of communications that will both provide major benefits in flow capacity as well as provide guaranteed stable performance. However, some benefits are realizable, and it may be possible to impose constraints on the maximum platoon size (via a less expensive communications link from traffic management) that provides the necessary limits for safe and stable operation.

Impact of Entering and Exiting on Stream Stability. It has been found that the effect on the traffic flow of vehicles entering and exiting the AHS effects must be accounted for in deriving the potential flow capacity increase benefits of an AHS, as well as used in any on-ramp flow control (to ensure the system is not overloaded). However, these effects do not appear to impose an obstacle to implementation of the AHS. There are some approaches that have been investigated that indicate substantial mitigation of these detrimental effects by communicating information regarding exit destination and utilizing this in the behavior of the vehicles (viz., platoon formation and dissolution). However, these will bring issues both of cost of implementation such communications links and algorithms as well as the problem of privacy.

Complexity of Vehicle Interactions. The AHS, like any road traffic system, is representative of a complex dynamic system, in which many entities interact asychronously based on local information and nonlinear rules of operation. Analysis and prediction in such systems are generally intractable, much like predicting the weather (which can be chaotic in the sense of sensitive dependence on initial conditions). Newly emerging concepts in the field of complex systems theory will need to be applied to bound the problem of performance evaluation, and ensure stable conditions will prevail.

Effect of Automation on Vehicle Neighborhoods. It seems clear that in the AHS, the coupling among vehicles will necessarily be increased. Thus, when an incident occurs, the effects will be much more widespread both in the number affected and the spatial extent. While one approach is to emphasize the rapid removal of problems, we feel that at least concurrent with this must be a careful design that ensures that the AHS is not too brittle, wherein every small disturbance is felt by every vehicle in a large region.

4.1.2 Malfunction Management and Analysis

Malfunction management strategies are proposed that would be implemented as operational functions. These operational functions would be enabled as the transition states after a malfunction occurs and is detected.

Check-in Phase Malfunctions

The two operational functions affected are "Entering the system" and "Transition from human to automatic control". Both malfunctions are initiated by a failure in "Manually maneuvering the vehicle", with the "Transition from human to automatic control" malfunction also initiated by a failure in "Normal maneuver coordination planning".

A logical transition from this general check-in phase, given a malfunction, would be to issue a rejection and debark the entering vehicle. However, concern regarding the failure of manual maneuver suggests a greater vehicle failure. Whether an AHS embraces responsibility for non-exclusive AHS operations and has legal/moral obligations to address such failures is beyond the scope of this study. Certainly, a rejection notice can be issued and the transition to a non-AHS state would suffice and is consistent with current operational functional requirements.

For a check-in phase malfunction due to a coordination planning failure that goes undetected, the consequences can be severe. If the configuration is IW, then the link must be closed off dictating the need for a "Stop" operational function. Similarly, if the configuration is VW, then the vehicle must be stopped and a "Stop" operational function is needed. Thus, an additional "Stop" operational function will be added.

An issue here is the detection of the malfunction. In an IW configuration, each adjoining links might query the processors of adjoining links with three votes allowing the detection of a failing link or the traffic incident detection surveillance system can be enhanced to identify anomalies in coordination planning to suggest a failed link processor. For a VW configuration, a similar querying by adjoining vehicles might occur or more likely, self-monitoring/self-diagnosis or reliance on the traffic surveillance system. Thus, an issue exists as to the requirements AHS will place on traffic management and roadside equipment and how soon should traffic management plan to accommodate these requirements. The significance of requiring fiber optic cable along all AHS roadway can be extreme high costs, compounded by prior requirements that might have laid out coaxial cable instead, i.e. some of the cost of the fiber optic cable might have been absorbed by initially planning for fiber optic cable.

Speed Control Malfunctions

The three operational functions affected are "Velocity regulation", "Spacing regulation", and "Longitudinal position regulation". All three malfunctions are initiated by failures in the "Speed regulation command", "Braking regulation command", "Actuation", or the "Information link between the regulation layer and the physical layer". The "Spacing regulation" and "Longitudinal position regulation" operational malfunctions are also initiated by a failure in "Sensing".

Given a malfunction initiated by the exclusively vehicle elemental functions of "Speed regulation command", "Braking regulation command", "Actuation", or "Information link between the regulation layer and the physical layer" and the "Spacing regulation" and "Longitudinal position regulation" malfunctions initiated by a "Sensing" failure for a VW configuration, a conservative transition from these operational functions would be to a "Stop" operational function. The assumption is that any one of the failures would be detected through some type of self diagnosis and that a redundant component would be enabled. The problem with continuing the mission is that the redundant component might also fail; hence, immediate removal of the vehicle from the AHS is required. The conservative approach says that allowing the vehicle to debark at the next available exit might not be soon enough and that the "Stop operational function must be immediately enabled. The link is closed until the vehicle can either debark in a manual mode or is towed away.

The less conservative approach initiates an immediate transition to debark at the next available exit using the existing operational functions.

For the "Spacing regulation" and "Longitudinal position regulation" malfunction initiated by a "Sensing" failure for an IW configuration, the sensing might be a roadway sensor. Thus, the logical transition would be to close the link with the malfunctioning sensor with an immediate "Stop" operational function within the link to minimize safety impacts.

Steering Control Malfunctions

The two operational functions affected are "Lane tracking" and "Steering for lane-changing". Both malfunctions are initiated by failures in the "Steering control command", "Sensing", "Actuation", and "Information link between the regulation layer and the physical layer". Additionally the "Steering for the lane-changing" operational function is initiated by the "Lane assignment" failure.

The malfunctions isolated to the vehicle are initiated by failures in the "Steering control command", "Sensing" for the VW configuration, "Actuation", and "Information link between the regulation layer and the physical layer" and for the "Steering for the lane-changing" operational function initiated by the VW configuration "Lane assignment" failure. Similar to the speed control malfunctions, the steering control malfunctions conservative approach would be to initiate transition to a "Stop" operational function and close the affected link until the vehicle can either debark in a manual mode or is towed away.

The malfunctions that can be IW initiated are initiated by the IW configuration "Sensing" failure and the "Steering for lane-changing" operational function initiated by the IW configuration "Lane assignment" failure. Again, similar to the speed control malfunctions, the logical transition would be to close the link with the malfunctioning roadway sensor or roadway processor with an immediate "Stop" operational function within the link to minimize safety impacts.

Coordination Malfunction

The operational function affected is "Maneuvering coordination management" and is distinguished by the IW and VW configurations. In either case, the logical transition would be to allow AHS operation without maneuver coordination, i.e. remain on the AHS as a free agent vehicle.

Check-out Phase Malfunctions

The operational function affected is the "Normal transition from automatic to human control" and is initiated by failures in the "Normal maneuver coordination planning", "Human-machine interface", "Information link between the coordination layer and the regulation layer", "Information link between the regulation layer and the physical layer", "Manually maneuver vehicle", and "Provide information". As this operational function takes place after the vehicle enters the exit area or transition lane, the major concern is the driver interface and driver condition. The exception is for the UE configuration where no transition lane exists and thus severe safety impacts can occur with coordination related failures. For all the situations, the logical transition would be to a "Stop" operational function immediately. The impact on those configuration with a transition lane would be minimal, with the UE configuration suffering from link closure.

Representative System Configurations

Examination of the number of high safety and efficiency severity levels assessed by the RSCs was performed. Tables E2 and E3 contain shaded boxes of non-high safety and efficiency severity levels for each of the RSCs. These shadings provide an indication of the differences between the four RSCs. While it may be premature to draw too much from these differences, especially as previously mentioned that the assessments are subjective, some distinct characteristics emerge.

- The IW UE RSC is undoubtedly the most risky system with respect to likelihood for malfunctions.
- BT is the safest regardless of IW or VW.
- The VW UE RSC becomes high risk due to the uncertainty surrounding the exit. If this could be resolved, it would indeed become the most promising and least expensive RSC.
- The VW RSCs are more efficient that the IW RSCs.

Two major observations are made. Most of the high safety malfunctions occur at the regulation or physical layer, i.e. on the vehicle, for both IW and VW configurations and only the IW configuration introduces another subsystem failure point of the control center information processor. Essentially all the high efficiency safety malfunctions are associated with the IW configuration, with the VW subsystems a subset of the IW subsystems.

We analyze the elemental malfunctions by layers.

Link Layer Malfunctions

The elemental functions failure performed in this layer that results in a high safety severity level malfunction is the "Lane assignment". This elemental function is rated high only for the IW UE configuration with allocation to the control center information processor.

As noted in the Rockwell Vehicle Operations Analysis report, the computational load could be significant for the "Lane assignment" elemental function. As this is an IW configuration, the allocated subsystem of a control center information processor allows two major benefits to mitigate the potential malfunction. The design and usage of redundancy is facilitated through the concept of using a link layer. Basic redundancy can be built into the system by using adjacent links with the downside being the increased computational load. Another benefit is that the design of the hardware and software should be better controlled if the public agency, the local department of transportation, manages their development. The drawback is that each malfunctions could have substantial consequences as it may affect many vehicles, while the IW BT and VW configurations have less severe consequences during the operational function of "Steering for lane-changing", as noted by the lack of a VW configuration high safety severity level assessment.

In addition to the control center information processor, the roadway sensors & instrumentations failure results in malfunctions with high efficiency severity levels. As the roadway sensors & instrumentations are generally publicly funded equipment, requirements for standardization and open systems should both lower cost and raise reliability through competition of these products.

Coordination Layer Malfunctions

The elemental functions failures performed in this layer that result in a high safety severity level malfunction are the "Normal maneuver coordination planning" and "Maneuvering coordination planning for hazardous conditions". These elemental functions are allocated to the control center information processor for the IW configurations and the vehicle information processor for the VW configuration.

As noted in the Rockwell Vehicle Operations Analysis report, the processing requirements for these two elemental functions are moderate. Thus the design and implementation with built-in redundancy through adjacent links should suffice for the IW configurations; drawback is greater impact of malfunctions. The VW configurations should also design with on-board redundancy using self monitoring/self diagnosis. However, the vehicle information processor hardware and software development raises many issues regarding developmental guidelines and standards. For example, automotive software development guidelines are yet to be established. It is suggested that the efforts of the Federal Rail Administration (FRA) with respect critical safety software development be reviewed for applicability for automobiles, along with expected guidelines developed by the Motor Industry Software Reliability Association in the United Kingdom. This dictates that software development be an integral part of the system development establishing software reliability from prototypes through production.

The high efficiency severity level malfunctions are all IW configurations due to control center information processor failures. Strategies developed from the safety perspective is also applicable for the efficiency perspective.

Regulation Layer Malfunctions

The elemental functions failure performed in this layer that results in a high safety severity level malfunction are the "Speed regulation command", "Braking command', and the "Steering control command". These elemental functions are all allocated to the vehicle information processor. The number of malfunctions due to failures at the regulation layer and specifically the vehicle information processor emphasizes the issues raised previously regarding standardization for automobile software development, especially with the safety critical ramifications.

Physical Layer Malfunctions

The elemental functions failures performed in this layer that result in a high safety severity level malfunction are the "Actuation", "Sensing", "Human-machine interface", "Information link between the network layer and the link layer", Information link between the coordination layer and the regulation layer", "Information link between the regulation layer and the physical layer, "Manually maneuver vehicle", and "Provide information".

The distinctions between high safety severity level malfunctions for the IW and VW configurations are that the VW configuration includes a vehicle external communication failure and the IW includes vehicle information processor and roadway sensors & instrumentation failures.

With the exception of the driver input, the mitigation strategies for the subsystems include general solutions such as developing an open, thus standardized system. Use redundancy wherever feasible and design in fail-safe mechanisms. However, for the driver input, the options are more limiting. Certainly issues such as driver training and the need to incorporate it as part of the system development is critical. Recognizing the driver inputs as a part of the AHS system, and then establishing requirements that are both achievable and testable are vital.

As with the regulation layer high efficiency severity level malfunctions, the high efficiency severity level malfunctions of the physical layer are addressed with the safety severity levels analysis of the vehicle information processor and the driver input.

4.1.3 Vehicle Operations Analysis

The following observations and conclusions were derived from the Vehicle Operations Analysis study:

1. Because of the significant communications requirements between the coordination and Regulation layer for the Maneuver planning function, it appears that the maneuver planning function of the Coordination layer should be done on the vehicle. This allows the coordination-regulation communications to be intra vehicle instead of infrastructure-vehicle communications.

Additional analysis must be done to examine other issues related to performing the coordination function on the vehicle. Stability must be examined within the context of specific algorithm approaches across expected operating regimes. System level performance evaluation will require treatment of the AHS as a complex adaptive system whose behavior is determined by the interaction among semi-autonomous individual entities that communicate largely asynchronously and employ limited information bases.

2. Because of the information processing requirements, it appears that the Link Layer should be performed by the infrastructure rather than the vehicle. Additional analyses are required to examine in more detail specific optimization algorithms and the associated processing requirements.

3. The communication function is critical for control of strings of vehicles based on the spacing distance control. Autonomous or time headway control approaches are more robust to losses of communication. With spacing control, the absence of communication does not guarantee us attenuation of errors down a string of vehicles. The errors in tracking can be reduced through accurate estimators. If spacing control methods are used the communication control is critical.

4. The noise experienced in a platoon is a percentage of the target spacing. Hence spacing errors will be larger at larger target spacings. Vehicles following at larger spacing, albeit safer, will not necessarily result in the best form of control. Low gain controllers must be designed to ensure that small variations in spacing errors do not translate into high control effort and actuator saturation.

5. The effect of actuator limitations was studied but it was found that throttle actuators at least as fast as 150 ms are fast enough for the frequency and type of maneuvers that can be expected in automatic vehicle control on highways. Brake actuators slower than 150 ms can lead to poor tracking performance during high jerk deceleration maneuvers.

6. The closing rate function is by far the most important function for longitudinal control. Performance is greatly degraded in the absence of closing rate information. In addition, if the communications are not working, potentially hazardous situations can arise due to large lags in acceleration tracking. The degradation of performance without closing rate and communication information is true regardless of the control approach used. The closing rate function is safety critical.

7. Self-diagnosis and self-monitoring technology can have significant benefit to improving the safety of AHS. Additional study is needed to determine the best technology approach and whether it is best to have a centralized self monitoring elemental function or to have a distributed monitoring capability with each element performing its own diagnostics.

4.2 RECOMMENDED FURTHER INVESTIGATIONS

4.2.1 Lateral and Longitudinal Control Analysis

1. Safety distance between two vehicles depends upon many deterministic and random factors, e.g., velocity, road surface condition, tires, and weather. Should the safety distance be established upon the worst scenario (e.g., brick wall stop) or probability basis?

2. Can safety distance between vehicles be preset realistically? If not, how to establish it adaptively in real time?

3. To standardize longitudinal control systems of automated vehicles the following requirements need to be defined: ride comfort, the mobility of vehicles in an AHS, the nominal gap, the maximum tolerable gap variation, the maximum tolerable impact energy for platooning.

4. While the efficiency of a Lane Change Maneuver can be optimized given a particular traffic condition, the optimization is often accomplished at the expenses of system robustness. The trade off between efficiency and robustness requires careful analysis, tuning, and tests in the future.

5. How much and when the driver will be given control of the vehicle to perform an LCM from an automated lane to a manual lane, and vice versa in UE mechanization?

6. How to estimate the necessary lead time to initiate an LCM which is constrained by the location and length of the opening of a physical barrier between an automated and transition lane as in a BT mechanization?

7. Since lateral and longitudinal control systems are always operated simultaneously, and they are usually designed and analyzed separately, the possibility of adverse cross-axis interactions should be minimized to ensure the total system integrity. For example, the minimization of the effect of weight shift between front and rear tires on lateral maneuverability when the vehicle is accelerating longitudinally.

8. What is the effect of LCM on lane keeping? Biasing the vehicle's reference lateral position to, perhaps, the center line of the receiving lane?

4.2.2 Malfunction Management and Analysis

AHS malfunctions were examined in context of operational functions, the four RSCs of an AHS, and the elemental functions and their allocated subsystems. Following are issues identified and addressed for each of these three areas where further investigations are recommended.

1. During an AHS "check-in," a malfunction due to coordination planning failure can occur and go undetected. If it is detected and if the configuration is IW, then an entire link would most likely be closed down. If the configuration is VW, then the vehicle must be stopped and an operational "Stop" function would be implemented and in either configuration, the malfunction effects can be eventually mitigated. However, the issue is with the detection of the malfunction.

An effective method of detecting this malfunction would be an extension of current traffic surveillance systems. As this was evaluated as a malfunction with high safety severity for all four configurations, it is highly likely that this malfunction and its mitigation must be addressed by any AHS design. If such a capability were to be developed, how and when should it be addressed by those building an AHS and what type of interface with it have with other roadside and vehicle detection mechanisms?

2. It is inevitable that a speed or steering control malfunction will occur. The cause of this malfunction ranges from actuator failure to speed regulation software error, i.e. a hardware stops working completely to an intermittent glitch. Due to the timing requirements for speed and steering control, detection methods might not provide enough fidelity. Thus, malfunction management strategies might rely upon Monte Carlo-type statistical results based upon simulations. One strategy is to hardwire a braking capability and apply full braking.

Defining malfunction strategies based upon probability of occurrence is straightforward. The difficulty would be in any required trade-offs between safety and efficiency. While one naturally wants always to prioritize safety, continuous stopping will certainty dissuade the most avid AHS user. Thus, a better definition of safety and efficiency requirements become necessary for detailing malfunction management strategies.

3. The resolving of many of the perceived risks of "check-out" through technology development, rather than malfunction management strategies, can cast positive light on AHS, specifically the VW UE configuration. As the VW UE configuration appears to be the least costly in terms of infrastructure costs, it appears to be the easiest concept to sell. Thus, to best promote an AHS, emphasis should be placed upon the resolving of the "check-out" risks specifically the operation of the transition from automatic to human control with potential failures such as proper manual vehicle maneuvering or driver capability testing.

4. Nearly 1/3 of the expected high safety severity level malfunctions are expected to arise with software related origins. Of these, most are listed as vehicle based, i.e., most probably due to a vehicle processor fail ure and/or embedded software error, and a few are listed as infrastructure based, i.e., most probably due to a roadside processor failure and/or software error. The area of software error in general has proven itself difficult to manage, with safety critical vehicle processor embedded software of high concern. The current Department of

Transportation and Federal Highway Administration attitude would appear to be a conservative approach to the software issue leveraging off the continuing improvements and advances in software without direct investment, along with revelations from studies undertaken in other industries. On the basis of review of software and safety status, software development, emerging standardization efforts, legislative aspects, and perspectives from other in dustries, it is recommended that the issue of automobile software development standardization be examined by the federal government. Issues to be addressed include the extent of involvement, i.e., should the software impacts to AHS only or automotive in general be analyzed, and gaining the detailed "lessons learned" from other industries.

5. Physical layer elemental functions with high safety and efficiency severity levels for IW and VW configurations allocated to the driver input include "Manually maneuver vehicle" and "Provide information". As these two functions are critical to entering and exiting the AHS, the driver is critical as evidenced by its definition as a major system of the AHS. Yet too often even if the human is an integral part of a system, the design does not consider human design constraints or requirements, rather human operational constraints or requirements result.

For the successful implementation of AHS, the driver and driver training issues must be considered as part of the system development. Just as technology assessment and infusion are considered for the design, driver training and expected driver changes must be considered, i.e., work to simulate driver reactions and incorporate human factors requirements should be extended to simulate how driver reactions can and are going to change and design for the incorporation of these changes.

4.2.3 Vehicle Operations Analysis

1. The maneuver planning function appears to be best performed on the vehicle. Issues relating to overall system stability, specific algorithm approaches, and system performance should be examined. Vehicle-based coordination layer functions should be investigated in the context of a complex adaptive system of interacting semi-autonomous agents.

2. Self diagnostic- self monitoring technology can significantly improve AHS fail-safety. Detailed analysis of failure mode time histories should be defined for key AHS sensors and actuators and specific self diagnosis algorithms developed and evaluated.