Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

AHS PSA Malfunction Management and Analysis

U.S. Department of Transportation
Federal Highway Administration
Publication No. FHWA-RD-96-049
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-96-050	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS AHS PSA Malfunction Management and Analysis		5. Report Date January 1996 6. Performing Organization Code
7. Author(s) R. Aikawa, Q. Marston		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, 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

The overall goal of this task included defining the boundaries of an AHS, establish 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.

This document type is resource materials.

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 135	22. Price

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

Table of Contents

List of Figures

List of Tables

1. EXECUTIVE SUMMARY

This document identifies potential malfunctions and develops mitigation strategies for these malfunctions that may be encountered when an AHS is operational. This documents the Rockwell Malfunction Management and Analysis task for the Precursor Systems Analysis of Automated Highway Systems.

The Rockwell team philosophy and approach are built around the goal of mitigating the numerous malfunctions that might arise in an operational AHS. Effort was expended to maintain a systems perspective and develop malfunction management strategies applicable to any AHS design.

Thus, as we step towards an automated highway, it was imperative that we 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. We developed operational sequences through which the functions were executed and identified subsystems which were then allocated functions. As with the understanding of system functionality, it was of equal importance to understand the malfunctions of the system. We defined metrics to gauge the severity of the malfunctions in terms of their effects on the goals of the system. We performed this analysis by attempting to understand the relationships 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 assumed system configuration. We looked for commonalities and differences between malfunctions and system configurations, then offered strategies to help mitigate or avoid these malfunctions and further, raised issues and risks involved with these malfunctions and strategies.

Confidence in the analysis was supported through the usage of a Computer Aided Software Engineering (CASE) tool, Statemate. It's modeling capability of both functional and behavior aspects of a system along with its structured analysis foundation provided a mean 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 the exercise to develop the model provided much guidance in our analyses.

1.1 METHODOLOGY

A six-step approach was used to perform this analysis. These six tasks were arranged to maximize the synergy between the tasks and what information was required before the start of 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.

1.1.1 Task 1 - Define Measures of Effectiveness

Measures of effectiveness were defined providing a foundation for the evaluation of the malfunctions. Both safety and efficiency (throughput) were described in terms of their impact due to the malfunctions.

1.1.2 Task 2 - 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 was in context of these operations relative to the RSCs that the malfunctions were examined.

1.1.3 Task 3 - Formulate Major System Categories for Malfunction Breakdown

Evaluation of malfunctions demanded an understanding of what subsystem malfunctioned. Thus, for each of the RSCs, allocations of AHS functions to major subsystems were made. On the basis of these allocations, evaluations of malfunctions were made.

1.1.4 Task 4 - Evaluate AHS Operation Severity

Given the completion of tasks 1, 2, and 3, an evaluation of AHS malfunctions was performed. An operational function malfunction was assumed for each RSC. On the basis of which elemental function and thus which major subsystem might have failed, an evaluation of the impact of the malfunction using the MOEs was performed.

1.1.5 Task 5 - Apply Malfunction Management Strategies for Deriving Issues and Risks and Analyze Options to Alleviate Risks

The results of task 4 were compiled and analyzed. Understanding of the significance of the various RSCs, the major subsystems, and operational functions, provided the foundation for development of mitigation strategies.

Various architectures were examined resulting in the adoption for this analysis of the two-layer functional architecture developed by PATH and Honeywell[6] and the five-layer communication and control architecture developed by PATH[7]. Namely, the functional requirements analysis, including the definition of elemental and operational functions, performed by the Rockwell Vehicle Operational Analysis[8] team was used as the baseline.

Two sets of complementary mechanizations, four RSC's, were proposed. These combinations are provided in table E1. These four RSC's were examined extensively as the analysis was performed.

Table E1. 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		

1.2 SUMMARY OF RESULTS

The AHS is comprised of three major systems: the roadway, the vehicle, and the driver. Each major system is in turn comprised of primary subsystems. Note that only specific components of the vehicle and actions of the driver are considered part of the AHS. The driver interfaces with the AHS at different layers dependent upon the specific design and only the direct actions that relate to input and the display or presentations of information to the driver are considered as part of the AHS.

The operational functions provide an AHS functional description in the time perspective of a single vehicle as it enters, operates on, and then exits the system. It was defined that a malfunction of an operational function occurs if one or more of the elemental functions malfunctions. The severity levels of these operational malfunctions are highly dependent upon the specific failures.

Collision severity evaluation criteria were used to ask the following questions:

- What are the anticipated changes in acceleration?
- What is the maximum acceleration?
- What is the maximum approach velocity?

Casualty estimation evaluation criteria were used to ask the following questions:

- Is this a platoon or free agent and what maneuvers and velocities were involved?
- What is the vehicle mass?
- What is the coefficient of friction?
- What was the delta velocity between colliding vehicles?
- What was the traffic flow?
- Were there any initiating incidents?
- What was the reliability requirement?

Efficiency evaluation criteria were used to ask the following questions:

- What is the expected impact on average travel speed?
- What is the expected impact on repeatability of travel time?

- What is the expected impact on how good the predicted travel time is compared to the actual travel time?

Malfunction severity levels were used in categorizing the subsystem failure of a particular operational malfunction in a defined RSC. The four RSC's were separated into IW and VW for primary subsystem categorization. Under these two categories, the primary subsystem and barrier plus transition and unrestricted-entry mechanizations headings were applied.

Tables E2 and E3 provided groupings of the high rated malfunctions by operational functions in terms of safety and efficiency effects, respectively. Shaded boxes highlight the differences between the RSC's. Tables E5 and E6 provided groupings of the high rated malfunctions by elemental functions in terms of safety and efficiency effects, respectively. Shaded boxes highlight the similarities between the IW and the VW configurations.

Table E2. Operational Function Malfunction Safety High Severity Levels

		RSC			
Operational Functions	**Elemental Functions**	**IW BT**	**IW UE**	**VW BT**	**VW UE**
Entering the system	Manually maneuver vehicle	High	High	High	High
Transition from human to automatic control	Normal maneuver coordination planning	High	High	High	High
Transition from human to automatic control	Manually maneuver vehicle	High	High	High	High
Velocity regulation	Speed regulation command	High	High	High	High
Velocity regulation	Braking command	High	High	High	High
Velocity regulation	Actuation	High	High	High	High
Velocity regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Spacing regulation	Speed regulation command	High	High	High	High
Spacing regulation	Braking command	High	High	High	High
Spacing regulation	Sensing	High	High	High	High
Spacing regulation	Actuation	High	High	High	High
Spacing regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Longitudinal position regulation	Speed regulation command	High	High	High	High
Longitudinal position regulation	Braking command	High	High	High	High
Longitudinal position regulation	Sensing	High	High	High	High
Longitudinal position regulation	Actuation	High	High	High	High
Longitudinal position regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Lane tracking	Steering control command	High	High	High	High
Lane tracking	Sensing	High	High	High	High
Lane tracking	Actuation	High	High	High	High
Lane tracking	Information link between the regulation layer and the physical layer	High	High	High	High
Steering for lane-changing	Lane assignment	Med	High	Med	Med
Steering for lane-changing	Steering control command	High	High	High	High
Steering for lane-changing	Sensing	High	High	High	High
Steering for lane-changing	Actuation	High	High	High	High
Steering for lane-changing	Information link between the regulation layer and the physical layer	High	High	High	High
Maneuvering coordination management	Maneuvering coordination planning for hazardous conditions	High	High	High	Med
Normal transition from automatic to human control	Normal maneuver coordination planning	Med	High	Med	High
Normal transition from automatic to human control	Human-machine interface	High	High	High	High
Normal transition from automatic to human control	Information link between the coordination layer and the regulation layer	Med	High	Med	High
Normal transition from automatic to human control	Information link between the regulation layer and the physical layer	Med	High	Med	High
Normal transition from automatic to human control	Manually maneuver vehicle	High	High	High	High
Normal transition from automatic to human control	Provide information	Med	High	Med	High

Table E3. Operational Function Malfunction Efficiency High Severity Levels

Operational Functions	Elemental Functions	RSC			
		IW BT	IW UE	VW BT	VW UE
Transition from human to automatic control	Normal maneuver coordination planning	High	High	Med	Med
Transition from human to automatic control	Manually maneuver vehicle	High	High	High	High
Steering for lane-changing	Lane assignment	High	High	Med	Med
Maneuvering coordination management	Regional traffic conditions monitoring and incident management	High	High	Med	Med
Maneuvering coordination management	Maneuvering coordination planning for hazardous conditions	High	High	Med	Med
Normal transition from automatic to human control	Human-machine interface	High	High	High	High

Table E4. Primary Subsystems Impacted by High Safety Severity Malfunctions.

Infrastructure-Weighted		Vehicle-Weighted	
Primary Subsystem	Number of High Safety Severity Malfunction	Primary Subsystem	Number of High Safety Severity Malfunction
Control center information processor	4		
Vehicle information processor	13	Vehicle information processor	12
Roadway sensor & instrumentation	4		
Vehicle external sensor	4	Vehicle external sensor	4
Vehicle internal actuator	5	Vehicle internal actuator	5
Vehicle internal sensor	4	Vehicle internal sensor	4
Control center communication	1	Control center communication	1
		Vehicle external communication	1
Vehicle internal communication	6	Vehicle internal communication	6
Driver input	4	Driver input	4

Table E5. Primary Subsystems Impacted by High Efficiency Severity Malfunctions.

Infrastructure-Weighted		Vehicle-Weighted	
Primary Subsystem	Number of High Efficiency Severity Malfunction	Primary Subsystem	Number of High Efficiency Severity Malfunction
Control center information processor	4		
Vehicle information processor	1	Vehicle information processor	1
Roadway sensor & instrumentation	1		
Driver input	1	Driver input	1

1.2.1 Operational Malfunction Management Strategies

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

"Stop" operational function and the invoking of a free-agent mode during the coordination management operational function.

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".

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 shall be added to the operational functions..

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 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.

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.

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 immediately transition to a "Stop" operational function. The impact on that configuration with a transition lane would be minimal, with the UE configuration suffering from link closure.

1.2.2 Representative System Configuration

Examination of the number of high safety and efficiency severity levels assessed by the RSC's was performed. Tables E2 and E3 contain shaded boxes of non-high safety and efficiency severity levels for each of the RSC's. These shadings provide an indication of the differences among the four RSC's. While it may be premature to draw too much information from these differences, especially in light of the subjective nature of the assessments previously mentioned, some distinct characteristics do 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 potentially least expensive RSC.
- The VW RSC's are more efficient that the IW RSC's.

1.2.3 Elemental Malfunction Management Strategies

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. Nearly all the high efficiency safety malfunctions are associated with the IW configuration, with the VW subsystems essentially a subset of the IW subsystems.

The elemental malfunctions are analyzed for each layer.

Link layer

The elemental functions failure 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.

In addition to the control center information processor, the roadway sensors & instrumentations failures result in malfunctions with high efficiency severity levels. As the roadway sensors & instrumentation's 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

The elemental functions failures 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.

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

The elemental functions failure 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

The elemental functions failures 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".

With the exception of the driver input, the mitigation strategies for the subsystems include general solutions such as developing an open, thus standardized systems, 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.

1.3 ISSUES

AHS malfunctions were examined in context of operational functions, the four RSC's 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.

1.3.1 Operational Functions

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 will 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, similar to the concept of a crashstop mode[14] followed by a stop mode.

Defining malfunction strategies based upon probability of occurrence is straightforward. The difficulty would be in any required trade-off 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 becomes necessary for the detailing of malfunction management strategies.

1.3.2 Representative System Configurations

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

The resolving of many of the perceived risks of "check-out" phase 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" phase 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.

1.3.3 Elemental Functions - Primary Subsystems

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

This report documents nearly 1/3 of the expected high safety severity level malfunctions to arise with software related origins. Of these, most are listed as vehicle based, i.e., most probably due to a vehicle processor failure 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 industries, 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 includes "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.

2. INTRODUCTION

2.1 DESCRIPTION OF ACTIVITY AREA

As today's highway system evolves into an Automated Highway System, the functionalities of our highway system will change as will its malfunctions and the strategies we will employ to manage these malfunctions. This analysis seeks to define the functional requirements of an AHS, propose operational configurations, identify potential malfunctions, evaluate the malfunction severity levels, develop malfunction management strategies, and surface issues and risks encountered during this process.

2.2 PURPOSE OF THIS EFFORT

Today's complete highway system includes fully controlled access freeways, principal or major arterials, minor arterials, collector roads and streets, and local roads.[1] These different classes are characterized by the nature, type, and length of trips, and general traffic volume. Freeways are fully controlled access highways, with no at-grade intersections or driveway connection designed to provide the highest level of safety and availability of service. Arterials carry longer-distance major traffic flows between important activity centers. While we are able to define the components of the system, the functional requirements especially with respect to defining the boundaries of this system are not as well defined. In fact, we call a flat tire, an overturned truck, and a road closure highway malfunctions. Yet without defining the boundaries of the highway system we are indeed saying that if a vehicle has a flat tire or is overturned, then the highway system has malfunctioned while in fact it is the vehicle that has malfunctioned. However in examining a road closure, we see that truly the highway itself has failed in providing the means for transporting people and good. As we step towards an automated highway, it is imperative that we seek first to define the boundaries of our system before analyzing its malfunctions.

Once functional requirements have been established, potential configurations are suggested upon which we perform initial analyses. We develop operational sequences through which the functions are executed and identify subsystems which have been allocated functions. As with understanding the functionality of the system, it is of equal importance to understand the malfunctions of the system. We define metrics to gauge the severity of the malfunctions in terms of their effect on goals of the system. We perform this analysis by attempting to understand the relationships of these malfunctions to the operational configurations we assumed and the contexts in which the malfunctions occurred, i.e. when during an operational sequence did the malfunction occur and what was the system configuration. We look for similarities and differences between malfunctions and system configurations, then offer strategies that help to mitigate or avoid these malfunctions and raise issues and risks involved with the malfunctions and their strategies.

Confidence in the analysis is supported 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 the exercise to develop the model provided much guidance in our analyses.

2.3 ISSUES ADDRESSED

Table 1 lists the malfunction management issues identified as compiled by the MITRE Corporation.[2] As indicated in the referenced document, this table is used to provide an indication of the issues addressed in this study relative to other malfunction management and analysis studies.

Table 1. 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 RSC's.

2.4 OVERALL APPROACH

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

These six tasks are arranged to illustrate the timing of the effort and what information is required before the start of 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. Task 4 requires the analysis to be performed after the completion of the prior three tasks. Task 5 requires analysis from task 4. Task 6 is the documentation of the final report.

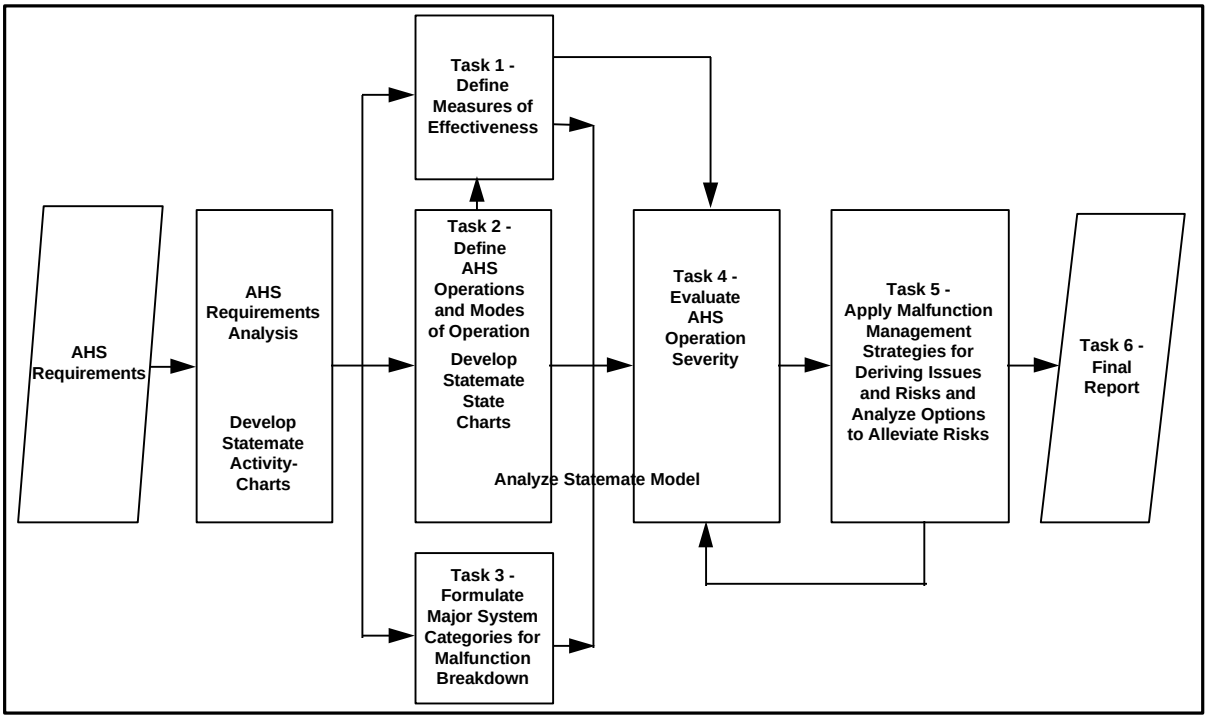


Figure 1. Malfunction Management and Analysis Task Flow.

2.4.1 Requirements Analysis

The requirements analysis examines the AHS program requirements as provided in the Broad Agency Announcement for Precursor Systems Analyses of Automated Highway Systems.[3]

Key program requirements, such as:

- All vehicle types supported in mature system,
- Vehicles contain instrumentation allowing AHS control,
- Instrumented vehicles able to operate on non-instrumented roadways,
- Only instrumented vehicles allowed to operate on instrumented roadways,
- Non-instrumented vehicles instrumented on retrofit basis,
- Operation on a freeway type roadway,
- Perform improvements in:
  - Safety,
  - Efficiency,
  - User comfort, and
  - Environmental impact,
- Operable in wide range of Continental United States weather conditions, and
- Primary control and guidance system rely on non-contact electronics-based technology

were analyzed.

Two products were developed prior to this study - a functional analysis and representative system configurations - based upon the AHS requirements. The functional analysis resulted from a search for an existing functional description of an AHS; the work performed by PATH (see the Guiding Assumptions section of this report) was adopted for this study. Similarly, the representative system configurations developed for the Rockwell tasks and documented in the submitted proprosal were utilized (see the Representative Systems Configurations section of this report).

The significance of these two products are emphasized throughout this report as they form the basis for the analyses.

2.4.2 Task 1 - 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 impacts due to the malfunction.

2.4.3 Task 2 - Define AHS Operations and Modes of Operation

In addition to focusing 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 RSC's and functions that the malfunctions are examined.

2.4.4 Task 3 - Formulate Major System Categories for Malfunction Breakdown

Evaluation of malfunctions demands an understanding of what subsystem malfunctioned. Thus, for each of the RSC's, allocation of AHS functions to major subsystems were made. Based upon these allocations, evaluation of malfunctions are made.

2.4.5 Task 4 - 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 - thus which major subsystem might have failed, an evaluation of the impact of the malfunction using defined MOEs is performed.

2.4.6 Task 5 - Apply Malfunction Management Strategies

The results of task 4 are compiled and analyzed. Understanding the significance of the various RSC's, the major subsystems, and operational functions, provides the foundation for development of mitigation strategies.

2.4.7 Comparative Fault and Failure Analysis Techniques

To compare this task approach against two commonly used fault and failure analysis techniques, brief explanations on Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) are presented.[4]

Fault Tree Analysis

A FTA is an analytical technique whereby a fault in the system is specified and the system is then analyzed to find all credible ways in which the fault can occur. The tree itself is a graphical model representing the various parallel and sequential combinations of faults that will result given the fault. Thus, the tree presents logical relationships that lead to the fault, where the fault resides at the top of the tree.

The FTA is not a model of all possible system failures or all their causes. The tree is tailored to the specific fault and those faults contributing to it, and examines only the most credible faults as assessed by the analyst.

The FTA is a qualitative model that can be evaluated quantitatively. Qualitative results provide: a) the smallest combination of component failures that can cause the system failure, b) qualitative component rankings with respect to its contribution to the system failure, and c) common cause potential failures identification due to a single failure cause. Quantitative results provide: a) numerical probabilities of system failures and distribution of the combination of component failures, or components themselves, leading to system failures, b) quantitative rankings of them, and c) sensitivity and relative probability evaluations to determine effects of implementing changes in maintenance times, component reliability, design modifications, etc.

Failure Mode and Effect Analysis

A FMEA studies the results or effects of item failure on the system and classifies each potential failure according to its severity. The two primary approaches is a hardware item approach listing individual hardware items and analyzes their possible failure modes and a functional approach analyzing each function. A combination of the two approaches is often used for complex systems. The study can be performed top-down or bottom-up until all failure modes are examined.

2.4.8 System Specifications Modeling with Statemate

The performance of a system malfunction analysis requires an understanding and subsequent derivation of the system requirements by means of system requirements analysis. Through this system requirements analysis, a functional analysis in conjunction with operational concepts is performed. In traditional development processes, ambiguities in system requirements go unresolved or undetected. Often, the system doesn't work as expected, may not fulfill operational requirements, or may completely fail. A malfunction analysis of such a system depends heavily upon the assumption that ambiguities don't exist. The use of a CASE tool proves to be an enormous asset in converting the ambiguities into certainties. Statemate, by i-Logix Inc., supports the development of clear, accurate, graphical specifications as a foundation for reliable and predictable systems.

The malfunction analysis of Automated Highway Systems (AHS) begins with the analysis of the functions required to be performed by the system. An understanding of the operation of the system provides a basis for relating the functions in a logical sequence. These two aspects of a system, namely the activities and behaviors, can be easily described using the Statemate Activity-Charts and Statecharts.

The Statemate Activity-Charts are similar to conventional data flow diagrams depicting data and control flows along with the system's external environment. These charts create a hierarchical decomposition of the system's processing capabilities using a visual graphical language. Similarly, the Statecharts represent the system's behavior over time depicting the control aspects of the functions. The system states and transitions are identified hierarchically. A third perspective of the system, the physical view using Module-Charts is also available to describe hardware and software components and their relationship to elements of the Activity-Charts and Statecharts. For this precursor analysis, decomposition of the system to the component level was not performed; hence, Module-Charts of the AHS were not created.

The development of the Activity-Charts and Statecharts alone do not provide the total means for a thorough system requirements analysis methodology. The systematic approach demands a better understanding of the system's functionality with logic and syntax checks. Additional Statemate analysis tools allow such an analysis of the Activity-Chart/Statechart model. These tools perform simulations and prototyping. The simulation capability allows identification of unacceptable system behavior. With the ability to create panels, the model animates in response to inputs providing clear visual results of specifications. Batch mode simulations, in addition to an interactive mode, allow analysis of complex and random scenarios as well as creating situations not explicitly created. This, in effect, creates a set of preliminary test requirements. Statemate than enables rapid, early prototyping translating the system model into high-level programming languages such as Ada or C. The prototype can then be hosted in the target environment and executed.

Along with these analyses capabilities, Statemate retrieves model and analysis information and produces documentation in useful formats. Working documents, standard format reports, and custom reports from a variety of templates allows accurate and complete documenting without heavy schedule impacts. In working with customers, the ability to verify and validate system specifications up front in the program is created. The conventional waterfall life cycle model and subsequent validation are shortened allowing rapid prototyping with customer interface.

The true usefulness of Statemate for this AHS Precursor Analysis on malfunctions has been the necessity of defining what the Automated Highway System is, what is external to it, and their interactions. As with any analysis, the assumptions are underlying to the conclusions. Using a CASE tool such as Statemate, the analysis exercise that is usually largely paper and pencil driven can be examined for logical flow and visual substantiation. To fully benefit from Statemate, all the state transitions must be accurately described with algorithms. On this precursor study, state transitions to allow two malfunctions to be analyzed were developed. The analysis of the remaining malfunctions is truly qualitative; however, the system and operational functions have been logically checked with Statemate. Within this report, references to Statemate will be made. The usefulness of Statemate shall be apparent as malfunctions are analyzed. The documentation of the Statemate modeling and simulation is provided in appendix A.

2.5 GUIDING ASSUMPTIONS

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 systems can be developed...". In

defining AHS, the term "fully automated intelligent vehicle-highway system" is interpreted 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 instrumented.[5]

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, as illustrated in figure 2, 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.

2.5.1 Functional Requirements

Rather than redevelop functional requirements, various architectures were examined with the two-layer functional architecture developed by PATH and Honeywell[6] and the five-layer communication and control architecture developed by PATH[7] adopted for this analysis. Namely, the functional requirements analysis, including the definition of elemental and operational functions, performed by the Rockwell Vehicle Operational Analysis team[8] was used as the baseline. The referenced document provides complete details on the functional requirements development and analysis.

As documented in the Rockwell Vehicle Operational Analysis team's report, the AHS control architecture includes the five layers shown in figure 3. The architecture slice, as enclosed by the bolded box in figure 3, is the method used to build the Statemate model, i.e., the slice provided a model of all of the elements of the architecture with the model growing through modular expansion (refer to Appendix A for complete details).

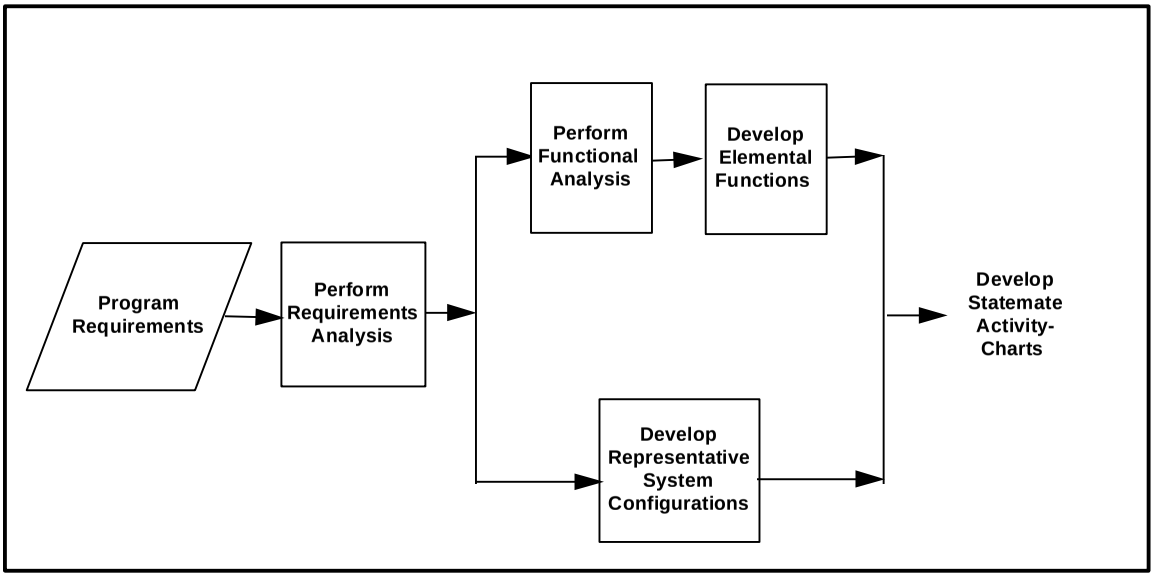


Figure 2. AHS Requirements Analysis.

The network layer provides overall route selection and flow control. The link layer provides path and lane selection and local congestion control. The coordination layer provides

coordination between vehicles. The regulation layer provides individual vehicle control and actuator control commands. The physical layer provides vehicle actuation and sensors. Attached to this five layer architecture are essential human factors that tie into the architecture at different layers depending upon the specific configuration.

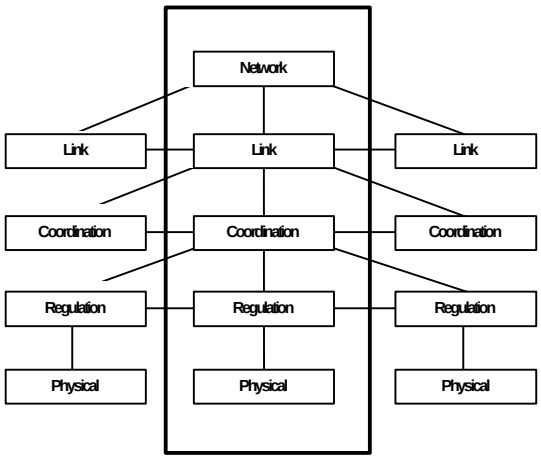


Figure 3. AHS Functional Hierarchical Architecture Slice.

2.5.2 Elemental Functions

Following are AHS functional requirements grouped into the five layers. Based upon the layered architecture, each layer is built on top of the lower layer and performs tasks with minimal support from other layers. These functions are called elemental functions; these are the functional requirements necessary to achieve an AHS. Also listed are functions that must be performed by human operators called essential human functions.

Network Layer

N1. Monitoring traffic conditions and predicting congestion: The network layer manages network traffic data and predicts when and where congestion will occur based on real-time traffic information.

N2. Vehicle ID assignment: Upon approving the request for entering, the network assigns an identification code to a vehicle. During the entire trip this ID code will be used for obtaining special instructions from the coordination or higher layers, and for coordinating maneuvers with other vehicles.

N3. Route recommendation: The route recommendation is developed based on users' requests and traffic conditions. Upon receiving the location and the destination of a vehicle, the network layer may recommend the shortest/fastest route. Route recommendation may be provided at the beginning of a trip or anytime during the trip. Route selection or route change may be requested by the vehicle operator or mandated by the network due to changes in traffic flow.

Link Layer

L1. Lane assignment: The link layer may provide lane assignments in accordance with the selected route and traffic conditions. Lane assignments may be given before lane-changing is needed, and at locations such as entrance, exit, or diverging points where decisions are needed for choosing a path.

L2. Target speed: The target speed is provided in accordance with the local traffic conditions.

L3. Maximum group size: When groups are used, the maximum size of group is provided based on the current traffic conditions.

L4. Minimal separations: The required minimal headway is provided in accordance with the weather and roadway conditions. In a system with groups the spacing between groups are provided.

L5. Prioritizing vehicle operations: Vehicles with special missions, such as ambulances or fire engines or high occupancy vehicles, are given priority over other vehicles.

L6. Regional traffic conditions monitoring and incident management: Traffic conditions are monitored. In the incident conditions, the link layer selects paths for vehicles, adjusts target speed, or instructs vehicles to changes lane for diversion around incidents.

Coordination Layer

C1. Off-vehicle inspection and monitoring: The vehicle inspection could be performed before the vehicle enters the AHS, or while the vehicle is on the AHS. The inspection and monitoring functions, which may work together with on-vehicle detection/diagnosis devices, provide vehicle health or condition reports.

C2. Issuing permission/rejection: Based on the inspection/monitoring outcome, the coordination layer issues permission for entering or remaining on the AHS. Should a fault(s) be detected, a rejection command will be issued.

C3. Maneuvering coordination planning: Maneuvering coordination planning determines the sequence of a number of vehicles performing a coordinated maneuver. Maneuvering coordination planning is performed for both normal and abnormal conditions.

C3.1 Normal maneuver coordination planning: Normal maneuvers that require coordination between vehicles, such as lane-changing, merging, entering or exiting an AHS, or joining or splitting a group, are handled by the coordination layer. A series of control commands which may include time and/or location for performing a specific maneuver will be developed for the affected vehicles in order to coordinate the sequences of coordination maneuvers. The coordination layer also sets up coordination protocols among the involved vehicles and determines commanded speed, location, and conditions for maneuvering action.

C3.2 Maneuvering coordination planning for hazardous conditions: Under hazardous conditions, the coordination layer provides information regarding specific hazards to vehicles which are potentially affected, and provides commands or instructions for avoiding collisions.

C4. Supervising the sequence of the coordinated maneuvers: The coordination maneuvers will be monitored by the coordination layer.

C5. Monitoring road surface conditions and weather: The coordination layer senses and provides information regarding weather and road surface conditions.

Regulation Layer

R1 Steering control command: Commands for providing the required lateral motion are constantly updated based on information regarding the vehicle's lateral position, yaw motions, lateral acceleration, and upcoming road geometry.

R2 Speed regulation command: The speed control command is issued based on the instruction provided by the coordination layer and sensor and vehicle performance feedback from the physical layer.

R3 Braking command: The braking command is issued when reduction of the vehicle speed is required. The braking command can be issued in combination with the speed control command.

R4 Vehicle condition monitoring and failure detection/diagnosis: Vehicle conditions will be monitored using the sensory information provided by the physical layer. Failure detection and diagnosis will be performed when a system fault is discovered.

R5 Trip progress monitoring: The trip progress will be monitored by reporting to the operator the information regarding vehicle location and traffic conditions and estimated arrival time.

Physical Layer

P1 Sensing: Five groups of sensory information are needed. The sensory information can be obtained through direct sensing or combined sensing and signal processing. These information include: sensing states of vehicle, sensing conditions of vehicle, sensing information about the infrastructure, sensing weather conditions, and sensing traffic signal/sign information.

P2 Actuation: Actuation is provided in two dimensions, steering and speed control. The speed control includes control of both the propulsion and the braking systems.

P3 Human-machine interface: The human-machine interface enables the human operator to monitor the performance of the vehicle, to adjust performance parameters within a reasonable working range, to be aware of hazardous conditions, and to take over control tasks if necessary. It may be implemented using audio, visual, or tactile displays, voice or key input devices, and steering and speed control mechanisms. These interfaces include: information display/warning, human input/inquiry, and manual control mechanisms.

P4.1 Information link between the network layer and the link layer: The network layer receives information regarding traffic conditions and route selection requests from the link layer. The network layer also provides information regarding route recommendation, traffic condition prediction information, and vehicle ID assignment to the link layer or to the intended recipient via the link layer.

P4.2 Information exchange between the link layer and the coordination layer: The link layer receives information regarding traffic conditions of the subsections within the link, designated destination of a vehicle, and information addressing the network layer from the coordination

layer. The link layer also provides information regarding vehicle operation parameters such as target speed and minimal separation to the coordination layer or to the intended recipient via the coordination layer.

P4.3 Information link between the coordination layer and the regulation layer: The coordination layer receives information regarding the requests for a coordinated maneuver, status information about affected vehicles from the regulation layer, and information addressing the link layer or the network layer, such as driver's inquiry, from the regulation layer. The coordination layer also provides information regarding operation commands which defines the sequences of coordination maneuvers, information such as road surface conditions and weather to the regulation layer, and information addressing the regulation layer from the link layer or the network layer.

P4.4 Information link between the regulation layer and the physical layer: The regulation layer receives information regarding sensory measurements and user's requests from the physical layer. The regulation layer also provides control commands to the physical layer.

Essential Human Functions

H1 Manually maneuver vehicle: The driver will be required to perform manual speed and steering control during the following operations: merging into mixed stream of traffic in the transition lane during entry, driving in a mixed stream of traffic prior to control transfer to the automated system during entry, merging into the stream of manual traffic to complete an exit, and driving in the mixed stream of traffic following a return to manual control on exit.

H2 Request information: The driver may request various kinds of information from the system, including: vehicle status, trip progress, and traffic conditions

H3 Receive information: The driver will receive information from the vehicle, the roadside, and the traffic management center.

H4 Provide information: The driver will be required to provide information to the system, including the following: requests to enter the AHS, destination, requests to immediately exit AHS, authorization for change from manual to automated mode, and responses to interrogation about readiness to resume manual control.

Two figures are provided that present illustrations of the elemental functions in context of the RSC's. After defining the system boundaries, the external interfaces to the system present the differences between the RSC's. Figures 4 and 5 depict the elemental functions within the infrastructure-weighted and vehicle-weighted RSC's respec-

tively.

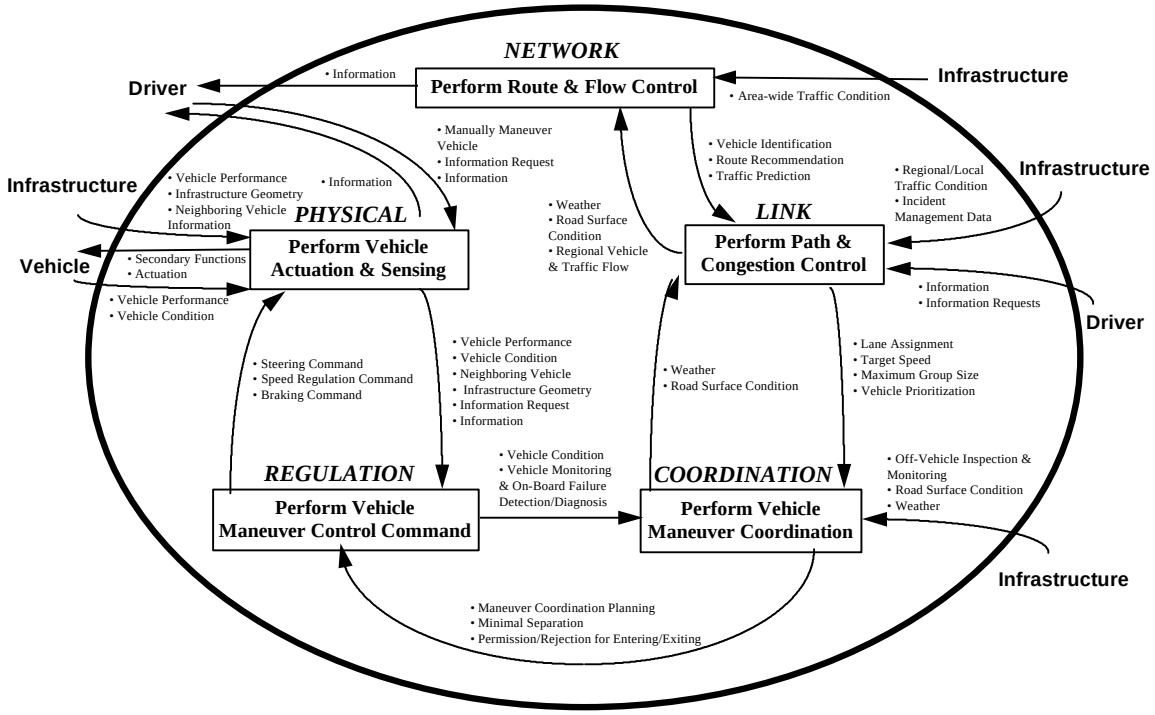


Figure 4. Functional Analysis for Infrastructure-Weighted Configuration.

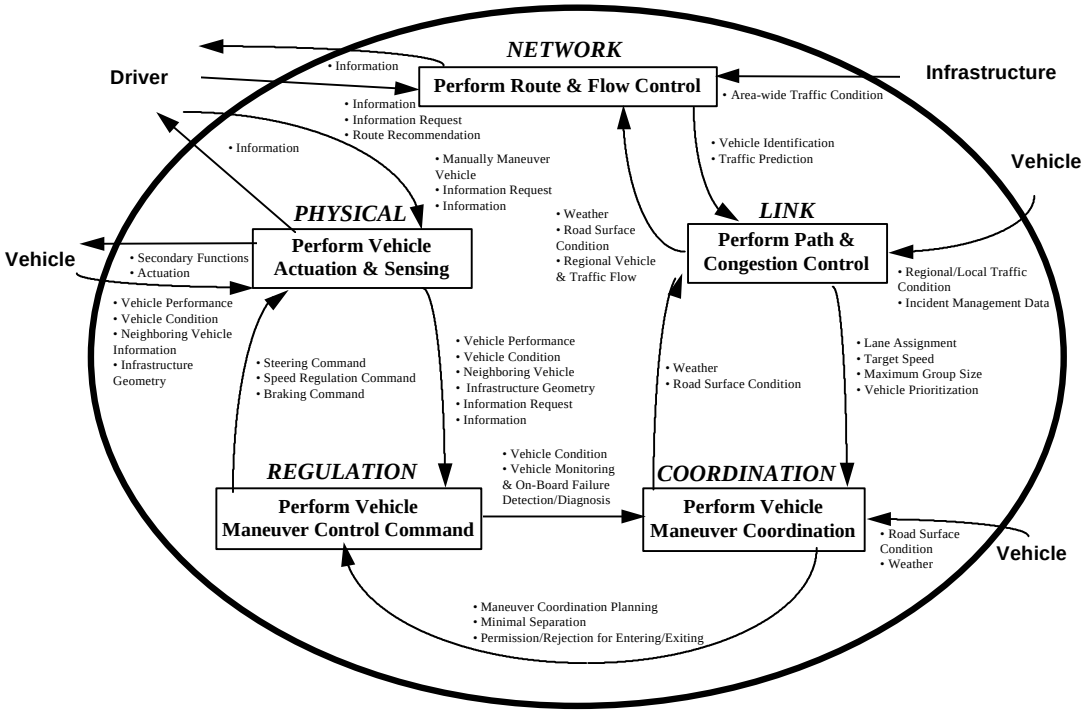


Figure 5. Functional Analysis for Vehicle Weighted Configuration.

3. REPRESENTATIVE SYSTEM CONFIGURATIONS

Four Representative System Configurations (RSC) have been identified that exemplify the contrasting features of the AHS characteristics. These four RSC's 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 RSC's.

The elemental functions (described in the previous section) must be carried out to effect an AHS. While each RSC must carry out all of these functions, the RSC's differ from one another in where and how each function is carried out. Although this can lead to much detail, i.e., what type of active or passive sensor, what kind of communication, or the specific control algorithms, this analysis will only allocate the functions to a primary subsystem. Allocation to a primary subsystem is assumed to be sufficient decomposition for the purpose of identifying issues and risks for this malfunction analysis.

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 is 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 affects 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 RSC's, are proposed. These combinations are provided in table 2. These four RSC's will be examined extensively as we perform this analysis.

Table 2. Representative System Configuration Characteristics Mapping.

	AHS Characteristics			
Selected RSC's	**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		

4. MEASURES OF EFFECTIVENESS

4.1 STRUCTURE AND PURPOSE

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.

4.2 ANALYSIS/ASSESSMENTS

Measures of Effectiveness (MOEs) are developed to evaluate functional performances, subsequently the performances in the presence of malfunctions (severity levels of malfunctions), and finally performances in the presence of malfunctions with malfunction management strategies (effectiveness of malfunction management strategies). A paraphrase of Mil-Std-499B definition of MOE is that of a metric used to quantify the performance of system functions in terms that describe the utility or value when executing the system mission. These MOEs are used for performance requirements assessments, including quantitative (how many or how much), qualitative (how well), timeliness (how responsive, how frequent), and readiness (availability, MTBF).

There are four key areas of improved performance expected from AHS compared to today's highway system. These areas are: (1) improved safety, (2) reduction in congestion, (3) reduced user strain and increased user confidence, and (4) reduction in harmful vehicle emissions. Malfunction management strategies will have the largest impact on safety and congestion (throughput).[5] Therefore, the MOEs are described around these two areas.

4.3 KEY RESULTS/CONCLUSIONS/ISSUES

4.3.1 Travel Safety

Travel Safety is measured in terms of Fatalities, Injuries, and Property Damage.[9] For safety, MOEs are the number of fatalities, injuries, and amount of property damage that (would) occur if the functional performance is compromised, i.e., a malfunction occurs. Thus, malfunctions are measured using these same MOEs.

To evaluate severity levels using the MOEs, the following Evaluation Criteria (EC) in the area of collision severity measures and casualties estimation are used:

1) Collision Severity Measures[10]: f(mean personal rating, maximum absolute acceleration, maximum approach velocity)

- Mean Personal Rating - relates to passenger discomfort as a function of changes in acceleration over time,
- Maximum Absolute Acceleration - relates to impact force, and
- Maximum Approach Velocity - relates to relative damage.

2) Casualties Estimation[11]: f(vehicle movement, masses and coefficients of friction, delta velocity, flow pattern, number of initiating incidents, reliability)

- Vehicle Movement - maneuver, velocity, and platoon/free agent,
- Masses - probability of casualty as a function of vehicle mass,
- Coefficients of Friction - probability of casualty as a function of coefficients of friction,
- Delta Velocity - probability of fatality/vehicle as a function of delta velocity,
- Flow Patterns - traffic flow, perhaps time of day dependent,
- Number of Initiating Incidents - scenario which results in casualties,

or propose an "acceptable" casualty rate to establish reliability requirements.

4.3.2 Travel Efficiency

Evaluation criteria for travel efficiency (throughput) are provided in terms of Average Speed, Reliability, Predictability[9]. For throughput, MOEs are the amount of time, the average speed, the reliability and predictability of the travel time, and the availability of the AHS segments.

Time: f(travel average speed, reliability of travel time , predictability of travel time).

- Travel Average Speed - directly relates to travel time,
- Reliability of Travel Time - repeatability of the trip time, and
- Predictability of Travel Time - how good prediction is compared to actual travel times.

5. MODES OF OPERATION

5.1 STRUCTURE AND PURPOSE

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 context of these operations relative to the RSCs that the malfunctions are examined.

5.2 ANALYSES/ASSESSMENTS

5.2.1 Operational Functions

The operational functions[8] are the functions that implement operational events in a mission oriented order. These operational functions are defined to be independent of physical implementation and can function concurrently with each other. Three functions have been deleted from the set presented by Mazer, Clare, and Zhang. These functions, OP11 - Incident management, OP12 - Pause, OP13 - Steering to Avoid Collision, and OP14 - Human backup for non recoverable failures, were deleted from the set as they are functions that perform malfunction management and indeed present a malfunction management strategy.

OP1 Vehicle check-in: Vehicle check-in is performed before the vehicle enters the automated highway by a combination of roadside and on-vehicle systems. The check-in process may include both static inspection and dynamic testing of the vehicle to ensure that its safety-critical components function as specified. Only those that pass the inspection are issued permission to enter.

OP2 Entering the system: The vehicle is driven manually onto the on-ramp or the transition lane following instructions provided by the system. If an on-ramp is directly connected to the inspection station, the automated control system guides the vehicle to the on-ramp.

OP3 Transition from human to automatic control: manual control is released after the automated control system has reliably taken over the control tasks. In the transition process, the driver is instructed to release manual control in a given sequence.

OP4 Route Selection: Route selection can take place before or when the vehicle enters the AHS network and during the trip, upon approval by the system. The driver inputs the origin, destination, and designated locations along the route. The system recommends a route according to the request and the traffic conditions. Alternative routes may also be recommended upon request. During the trip, the system may provide updated route recommendations should an incident be detected on the selected route. The driver has the responsibility of finalizing the route selection.

OP5 Velocity regulation: Velocity regulation will be performed to cause the vehicle to match a nominal speed or commanded speed profile. The nominal speed is set by the system abased on the speed limit, road surface, and traffic condition. The commanded speed profile is given when a coordination maneuver such as lane-changing is performed.

OP6 Spacing regulation: Spacing regulation is enacted when there is a vehicle within range in front of the controlled vehicle and a minimum target separation has been given. A target separation represents the minimum allowed separation between vehicles.

OP7 Longitudinal position regulation: The longitudinal position regulation is performed to cause a vehicle to keep a spacing greater than an instructed minimal distance from a specific geometric location for a given period of time in order for another vehicle to accomplish a location constrained lane-changing maneuver.

OP8 Lane tracking: The lane-tracking operation is performed to keep the vehicle within a traffic lane. Lane-tracking allows the system to follow a reference line installed in the center or on the edge of a traffic lane to within a given tolerance.

OP9 Steering for lane-changing: The lane-changing operation is performed according to a new lane assignment. The new lane-assignment can be given when there is a request for lane-changing, or at locations where two lanes combine into one or one traffic lane separates into two lanes.

OP10 Maneuvering coordination management: Maneuvering coordination management provides instructions to vehicles for coordinating lane-change, merging, and any other maneuvers that require close coordination with neighboring vehicles. In a system with platoons, maneuvering coordination management is also responsible for forming, joining, and splitting groups of vehicles.

OP15 Exit to a transition lane: In this operation, the vehicle will be guided to a transition lane near the exit

OP16 Normal transition from automatic to manual control: the normal transition from automatic control to manual control will take place after the vehicle enters the exit area or transition lane.

5.3 KEY RESULTS/CONCLUSIONS/ISSUES

5.3.1 Operational and Elemental Functions Mappings

Each of the operational functions performs one or more of the system elemental functions. While it is more straightforward to examine the AHS from an operational sequence perspective, the AHS foundation is indeed the elemental functions. Therefore, an identification of which elemental functions are invoked for each operational function is required. Table 3 lists the operational functions and their mappings to elemental functions. This mapping is critical to the severity level assessment as each operational function malfunction is assessed by examining the mapped elemental functions.

Table 3. Operational and Elemental Functions.

	Operational Functions											
Elemental Functions	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**15**	**16**
Monitoring traffic conditions and predicting congestion				✓						✓		
Vehicle ID assignment	✓											
Route recommendation				✓						✓	✓	
Lane assignment								✓	✓	✓	✓	
Target speed					✓							
Maximum group size										✓		
Minimal separations						✓						
Prioritizing vehicle operations										✓		
Regional traffic conditions monitoring and incident management				✓						✓		
Off-vehicle inspection and monitoring	✓											
Issuing permission/rejection	✓											
Normal maneuver coordination planning		✓	✓							✓	✓	✓
Maneuvering coordination planning for hazardous conditions										✓		
Supervising the sequence of the coordinated maneuvers					✓	✓	✓	✓	✓			
Monitoring road surface conditions and weather				✓								
Steering control command								✓	✓			
Speed regulation command					✓	✓	✓					
Braking command					✓	✓	✓					
Vehicle condition monitoring and failure detection/diagnosis	✓											
Trip progress monitoring				✓								
Sensing					✓	✓	✓	✓	✓			
Actuation					✓	✓	✓	✓	✓			
Human-machine interface	✓	✓	✓	✓								✓
Information link between the network layer and the link layer	✓			✓						✓	✓	
Information exchange between the link layer and the coordination layer	✓			✓						✓	✓	
Information link between the coordination layer and the regulation layer		✓	✓	✓						✓		✓
Information link between the regulation layer and the physical layer		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Manually maneuver vehicle		✓	✓									✓
Request information												
Receive information	✓	✓	✓	✓								
Provide information	✓			✓						✓		✓

6. MALFUNCTION IDENTIFICATION

6.1 STRUCTURE AND PURPOSE

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. On the basis of these allocations, evaluation of malfunctions conjectured are made.

6.2 ANALYSES/ASSESSMENTS

6.2.1 Malfunction Definition

For this study, the following definitions shall apply[12,13]:

- Failure: Occurs when the delivered service deviates from the specified service. Service can be delivered by a chip as viewed by another chip, or by the system as viewed by the user.
- Fault: Erroneous state of hardware or software resulting from failures of components, physical interference from the environment, operator error, or incorrect design.
- Error: Manifestation of a fault within a program or data structure.
- Permanent: Describes a failure, fault, or error that is continuous and stable. (Interchangeable with the word hard.)
- Intermittent: Describes a fault or error that is only occasionally present due to unstable hardware or varying hardware or software states.
- Transient: Describes a fault or error resulting from temporary conditions. (Interchangeable with the word soft).

The difference between a malfunction and failure is defined by using the analogy of the difference between a function and its allocation, i.e., a malfunction is defined relative to a function and a failure is defined relative to its allocation from a system down to a hardware component or software module. For this study, we use operational functions to examine malfunctions as the effects of operational malfunctions are easier to analyze. These operational functions are mapped to one or many elemental functions; the elemental functions in term have been allocated to subsystem(s). The convention adopted has been to refer to elemental functions in terms of failures and operational functions in terms of malfunctions. Thus, a malfunction results from one or more failures and is defined as the following:

- Malfunction: Deviation of a function to a degraded or inoperative mode such that the function fails to operate normally.

6.3 KEY RESULTS/CONCLUSIONS/ISSUES

6.3.1 Primary Subsystem Identification of Malfunctions

The AHS is comprised of three major systems: the roadway, the vehicle, and the driver. Each major system is in turn comprised of primary subsystems. Figure 6 depicts the primary subsystems of an AHS. Note that only specific components of the vehicle and actions of the driver are considered part of the AHS. As noted previously, the driver interfaces with the AHS at different layers dependent upon the specific design and only the direct actions that relate to input and the display or presentations of information to the driver are considered as part of the AHS.

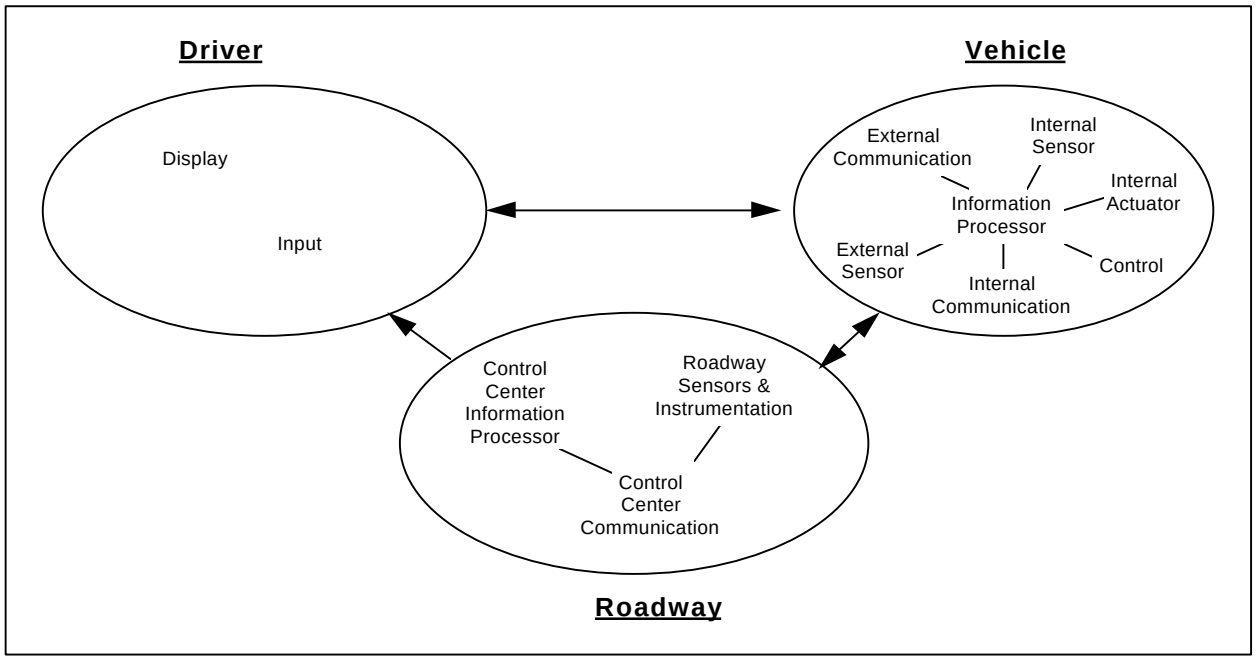


Figure 6. AHS Primary Subsystems.

The system requirements analysis process presented previously, including review of Representative System Configurations (RSCs), resulted in the functional allocation for the infrastructure-weighted and vehicle-weighted RSCs as provided in tables 3 and 4, respectively. Additionally, these tables present the identified potential malfunctions (each function by definition is a potential malfunction) and the allocated primary subsystem (potential failure point).

Table 4. Primary Subsystem Allocation of Elemental Functions for the Infrastructure-Weighted Representative System Configuration.

Layer/Elemental Function	Major System	Primary Subsystem
Perform Route & Flow Control (Network)		
Monitor Traffic Conditions and Predict Congestion	Roadway	Roadway Sensors & Instrumentation Control Center Information Processor
Vehicle ID Assignment	Roadway	Control Center Information Processor
Route Recommendation	Roadway	Control Center Information Processor
Perform Path & Congestion Control (Link)		
Assign Lane	Roadway	Control Center Information Processor
Set Target Speed	Roadway	Control Center Information Processor
Determine Maximum Group Size	Roadway	Control Center Information Processor
Set Minimal Separations	Roadway	Control Center Information Processor
Prioritize Vehicle Operations	Roadway	Control Center Information Processor
Monitor Regional/Local Traffic Condition and Incident Management	Roadway	Roadway Sensors & Instrumentation Control Center Information Processor
Perform Vehicle Maneuver Coordination (Coordination)		
Perform Off-vehicle Inspection and Monitoring	Roadway	Control Center Information Processor Roadway Sensors & Instrumentation
Issue Permission/Rejection for Entering/Exiting	Roadway	Control Center Information Processor
Plan Normal Maneuver Coordination	Roadway	Control Center Information Processor
Plan Hazardous Conditions Maneuver Coordination	Roadway	Control Center Information Processor
Supervise Maneuvers Sequence	Roadway	Control Center Information Processor
Monitor Road Surface and Weather Conditions	Roadway	Roadway Sensors & Instrumentation Control Center Information Processor
Provide Vehicle Maneuver Control Command (Regulation)		
Issue Steering Command	Vehicle	Vehicle Information Processor
Issue Speed Regulation Command	Vehicle	Vehicle Information Processor
Issue Braking Command	Vehicle	Vehicle Information Processor
Perform Vehicle Monitoring & On-Board Failure Detection/Diagnosis	Vehicle	Vehicle Internal Sensor Vehicle Information Processor
Monitor Trip Progress	Vehicle	Vehicle Information Processor
Perform Vehicle Actuation & Sensing (Physical)		
Sensing	Vehicle	Vehicle Internal Sensor Vehicle External Sensor Vehicle Information Processor Roadway Sensors & Instrumentation
Provide Actuation	Vehicle	Vehicle Internal Actuator
Human-Machine Interface	Vehicle	Vehicle Information Processor
Provide Information Link Between the Network Layer and the Link Layer	Roadway	Control Center Communication
Provide Information Exchange Between the Link Layer and the Coordination Layer	Roadway	Control Center Communication
Provide Information Link Between the Coordination Layer and the Regulation Layer	Roadway-Vehicle	Control Center Communication Vehicle External Communication
Provide Information Link Between the Regulation Layer and the Physical Layer	Vehicle	Vehicle Internal Communication
Manually Maneuver Vehicle	Driver	Driver Input
Request Information	Driver	Driver Input
Receive Information	Driver	Driver Display
Provide Information	Driver	Driver Input

Table 5. Primary Subsystem Allocation of Elemental Functions for the Vehicle-Weighted Representative System Configuration.

Layer/Elemental Function	Major System	Primary Subsystem
Perform Route & Flow Control (Network)		
Monitor Traffic Conditions and Predict Congestion	Roadway	Roadway Sensors & Instrumentation Control Center Information Processor
Vehicle ID Assignment	Roadway	Roadway Sensors & Instrumentation Control Center Information Processor
Route Recommendation	Vehicle	Vehicle Information Processor
Perform Path & Congestion Control (Link)		
Assign Lane	Vehicle	Vehicle Information Processor
Set Target Speed	Vehicle	Vehicle Information Processor
Determine Maximum Group Size	Vehicle	Vehicle Information Processor
Set Minimal Separations	Vehicle	Vehicle Information Processor
Prioritize Vehicle Operation	Vehicle	Vehicle Information Processor
Monitor Regional/Local Traffic Condition and Incident Management	Vehicle	Vehicle External Sensor Vehicle Information Processor
Perform Vehicle Maneuver Coordination (Coordination)		
Perform Off-vehicle Inspection and On-Board Failure Detection/Diagnosis	N/A	N/A
Issue Permission/Rejection for Entering/Exiting	Vehicle	Vehicle Information Processor
Plan Normal Maneuver Coordination	Vehicle	Vehicle Information Processor
Plan Hazardous Conditions Maneuver Coordination	Vehicle	Vehicle Information Processor
Supervise Maneuvers Sequence	Vehicle	Vehicle Information Processor
Monitor Road Surface and Weather Conditions	Vehicle	Vehicle External Sensor Vehicle Information Processor
Provide Vehicle Maneuver Control Command (Regulation)		
Issue Steering Command	Vehicle	Vehicle Information Processor
Issue Speed Regulation Command	Vehicle	Vehicle Information Processor
Issue Braking Command	Vehicle	Vehicle Information Processor
Perform Vehicle Monitoring & Failure Detection/Diagnosis	Vehicle	Vehicle Information Processor Vehicle Internal Sensor
Monitor Trip Progress	Vehicle	Vehicle Information Processor
Perform Vehicle Actuation & Sensing (Physical)		
Sensing	Vehicle	Vehicle Internal Sensor Vehicle External Sensor
Provide Actuation	Vehicle	Vehicle Internal Actuator
Human-Machine Interface	Vehicle	Vehicle Information Processor
Provide Information Link Between the Network Layer and the Link Layer	Roadway	Control Center Communication
Provide Information Exchange Between the Link Layer and the Coordination Layer	Vehicle-Roadway	Vehicle External Communication Control Center Communication
Provide Information Link Between the Coordination Layer and the Regulation Layer	Vehicle	Vehicle Internal Communication
Provide Information Link Between the Regulation Layer and the Physical Layer	Vehicle	Vehicle Internal Communication
Manually Maneuver Vehicle	Driver	Driver Input
Request Information	Driver	Driver Input
Receive Information	Driver	Driver Display
Provide Information	Driver	Driver Input

7. ASSESSMENT OF SEVERITY LEVEL

7.1 STRUCTURE AND PURPOSE

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. On the basis of which elemental function and thus which major subsystem might have failed, an evaluation of the impact of the malfunction using the MOEs is performed. The Key Results/Conclusions/Issues section is provided in the attachment Appendix B.

7.2 ANALYSES/ASSESSMENTS

As detailed earlier, the operational functions provide an AHS functional description in the time perspective of a single vehicle as it enters, operates on, and then exits the system. In terms of our function-state (activity-behavior) definitions, these operational functions are presented as the states of the system. During each of these states, elemental functions are performed. It is defined that a malfunction of an operational function occurs if one or more of the elemental functions malfunctions, i.e. the allocated subsystem fails or deviates from its specified service. The severity levels of these operational malfunctions, as illustrated in figure 7, are highly dependent upon the specific failures. Thus, we initially examine the determination of the likelihood of malfunction effects through the use of the MOEs. We examine them from a pure functional perspective without regard to an operational timeline or configuration.

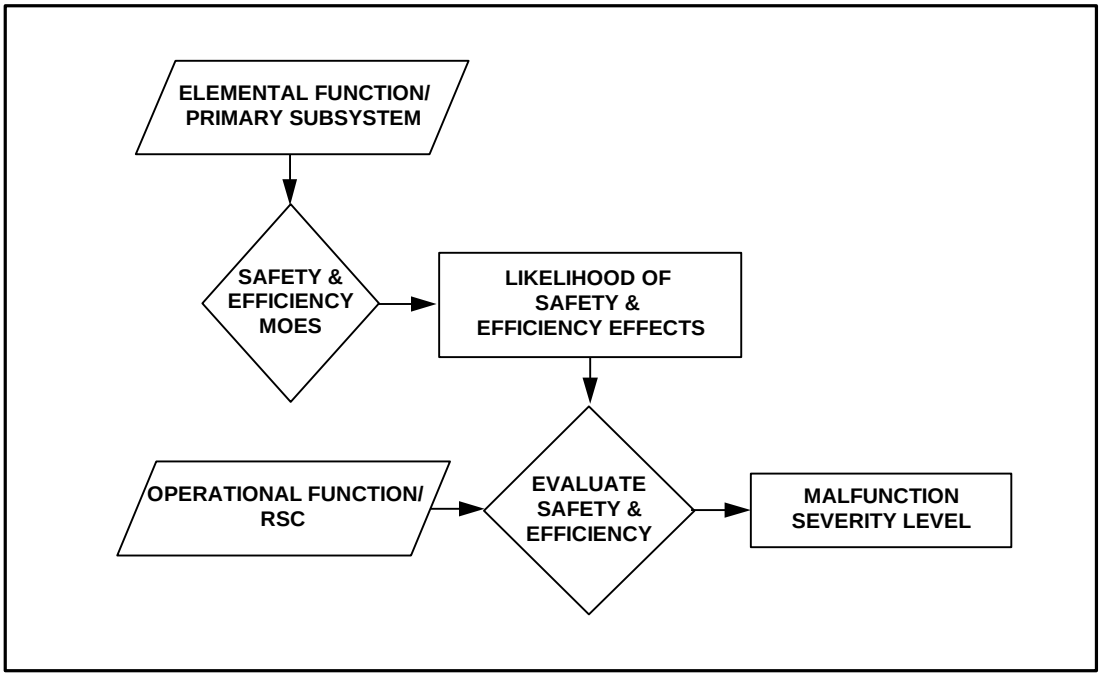


Figure 7. Malfunction Severity Level Assessment Approach.

The likelihood of effects is not the likelihood of occurrence as would be estimated in a risk analysis. Rather, it is providing an intermediate step in estimating the severity level of these effects based upon a cursory examination of the elemental functions involved. Then, the

operational functions are examined in context of a specific RSC and an operational function. Safety and efficiency severity levels from failures of allocated elemental functions, i.e., primary subsystems, are assessed using the evaluation criteria. Those failures with high severity levels are highlighted and are addressed in the malfunction management strategies section.

7.2.1 Elemental Function Failure

A three-level grading system, table 6, shall be used for the qualitative analysis of the likelihood of malfunction effects in terms of safety and efficiency.

Table 6. Elemental Function Failure Levels.

Elemental Function Failure Level	Description
Unlikely	The failure of this elemental function is unlikely to cause safety or efficiency loss.
Possible	The failure of this elemental function may cause some safety or efficiency loss.
Likely	The failure of this elemental function is likely to cause safety or efficiency loss.

Each of the elemental functions is analyzed with respect to safety and efficiency. The results are presented in table 7. Specifically for each elemental function, a failure is assumed (again independent of operation and configuration), and safety and efficiency MOEs are examined separately. The failure levels are used to classify potential safety and efficiency effects. As explained in the following section, this step provides an incremental understanding of the elemental functions and is used as a building block to evaluate the malfunction severity levels; it is not an assessment of the malfunction nor is it the likelihood of occurrence (likelihood of occurrence will be examined in the development of malfunction management strategies).

Table 7. Elemental Function Failure Analysis.

Elemental Function	Safety - Are fatalities or injuries likely to occur given this failure?	Efficiency - Is average travel speed, or travel time reliability or predictability likely to be affected given this failure?
Monitoring traffic conditions and predicting congestion	Unlikely. This function mostly supports efficiency.	Possible. Failure would cause disruption in predicting ahead resulting in less than optimal routes and unreliable travel times.
Vehicle ID assignment	Unlikely. Failure effect depends on the RSC, but ID is used primarily for communication.	Likely. Lack of assigned ID communication will hinder travel efficiency.
Route recommendation	Unlikely. This function mostly supports efficiency.	Likely. Without a planned route, travel time is ad hoc at best.
Lane assignment	Possible. While this function assists the coordination layer and is not mandatory, it can still impact safety.	Possible. Link-level lane assignment in accordance with routes and traffic conditions aids travel time.
Target speed	Possible. Failure to set the speed in accordance with traffic conditions could cause safety problems.	Likely. Without target speeds, speeds would be adjusted on local levels resulting in efficiency problems.
Maximum group size	Possible. If group sizes are too large, maneuvering within and around groups can cause safety problems.	Possible. If group sizes are too large, maneuvering issues can impact efficiency.
Minimal separations	Possible. Failure to maintain required minimal headway can cause major safety problems.	Likely. Failure to maintain required minimal headway will most likely cause disruptions in vehicle flow.
Prioritizing vehicle operations	Likely. Loss of giving priority to special mission vehicles can result in extra fatalities or increased injuries due to delays in reaching victims.	Likely. Loss of giving priority to special mission vehicles can result in increased delays and congestion from incidents.
Regional traffic conditions monitoring and incident management	Possible. Improper incident management can result in additional incidents.	Likely. Lack of traffic information results in reactive management and slower average speeds and unpredictable travel times.

Off-vehicle inspection and monitoring (during vehicle check-in)	Likely. Especially for the Roadway weighted RSCs, on-vehicle inspection will not complement this failure.	Possible. Using on-vehicle inspection and monitoring only will degrade efficiency for the Roadway weighted RSCs.
Issuing permission/rejection (during vehicle check-in)	Likely. Issuing incorrect permission to unsafe vehicles could lead to highest safety consequences.	Likely. Unsafe vehicles allowed on AHS compromises the system efficiency.
Normal maneuver coordination planning	Likely. Failure can result in accidents.	Likely. Failure can result in no maneuvers, thus decreased average speeds.
Maneuvering coordination planning for hazardous conditions	Likely Failure can result in not avoiding hazards or collisions.	Likely. Failure can result in no maneuvers, thus decreased average speeds.
Supervising the sequence of the coordinated maneuvers	Possible. Without supervision, maneuvers might not be performed	Possible. Without supervision, some maneuvers might not be performed causing slower speeds.
Monitoring road surface conditions and weather	Possible. At the coordination layer, lack of information can affect maneuver coordination.	Possible. At the coordination layer, lack of information can affect maneuver coordination.
Steering control command	Likely. Failure can result in severe compromise of safety.	Likely. Ineffective commands compromise efficiency.
Speed regulation command	Likely. Failure can result in severe compromise of safety.	Likely. Ineffective commands compromise efficiency.
Braking command	Likely. Failure can result in severe compromise of safety.	Likely. Ineffective commands compromise efficiency.
Vehicle condition monitoring and failure detection/diagnosis	Likely. Health and status of vehicle and its equipment are required to properly regulate vehicle commands.	Possible. Efficiency effects are indirectly associated with monitoring at the regulation layer.
Trip progress monitoring	Unlikely. This is a support function.	Unlikely. This is a support function.
Sensing	Likely. Sensory information is used for direct measurements.	Likely. As sensory information degrades, efficiency performance is compromised.
Actuation	Likely. Failure of actuators can affect directly safety.	Likely. Failure of actuation affects efficiency.
Human-machine interface	Likely. Safety affected by manual control mechanisms.	Likely. Efficiency directly associated with human interface optimizing performance.
Information link between the network layer and the link layer	Unlikely. Information link effects are directly associated with the information with network layer information not safety critical.	Possible. Information link effects are directly associated with the information with efficiency a network concern.
Information link between the link layer and the coordination layer	Possible. Information link effects are directly associated with the information.	Likely. Information link effects are likely with efficiency directly associated with the information at this layer.
Information link between the coordination layer and the regulation layer	Likely Information link effects are likely with safety directly associated with the information at this layer.	Likely. Information link effects are likely with efficiency directly associated with the information at this layer.
Information link between the regulation layer and the physical layer	Likely. Information link effects are likely with safety directly associated with the information at this layer.	Likely. Information link effects are likely with efficiency directly associated with the information at this layer.
Manually maneuver vehicle	Likely. It is very safety critical for driver to perform this essential function properly.	Possible. Throughput can be affected depending upon the operation.
Request information	Unlikely. Improper or incomplete requests for information by the driver will either by ignored by the system or provided with proper responses that will be ignored by the driver.	Unlikely. Improper or incomplete requests for information by the driver will either by ignored by the system or provided with proper responses that will be ignored by the driver.
Receive information	Possible. Incorrect information received by the driver might induce driver interference when not warranted causing disturbance in the system with possible safety consequences.	Possible. Incorrect information received by the driver might induce driver interference when not warranted causing possible efficiency impacts.
Provide information	Unlikely. Incorrect information provided to the system should not cause any safety impacts in of itself.	Likely. Incorrect information such as the wrong destination provided to the system is likely to cause efficiency impacts.

7.2.2 Malfunction Severity Level

Malfunction severity will be analyzed using the elemental function failure analysis, i.e., an operational function malfunction results from an elemental function malfunction or equivalently a primary subsystem failure and this "elemental function failure" has been analyzed as to the likelihood of safety and efficiency impacts. The likelihood of safety and efficiency impacts using the MOEs is used as the first step in assessing the severity levels. The next step is to use the evaluation criteria to assess the effects of the malfunctions on safety and efficiency keeping in mind the operational function and the RSC and provide a grade of "low", "medium", or "high" severity level to the malfunction. In summary, these steps are as follows (refer to figure 7):

1) Assume an operational malfunction.

2) Assume an elemental function malfunction/primary subsystem failure.

3) Use safety and efficiency impact likelihood levels (table 7) as first step in assessing elemental function malfunction/primary subsystem failure.

4) Recall characteristics of specific RSC (table 2).

5) Use safety and efficiency evaluation criteria to assess malfunction severity level.

Collision severity evaluation criteria are used to ask the following questions:

- What are the anticipated changes in acceleration?
- What is the maximum acceleration?
- What is the maximum approach velocity?

Casualty estimation evaluation criteria are used to ask the following questions:

- Is this a platoon or free agent and what maneuvers and velocities were involved?
- What is the vehicle mass?
- What is the coefficient of friction?
- What was the delta velocity between colliding vehicles?
- What was the traffic flow?
- Were there any initiating incidents?
- What was the reliability requirement?

Efficiency evaluation criteria are used to ask the following questions:

- What is the expected impact on average travel speed?
- What is the expected impact on repeatability of travel time?
- What is the expected impact on how good the predicted travel time is compared to the actual travel time?

The outcome of this evaluation is qualified in terms of severity levels. For evaluation of issues and risks in malfunction management, qualitative descriptions such as low, medium, or high will be the appropriate levels for evaluating severity of malfunctions. These descriptive terms and meanings are defined in table 8.

Table 8. Evaluation Criteria for Malfunction Severity.

Severity Levels	AHS Reaction	Nature of Urgency	Major System Impact
Low	Warning	Alert	Possible impact on vehicle and/ or driver
Medium	Serious	Disruptive consequence	Definite impact on vehicle and/ or driver
High	Critical	Dangerous & Disruptive consequence	Immediate impact on vehicle and/ or driver

Low severity level is the catch-all level with possible impact on vehicles and/or driver. It is assumed that, by itself, the failure that warranted a low severity level will not cause any disruptive consequences. Thus, the reaction is for a warning to be issued. The medium severity level encompasses a wide range of definite impact failures. The safety and efficiency goals are weighted evenly for this evaluation, i.e., although safety ranks high in importance, efficiency loss will substantiate a medium severity level assessment. High severity levels are assessed as a result of immediate impact on vehicle and/or driver with dangerous as well as disruptive consequences.

The malfunction severity levels will be used in categorizing the subsystem failure of a particular operational malfunction in a defined RSC. The four RSCs are separated into IW and VW for primary subsystem categorization. Under these two categories, the primary subsystem, and barrier plus transition and unrestricted-entry mechanizations headings are applied. For each of the elemental functions for the specific operational function (refer to table 3), the primary subsystem(s) is listed (refer to tables 4 and 5. Also listed are the results of the elemental function failure (refer to table 7).

It is indeed reasonable to assume that a failure that is "Unlikely" to impact safety or efficiency will have a "Low" severity level for any operational malfunction in any RSC. However, for "Possible" or "Likely" failures, the severity level is highly dependent upon the operational malfunction, i.e., when, in an operational sequence, did this failure occur, and upon the RSC, i.e. were barriers, thus high speeds, a part of the scenario. (Recall table 1 and the characteristics of the four RSCs.) For these failures with "Possible" or "Likely" safety or efficiency impacts, the EC's were used to assess a "Low", "Med", or "High" severity level.

Following are the malfunction severity level assessments for each of the Operational Functions.

7.2.3 Malfunction: Vehicle Check-in

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage occur or whether the average travel speed, or travel time reliability or predictability is likely to be affected if the vehicle check-in process either can't issue permission or improperly issues permission to enter.

Vehicle ID Assignment

The assignment of vehicle ID is independent of a BT or UE mechanization and involves the same functional allocation of a control center information processor. The difference exists in the usage of the vehicle ID between an IW and VW configuration. As we see that only efficiency impacts are expected and are in fact "Likely", we use the efficiency EC to ask what the expected impacts on average speed and travel time repeatability and predictability are.

For an IW configuration, the highly synchronous vehicle maneuvers will be impacted to localized maneuvers, i.e., vehicle to vehicle communication, resulting in a serious disruption in AHS performance warranting a medium severity level assessment. The vehicle weighted configuration relies more on autonomous vehicle maneuvers but efficiency could still be enhanced with a network level vehicle identification; thus, a warning is issued with a low severity level. The safety severity levels are low for all configurations.

Off-Vehicle Inspection and Monitoring

Recall that while this elemental function can also be performed while the vehicle is on the AHS, it is examined here specifically for the vehicle check-in operation. Also note that this elemental function is not applicable for VW configurations. During this check-in operation, no distinction between BT and UE mechanizations is made as implementation ease or cost are not issues for this analysis. Hence, for the IW configuration, we only examine the "Likely" safety impacts and "Possible" efficiency impacts given the failure of either the roadway sensors & instrumentation and/or the control center information processor. If the sensors & instrumentation fail, then the consequence will be in efficiency as vehicles will not be able to pass their inspection and enter the AHS. If the processor and/or the software it processes fail, then the consequences can be much more severe and warrants a medium efficiency severity level.. With respect to collision and casualty estimation, worst case scenarios may result

Issuing Permission/Rejection

This function bases its decision upon the off-vehicle and on-vehicle inspection/monitoring. Again no distinction between BT and UE mechanizations is made. For the infrastructure weighted configuration, the failure of the control center information processor could issue permission to vehicles that did not pass the inspection or issue rejection to those that passed. Worst case scenarios for incorrect permission issuance for collision and casualty estimation warrant a medium safety severity level with compounded effects for each additional vehicle issued incorrect permission. For the VW configuration, the same scenarios exist for the failure of the vehicle information processor with a safety medium severity level. However, as we will see when we provide management strategies, the compounded effects are not present. Similarly, the impact on efficiency is compromised with trip predictability compromised and incidents affecting trip reliability and AHS availability. This definite impact warrants a medium se

Vehicle Condition Monitoring and Failure Detection/Diagnosis

This function is a complementary function to the off-vehicle inspection and monitoring and it too, is independent of BT and UE mechanization. This function is examined only in context to its functionality during the vehicle check-in operation. For the IW configuration, it is viewed as a backup function to the off-vehicle inspection and monitoring; thus, the failure of the vehicle internal sensor and information processor during this operation has a low severity for both safety and efficiency. For the VW configuration, it is analogous to the importance of the off-vehicle inspection and monitoring for an IW configuration and results in a medium severity level for both safety and efficiency

Human-Machine Interface

This elemental function allows the driver to monitor the check-in operation. It would ultimately provide information for the driver to enter the system. Thus, for a BT mechanization, efficiency

impact would result and a warning would be issued with a low severity level. For a UE mechanization, the transition from manual to AHS would be more seamless and less impact is expected, but a warning would still be issued with a low safety and efficiency severity level as the notification that the vehicle information processor has failed is provided. This function also provides the mechanisms for propulsion, braking, and steering of the vehicle, i.e., normal non-AHS driving. However, since the vehicle is not yet on the AHS, this aspect of the human-machine interface shall not be considered as an AHS function.

Information Link Between the Network Layer and the Link Layer

During vehicle check-in, the information provided would be the vehicle ID assignment. The same severity levels as provided for vehicle ID assignment exist.

Information Exchange Between the Link Layer and the Coordination Layer

This function is a carry over from the information link between the network and link layers as the vehicle ID assignment is eventually provided to the coordination layer. Thus, the same severity levels as provided for vehicle ID assignment exist.

Receive and Provide Information

These two essential human functions of receiving information about permission to enter and providing request to enter are neither safety or efficiency critical.

7.2.4 Malfunction: Entering The System

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while the vehicle is manually driven onto the on-ramp or transition lane.

Normal Maneuver Coordination Planning

This coordination between vehicles entering the AHS includes control commands that may include the time for the entering of a vehicle to be developed in coordination with vehicles already on the AHS and the set up of protocols among these vehicles. While the BT mechanization implies higher speeds and concern about safety and efficiency ramifications from lack of coordination efficiency as vehicles enter the AHS, BT also implies synchronous timing and thus implicit better coordination. Similarly the UE mechanization implies slower speeds and less concern about coordination efficiency, however UE also implies autonomous traffic synchronization and more concern about coordination efficiency. For the IW configuration, the failure of the control center information processor during the entering of the AHS would have disruptive consequences; however, not yet on the AHS, only potential impact is assume and warrants a medium severity level for both the BT and UE mechanization.

Human-machine interface

While entering the AHS, this interface is limited to providing information leading up to the transfer to the automated control. As with the vehicle check-in operation, mechanisms for propulsion, braking, and steering are included in this function, but are excluded for this entering the AHS operation. Hence, failure of this function is deserving of an alert only and a low severity level irrespective of configuration.

Information Link Between the Coordination Layer and the Regulation Layer

For all configurations of this elemental function, this link is merely a conduit for the information to be displayed. Thus, its malfunction would not be serious and is assessed a low severity level.

Information Link Between the Regulation Layer and the Physical Layer

Similar to the link between the coordination and regulation layers, a failure of this link is not serious for this elemental function and is assessed a low severity level.

Manually Maneuver Vehicle

This essential human function irrespective of the configuration will have a critical reaction and a high safety severity level. Efficiency impacts will occur, but less severe with a medium severity level.

Receive Information

This essential human function during the entering the system operation will not cause any disruptive consequence upon failure and is a low severity level malfunction.

7.2.5 Malfunction: Transition From Human to Automatic Control

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while manual control is being released.

Normal Maneuver Coordination Planning

This coordination during the transition to automatic control is a continuation of the coordination between vehicles entering the AHS. Total coordination must exist when automated control is effective as the vehicle would be on the AHS. Certainly looking at safety impacts, collisions can be quite severe with respect to maximum acceleration and velocity and casualties estimations are high given potentially large delta velocities however can be lessened through the usage of free agent entries on the AHS. While the BT mechanization can isolate the incidents, again, the impacts from higher velocities offset this safety advantage. Whether it is the control center or vehicle information processor that fails, the impact would be immediate and critical with a high severity level. The efficiency impacts are more localized single events and result in medium severity levels.

Human-Machine Interface

During this transition to automated control, speed and steering control mechanisms and information displays are utilized. This is the interface that allows the driver to take back control if necessary, thus its failure is of secondary nature, i.e., it needs to be available if another failure occurred.

Information Link Between the Coordination Layer and the Regulation Layer

For all configurations of this elemental function, this link is merely a conduit for the information to be displayed. Thus, its malfunction would not be serious and is assessed a low severity level.

Information Link Between the Regulation Layer and the Physical Layer

Similar to the link between the coordination and regulation layers, a failure of this link is not serious for this elemental function and is assessed a low severity level.

Manually Maneuver Vehicle

This essential human function irrespective of the configuration will have a critical reaction and a high safety severity level.

Receive Information

This essential human function during the entering the system operation will not cause any disruptive consequence upon failure and is a low severity level malfunction.

7.2.6 Malfunction: Route Selection

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected by route selection malfunction.

Monitoring Traffic Conditions and Predicting Congestion

This network layer function has possible efficiency effect. In context of route selection, the network level traffic information can provide congestion prediction information reducing travel times and allowing more predictable travel times. This effect is independent of BT or UE mechanization. This function is performed by the control center information processor for both IW and VW configurations. Due to the efficiency effects, its failure might result in potential impact on the vehicle and driver and warrants a medium efficiency severity level.

Route Recommendation

The route recommendation may occur anytime during the trip and is independent of BT or UE mechanization. It is however, highly dependent upon instrumentation as the control center information processor performs this function in an IW configuration, while the vehicle information processor performs this in a vehicle weighted configuration. We see that for the IW configuration, the impact can be quite large by affecting all vehicles causing disruptive consequences and a medium efficiency severity level. The VW configuration will impact only the one vehicle and will cause more inconvenience than disruption warranting a low severity level.

Regional Traffic Conditions Monitoring and Incident Management

The regional traffic conditions monitoring is analogous to the monitoring of traffic conditions except that it is performed at the link layer rather than the network layer. It is the incident management component that can present a critical functionality. It is anticipated that if this function fails, then the link layer will fail to select paths for vehicles, adjust their target speed,

and instruct lane changes around the incident. The consequence is that the vehicle must react individually. Our coarse simulation of such an event indicates that the timing involved to perform maneuvers are substantial, i.e., on the order of twice the normal timing given that maneuvers are generally performed without much braking. The underlying result is that hard braking is required, but that maneuvering is possible. It would be presumptuous that multiple failures occur and a worst case condition of collision occurs. Granted the collision severity can be quite high with the anticipated changes in deceleration from the maximum approach velocity and casualty estimation is also quite high due to potentially high delta velocities. However, consistent with the analysis of single failures, such collision should be avoided. While the BT configuration might require harder braking, all of the configurations have medium severity levels.

Monitor Road Surface Conditions and Weather

The failure of this elemental function could reduce the reliability of the travel time and reduce travel speed; however, for all RSCs, the effect will be a low severity level.

Trip Progress Monitoring

The failure of this elemental function would only have a low severity level for all RSCs.

Human-Machine Interface

This function allows the driver to provide route selection information and receive information. While its failure might produce either no route selected or the wrong route selected for driver input, its consequences would be minor with a low severity level for all RSCs.

Information Link Between the Network Layer and the Link Layer

On the basis of the traffic conditions monitoring information passed between the network and link layers, the IW configuration is assessed a medium efficiency severity level and the VW configuration is assessed a high efficiency severity level. Safety impacts are low for all RSCs.

Information Exchange Between the Link Layer and the Coordination Layer

The failure to exchange information between these layers is not serious and warrants a low severity level.

Information Link Between the Coordination Layer and the Regulation Layer

The failure to exchange information between these layers is not serious and warrants a low severity level.

Information Link Between the Regulation Layer and the Physical Layer

The failure to exchange information between these layers is not serious and warrants a low severity level.

Receive Information

This essential human function allows the driver to receive route selection information. The failure of this function will have a low severity level effect.

Provide Information

This essential human function allows the driver to input route selection information. The failure of the function will have a low severity level effect.

7.2.7 Malfunction: Velocity Regulation

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while vehicle matches the nominal speed or commanded speed profiles.

Target Speed

Target speed information is to be provided in accordance with local traffic conditions; however, a malfunction may cause the information to be absent or incorrect. We examine a worst case excessive speed situation. Collision severity can be extreme with potentially large changes in acceleration, high accelerations, and high approach velocities. Casualty estimations can also be extreme with potentially high delta velocities, large platoons in maneuvers, and high traffic flow. IW configurations lend themselves to many initiating incidents, although the BT mechanization can limit these, with worst case scenarios of different vehicles receiving different target speeds. Efficiency impacts can also be large with little or no predictability of travel times. Again, the VW configuration vehicle information processor limits malfunctions to single vehicles. In all configurations, a serious reaction is minimal with a medium severity level assessment.

Supervising the Sequence of the Coordinated Maneuvers

The malfunction of this monitoring by the coordination layer of the maneuvers can raise the severity level of another malfunction; however, by itself, a warning is the expected reaction.

Speed Regulation Command

During velocity regulation, the malfunction of a speed regulation command can lead to an immediate safety impact with critical reaction independent of the RSC. While efficiency will be impacted, it will only be a local single or limited number of vehicles event.

Braking Command

As braking commands are issued when reduction in vehicle speed is required, this malfunction can have immediate safety impact for all RSCs. Efficiency impacts are secondary.

Sensing

In order to accurately regulate the velocity, a sensor to measure velocity is needed. Additionally, sensing the vehicle propulsion and braking systems conditions, along with other vehicle, infrastructure, and environmental conditions, are performed. BT mechanization with its higher speeds is more sensitive to velocity regulation variations. IW configuration roadway sensors and instrumentation failures affect many vehicles as opposed to the VW configuration. Thus, both IW configurations and the VW-BT configuration can have a disruptive consequence and medium safety severity level. The VW-UE configuration with lower speeds and only single

vehicle failure will have only possible impact and a low safety severity level. All configuration will have direct impact on efficiency

Actuation

Speed control actuation failure will have immediate impact and a high safety severity level.

Information Link Between the Regulation Layer and the Physical Layer

As important as speed and braking commands and the actuation is, the vehicle communication link providing the commands is as important. Thus, its failure will have an immediate safety impact and is assessed a high safety severity level.

7.2.8 Malfunction: Spacing Regulation

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while the vehicle maintains a minimum allowed separation to the vehicle in front.

Minimal Separations

The required minimal headway is provided in accordance with weather and roadway conditions. This headway is for vehicles in platoons and between platoons. This malfunction in terms of performing spacing regulation implies that vehicles will not know the minimal distance to maintain to the vehicle in front or be given an incorrect headway measurement. The BT mechanization allows absorption of the collision impacts. Casualty estimations will not be too high as delta velocities should not be great. Efficiency effects can be high if spacing regulation falls back to velocity regulation. IW configuration effects should be larger than VW configurations with compounded effects of a single control center information processor versus the single vehicle information processor failure. Thus, the IW configurations will have immediate impacts.

Supervising the Sequence of the Coordinated Maneuvers

The malfunction of this monitoring by the coordination layer of the maneuvers can raise the severity level of another malfunction; however, by itself, a warning is the expected reaction.

Speed Regulation Commands

During spacing regulation, the malfunction of speed regulation commands can lead to immediate impacts with high severity levels.

Braking Commands

During spacing regulation, the malfunction of braking commands can lead to immediate impact with high severity levels.

Sensing

To accurately and properly perform spacing regulation, distance sensing to the preceding vehicle is necessary. Additionally, sensing the vehicle propulsion and braking systems

condition, along with other vehicle, infrastructure, and environmental conditions, are performed. BT mechanization with its barriers allows for better safety in case of collision. IW configuration roadway sensors and instrumentation failures affect many vehicles as opposed to the VW configuration. However, for spacing regulation, the sensing function is directly related to the minimal spacings and results in high severity levels for all RSCs.

Actuation

Speed control actuation failure will have immediate impact and a high severity level.

Information Link Between the Regulation Layer and the Physical Layer

As important the speed and braking commands and the actuation is, the vehicle communication link providing the commands is as important. Thus, its failure will have an immediate impact and is assessed a high severity level.

7.2.9 Malfunction: Longitudinal Position Regulation

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while a vehicle maintains a spacing greater than an instructed minimal distance from a specific geometric location for a given period of time in order for another vehicle to accomplish a location constrained lane-change maneuver.

Supervising the Sequence of the Coordinated Maneuvers

The malfunction of this monitoring by the coordination layer of the maneuvers can raise the severity level of another malfunction; however, by itself, a warning is the expected reaction.

Speed Regulation Commands

During longitudinal position regulation, the malfunction of speed regulation commands can lead to immediate impacts with high severity levels.

Braking Commands

During longitudinal position regulation, the malfunction of braking commands can lead to immediate impact with high severity levels.

Sensing

To accurately and properly perform longitudinal position regulation, sensing of distance to specific geometric location for a period of time is necessary. Additionally, sensing the vehicle propulsion and braking systems condition, along with other vehicle, infrastructure, and environmental conditions, are performed. BT mechanization with its barriers allows for better safety in case of collision. IW configuration roadway sensors and instrumentation failures affect many vehicles as opposed to the VW configuration. However, for longitudinal position regulation, the sensing function is directly related to the geometric location position and results in high severity levels for all RSCs.

Actuation

Speed control actuation failure will have immediate impact and a high severity level.

Information Link Between the Regulation Layer and the Physical Layer

As important as speed and braking commands and the actuation is, the vehicle communication link providing the commands is as important. Thus, its failure will have an immediate impact and is assessed a high severity level.

7.2.10 Malfunction: Lane Tracking

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while the vehicle is maintained within a traffic lane.

Lane Assignment

The failure to properly assign, not assign or give wrong assignment, during lane tracking will have significant impact on efficiency independent of configuration. It is anticipated that much driver interface will occur to select lane changes for exiting with consequence to the AHS is in lower efficiency. This failure will produce disruptive consequences and a medium efficiency severity level. Safety impacts may occur, but only in conjunction with coincident malfunctions.

Supervising the Sequence of the Coordinated Maneuvers

The malfunction of this monitoring by the coordination layer of the maneuvers can raise the severity level of another malfunction; however, by itself, a warning is the expected reaction.

Steering Control Commands

During lane tracking, the malfunction of a steering control command can lead to an immediate impact with critical reaction independent of the RSC.

Sensing

To accurately and properly perform lane tracking, sensing of lane markers, lane edge, or some lane reference is required. Additionally, sensing the vehicle steering system condition along with other vehicle, infrastructure, and environmental conditions are performed. BT mechanization with its barriers allows for better safety in case of failure. IW configuration roadway sensors and instrumentation failures affect many vehicles as opposed to the VW configuration. However, for lane tracking, the sensing function is directly related to the lateral movement and warrants high severity levels for all RSCs.

Actuation

Steering control actuation failure will have immediate impact and a high severity level.

Information Link Between the Regulation Layer and the Physical Layer

As important as steering commands and the actuation is, the vehicle communication link providing the commands is as important. Thus, its failure will have an immediate impact and is assessed a high severity level.

7.2.11 Malfunction: Steering for Lane-Changing

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while effecting a lane-change after receiving a new lane assignment.

Lane Assignment

The failure to properly assign, not assign or give wrong assignment, during the steering for lane-changing will have significant impact on safety. For a worst case scenario, a vehicle changes into the wrong lane, the UE mechanization poses a much higher safety concern than BT as the open lanes allow higher probability of wrong lane change and higher consequences of an incident. The IW configuration poses yet another concern of higher probability of multiple vehicles involved in the same maneuver receiving the wrong lane assignment. Thus, the IW-UE is assessed a high safety severity level. The VW and the IW-BT are assessed medium safety severity levels. Throughput for VW is more localized with medium severity impacts, while the IW are more immediate with high severity impacts.

Supervising the Sequence of the Coordinated Maneuvers

The malfunction of this monitoring by the coordination layer of the maneuvers can raise the severity level of another malfunction; however, by itself, a warning is the expected reaction.

Steering Control Command

During steering for a lane-change, the malfunction of a steering command can lead to an immediate impact with critical reaction independent of the RSC.

Sensing

To accurately and properly perform steering for a lane-change, sensing of lane markers, lane edge, or some lane reference is required. Additionally, sensing the vehicle steering system condition along with other vehicle, infrastructure, and environmental conditions are performed. BT mechanization with its barriers allows for better safety in case of failure. IW configuration roadway sensors and instrumentation failures affect many vehicles as opposed to the VW configuration. However, for lane tracking, the sensing function is directly related to the lateral movement and warrants high severity levels for all RSCs.

Actuation

Steering control actuation failure will have immediate impact and a high severity level.

Information Link Between the Regulation Layer and the Physical Layer

As important the steering commands and the actuation are, the vehicle communication link providing the commands are as important. Thus, their failure will have an immediate impact and is assessed a high severity level.

7.2.12 Malfunction: Maneuvering Coordination Management

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability is likely to be affected while instructions are provided to vehicles for coordinating lane-changing, merging, or any other maneuvers requiring close coordination with neighboring vehicles.

Monitoring Traffic Conditions and Predicting Congestion

The failure of this function may have some efficiency effect, such as planning a maneuver earlier in anticipation of congestion in some upcoming link. The effect on the maneuvering coordination management, irrespective of configuration, is a low safety severity level assessment.

Route Recommendation

While maneuvers will indeed be performed in conjunction with routes, the failure of this function will not affect safety and will have minor impact on efficiency.

Lane Assignment

In an IW configuration, if the lane assignment function fails and an incorrect lane is assigned, efficiency is compromised. As this maneuvering coordination management function is a coordination operation and not the actual lane change function, safety would not be compromised as the following operation would be responsible for the actual lane change. Thus, irrespective of the configuration, only a warning would be issued with a low safety severity level assessed.

Maximum Group Size

When groups are used, a failure of this function would be in exceeding the maximum group size. Performing maneuvering coordination management with excessive group size can cause efficiency and perhaps safety issues as timing to perform maneuvers might be incorrect. In conjunction with hazards, this timing problem could cause severe difficulties in a BT mechanization where there is less freedom to avoid obstacles. This failure in itself is not serious and is thus assessed a low for all configurations.

Prioritizing Vehicle Operations

The providing of instructions to vehicles for coordinating the maneuvers considers vehicle prioritization for emergency vehicles. The failure to provide prioritization will result in possible safety compromises as fatalities due to delayed emergency services might increase. This results in a medium safety severity level assessment.

Regional Traffic Conditions Monitoring and Incident Management

The failure of this function will definitely have efficiency impact with the lack of link level traffic data. For incident conditions, this failure will also cause efficiency impacts. Additionally, if the incident management function selects an incorrect path, an incorrect speed, or provides incorrect instructions for diversion, then possible safety impact can also result. For efficiency, IW configurations have high severity levels, and VW have medium severity levels. The safety impacts are low for all configurations.

Normal Maneuver Coordination Planning

The failure of this function results in efficiency impacts. For an IW configuration, the effect will be more severe than a VW configuration as multiple vehicles/groups will be affected. However, both configurations will have definite impacts with medium efficiency severity levels. Safety impacts will be secondary as incorrect maneuvers need to be implemented by other operations.

Maneuvering Coordination Planning for Hazardous Conditions

The failure of this function is more time critical than the normal maneuver coordination planning function resulting in safety as well as efficiency impacts. The potentially high accelerations and velocities, along with the vehicle maneuver can result in high collision severity and casualty estimations. The failure in a BT mechanization is more severe as the time criticality is substantial. IW configuration might result in multiple groups failing to maneuver for the same hazard. Thus, the failure of this function is critical with a high severity level assessment, except for the VW-UE configuration. As shown in the Statemate simulation for a three-car platoon, whether the instrumentation is IW or VW, the timing for a hazardous versus normal maneuver is substantial and in the event of a hazardous condition, given a UE mechanization, sufficient time to maneuver should result. The repercussions of the maneuver might be in a high mean personal discomfort rating with potential injuries; however, casualties

Information Link Between the Network Layer and the Link Layer

The information between the network and link layers supports functions whose failure would be of low severity level, thus the link failure is of low severity.

Information Exchange Between the Link Layer and the Coordination Layer

The information between the link and coordination layers supports functions whose failures could be of medium severity, thus the exchange failure is of medium severity

Information Link Between the Coordination Layer and the Regulation Layer

The information from the regulation to coordination layer is the driver input, thus this failure would be of low severity.

Information Link Between the Regulation Layer and the Physical Layer

The information from physical to regulation would be the driver input, thus this failure would be of low severity.

Provide Information

The failure to have input from the driver to initiate a maneuver or an incorrect input could have efficiency impact and is independent of configuration. Thus, the severity level assessed is low with a warning reaction.

7.2.13 Malfunction: Exit to a Transition Lane

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while the vehicle is guided to a transition lane near the exit.

Route Recommendation

In exiting to a transition lane, the failure of the route recommendation will definitely result in efficiency impacts irregardless of the configuration. Safety impacts are low for all configurations.

Lane Assignment

The failure to provide the proper lane assignment during this operational function will result in definite efficiency impacts warranting a medium severity level assessment. Safety impacts are low for VW and medium for IW configurations.

Normal Maneuver Coordination Planning

The failure in coordinating maneuvers for exit can have serious reaction with a medium severity level.

Information Link Between the Network Layer and the Link Layer

Consistent with the function using the information, a medium severity level is assessed.

Information Exchange Between the Link Layer and the Coordination Layer

Consistent with the function using the information, a medium severity level is assessed.

7.2.14 Malfunction: Normal Transition from Automatic to Manual Control

Safety and efficiency goals are examined in terms of whether fatalities, injuries, or property damage or whether the average travel speed, or travel time reliability or predictability are likely to be affected while automatic to manual control is normally effected after the vehicle enters the exit area or transition lane.

Normal Maneuver Coordination Planning

Unlike the failure during transition from the manual to automatic control, this coordination is a continuation of the exit to a transition lane which should have already begun separating the vehicle from the platoon. This continuation will have much high consequence for the UE mechanization as there are no separate transition lanes. Thus, the safety severity levels for the UE mechanizations are critical with high severity levels and the severity levels for the BT mechanizations are serious with medium severity levels. Efficiency impacts are medium for IW and low for VW configurations.

Human-Machine Interface

The failure of the manual control mechanisms during this operation will have immediate impact.

Information Link Between the Coordination Layer and the Regulation Layer

Failure of this link will have severe safety impact during this operation for the UE configuration as previously discussed in the "Normal maneuver coordination planning" section.

Information Link Between the Regulation Layer and the Physical Layer

Failure of this link will have severe safety impact during this operation for the UE configuration as previously discussed in the "Normal maneuver coordination planning" section.

Manually Maneuver Vehicle

This essential human function failure will have immediate impact during this operation.

Provide Information

This essential human function failure will definite impact efficiency if responses for resuming human control are unanswered and can impact safety if responses are incorrectly answered. It is expected that travel speeds are reduced thus impact levels are lower for collision; however, delta velocities can be high as vehicle exit the system without proper human responses. The impact will be immediate and warrants a high severity level for the UE mechanizations. The BT mechanization has built in safety features to lessen the effect although the impact will still be definite and warrants a medium safety severity level.

7.3 KEY RESULTS/CONCLUSIONS/ISSUES

Refer to Appendix B for tables containing the key results of this section.

8. MALFUNCTION MANAGEMENT STRATEGIES

8.1 STRUCTURE AND PURPOSE

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.

8.2 ANALYSES/ASSESSMENTS

As a first step towards developing malfunction management strategies, categories of malfunctions with respect to RSCs are grouped. These groupings by operational functions allow the proposing of operations that provide malfunction management as well as provide insight to differences between the RSCs in terms of expected malfunctions. Another grouping by elemental functions provides insight to differences of probable subsystem malfunctions in terms of RSCs.

This process of examining groupings of malfunctions enables us to filter the number of malfunctions and places more emphasis on malfunction differences and similarities, rather than the malfunctions themselves. The impact of this decision to examine differences and similarities are that focus is shifted from the educated, but subjective, ratings of individual malfunctions to address system level effects, i.e. rather than analyze each individual malfunction assessment for accuracy or bias, the common assumptions for all malfunction assessment are stated and an overview of theses AHS malfunctions can be developed. It is not the intent of this study to denounce or expound virtues of AHS or of a specific RSC as that would require much more detailed analysis to justify the malfunction ratings. It is the intent to examine four AHS RSCs with respect to malfunctions and develop malfunction management strategies and raise issues and risks in such a manner that an ensuing analysis can benefit from this study.

Specifically, the objectives of this task are to:

1. Suggest operational functions that implement malfunction management strategies based upon existing operational malfunctions that have been assessed high severity levels. Identify issues associated with baseline operational functions.

2 Identify benefits and issues of the RSCs based upon their differences and similarities given potential malfunctions.

3. Examine elemental functions and their allocated subsystems for common sources of operational malfunctions and suggest malfunction management strategies to mitigate these malfunctions. Identify issues and risks associated with baseline elemental functions and allocated subsystems.

Tables 9 and 10 provide groupings of the high rated malfunctions by operational functions in terms of safety and efficiency effects, respectively. Tables 11 and 12 provide groupings of the high rated malfunctions by elemental functions in terms of safety and efficiency effects, respectively. Appendix C provides additional tables of all the malfunctions in operational and elemental functions groupings.

8.3 Key Results/Conclusions/Issues

8.3.1 Operational Malfunction Management Strategies

Tables 9 and 10 present the high safety and efficiency severity level malfunctions sorted by operational functions. Distinctions of the non-high severity level malfunctions are provided as shaded boxes.

Table 9. Operational Function Malfunction Safety Severity Levels

		RSC			
Operational Functions	**Elemental Functions**	**IW BT**	**IW UE**	**VW BT**	**VW UE**
Entering the system	Manually maneuver vehicle	High	High	High	High
Transition from human to automatic control	Normal maneuver coordination planning	High	High	High	High
Transition from human to automatic control	Manually maneuver vehicle	High	High	High	High
Velocity regulation	Speed regulation command	High	High	High	High
Velocity regulation	Braking command	High	High	High	High
Velocity regulation	Actuation	High	High	High	High
Velocity regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Spacing regulation	Speed regulation command	High	High	High	High
Spacing regulation	Braking command	High	High	High	High
Spacing regulation	Sensing	High	High	High	High
Spacing regulation	Actuation	High	High	High	High
Spacing regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Longitudinal position regulation	Speed regulation command	High	High	High	High
Longitudinal position regulation	Braking command	High	High	High	High
Longitudinal position regulation	Sensing	High	High	High	High
Longitudinal position regulation	Actuation	High	High	High	High
Longitudinal position regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Lane tracking	Steering control command	High	High	High	High
Lane tracking	Sensing	High	High	High	High
Lane tracking	Actuation	High	High	High	High
Lane tracking	Information link between the regulation layer and the physical layer	High	High	High	High
Steering for lane-changing	Lane assignment	Med	High	Med	Med
Steering for lane-changing	Steering control command	High	High	High	High
Steering for lane-changing	Sensing	High	High	High	High
Steering for lane-changing	Actuation	High	High	High	High
Steering for lane-changing	Information link between the regulation layer and the physical layer	High	High	High	High
Maneuvering coordination management	Maneuvering coordination planning for hazardous conditions	High	High	High	Med
Normal transition from automatic to human control	Normal maneuver coordination planning	Med	High	Med	High
Normal transition from automatic to human control	Human-machine interface	High	High	High	High
Normal transition from automatic to human control	Information link between the coordination layer and the regulation layer	Med	High	Med	High
Normal transition from automatic to human control	Information link between the regulation layer and the physical layer	Med	High	Med	High

Normal transition from automatic to human control	Manually maneuver vehicle	High	High	High	High
Normal transition from automatic to human control	Provide information	Med	High	Med	High

Table 10. Operational Function Malfunction Efficiency Severity Levels

		RSC			
Operational Functions	**Elemental Functions**	**IW BT**	**IW UE**	**VW BT**	**VW UE**
Transition from human to automatic control	Normal maneuver coordination planning	High	High	Med	Med
Transition from human to automatic control	Manually maneuver vehicle	High	High	High	High
Steering for lane-changing	Lane assignment	High	High	Med	Med
Maneuvering coordination management	Regional traffic conditions monitoring and incident management	High	High	Med	Med
Maneuvering coordination management	Maneuvering coordination planning for hazardous conditions	High	High	Med	Med
Normal transition from automatic to human control	Human-machine interface	High	High	High	High

Examination of the operational malfunctions with high safety severity levels suggests the need for five classes of malfunction management strategies. These five classes and the operational functions they involve are:

A. Check-in Phase - Entering the system, Transition from human to automatic control

B. Speed control - Velocity regulation, Spacing regulation, Longitudinal position regulation

C. Steering control - Lane tracking, Steering for lane-changing

D. Coordination - Maneuvering coordination management

E. Check-out Phase - Normal transition from automatic to human control

We propose malfunction management strategies that would be implemented as operational functions. These operational functions would be enabled as the transition states after a malfunction occurs and is detected. (Techniques to indicate a malfunction are not addressed in this study. Refer to Precursor Systems Analyses of Automated Highway Systems tasks on Check-In, Vehicle Operational Analysis, and Check-Out. For example, the Rockwell Vehicle Operational Analysis examines self-diagnosis techniques.)

In task 2 of this study, operational functions that implement an AHS in a mission oriented order were baselined. The proposed additional operational functions would operate in conjunction to these twelve already adopted. An examination of each of the five classes of operational malfunctions follows.

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 failure 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 associated 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 configurations with a transition lane would be minimal, with the UE configuration suffering from link closure.

8.3.2 Representative System Configuration

Examination of the number of high safety and efficiency severity levels assessed by the RSCs was performed. Tables 9 and 10 contain shaded boxes of non-high safety and efficiency

severity levels for each of the RSCs. These shadings provide an indication of the differences among 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.

8.3.3 Elemental Malfunction Management Strategies

Tables 11 and 12 present the high safety and efficiency severity level malfunctions sorted by elemental functions. Distinction of the non-high severity level malfunctions is provided as shaded boxes.

Table 11. Elemental Function Malfunction Safety High Severity Levels

Elemental Functions	Operational Functions	RSC			
		IW BT	IW UE	VW BT	VW UE
Actuation	Velocity regulation	High	High	High	High
Actuation	Spacing regulation	High	High	High	High
Actuation	Longitudinal position regulation	High	High	High	High
Actuation	Lane tracking	High	High	High	High
Actuation	Steering for lane-changing	High	High	High	High
Braking command	Velocity regulation	High	High	High	High
Braking command	Spacing regulation	High	High	High	High
Braking command	Longitudinal position regulation	High	High	High	High
Human-machine interface	Normal transition from automatic to human control	High	High	High	High
Information link between the coordination layer and the regulation layer	Normal transition from automatic to human control	Med	High	Med	High
Information link between the regulation layer and the physical layer	Velocity regulation	High	High	High	High
Information link between the regulation layer and the physical layer	Spacing regulation	High	High	High	High
Information link between the regulation layer and the physical layer	Longitudinal position regulation	High	High	High	High
Information link between the regulation layer and the physical layer	Lane tracking	High	High	High	High
Information link between the regulation layer and the physical layer	Steering for lane-changing	High	High	High	High
Information link between the regulation layer and the physical layer	Normal transition from automatic to human control	Med	High	Med	High
Lane assignment	Steering for lane-changing	Med	High	Med	Med
Maneuvering coordination planning for hazardous conditions	Maneuvering coordination management	High	High	High	Med
Manually maneuver vehicle	Entering the system	High	High	High	High
Manually maneuver vehicle	Transition from human to automatic control	High	High	High	High
Manually maneuver vehicle	Normal transition from automatic to human control	High	High	High	High
Normal maneuver coordination planning	Transition from human to automatic control	High	High	High	High
Normal maneuver coordination planning	Normal transition from automatic to human control	Med	High	Med	High
Provide information	Normal transition from automatic to human control	Med	High	Med	High
Sensing	Spacing regulation	High	High	High	High
Sensing	Longitudinal position regulation	High	High	High	High
Sensing	Lane tracking	High	High	High	High
Sensing	Steering for lane-changing	High	High	High	High
Speed regulation command	Velocity regulation	High	High	High	High
Speed regulation command	Spacing regulation	High	High	High	High
Speed regulation command	Longitudinal position regulation	High	High	High	High
Steering control command	Lane tracking	High	High	High	High
Steering control command	Steering for lane-changing	High	High	High	High

Table 12. Elemental Function Malfunction Efficiency High Severity Levels

		RSC			
Elemental Functions	**Operational Functions**	**IW BT**	**IW UE**	**VW BT**	**VW UE**
Human-machine interface	Normal transition from automatic to human control	High	High	High	High
Lane assignment	Steering for lane-changing	High	High	Med	Med
Maneuvering coordination planning for hazardous conditions	Maneuvering coordination management	High	High	Med	Med
Manually maneuver vehicle	Transition from human to automatic control	High	High	High	High
Normal maneuver coordination planning	Transition from human to automatic control	High	High	Med	Med
Regional traffic conditions monitoring and incident management	Maneuvering coordination management	High	High	Med	Med

In examining elemental malfunctions, it is necessary to examine more closely the allocated subsystems that failed. Tables 14 and 15 list the elemental functions and the allocated subsystem that can possibly fail resulting in malfunctions with high safety and efficiency severity levels. The primary subsystems are listed by IW or VW configuration without specification of BT or UE as BT and UE are configurations associated with operational functions.

References to analysis performed by the Rockwell Vehicle Operations Analysis[8] are made throughout the elemental functions analysis and designated as Mazer, et al.

Two major observations are made in examining tables 14 and 15. 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

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 by Mazer, et al, 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 are 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

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 by Mazer, et al, 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 raise 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

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

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 distinction 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.

Table 14. Primary Subsystems Impacted by High Safety Severity Level Malfunctions.

Elemental Functions	Primary Subsystems	
	IW	VW
Link Layer		
Lane assignment	Control center information processor	N/A
Coordination Layer		
Normal maneuver coordination planning	Control center information processor	Vehicle information processor
Maneuvering coordination planning for hazardous conditions	Control center information processor	Vehicle information processor
Regulation Layer		
Speed regulation command	Vehicle information processor	Vehicle information processor
Braking command	Vehicle information processor	Vehicle information processor
Steering control command	Vehicle information processor	Vehicle information processor
Physical Layer		
Actuation	Vehicle internal actuator	Vehicle internal actuator
Sensing	Vehicle internal sensor Vehicle external sensor Vehicle information processor Roadway sensors & instrumentation	Vehicle internal sensor Vehicle external sensor
Human-machine interface	Vehicle information processor	Vehicle information processor
Information link between the network layer and the link layer	Control center communication	Control center communication
Information link between the coordination layer and the regulation layer	Control center communication	Vehicle external communication Control center communication
Information link between the regulation layer and the physical layer	Vehicle internal communication	Vehicle internal communication
Manually maneuver vehicle	Driver input	Driver input
Provide information	Driver input	Driver input

Table 15. Primary Subsystems Impacted by High Efficiency Severity Level Malfunctions.

Elemental Functions	Primary Subsystems	
	IW	VW
Link Layer		
Lane assignment	Control center information processor	N/A
Monitor regional/local traffic condition and incident management	Control center information processor Roadway sensors & instrumentation	
Coordination Layer		
Normal maneuver coordination planning	Control center information processor	N/A
Maneuvering coordination planning for hazardous conditions	Control center information processor	N/A
Physical Layer		
Human-machine interface	Vehicle information processor	Vehicle information processor
Manually maneuver vehicle	Driver input	Driver input

We then look at the primary subsystems affected and the frequency with which these subsystems' failures have high severity level malfunctions impacts with respect to IW and VW configurations. Tables 16 and 17 list the subsystems comparing infrastructure and vehicle weighted configurations for safety and efficiency respectively.

For the high safety severity level malfunctions, the overwhelming result from reviewing table 16 is that virtually all the failures that occur for the VW configuration also occur for the IW configuration. As we examine the differences, it is noted that the IW configuration includes the control center information processor and roadway sensor & instrumentation. The VW configuration excludes these two subsystems and also includes the vehicle external communication. The brash conclusion is that essentially all the malfunction mitigation strategies required for the VW configuration would be needed for the IW configuration plus more. Hence, from the standpoint from subsystems and the quantity of their malfunctions, the VW configuration is most likely the most economic and reliable system.

Table 16. Primary Subsystems Impacted by High Safety Severity Malfunctions.

Infrastructure-Weighted		Vehicle-Weighted	
Primary Subsystem	**Number of High Safety Severity Malfunction**	**Primary Subsystem**	**Number of High Safety Severity Malfunction**
Control center information processor	4		
Vehicle information processor	13	Vehicle information processor	12
Roadway sensor & instrumentation	4		
Vehicle external sensor	4	Vehicle external sensor	4
Vehicle internal actuator	5	Vehicle internal actuator	5
Vehicle internal sensor	4	Vehicle internal sensor	4
Control center communication	1	Control center communication	1
		Vehicle external communication	1
Vehicle internal communication	6	Vehicle internal communication	6
Driver input	4	Driver input	4

Table 17. Primary Subsystems Impacted by High Efficiency Severity Malfunctions.

Infrastructure-Weighted		Vehicle-Weighted	
Primary Subsystem	**Number of High Efficiency Severity Malfunction**	**Primary Subsystem**	**Number of High Efficiency Severity Malfunction**
Control center information processor	4		
Vehicle information processor	1	Vehicle information processor	1
Roadway sensor & instrumentation	1		
Driver input	1	Driver input	1

9. CONCLUSIONS

AHS malfunctions were examined in context of operational functions, the four RSC's 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.

9.1 OPERATIONAL FUNCTIONS

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

During the AHS "check-in" phase, a malfunction due to coordination planning failure may occur and not be detected. 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. For both the IW and VW configurations, the malfunction effects can be mitigated. However, an issue with the detection of the malfunction exists.

An effective method of detecting this malfunction might be through an extension of current traffic surveillance systems capabilities. Given that this was evaluated as a malfunction with high safety severity for all four configurations, it is highly likely that this malfunction and its mitigation strategy will be directly addressed by any AHS design. If such an extended capability were to be developed, then the questions of how and when should it be addressed by those building an AHS must be answered. Additionally, the type of interface that it will have with other roadside and vehicle detection mechanisms must be identified.

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

It is inevitable that speed and steering control malfunctions will occur in the course of AHS operations. The causes of these malfunctions range from actuator failure to speed regulation software error. Due to the timing requirements for speed and steering control, detection methods might not provide sufficient accuracy. Thus, malfunction management strategies might rely upon Monte Carlo-type statistical results based upon simulations and analyses. One strategy might be to hardwire braking capability and implement full braking as the fail-safe mode, similar to the concept of a crashstop mode[14] followed by a stop mode.

Defining malfunction management strategies based upon probability of occurrence is straightforward. The difficulty would be in any required trade-offs between safety and efficiency. While it is imperative that safety is prioritized, continuous stopping will most probably dissuade even the most avid AHS user. Thus, an issue exists with respect to a better definition of safety and efficiency requirements for the detailing of malfunction management strategies.

9.2 REPRESENTATIVE SYSTEM CONFIGURATIONS

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

The resolving of many of the perceived risks during the "check-out" phase 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 have the lowest cost impacts due to expected infrastructure costs, it is anticipated to be the concept with least resistance. Thus, in order to best promote an AHS program, emphasis should be placed upon the resolving of the "check-out" phase 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.

9.3 ELEMENTAL FUNCTIONS - PRIMARY SUBSYSTEMS

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

This report documents 29 out of 82 expected high safety severity level malfunctions to arise with software related origins. Of the 29 malfunctions, 25 are listed as vehicle based, i.e., most probably due to a vehicle processor failure and/or embedded software error, and 4 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 industries, 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.

It is estimated that electronics with account for up to 30% of the value of a medium sized family car by the year 2000[17]. In fact, in 1993, a luxury car is reported to contain up to 30 electronic systems. This growth in electronics leads to greater exposure of the public to safety-critical software. The sheer volume of automobiles makes this exposure more common than most other applications. With public awareness of software difficulties growing, it is essential that such software is not only correct, but perceived as being correct.

Software and Safety

This section presents the status of safety-critical software and its role in the automotive industry.

The status of critical-safety software is summarized by a quote by Gilles Kahn, the scientific director of France's INRIA research laboratory, "It is not clear that the methods that are currently used for producing safety-critical software, such as that in nuclear reactors or in cars, will evolve and scale up adequately to match our future expectations."[18]

To back up a step and better understand the concept of safety-critical software, some definitions offered by N. Leveson[19] are provided. "An accident or mishap is traditionally defined by engineers as an unplanned event or series of events that leads to an unacceptable

loss such as death, injury, illness, damage to or loss of equipment or property, or environmental harm. Accidents usually involve unwanted and unexpected releases of energy or dangerous substances. By this definition, computers are relatively safe devices: they rarely explode, catch on fire, or cause physical harm. However, computers can contribute substantially to accidents when they operate as a subsystem within a potentially dangerous system. Because computers are not unsafe when considered in isolation and only indirectly contribute to accidents, software safety needs to be evaluated within the context of system safety." Leveson goes on to discuss the impact of software errors in the Therac-25 incidents and how system hazard analysis could have anticipated these incidents and been used to develop malfunction management strategies. This systems perspective was reiterated recently during the IVHS Software Quality/Safety Workshop. Specifically it was said that "two fundamental principles of software safety are that the safety is a systems issue, with software may be a part of the system, and software safety requires a comprehensive approach using more than one technique - testing, formal methods, expert judgment, independent review and assessment[20].

Software Development

A note regarding software development is that the relatively unusual situation the automotive industry creates by designing both the hardware and software together. It should be remembered that software in the computer industry is usually developed for a standard hardware platform, whereas in the motor industry, hardware and software are designed together[21].

Yet, software itself is undergoing a change. Abundant in technological innovations such as the paradigms of structure analysis, CASE tools, object oriented design, 3rd, 4th, and 5th generation programming languages, to reuse repositories, software still struggles[22]. Massive changes are expected, driven by computer usage changes. In fact, with the institutional yielding to quantitative measurements, the handcrafting art form is in transition to a science, e.g., the usage of formal methods with mathematical foundations of discrete mathematics and predicate calculus and the adoption of Cleanroom software engineering[23].

Further explanation of formal methods is provided by the following definition by M. Thomas[24]. "Formal methods use the rigor of mathematics to strengthen the process of software development. These mathematical foundations are powerful for three main reasons: they are descriptive eliminating ambiguity, they are predictive, and they are constructive. Because computer systems are discrete, the use of methods based upon discrete mathematics - mathematical logic - are used to describe such systems." Much experience already exists using formal methods for vehicle and traffic control, such as the Australian national railways railway signaling, the Paris area railway signaling, and in air-traffic control, Praxis is developing the Central Display Information System using formal methods for requirements analysis and specifications.

With the recognition that much of the vehicle processing will be performed using embedded software, much interest exists in ensuring correctness of these safety-critical embedded systems. The use of embedded software gives greatly increased functionality and flexibility and on the other hand it provides unprecedented possibility for errors[25]. As noted in the reference, one way of addressing these potential problems is through the technique of formal methods. One issue raised regarding standards is that if particular methods are recommended or mandated in a standard, then it is possible for the supplier to assume that the method will produce the desired results and blame the standards body if it does not. Thus,

the push for standardization is tempered by this potential reduction of responsibility and accountability of the supplier coupled with a decrease of safety. As noted in the reference, "Any recommendations in standards concerning the use of particular techniques should be regularly checked and updated in the light of recent advances and experience.".

But, with a typical 18 years of transition to standardize techniques, it isn't until early next decade that software itself will finally address some its immaturities. So, investigation of current emerging standardizations was performed.

Emerging Standardization Efforts

An examination of current standardization efforts highlights the pioneer work being performed in Europe and especially the United Kingdom. In the United Kingdom, the Motor Industry Research Association (MIRA) has created a consortium to examine the need for software development standardization in light of the increasing number of safety-critical and safety-related systems appearing in vehicles with required functional reliability[17]. The motivation is reported to be threefold: "specific legislation and regulations, such as electromagnetic compatibility (EMC), product liability, and customer acceptance and satisfaction. Specific procedures must be used during the development and validation of software." In early 1993, it was recognized that no national or international standards or guidelines existed that applied specifically to in-vehicle software. MIRA, with partial funding by the U.K. Department of Trade and Industry, created a consortium called the Motor Industry Software Reliability Association (MISRA) to produce guidelines to assist in the application and creation within a vehicle system of safe, reliable software. MISRA is composed of automotive manufacturers, both vehicle and component, and software engineering consultants. The implication of these guidelines is that "suppliers will have a clear set of guidelines to follow in producing embedded software for their products. Manufacturers will need to work closely with suppliers and assessors, providing high quality specifications.".

The perspective of one automotive manufacture, Ford Motor Company of the U.K., has been to develop in-house standards for the procurement of power-train management control systems from external suppliers[26]. "These standards not only cover conventional software engineering, but include many technologies and disciplines associated with production and encompasses involvement with the supplier throughout the development process rather than accepting delivery based only on requirements and acceptance specifications."

At the European level, the Dedicated Road Infrastructure for Vehicle safety in Europe (DRIVE), is an R&D program initiated by the Commission of the European Communities concerned with the application of information technology to European Road Transport. One of its end products of Project V1051, "Procedure for Safety Submissions for Road Transport Informatics (RTI)," will be a set of proposals for a standard for the production of software for RTI and a set of proposals for a standard for the certification of that software[27,28]. The proposed standard for RTI addresses the following problems simultaneously: "it must give guidance as to how safe software should be designed and implemented at a time when there is no absolute consensus as to how this should be done, it must introduce the certification of software into the existing type approval systems, and it must provide a mechanism for providing a meaningful way of handling the safety integrity of a software subsystem."

The emergence of these potential standards and the current software failures raise legal questions.

Legislation

It was as recent as the late 1980's that computer-controlled systems with serious safety concerns were only used in industries such as aerospace, defense and industrial control where the volumes are tiny compared to the output of any volume car maker[29]. And the cost per unit of complexity in those industries was much smaller than that of the motor industry, so it has traditionally been possible to manage the risk of malfunction by means of redundancy, both hardware and software, all installed at great extra expense. But with most of the motor industry's output targeted at a mass consumer market, with its associated cost parameters, embedded software can have major consequences if a failure occurs. As noted in the reference, "there are long established standards, many backed by legislation, for the design, manufacture, and inspection of most components in the vehicle to ensure their integrity; however, the production of software is a new activity applied to an industry well used to designing its products to meet safety standards. Thus, the associated risks need to be assessed and procedures put in place to control and minimize them.".

As noted by T.R. Kendall[30], "for legislation, the legal position for product liability in the USA and Europe embodies three main principles for use by a plaintiff in a civil action, or the state in a criminal action, against a supplier of goods: breach of contract, negligence and most recently strict liability." If we examine embedded software faults in a vehicle, they could, in theory, be argued under any of the three principles, "although in practice it may be difficult because of the complexity and intangibility of software. There are several initiatives in different sectors of the legislature which will address the subject in such a manner as to impact directly the software design and development process as well as the end product."

Case precedence was recently set in the United States[31], where a software malpractice law suit was upheld through an appeals court. While the case does not reflect direct responsibility for software failures to the software developer, the responsibilities of the software developers are being better defined with the potential to establish requirements for credential. The specific Indiana case, reports that, "In general, persons can incur legal liability for acts relating to computers based on the criminal law, contract law, tort law, and other civil law theories. Tort law includes intentional torts (such as assault or battery) and negligent torts. "Software engineering malpractice" is a variety of negligence. The complexity of many software systems makes it difficult to establish a case of negligence. The courts are also unfamiliar with software engineering malpractice cases since most computer negligence cases have involved hardware. Nevertheless, negligence actions against software developers have been gaining increased attention. Software engineering malpractice arises from the failure of a software engineer to conform to a meet of duty of reasonable care. Software engineers cannot conform to a professional standard unless they know what the standards are. The law will impose malpractice liability based on a breach of a professional standard regardless of whether the professional actually knows the standard. Therefore it is imperative for software engineers to participate in current standards-drafting activities, and to know the standards agreed upon by the profession."

The best starting point for AHS would be the effort by MISRA in the U.K. and the perspectives from other industries.

Perspectives from Other Industries

A recent workshop for IVHS software quality and safety provided much information about the steps being taken by industries regarding software development. One industry undergoing

change is the rail industry where the Federal Rail Administration (FRA) has responsibility over conventional rail and high-speed rail systems. As reported during the workshop[32], concern exists over the use of computer technology in safety critical functions. Without federal regulation or industry standards for development or assessment and the technology changing from "vital relays" to complex computer systems, the issue of software safety headed a list of concerns. Thus, a program was established to develop an industry standards "safety validation methodology" with emphasis on demonstrating (proving) safety of computer systems, not just software alone. The methodology development approach is reported to develop a glossary, conduct state-of-the-art survey in safety assurance methodologies worldwide, assess based upon applicability and level of assure safety and then develop a FRA-specific methodology.

Other industries that have directly addressed safety critical software in the United States have been the medical and avionics industries[33]. "The American medical industry is closely controlled by the Food and Drug Administration. Before any drug or medical device is introduced into the human body, it must undergo extensive safety certification. Many years of testing, clinical trials and analysis are often required before a drug or device is approved for use by the general public. Because the malfunction of implantable devices such as pacemakers and defibrillators may cause death or serious injury, the FDA verifies their safety through a regulatory acceptance process. Careful safety analysis is performed on every component of the device including the embedded software. The Avionics industry has taken the lead in the development of safety certification standards for computer programs. Before an airplane may carry fare-paying passengers, it must undergo a thorough certification process to provide an acceptable level of confidence in its safety. Since many of the components of an airplane are controlled by computer software, the safety of the components is directly dependent on the safety of the embedded software."

9.3.2 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.

REFERENCES

1. American Association of State Highway and Transportation Officials, "A Policy on Geometric Design of Highways and Streets", 1990.

2. MITRE Corporation, Automated Highway System Precursor Systems Analyses Compendium of Research Summaries, Feb. 1994.

3. Federal Highway Administration, "Precursor Systems Analyses of Automated Highway Systems", (BAA) RFP No. DTFH61-93-R-00047, November 27, 1992.

4. Haasl, D. F., Roberts, N. H., Vesely, W. E., Goldbert, F. F., Fault Tree Handbook, U.S. Nuclear Regulatory Commission, Jan. 1981.

5. Department of Transportation, "IVHS Strategic Plan Report to Congress", Dec. 18, 1992.

6. Zhang, W.-B., Shladover, S., Hall, R., and Plocher, T., "A Functional Definition of Automated Highway Systems", TRB Paper No. 940168, January 1994.

7. Varaiya, P. and Shladover, S., "Sketch of an IVHS Systems Architecture: PATH Research Report UCB-ITS-PRR-91-3, revised February 2, 1991.

8. Mazer, N., Clare, L., and Zhang, W.B., "Vehicle Operational Analysis: AHS Runctional Requirements, An interim report", Precursor Systems Analysis of Automated Highway Systems, Feb. 15, 1994.

9. Pline, J. L., Traffic Engineering Handbook, ITE, 1992.

10. Tongue, B. H., "Platoon Collision Dynamics and Emergency Maneuvering", University of California, Berkeley, 1994.

11. Hitchcock, A., "The Safe Automated Freeway", PATH, 1994.

12. Laprie, J.C., "Dependable computing and fault-tolerance: concepts and terminology", Fifteenth Annual Int. Sump. Fault-Tolerat Computing, IEEE Computer Society, June 1985.

13. Avizienis, A., "Architecture of fault-tolerant computing systems", Digest Fifth Int. Symp. Fault-Tolerant Computing, IEEE Computer Society, 1975.

14. Hitchcock, A., "A First Example Specification of an Automated Freeway", PATH Research Report, UCB-ITS-PRR-91-13, June 1991.

15. Ma, L. "Interim Report on AHS PSA Lateral and Longitudinal Control Analysis", April 15, 1994.

16. Ioannou, P. and Xu, Z., "Vehicle Model", Southern California Center for Advanced Transportation Technologies, University of Southern California, January 19, 1994.

17. Ward, D.D., "Development of Guidelines for In-Vehicle Software", IEE "The Integrity of Automotive Electronic Systems", March 22, 1993.

18. Gibbs, W.W, "Software's Chronic Crisis", Scientific American, September 1994.

19. Leveson., N., "Evaluation of Software Safety", 1990 IEEE 12th International Conference on Software Engineering.

20. Lawrence, J.D., "Safety Verification Intervention in the Software Development Process", IVHS Software Quality/Safety Workshop, April 17, 1994.

21. Moon, T., "Vehicle Control Systems - Reliability through Simplicity", IEE Critical Systems Series on "Safety Critical Software in Vehicle and Traffic Control", Feb. 13, 1990.

22. Gibbs, W.W., "Software's Chronic Crisis", Scientific American, September 1994.

23. Hausler, P.A., Linger, R.C., and Trammell, C.J., "Adopting Cleanroom software engineering with a phased approach", IBM Systems Journal, Vol. 33, No. 1, 1994.

24. Thomas, M., "The Role of Formal Methods in Developing Safety-Critical Software", IEE Critical Systems Series on "Safety Critical Software in Vehicle and Traffic Control", Feb. 13, 1990.

25. Bowen, J., "Formal Methods in Safety-Critical Standards", Software Engineering Standards Symposium, August 30, 1993.

26. Davey, C. and Newman, D., "Managing the Diversity of Systems Technologies for Automotive Electronic Control", IEE Colloquium on 'Managing Critical Software Projects', June 20, 1991.

27. Buckley, T.F., Jesty, P.H., Hobley, K., and West, M., "DRIVE-ing Standards: - A Safety Critical Matter", 8th International Conference Automotive Electronics, Oct. 28-31, 1991.

28. Jesty, P.H., Buckely, T.F., and West, M.M., "Safe FTI Systems - A Proposal for a Standards", 8th International Conference Automotive Electronics, Oct. 28-31, 1991.

29. Moon, T., "Managing the Risks Associated with Software in Vehicle Programmes", 8th International Conference Automotive Electronics, Oct. 28-31, 1991.

30. Kendall, T.R., "Some Issues for Software Assessment in the Motor Industry", IEE Assessment and Certification of Software, Nov. 9, 1993.

31. Palermo, C.J., "Software Engineering Malpractice and Its Avoidance", Third International Sumposium on Software Reliability Engineering, Oct. 7-10, 1992.

32. Luedeke, J.F., "Proving Computer System Safety in Railway Application", IVHS Software Quality/Safety Workshop, April 17, 1994.

33. Alsys, Inc. "The Safety Critical Handbook", 1994.

APPENDIX A- FUNCTIONAL SIMULATION AND PROTOTYPE OF AN AHS OPERATIONAL EVENT WITH STATEMATE

A.1 INTRODUCTION

Statemate, a Computer-Aided Software Engineering (CASE) tool from the i-Logix Corporation, was used to better understand and help evaluate the functionality and malfunctions of an AHS for the Precursor Systems Analysis of Automated Highway Systems Malfunction Management and Analysis Task.

Statemate enabled Rockwell engineers to execute and evaluate, not just draw, models of proposed AHS communications layers and operational events. Rockwell has found that the use of tools such as Statemate improve the quality of the system model and therefore the final system design. Three Statemate tools (the Kernel, Analyzer, and Prototyper) were used to create a functional/behavioral model, perform analyzes and run simulations of the model, and create an executable C code prototype and graphic panel of the model.

The following paragraphs explain the methodology of how Statemate was applied to this investigation, along with a discussion of the artifacts created (i.e.; graphic model, simulation and prototype) and results obtained. (Note: This appendix has a very narrow scope relative to AHS malfunction issues, it is limited to a few functional aspects for which Statemate was used to analyze. For a broader discussion, refer to the main article.)

A.2 STATEMATE KERNEL - DESCRIBING THE AHS FUNCTIONAL & BEHAVIORAL MODEL

The Statemate Kernel (see figure A1) provided the means to graphically represent the AHS behavior and functionality. Related views of the AHS were captured by drawing diagrammatic representations of the model using the kernel's graphic editors. The *Activity-chart* graphic editor was used to define the functional view and the *Statechart* graphic editor was used to define the behavioral view. These two views provided a comprehensive, clear, and precise way to specify the AHS functional decomposition and the elemental and operational functions associated with the different communications layers; as well as providing a mean to describe an operational event associated with this model.

A.2.1 Top-down Functional Decomposition

Activity-charts describe the functions of a system; similar to conventional data flow diagrams, Activity-charts show data and control flows along with the system's external environment. The charts treat the system's processing capabilities hierarchically, forming a functional decomposition of the system. The first task was to develop a Statemate model using activity-charts of the 5-layer AHS communications architecture.[7] To bound (or limit the size of) the model so that it represented the communications interfaces, a slice of the overall model was taken. This slice became the top-level activity (AHS_A) in shown figure A2 by the outermost solid rectangle. External communications interfaces to this slice were then identified, as shown by the dashed boxes. Inside the slice, functions - activities in Statemate - representing the 5 layers of the AHS communications were drawn; as shown by the second tier solid boxes. Inside the slice, the communication links between these activities (layers) were drawn. Finally,

the external communication links between the internal functions and the external interfaces were drawn.

The next step was to decompose each level-one activity (the 5 functions representing the communication layers) into their own activity-charts. This was done automatically by Statemate, upon request. The internal and external interfaces from the level-one activity chart were preserved; however, they were both represented as external interfaces on the second-level activity-charts. The top-level activity of each of these charts was then populated with the elemental functions (activities) associated with that particular communications layer, as described in the PATH and Honeywell paper[6] (see figures A3 through A7).

A.2.2 Describing the Behavior (State Transitions Between Operational Functions) at One Level

Statecharts represent the system's behavior over time in its environment and describe the dynamics of a system, showing the control aspects of the system's functions. The charts identify all possible states and the transitions between the states. Labels on the transitions indicate exactly when and under what conditions each transition will take place. Unlike traditional state transition diagrams, Statecharts are hierarchical and support concurrency. A Statechart for the regulation layer was developed (see figure A8). This chart illustrates an early interpretation of the transitions (sequence), hierarchy and concurrencies of the operational functions (or states in Statemate) for the regulation communications layer.

A.2.3 Describing the Behavior of an Operational Event

After capturing the AHS communication layers model, the scope of the Statemate modeling effort was narrowed to allow a more focused analysis of a single operational event; thus providing a better understanding of potential malfunctions relative to that particular functionality. It was decided that the lane change maneuver, as described by PATH and Honeywell[6], would be suitable as such an operational event. Not all the stated requirements were considered, only the functionality needed to perform a coordinated incident-induced lane-change maneuver was studied. At this point the development was started using statecharts that represented the behavior of the system relative to the physical, regulation and coordination layer elemental functions required to perform a coordinated lane change (or operational event).

A.2.4 Performance Modeling using Matlab® with Simulink™

While developing the statechart, a better understanding of the data processing algorithms was needed. Acceleration and braking "g" factors and times required to perform portions of the maneuver, such as lane changing, had to be derived. A tool better suited for performance modeling than Statemate was needed; therefore, Matlab with Simulink from The Mathworks Inc., was used to characterize vehicle performance. Simulink models were created from vehicle models obtained from Longitudinal and Lateral Control research performed by Rockwell and USC.[15,16] Using Simulink, simulations of vehicle acceleration, deceleration (engine-braking), braking and lane-changing were performed and the averaged results were manually embedded into the statechart algorithms. These algorithms, for the most part, are simple linear functions, as they are intended to be representative of average vehicle performance between the range of 80-110 kph. The following factors were chosen:

longitudinal acceleration, 0.0625 "g"; deceleration, 0.0625 "g"; braking deceleration, 0.8 "g"; lateral velocity during normal-steer lane change, 1.2 meters/s (mps); and lateral velocity during hard-steer lane change, 3.7 mps. (Normal-steer and hard-steer are described latter.) See figure A9 for a screen capture of a simulation performed with Simulink (using the USC model).

(Note: For future traffic simulations, Rockwell hopes to automatically interface Statemate with Simulink, allowing dynamic execution (within the Statemate environment) of embedded control system functions. Statemate simulations and prototypes can call and share parameters with externally coded software programs. Rockwell is pursuing the use of a utility from Matlab (which automatically produces C code from the Simulink model) as a way to produce control system programs which can be bound to the Statemate model during simulation and prototype compilation.)

The statechart, in it's final form, is shown in figure A10. This statechart is simply replicated for each vehicle in the model; Statemate supports instantiation. The statechart is partitioned into subsystem data processing states (i.e.; forward sensor processing states, transmission speed sensor simulation states, steering control system states, etc.).

Most of the model dynamics (i.e., conditioning for state transitions) and data processing algorithms are contained within Statemate *forms* (or data dictionary processing forms) which are associated with each element within a Statemate model. Figure A11 shows an example of a pop-up form for the state "emer_backaway."

A.3 STATEMATE ANALYZER - TESTING & SIMULATING THE AHS MODEL

A.3.1 Simulating a Lane Change Maneuver

Once a statechart model of the vehicle was created, detailed analyzes through simulations and prototyping were performed. The Statemate Analyzer was used to execute the AHS system model created with the graphic editors and forms and determine whether the lane change maneuver algorithms specified in the statechart model provided the desired results. Testing and analysis of the model was performed iteratively during the model development, rather than waiting until the entire lane change operational event model was completed.

The Analyzer's simulation capability allowed identification of unacceptable system behavior early in the design process. Using interactive simulation, the system's environment was emulated. For this step-by-step interactive analysis, the designer plays the role of the environment, generating events and setting conditions and data values. The model animates (with movement and color) as it responds to the designer's inputs, allowing the designer to easily see the outcome of what is specified. (See figure A12 for an example of the display screen during Statemate simulation; the figure does not include color.)

In addition to executing the model interactively, program simulations were run in batch mode. Simulations were programmed using Statemate's Simulation Control Language (SCL) and vehicle braking maneuvers and other scenarios were created and performed in batch mode. Statemate's simulation capability enabled the designer to establish test criteria for use throughout the development process. Break-points were set, causing the execution to stop and take certain actions when a particular situation developed. The system model functions as the reference point for each test and enables the designer to run test cases against the original specification.

Another feature of the Analyzer is that simulations can be tied to PGE panels (discussed later). Figure A13 shows a Statemate simulation session that includes animation of a PGE panel (at the very bottom of the screen).

The Statemate Analyzer also supports dynamic exhaustive testing, used to perform rigorous tests on the model to look for unacceptable values or ranges for data items and unknown operational constraints, such as state-reachability, nondeterminism, deadlock conditions, and unused transitions. Due to time constraints, only a few dynamic exhaustive tests were performed on the model created. It was evident, because of intermittent incorrect model executions, that the final model would have been less prone to error had a more thorough job of testing the model been performed.

A.4 PROTOTYPER - "DRIVING" THE AHS MODEL

The Statemate Prototyper was then used to translate the AHS lane change model into C code. The resulting code was compiled and executed on a Sun workstation. Executing this Statemate generated code enables rapid, early prototyping for testing system performance in close-to-real conditions. It translates the system model into a high-level programming language such as Ada or C. The code is entirely consistent with the Statemate model, including any anomalies, which can then be found and traced back directly to the specification. This prototype code can then be executed in a simulation of the target environment or in the final environment itself.

Statemate Prototyper includes a panel graphics editor (PGE) modeling tool, which was used to build a mock-up panel representing graphically, and in animation (when executed) the performance of the three vehicles as they executed the lane change maneuver. The panel can be displayed on the Sun workstation and is manipulated by the user through the mouse. The AHS lane change panel was linked directly to the AHS statechart model. Panel creation and enhancements were performed simultaneously along with the model development and simulations, as it was found that "driving" the panel was a most effective way of debugging the model algorithms. The panel was executed both through the Statemate simulator and by executing the compiled code. The panel code was compiled to include the prototyper debugger utility. As was the case with the simulator, the prototyper with the debugger option enabled model analysis, testing and debugging. Figure A14 shows a Statemate Prototyper session with the debugger option active. (Note the user input at bottom of screen through debugger command language.)

The panel portrays a 158.5 meter length of AHS highway with three autonomously operated vehicles traveling on it (identified as Cars 1, 2 and 3). All movements of the panel objects (highway markers, Cars 2 and 3, and the lane obstruction) are relative to Car 1 that is traveling at a constant velocity of 94 kph throughout the entire maneuver. Therefore, Car 1 remains stationary on the screen. The three lanes are each 3.7 meter wide. Lane 3 is the left-most lane (at the top of the screen). The vehicles are each 1.8 meter wide and 4.3 meters long. Lane 1, which is not used during the maneuver, is the transition lane. There is a barrier separating lanes 1 and 2. Lanes 2 and 3 are the automated AHS lanes. Below the stretch of highway, there are four separate panels providing (model output) information showing the states of each vehicle and the status of the current maneuver. There is a panel that breaks down the time associated with each portion of the maneuver, along with panels that each shows the status of each vehicle relative to the functions they are currently performing: operational functions, sensing elemental functions, and actuation elemental functions. There

is also an area for input (via mouse clicks) from the user to initialize and reset two maneuvers labeled "normal" and "brake-assisted hard steer."

A.4.1 Normal Maneuver

This maneuver is performed without the assistance of brakes (i.e., uses only engine-deceleration) and involves only normal-steer lateral velocity (1.2 mps). Upon initiation by the user, the panel execution begins with Car 1 traveling at a constant 94 kph (velocity regulation - Op5) in lane 3 and performing the role of a leader. Car 2 is a follower, holding to a 3.7 meter headway behind Car 1 (spacing regulation - Op6). Car 3 is a free-agent, traveling in lane two at a constant 102 kph (velocity regulation - Op5) and about ready to overtake Cars 1 and 2 (see figure A15). All three cars are performing lane tracking (Op8).

A stationary object obstructing lane 2 is sensed by the lead vehicles as Car 3 is about to pass Car 1. This is confirmed by the vehicles' front sensor distance and closing rate readouts. Because of the proximity of the vehicles to each other, rather than Car 3 independently performing "steering to avoid collision" (Op12), all three cars begin to perform a coordinated lane change maneuver to get Car 3 out of lane 2. Car 1, as leader (coordination controller), performs Op10 (maneuvering coordination management) to perform the required calculations and to communicate command sequences to the other vehicles, who also perform Op10 to receive these maneuver parameters (see figure A16).

Cars 2 transitions to velocity regulation and temporarily adjust its speed downward to increase its spacing to Car 1 in order to allow Car 3 to be inserted in between them (with a 6.1 meter car headway). At the same time, Car 3 begins to adjust its speed downward to position itself adjacent to the midway point between Cars 1 and 2 (see figure A17).

Car 2, having increased the spacing from 3.7 to 16.8 meters, now transitions back to spacing regulation. The time required for Car 2 to complete this repositioning is recorded (see figure A18). Once Car 3 has positioned itself at the midway point it maintains its velocity constant with Cars 1 and 2. The time required to complete its repositioning is recorded (see figure A19).

Car 3 now transitions out of lane tracking (Op8) into steering for lane-changing (Op9) and begins to change from lane 2 to 3 (see figure A20).

Once Car 3 is behind Car 1, its front sensor readings now reflect distance and closing rate to Car 1. The front sensor of Car 1 still registers the object in lane 2, which is now present on the screen (see figure A21).

When Car 3 has completed the lane change, it returns to lane tracking (Op8) and the times to change lane and to clear lane 2 (which includes backing away time) are recorded. This also initiates the next sequence of actions in the planned maneuver; namely, to close up the gaps from 6.1 back to 3.7 meters. Car 2 returns to velocity regulation, and along with Car 3, begins to accelerate. The front sensor readings of Car 1 change to zeros when the object is passed (see figures A22 and A23).

Once the gap has been closed, Cars 2 and 3 change to spacing regulation and the times to close the gap and for the total operation are recorded (see figure A24).

A.4.2 Brake-Assisted Hard Steer Maneuver

This maneuver for the most part is the same as the (normal) maneuver just described. The difference is that both Cars 2 and 3 momentarily apply their brakes to speed the time required to perform the back-away, and the lateral velocity of Car 3 during lane changing is increased (to 3.7 mps).

Just as before, a stationary object obstructing lane 2 is sensed by the lead vehicles as Car 3 is about to pass Car 1 and all three cars begin to perform Op10, maneuvering coordination management (see figure A25).

However, this time, in performing the back-away portion of the maneuver, Car 2 and 3 temporarily apply their brakes along with releasing the throttle (see figure A26) which makes their back-away time much shorter than before. As before, Car 3 transitions into steering for lane-changing (Op9) once it is in position; but this time hard-steering is performed (see figure A27).

As indicated by the final times recorded for this maneuver, the addition of braking and faster lateral velocity greatly reduces the time to position Car 3 out of lane 2 with much more lead time before reaching the obstacle (see figure 28).

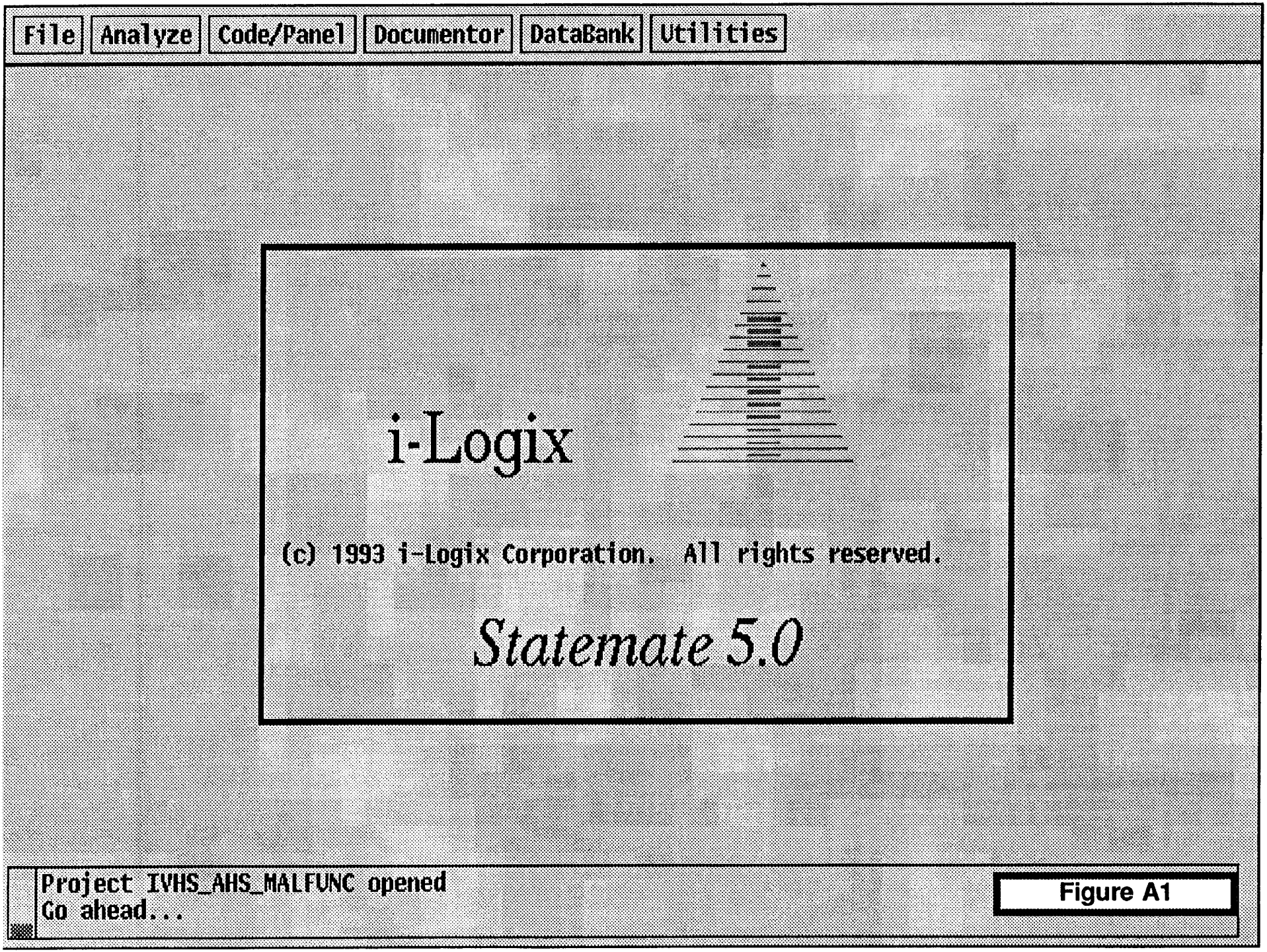

File
Analyze
Code/Panel
Documentor
DataBank
Utilities
i-Logix
(c) 1993 i-Logix Corporation. All rights reserved.
Statemate 5.0
Project IVHS_AHS_MALFUNC opened
Go ahead...

Figure A1

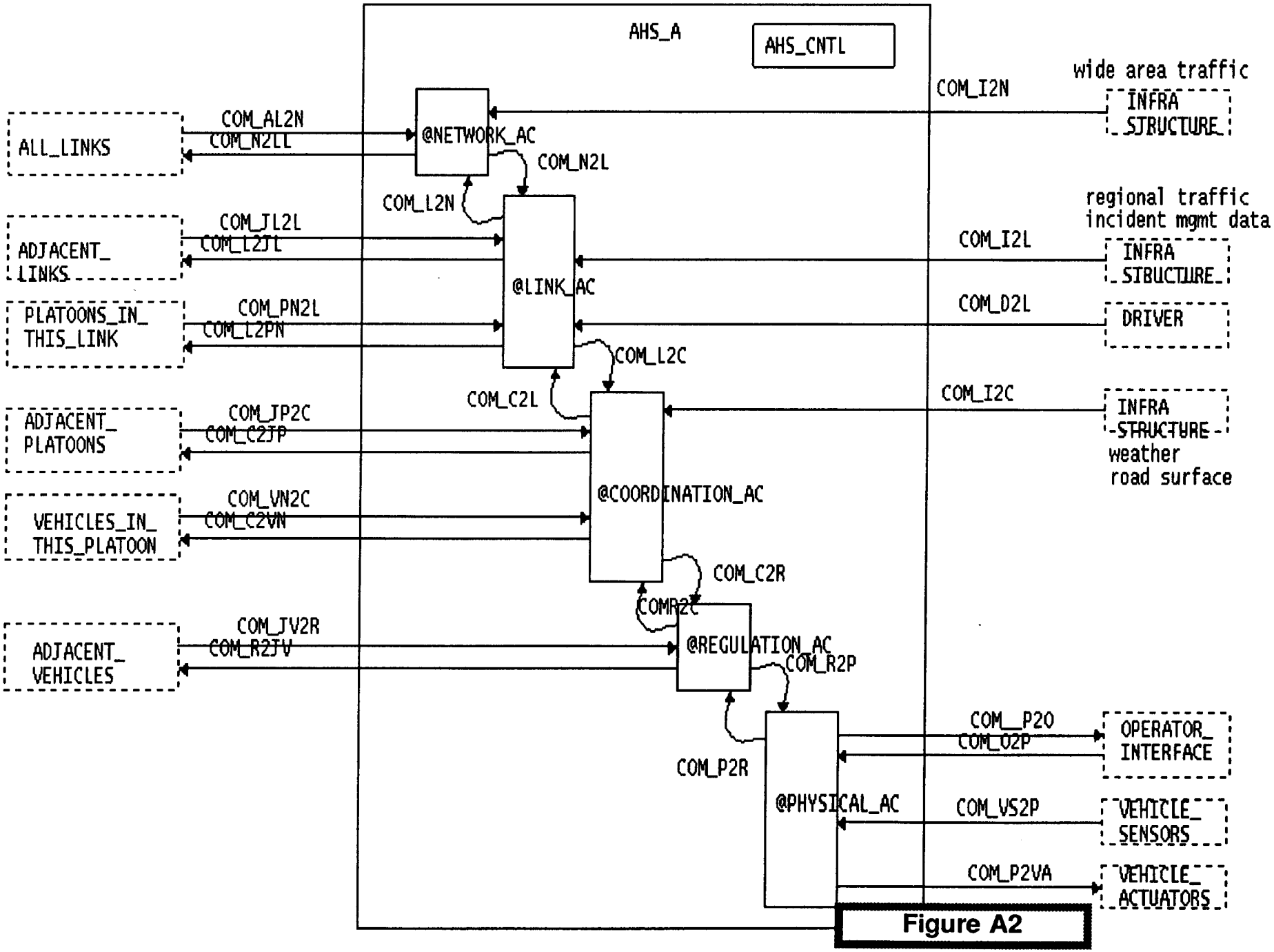

AHS_A
AHS_CNTL
wide area traffic
COM_I2N
INFRA STRUCTURE
COM_AL2N
COM_N2LL
ALL_LINKS
@NETWORK_AC
COM_N2L
COM_L2N
regional traffic incident mgmt data
COM_JL2L
COM_L2JL
ADJACENT_ LINKS
@LINK_AC
COM_I2L
INFRA STRUCTURE
COM_PN2L
COM_L2PN
PLATOONS_IN_ THIS_LINK
COM_D2L
DRIVER
COM_L2C
COM_C2L
COM_I2C
INFRA STRUCTURE
weather
road surface
COM_JP2C
COM_C2JP
ADJACENT_ PLATOONS
@COORDINATION_AC
COM_VN2C
COM_C2VN
VEHICLES_IN_ THIS_PLATOON
COM_C2R
COM_R2C
COM_JV2R
COM_R2JV
ADJACENT_ VEHICLES
@REGULATION_AC
COM_R2P
COM_P2O
COM_O2P
OPERATOR_ INTERFACE
COM_P2R
@PHYSICAL_AC
COM_VS2P
VEHICLE_ SENSORS
COM_P2VA
VEHICLE_ ACTUATORS

Figure A2

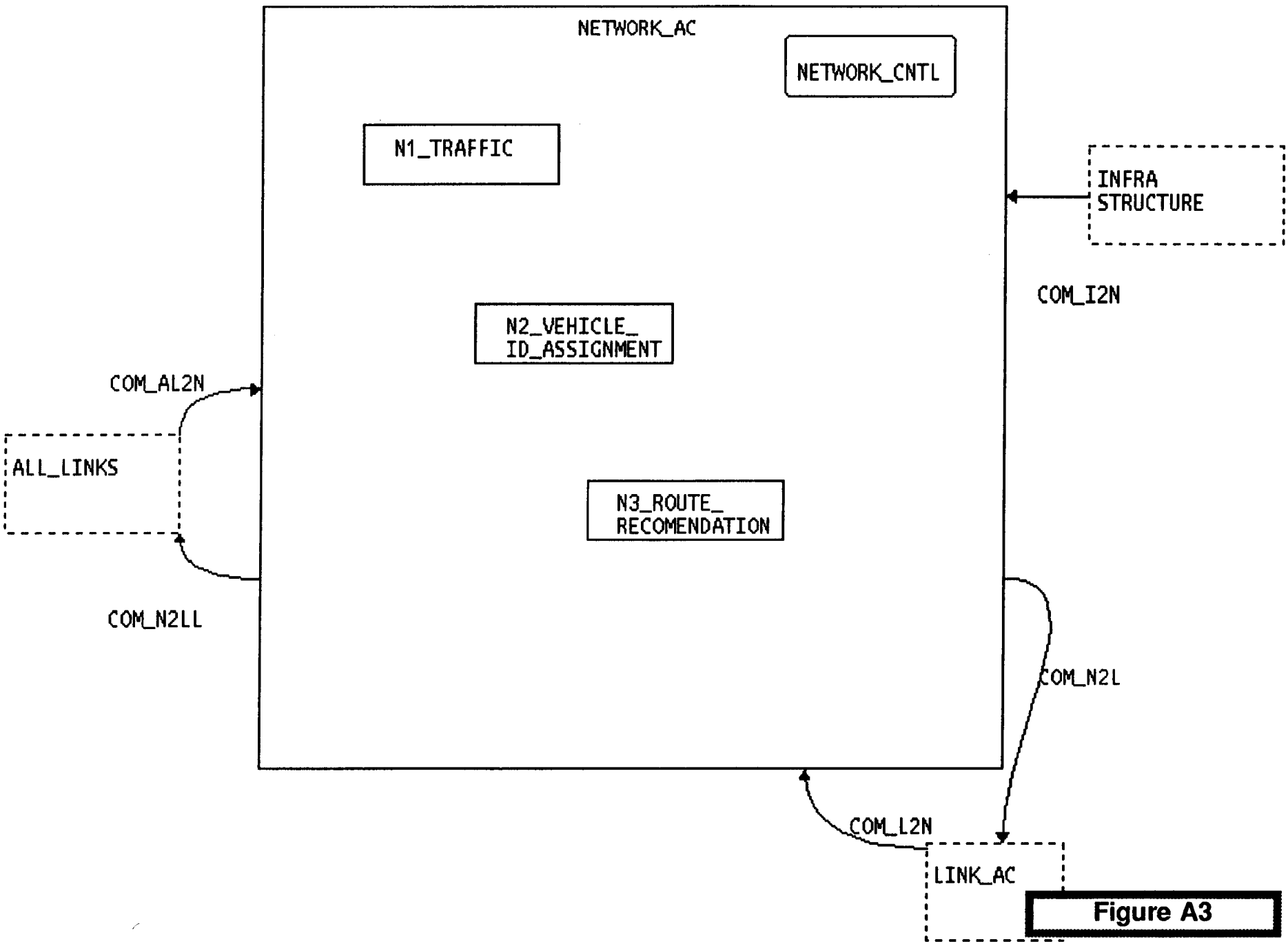

NETWORK_AC
NETWORK_CNTL
N1_TRAFFIC
INFRA
STRUCTURE
COM_I2N
N2_VEHICLE_
ID_ASSIGNMENT
COM_AL2N
ALL_LINKS
N3_ROUTE_
RECOMENDATION
COM_N2LL
COM_N2L
COM_L2N
LINK_AC

Figure A3

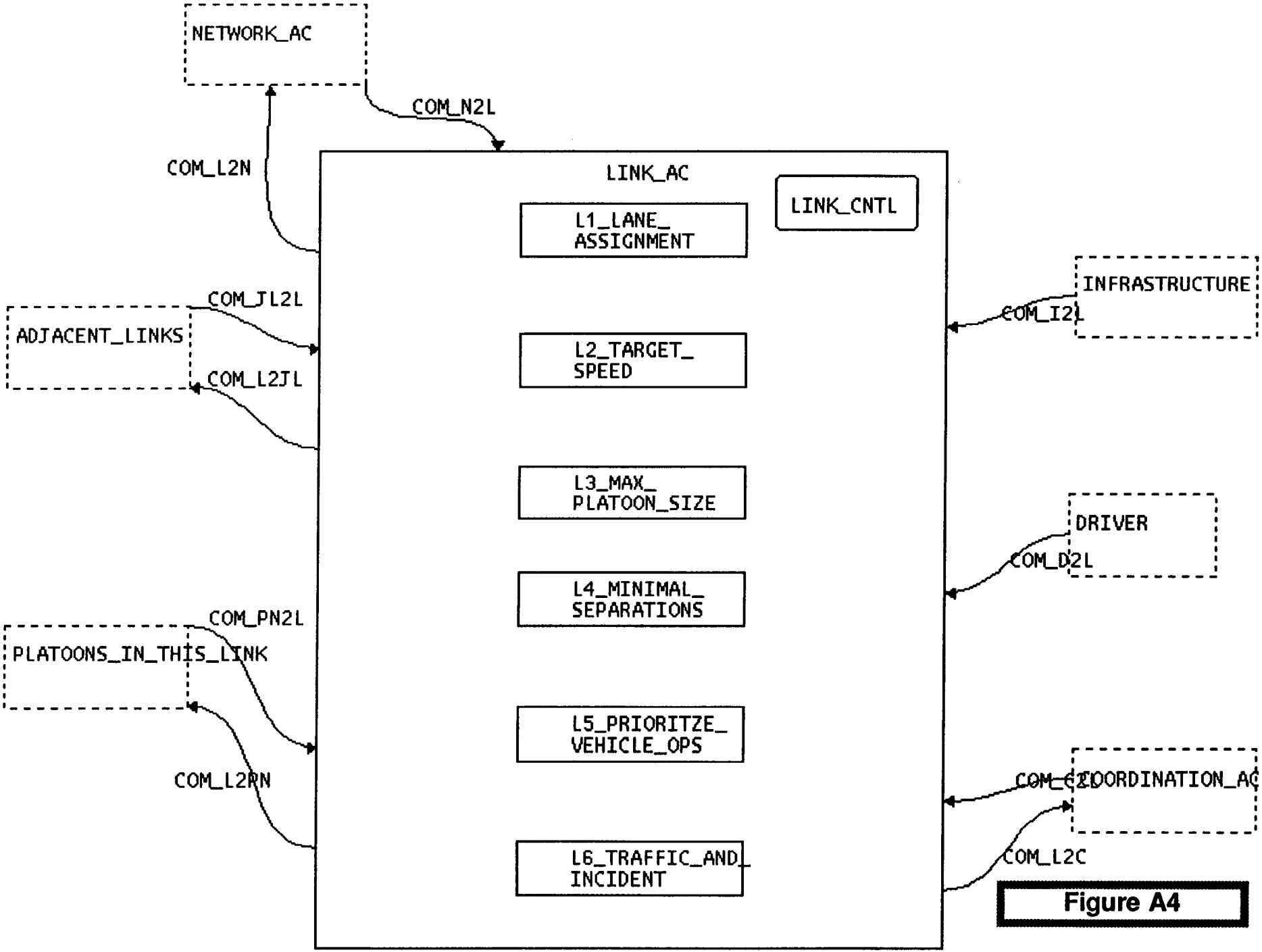

NETWORK_AC
COM_N2L
COM_L2N
LINK_AC
LINK_CNTL
L1_LANE_ ASSIGNMENT
INFRASTRUCTURE
COM_I2L
COM_JL2L
ADJACENT_LINKS
COM_L2JL
L2_TARGET_ SPEED
L3_MAX_ PLATOON_SIZE
DRIVER
COM_D2L
COM_PN2L
PLATOONS_IN_THIS_LINK
L4_MINIMAL_ SEPARATIONS
L5_PRIORITZE_ VEHICLE_OPS
COM_L2RN
COM_C2L
COORDINATION_AC
COM_L2C
L6_TRAFFIC_AND_ INCIDENT

Figure A4

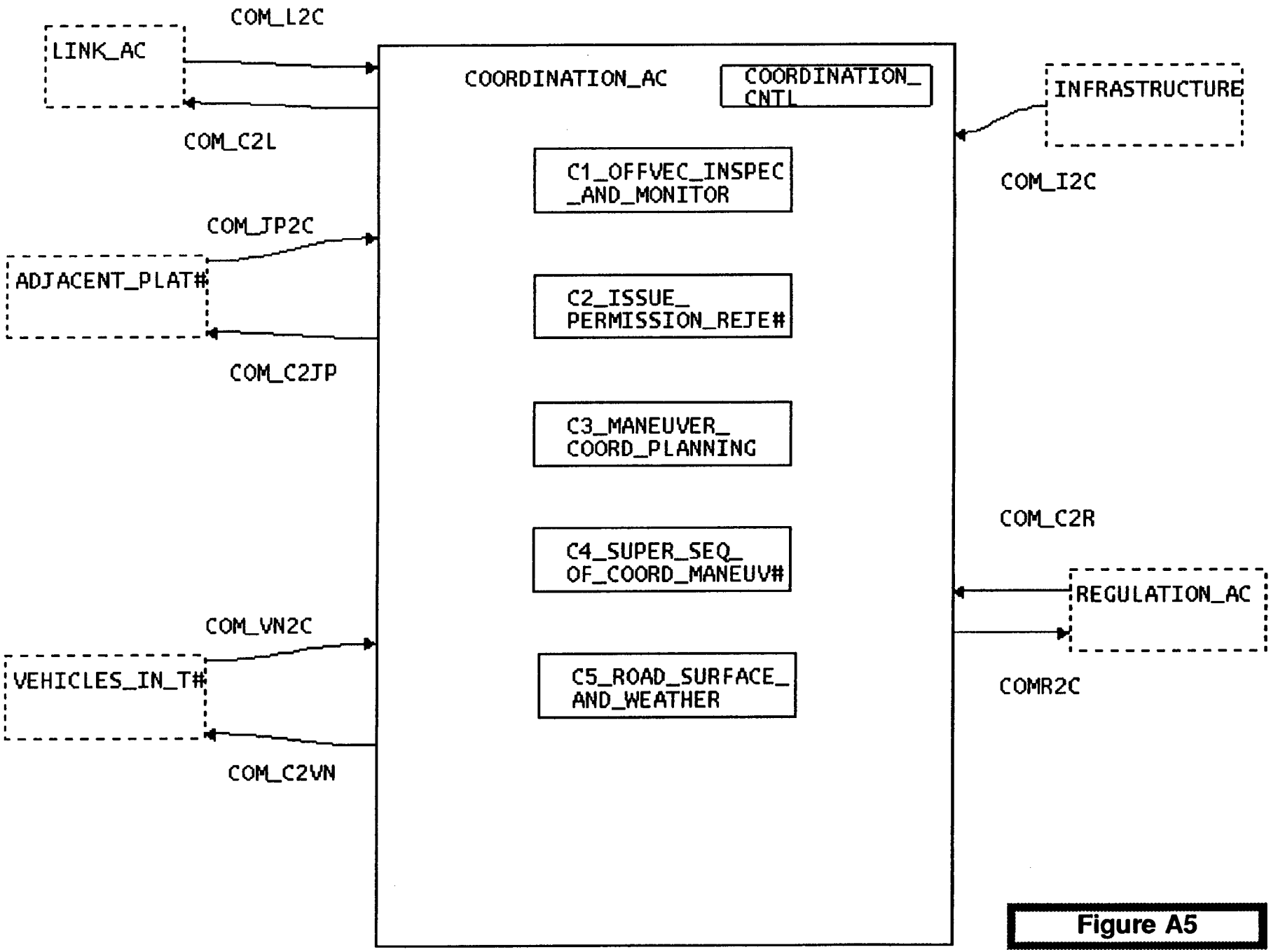

COM_L2C
LINK_AC
COORDINATION_AC
COORDINATION_CNTL
INFRASTRUCTURE
COM_C2L
C1_OFFVEC_INSPEC_AND_MONITOR
COM_I2C
COM_JP2C
ADJACENT_PLAT#
C2_ISSUE_PERMISSION_REJE#
COM_C2JP
C3_MANEUVER_COORD_PLANNING
COM_C2R
C4_SUPER_SEQ_OF_COORD_MANEUV#
REGULATION_AC
COM_VN2C
VEHICLES_IN_T#
C5_ROAD_SURFACE_AND_WEATHER
COMR2C
COM_C2VN

Figure A5

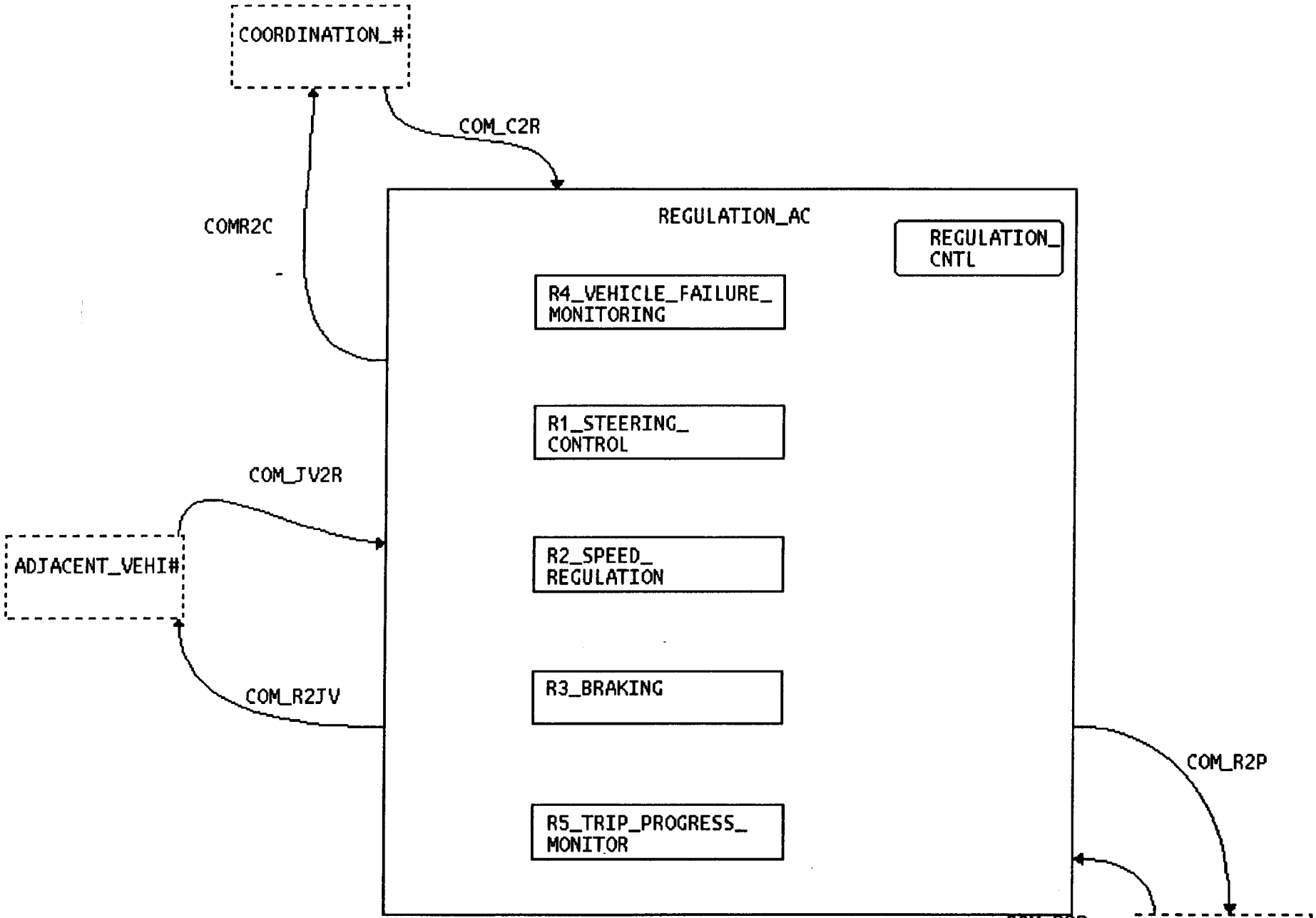

COORDINATION_#
COM_C2R
COMR2C
REGULATION_AC
REGULATION_
CNTL
R4_VEHICLE_FAILURE_
MONITORING
R1_STEERING_
CONTROL
COM_JV2R
ADJACENT_VEHI#
R2_SPEED_
REGULATION
COM_R2JV
R3_BRAKING
COM_R2P
R5_TRIP_PROGRESS_
MONITOR
COM_P2R
PHYSICAL_AC

Figure A6

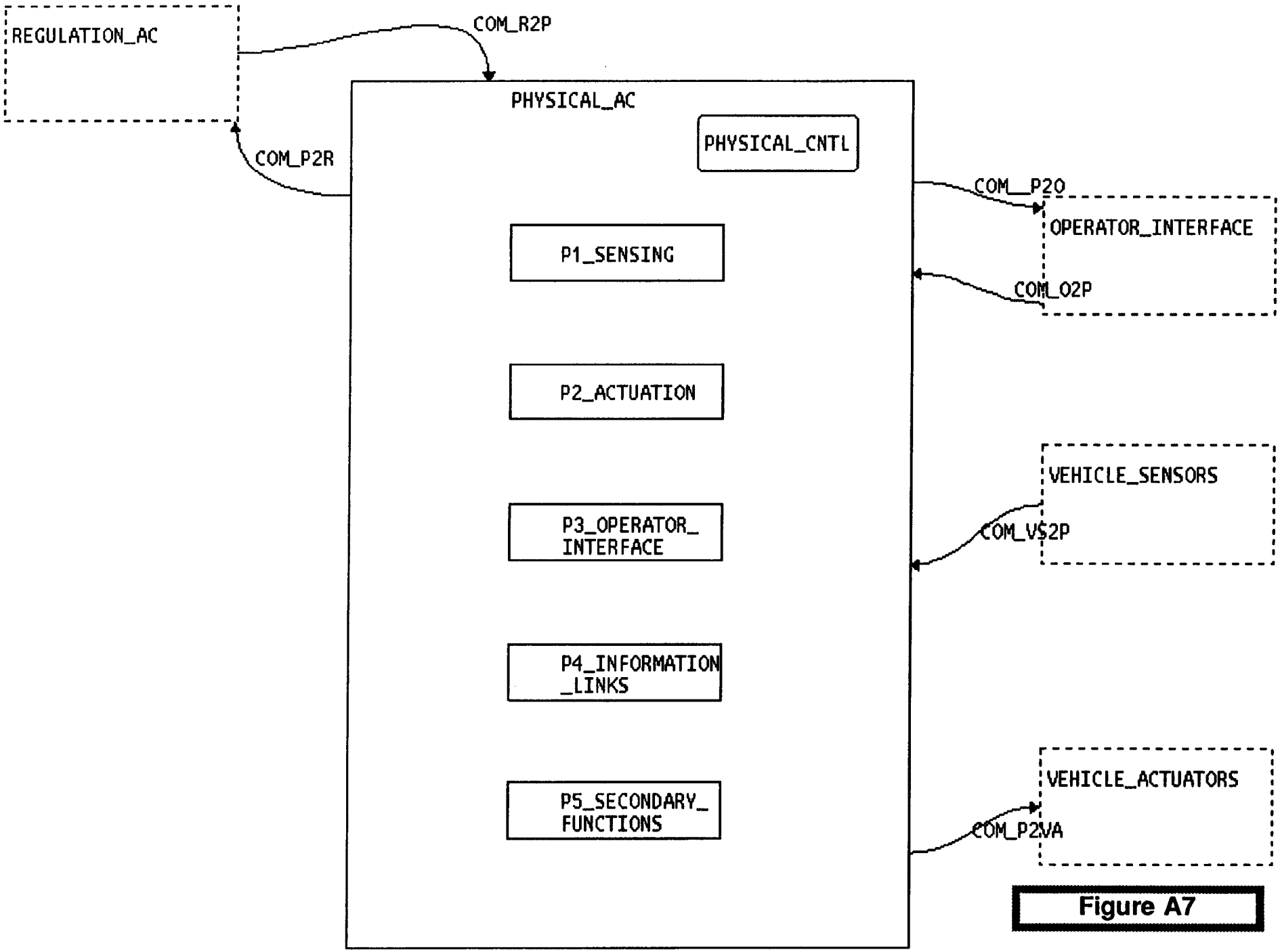

REGULATION_AC
COM_R2P
COM_P2R
PHYSICAL_AC
PHYSICAL_CNTL
P1_SENSING
P2_ACTUATION
P3_OPERATOR_
INTERFACE
P4_INFORMATION
_LINKS
P5_SECONDARY_
FUNCTIONS
COM_P2O
OPERATOR_INTERFACE
COM_O2P
VEHICLE_SENSORS
COM_VS2P
VEHICLE_ACTUATORS
COM_P2VA

Figure A7

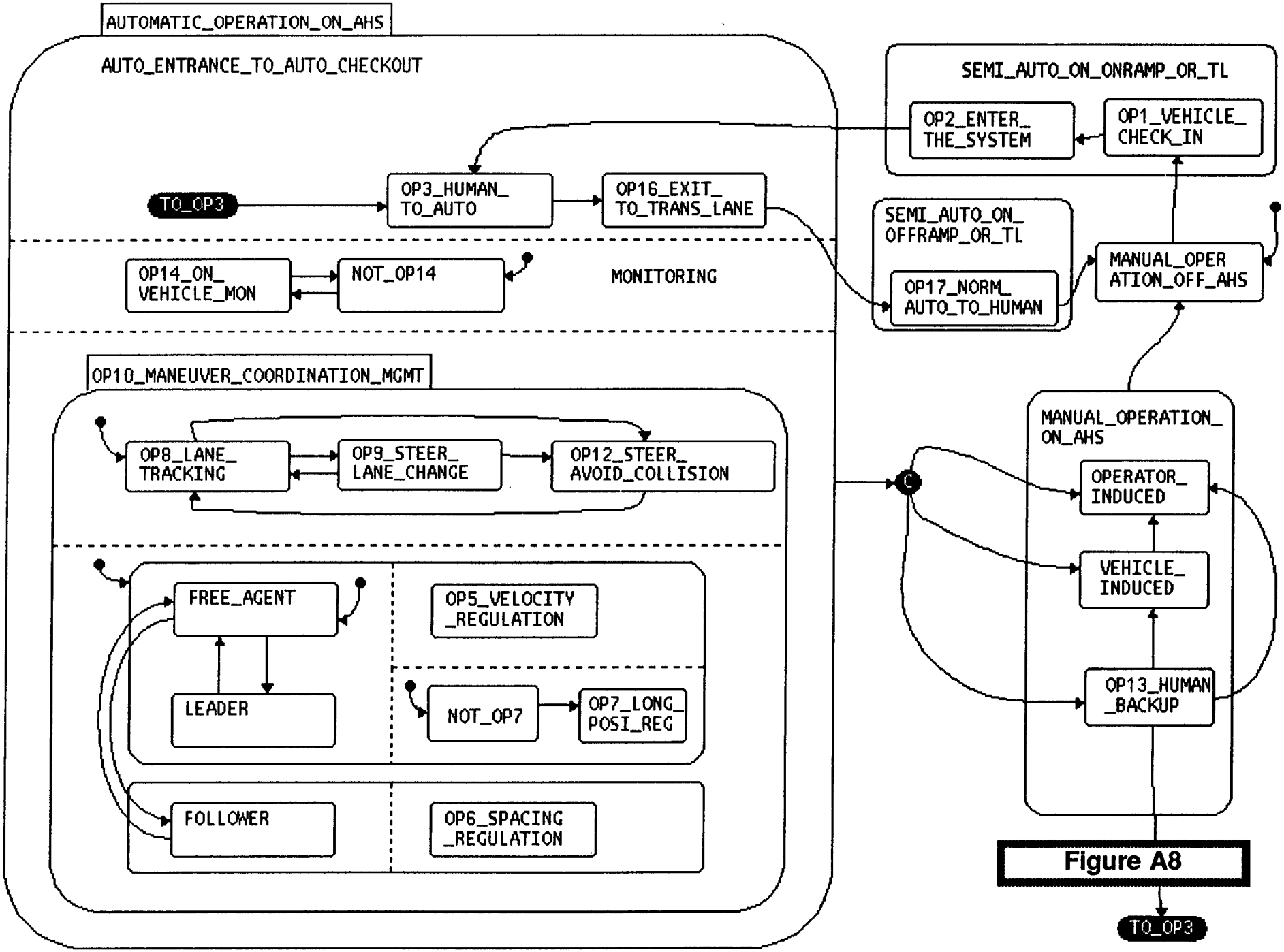

AUTOMATIC_OPERATION_ON_AHS
AUTO_ENTRANCE_TO_AUTO_CHECKOUT
TO_OP3
OP3_HUMAN_TO_AUTO
OP16_EXIT_TO_TRANS_LANE
OP14_ON_VEHICLE_MON
NOT_OP14
MONITORING
OP10_MANEUVER_COORDINATION_MGMT
OP8_LANE_TRACKING
OP9_STEER_LANE_CHANGE
OP12_STEER_AVOID_COLLISION
FREE_AGENT
LEADER
OP5_VELOCITY_REGULATION
NOT_OP7
OP7_LONG_POSI_REG
FOLLOWER
OP6_SPACING_REGULATION
SEMI_AUTO_ON_ONRAMP_OR_TL
OP2_ENTER_THE_SYSTEM
OP1_VEHICLE_CHECK_IN
SEMI_AUTO_ON_OFFRAMP_OR_TL
OP17_NORM_AUTO_TO_HUMAN
MANUAL_OPERATION_OFF_AHS
C
MANUAL_OPERATION_ON_AHS
OPERATOR_INDUCED
VEHICLE_INDUCED
OP13_HUMAN_BACKUP
TO_OP3

Figure A8

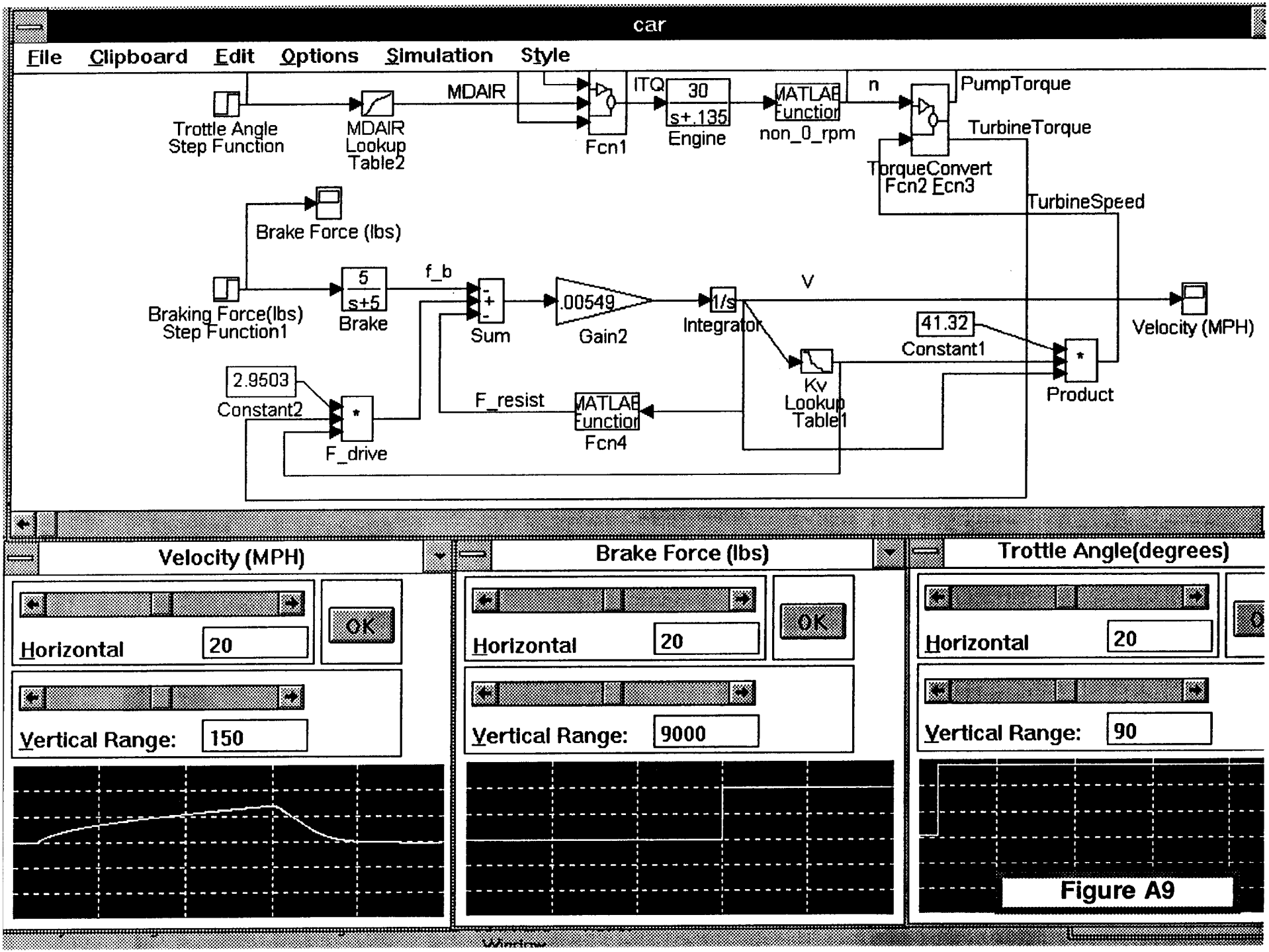

car
File Clipboard Edit Options Simulation Style
Trottle Angle Step Function
MDAIR Lookup Table2
MDAIR
Fcn1
ITQ
30
s+.135
Engine
MATLAB Function
non_0_rpm
n
PumpTorque
TurbineTorque
TorqueConvert Fcn2 Ecn3
TurbineSpeed
Brake Force (lbs)
Braking Force(lbs) Step Function1
5
s+5
Brake
f_b
Sum
.00549
Gain2
1/s
Integrator
V
Velocity (MPH)
41.32
Constant1
Product
Kv Lookup Table1
2.9503
Constant2
F_drive
F_resist
MATLAB Function
Fcn4
Velocity (MPH)
Horizontal
20
OK
Vertical Range:
150
Brake Force (lbs)
Horizontal
20
OK
Vertical Range:
9000
Trottle Angle(degrees)
Horizontal
20
Vertical Range:
90

Figure A9

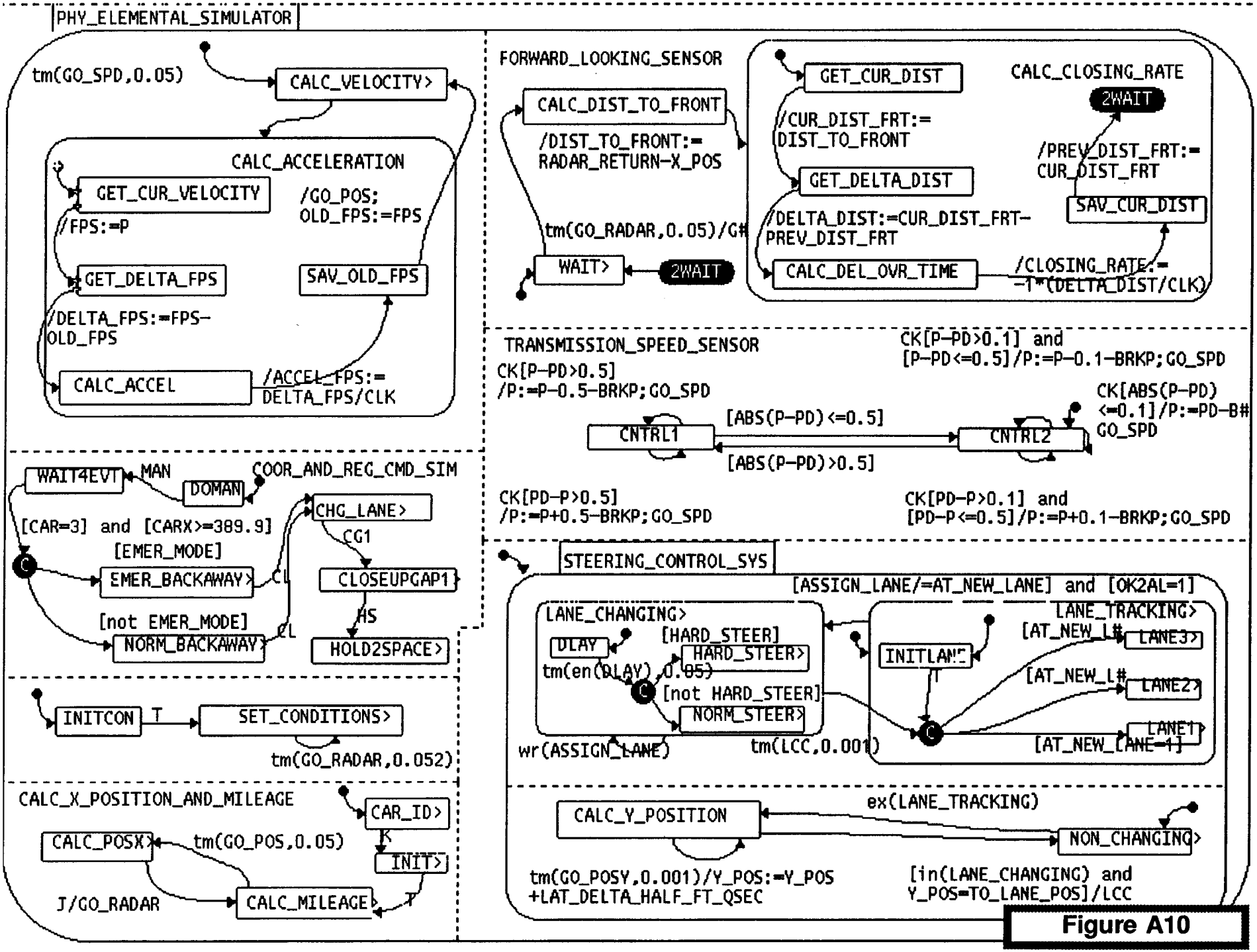

PHY_ELEMENTAL_SIMULATOR
tm(GO_SPD,0.05)
CALC_VELOCITY>
CALC_ACCELERATION
GET_CUR_VELOCITY
/GO_POS;
OLD_FPS:=FPS
/FPS:=P
GET_DELTA_FPS
SAV_OLD_FPS
/DELTA_FPS:=FPS-
OLD_FPS
CALC_ACCEL
/ACCEL_FPS:=
DELTA_FPS/CLK
FORWARD_LOOKING_SENSOR
CALC_DIST_TO_FRONT
/DIST_TO_FRONT:=
RADAR_RETURN-X_POS
tm(GO_RADAR,0.05)/G#
WAIT>
2WAIT
GET_CUR_DIST
CALC_CLOSING_RATE
2WAIT
//CUR_DIST_FRT:=
DIST_TO_FRONT
/PREV_DIST_FRT:=
CUR_DIST_FRT
GET_DELTA_DIST
SAV_CUR_DIST
//DELTA_DIST:=CUR_DIST_FRT-
PREV_DIST_FRT
CALC_DEL_OVR_TIME
/CLOSING_RATE:=
-1*(DELTA_DIST/CLK)
TRANSMISSION_SPEED_SENSOR
CK[P-PD>0.1] and
[P-PD<=0.5]/P:=P-0.1-BRKP;GO_SPD
CK[P-PD>0.5]
/P:=P-0.5-BRKP;GO_SPD
CK[ABS(P-PD)
<=0.1]/P:=PD-B#
GO_SPD
CNTRL1
[ABS(P-PD)<=0.5]
CNTRL2
[ABS(P-PD)>0.5]
CK[PD-P>0.5]
/P:=P+0.5-BRKP;GO_SPD
CK[PD-P>0.1] and
[PD-P<=0.5]/P:=P+0.1-BRKP;GO_SPD
WAIT4EVT
MAN
DOMAN
COOR_AND_REG_CMD_SIM
CHG_LANE>
[CAR=3] and [CARX>=389.9]
CG1
[EMER_MODE]
EMER_BACKAWAY>
CL
CLOSEUPGAP1
HS
[not EMER_MODE]
CL
NORM_BACKAWAY>
HOLD2SPACE>
STEERING_CONTROL_SYS
[ASSIGN_LANE/=AT_NEW_LANE] and [OK2AL=1]
LANE_CHANGING>
[HARD_STEER]
DLAY
HARD_STEER>
tm(en(DLAY),0.05)
[not HARD_STEER]
NORM_STEER>
wr(ASSIGN_LANE)
tm(LCC,0.001)
LANE_TRACKING>
INITLANE
[AT_NEW_L#
LANE3>
[AT_NEW_L#
LANE2>
LANE1>
[AT_NEW_LANE=1]
INITCON
T
SET_CONDITIONS>
tm(GO_RADAR,0.052)
CALC_X_POSITION_AND_MILEAGE
CAR_ID>
K
CALC_POSX>
tm(GO_POS,0.05)
INIT>
J/GO_RADAR
CALC_MILEAGE>
T
CALC_Y_POSITION
ex(LANE_TRACKING)
NON_CHANGING>
tm(GO_POSY,0.001)/Y_POS:=Y_POS
+LAT_DELTA_HALF_FT_QSEC
[in(LANE_CHANGING) and
Y_POS=TO_LANE_POS]/LCC

Figure A10

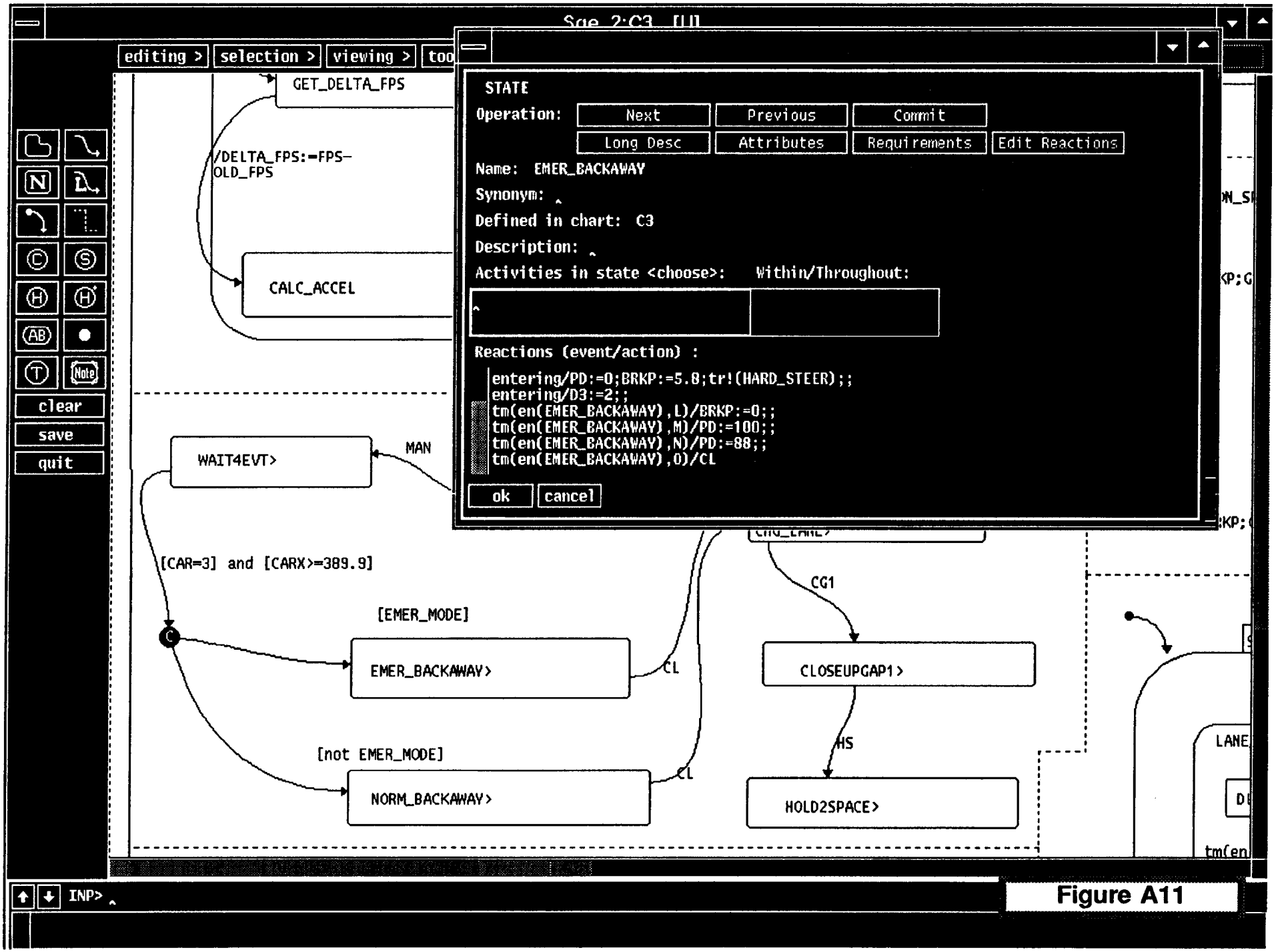

editing >
selection >
viewing >
GET_DELTA_FPS
/DELTA_FPS:=FPS-
OLD_FPS
CALC_ACCEL
clear
save
quit
STATE
Operation:
Next
Previous
Commit
Long Desc
Attributes
Requirements
Edit Reactions
Name: EMER_BACKAWAY
Synonym:
Defined in chart: C3
Description:
Activities in state <choose>:
Within/Throughout:
Reactions (event/action) :
entering/PD:=0;BRKP:=5.8;tr!(HARD_STEER);;
entering/D3:=2;;
tm(en(EMER_BACKAWAY),L)/BRKP:=0;;
tm(en(EMER_BACKAWAY),M)/PD:=100;;
tm(en(EMER_BACKAWAY),N)/PD:=88;;
tm(en(EMER_BACKAWAY),O)/CL
ok
cancel
WAIT4EVT>
MAN
[CAR=3] and [CARX>=389.9]
[EMER_MODE]
EMER_BACKAWAY>
CL
[not EMER_MODE]
NORM_BACKAWAY>
CL
CG1
CLOSEUPGAP1>
HS
HOLD2SPACE>
LANE
INP>

Figure A11

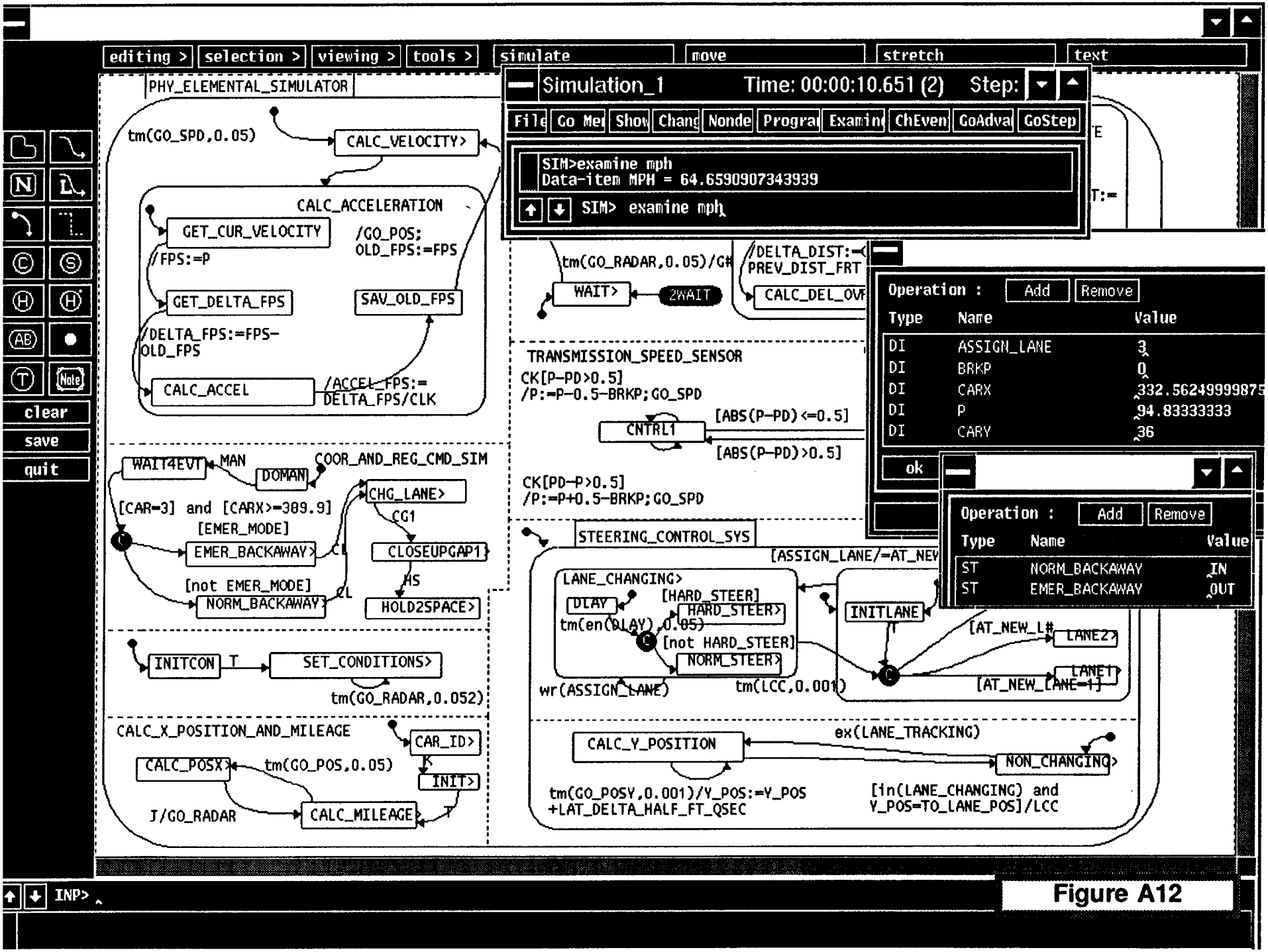

editing >
selection >
viewing >
tools >
simulate
move
stretch
text
clear
save
quit
PHY_ELEMENTAL_SIMULATOR
tm(GO_SPD,0.05)
CALC_VELOCITY>
CALC_ACCELERATION
GET_CUR_VELOCITY
/GO_POS;
OLD_FPS:=FPS
/FPS:=P
GET_DELTA_FPS
SAV_OLD_FPS
/DELTA_FPS:=FPS-
OLD_FPS
CALC_ACCEL
/ACCEL_FPS:=
DELTA_FPS/CLK
Simulation_1
Time: 00:00:10.651 (2)
Step:
File
Go Mer
Show
Chang
Nonde
Progra
Examin
ChEven
GoAdva
GoStep
SIM>examine mph
Data-item MPH = 64.6590907343939
SIM> examine mph
tm(GO_RADAR,0.05)/GH
WAIT>
2WAIT
/DELTA_DIST:=
PREV_DIST_FRT
CALC_DEL_OVF
Operation :
Add
Remove
Type
Name
Value
DI
ASSIGN_LANE
3
DI
BRKP
0
DI
CARX
332.56249999875
DI
P
94.83333333
DI
CARY
36
ok
TRANSMISSION_SPEED_SENSOR
CK[P-PD>0.5]
/P:=P-0.5-BRKP;GO_SPD
CNTRL1
[ABS(P-PD)<=0.5]
[ABS(P-PD)>0.5]
CK[PD-P>0.5]
/P:=P+0.5-BRKP;GO_SPD
WAIT4EVT
MAN
DOMAN
COOR_AND_REG_CMD_SIM
CHG_LANE>
[CAR=3] and [CARX>=389.9]
[EMER_MODE]
CG1
EMER_BACKAWAY>
CL
CLOSEUPGAP1
[not EMER_MODE]
NORM_BACKAWAY>
HS
HOLD2SPACE>
STEERING_CONTROL_SYS
[ASSIGN_LANE/=AT_NEW
Operation :
Add
Remove
Type
Name
Value
ST
NORM_BACKAWAY
IN
ST
EMER_BACKAWAY
OUT
LANE_CHANGING>
DLAY
[HARD_STEER]
HARD_STEER>
tm(en(DLAY),0.05)
[not HARD_STEER]
NORM_STEER>
wr(ASSIGN_LANE)
tm(LCC,0.001)
INITLANE
[AT_NEW_L#
LANE2>
[AT_NEW_LANE=1]
LANE1>
INITCON
T
SET_CONDITIONS>
tm(GO_RADAR,0.052)
CALC_X_POSITION_AND_MILEAGE
CAR_ID>
CALC_POSX>
tm(GO_POS,0.05)
INIT>
J/GO_RADAR
CALC_MILEAGE>
CALC_Y_POSITION
ex(LANE_TRACKING)
NON_CHANGING>
tm(GO_POSY,0.001)/Y_POS:=Y_POS
+LAT_DELTA_HALF_FT_QSEC
[in(LANE_CHANGING) and
Y_POS=TO_LANE_POS]/LCC
INP>

Figure A12

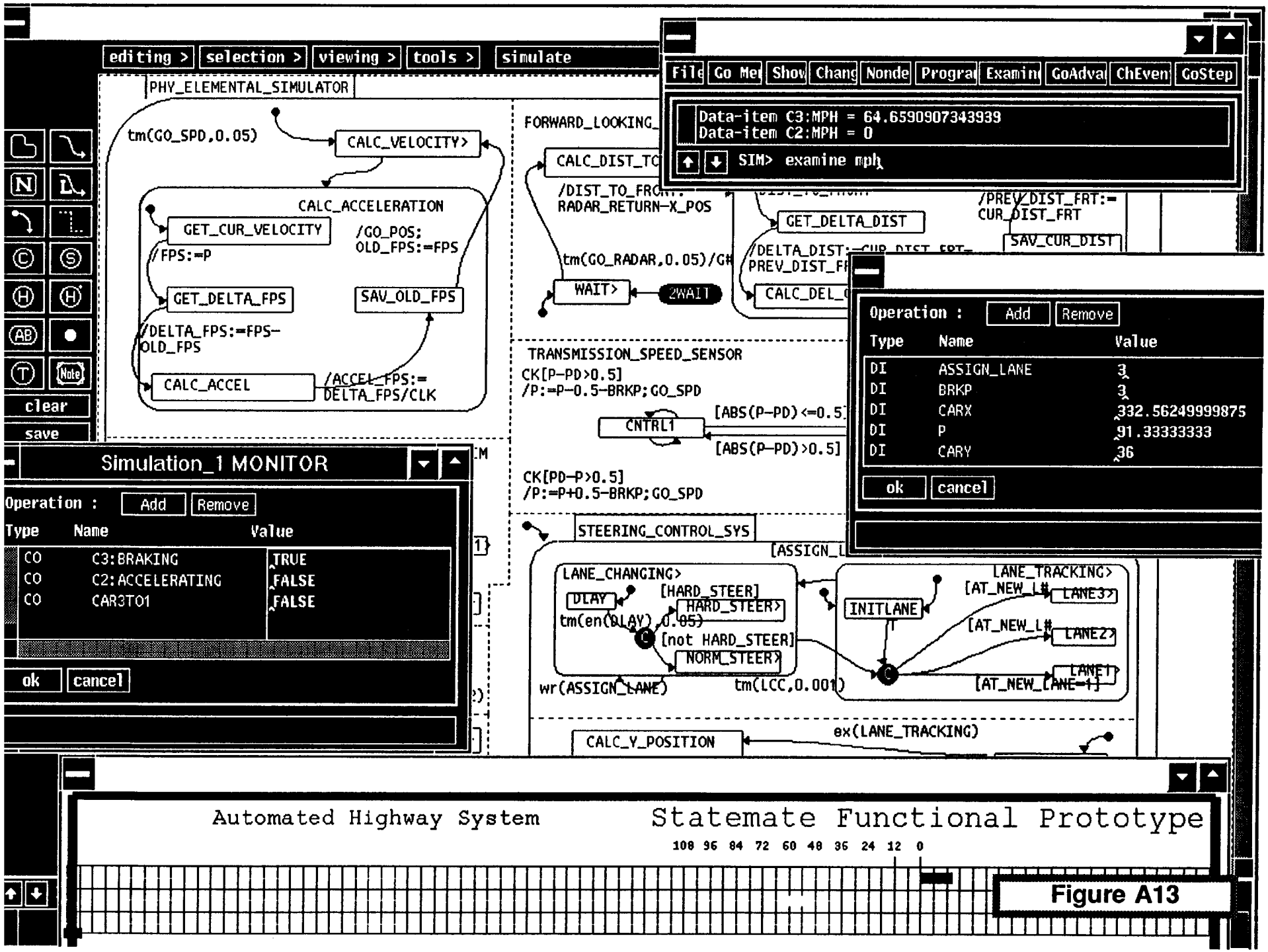
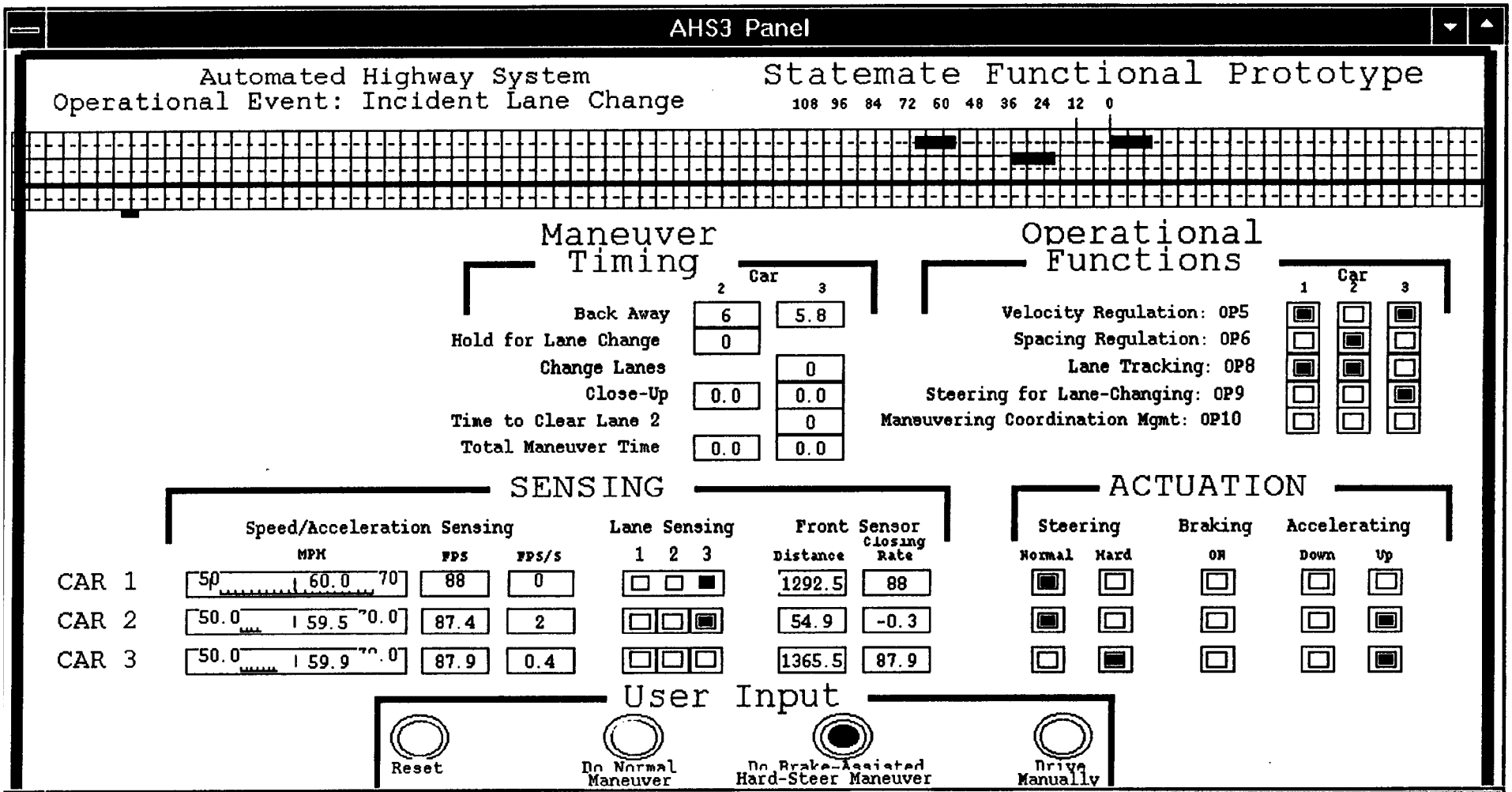

editing >
selection >
viewing >
tools >
simulate
PHY_ELEMENTAL_SIMULATOR
tm(GO_SPD,0.05)
CALC_VELOCITY>
CALC_ACCELERATION
GET_CUR_VELOCITY
/GO_POS:
OLD_FPS:=FPS
/FPS:=P
GET_DELTA_FPS
SAV_OLD_FPS
/DELTA_FPS:=FPS-
OLD_FPS
CALC_ACCEL
/ACCEL_FPS:=
DELTA_FPS/CLK
clear
save
FORWARD_LOOKING_
CALC_DIST_TC
/DIST_TO_FRONT:
RADAR_RETURN-X_POS
tm(GO_RADAR,0.05)/G#
WAIT>
2WAIT
GET_DELTA_DIST
/PREV_DIST_FRT:=
CUR_DIST_FRT
SAV_CUR_DIST
/DELTA_DIST:=CUR_DIST_FRT-
PREV_DIST_FR
CALC_DEL_
TRANSMISSION_SPEED_SENSOR
CK[P-PD>0.5]
/P:=P-0.5-BRKP;GO_SPD
CNTRL1
[ABS(P-PD)<=0.5]
[ABS(P-PD)>0.5]
CK[PD-P>0.5]
/P:=P+0.5-BRKP;GO_SPD
STEERING_CONTROL_SYS
[ASSIGN_L
LANE_CHANGING>
DLAY
[HARD_STEER]
HARD_STEER>
tm(en(DLAY),0.05)
[not HARD_STEER]
NORM_STEER>
wr(ASSIGN_LANE)
tm(LCC,0.001)
INITLANE
LANE_TRACKING>
[AT_NEW_L#
LANE3>
[AT_NEW_L#
LANE2>
LANE1>
[AT_NEW_LANE=1]
CALC_Y_POSITION
ex(LANE_TRACKING)
File
Go Me
Show
Chang
Nonde
Progra
Examin
GoAdva
ChEven
GoStep
Data-item C3:MPH = 64.6590907343939
Data-item C2:MPH = 0
SIM> examine mph
Operation :
Add
Remove
Type
Name
Value
DI
ASSIGN_LANE
3
DI
BRKP
3
DI
CARX
332.56249999875
DI
P
91.33333333
DI
CARY
36
ok
cancel
Simulation_1 MONITOR
Operation :
Add
Remove
Type
Name
Value
CO
C3:BRAKING
TRUE
CO
C2:ACCELERATING
FALSE
CO
CAR3TO1
FALSE
ok
cancel
Automated Highway System
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0

Figure A13




```
34 pdb > step 5
35 pdb > set data_item c3:pd:=103.5
36 pdb > show data c3:cary
     C3:CARY = 45.000000
37 pdb > show condition c3:braking
     C3:BRAKING = false
38 pdb > set event ck:=true
39 pdb > show condition c3:accelerating
     C3:ACCELERATING = true
40 pdb >
40 pdb >
40 pdb >
40 pdb >
40 pdb >
40 pdb > go
```

Figure A14

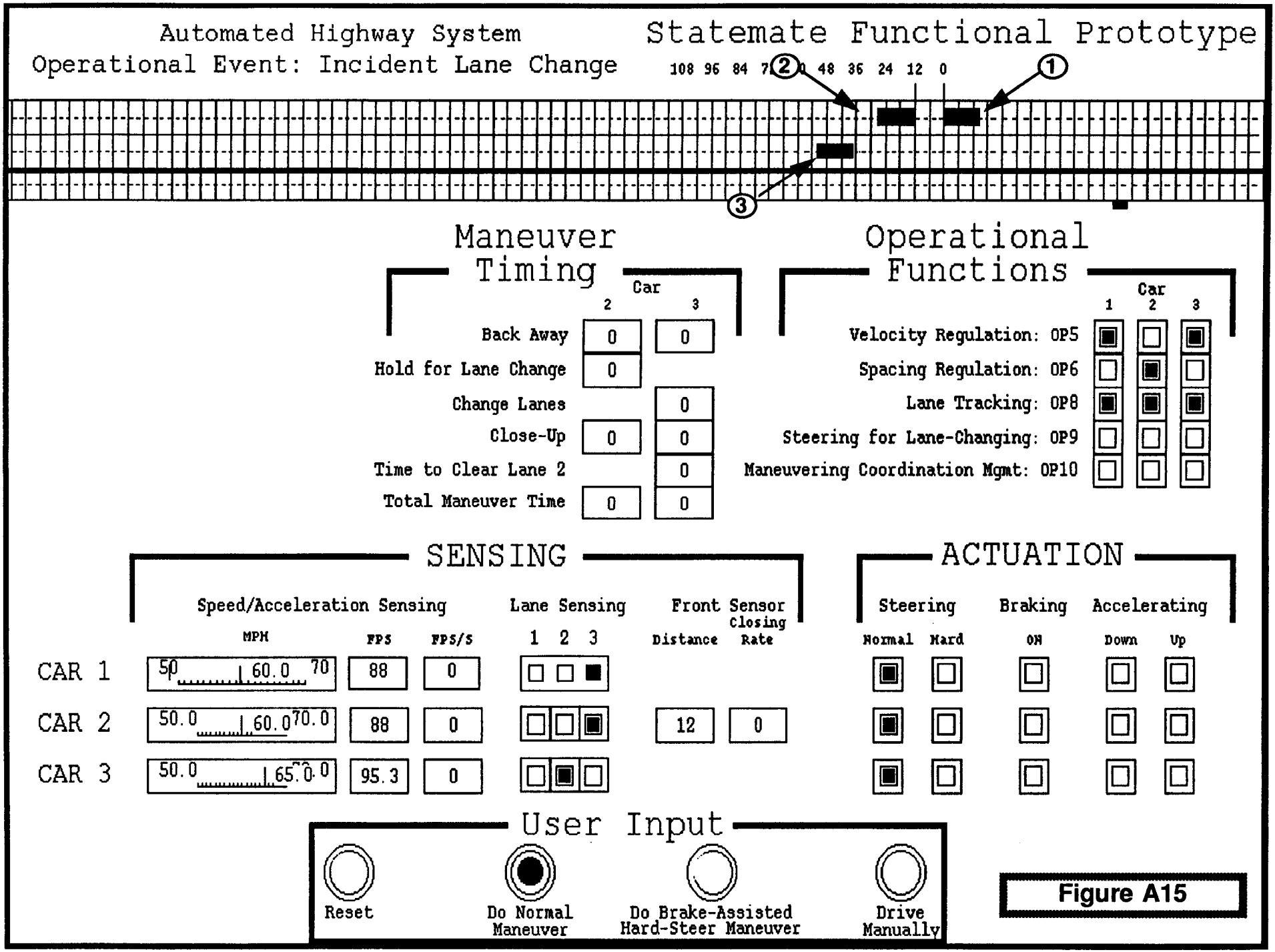

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
0
0
Hold for Lane Change
0
Change Lanes
0
Close-Up
0
0
Time to Clear Lane 2
0
Total Maneuver Time
0
0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50 60.0 70
88
0
CAR 2
50.0 60.0 70.0
88
0
12
0
CAR 3
50.0 65.0
95.3
0
ACTUATION
Steering
Braking
Accelerating
Normal
Hard
ON
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A15

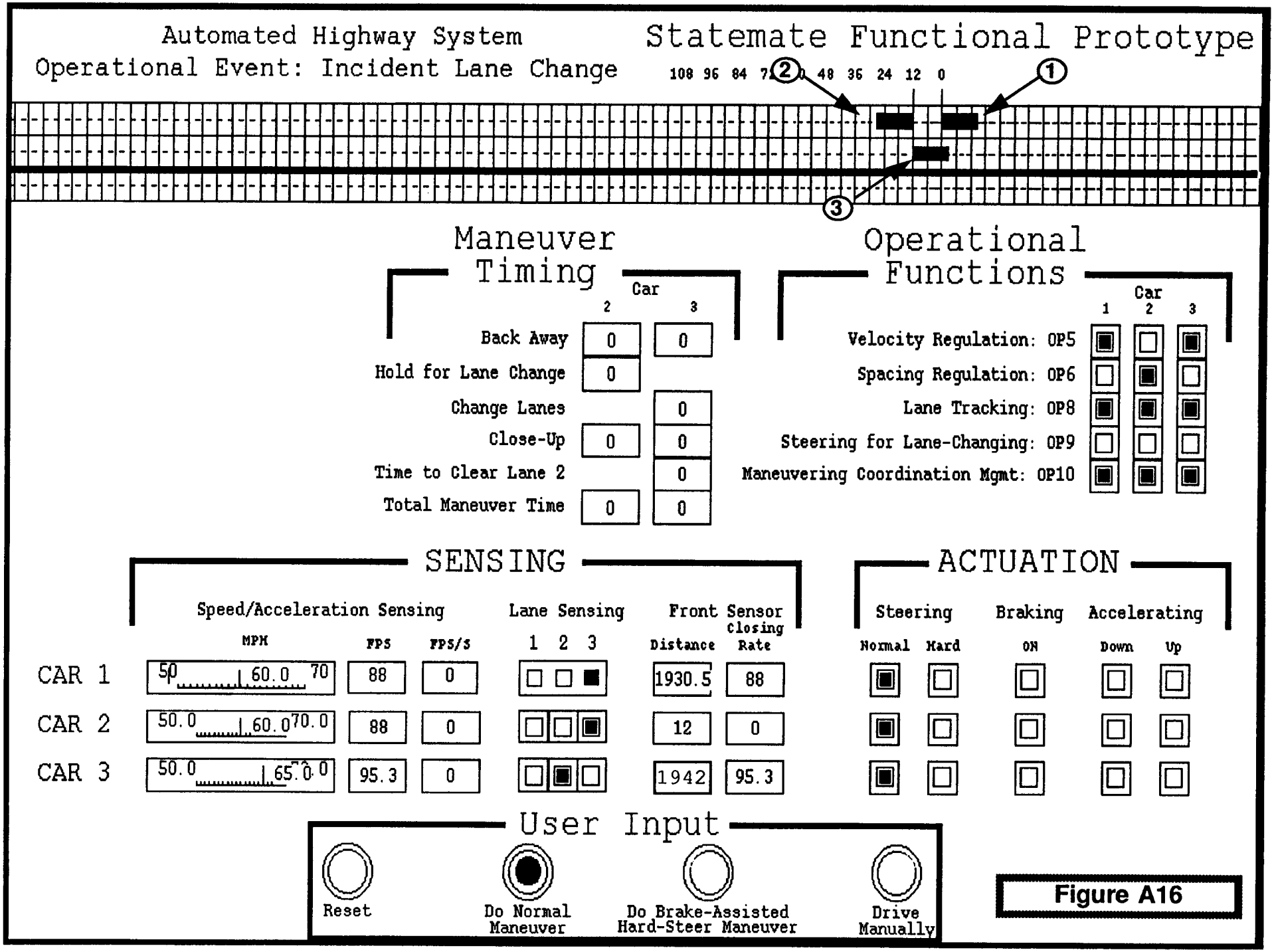

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
0
0
Hold for Lane Change
0
Change Lanes
0
Close-Up
0
0
Time to Clear Lane 2
0
Total Maneuver Time
0
0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50 60.0 70
88
0
1930.5
88
CAR 2
50.0 60.0 70.0
88
0
12
0
CAR 3
50.0 65.0 80.0
95.3
0
1942
95.3
ACTUATION
Steering
Normal
Hard
Braking
ON
Accelerating
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A16

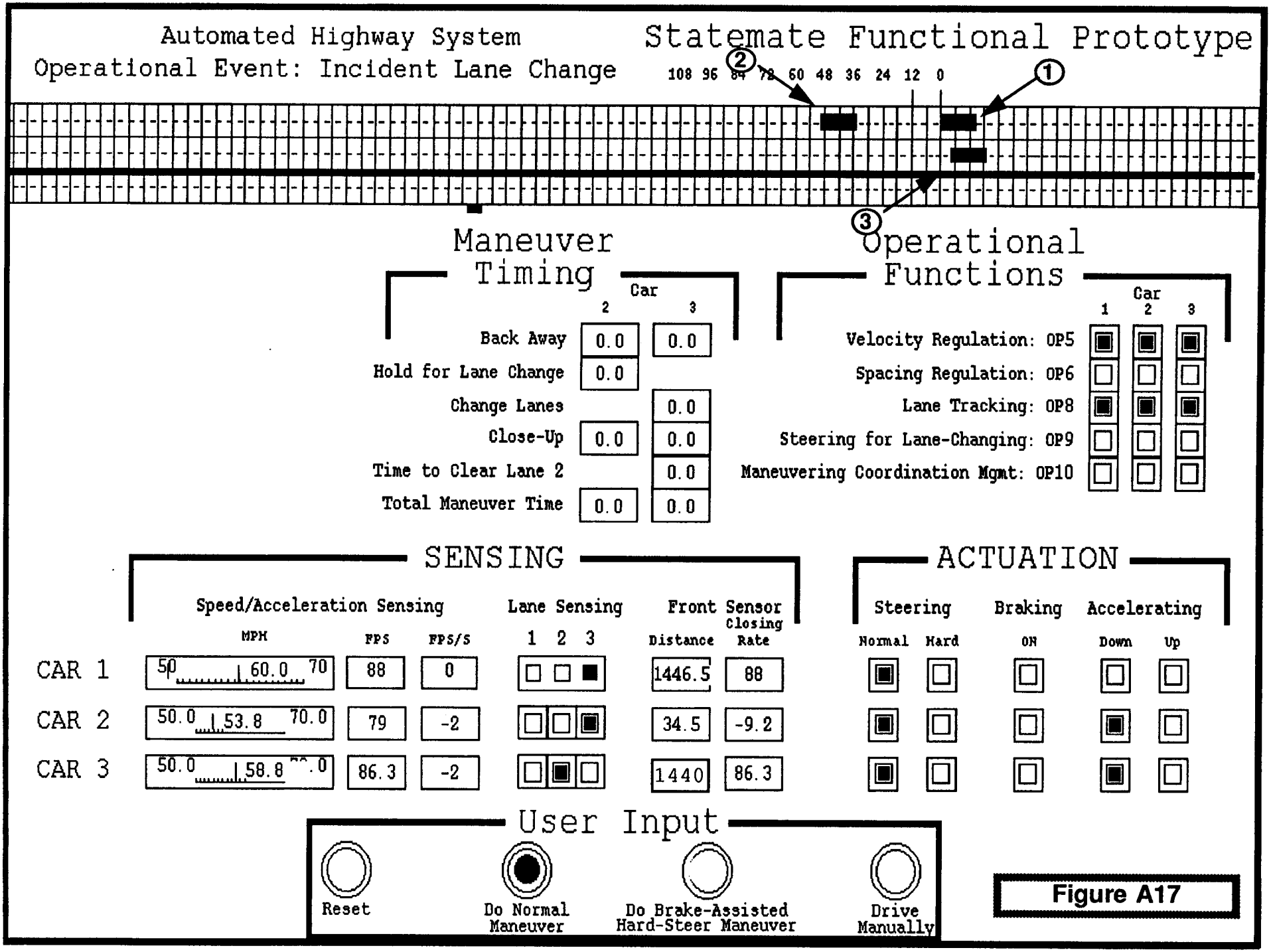

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
0.0
0.0
Hold for Lane Change
0.0
Change Lanes
0.0
Close-Up
0.0
0.0
Time to Clear Lane 2
0.0
Total Maneuver Time
0.0
0.0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50
60.0
70
88
0
1446.5
88
CAR 2
50.0
53.8
70.0
79
-2
34.5
-9.2
CAR 3
50.0
58.8
86.3
-2
1440
86.3
ACTUATION
Steering
Braking
Accelerating
Normal
Hard
ON
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A17

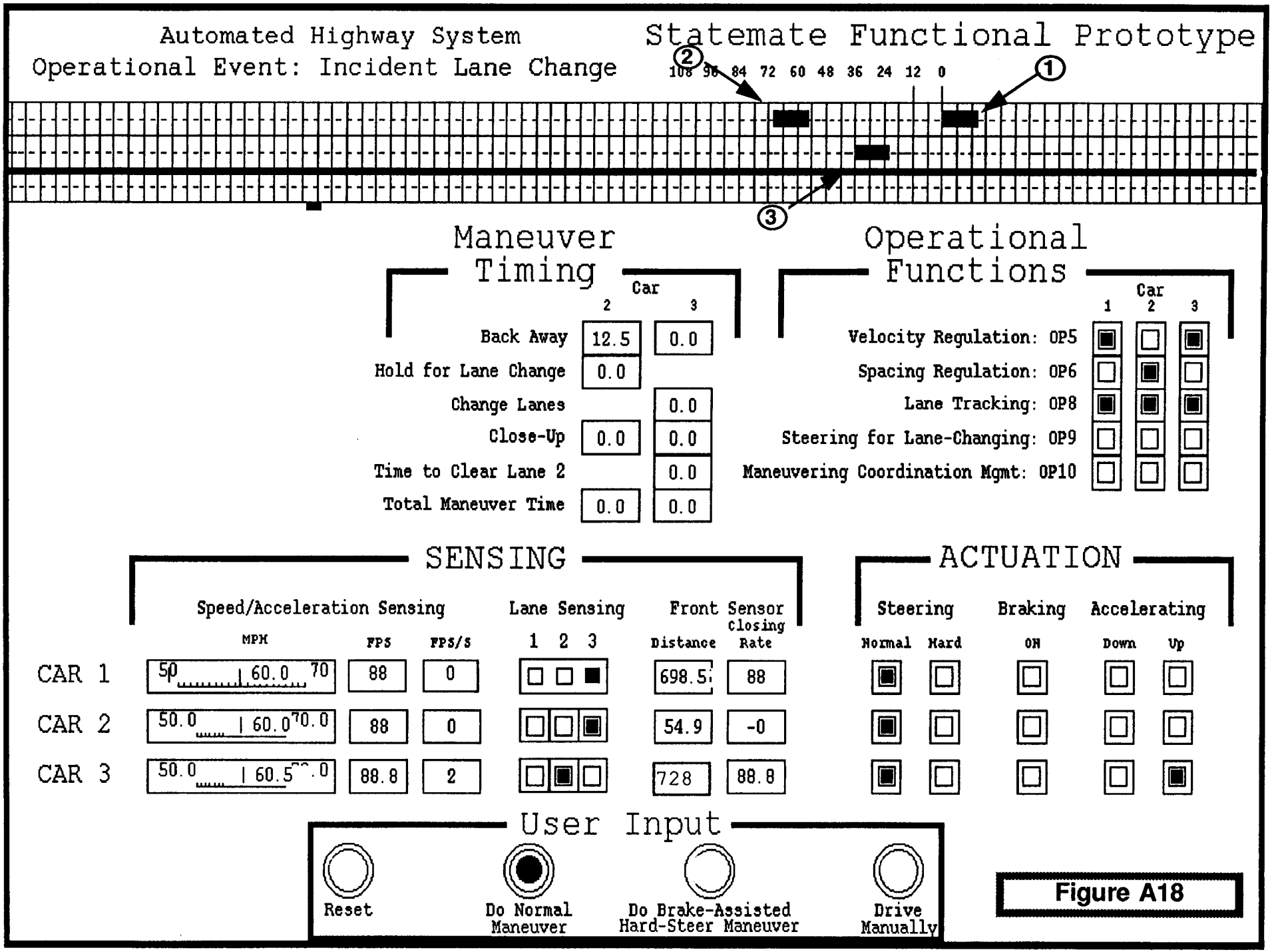

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
12.5
0.0
Hold for Lane Change
0.0
Change Lanes
0.0
Close-Up
0.0
0.0
Time to Clear Lane 2
0.0
Total Maneuver Time
0.0
0.0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50 60.0 70
88
0
698.5
88
CAR 2
50.0 60.0 70.0
88
0
54.9
-0
CAR 3
50.0 60.5 .0
88.8
2
728
88.8
ACTUATION
Steering
Normal
Hard
Braking
ON
Accelerating
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A18

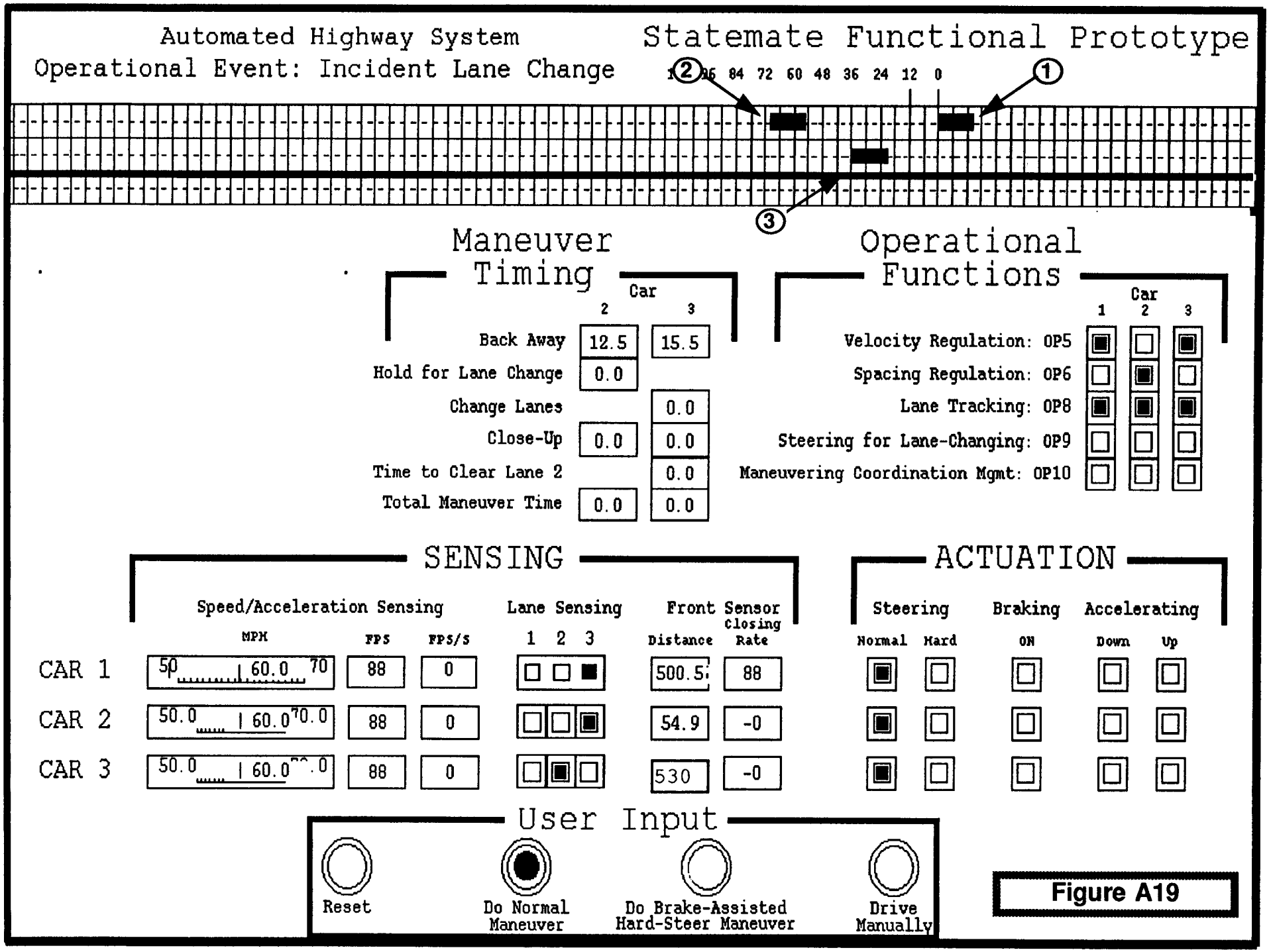
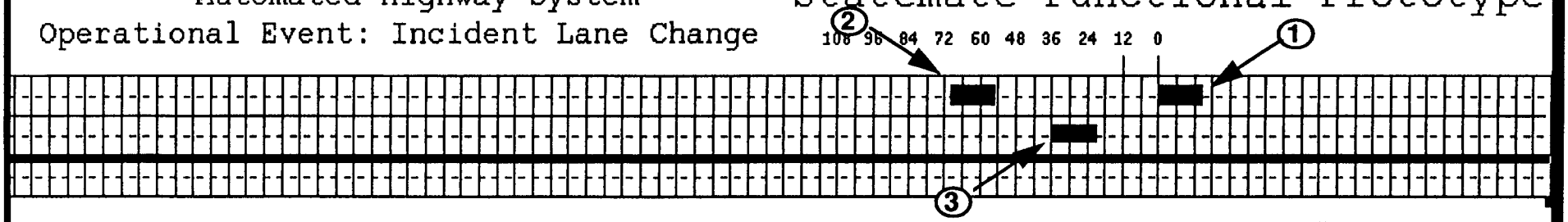

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
12.5
15.5
Hold for Lane Change
0.0
Change Lanes
0.0
Close-Up
0.0
0.0
Time to Clear Lane 2
0.0
Total Maneuver Time
0.0
0.0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50
60.0
70
88
0
500.5
88
CAR 2
50.0
60.0
70.0
88
0
54.9
-0
CAR 3
50.0
60.0
88
0
530
-0
ACTUATION
Steering
Braking
Accelerating
Normal
Hard
ON
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A19

Automated Highway System
Operational Event: Incident Lane Change

Statemate Functional Prototype



Maneuver Timing

	Car 2	Car 3
Back Away	12.5	15.5
Hold for Lane Change	0.0	
Change Lanes		0.0
Close-Up	0.0	0.0
Time to Clear Lane 2		0.0
Total Maneuver Time	0.0	0.0

Operational Functions

	Car 1	Car 2	Car 3
Velocity Regulation: OP5	■	□	■
Spacing Regulation: OP6	□	■	□
Lane Tracking: OP8	■	■	□
Steering for Lane-Changing: OP9	□	□	■
Maneuvering Coordination Mgmt: OP10	□	□	□

SENSING

	Speed/Acceleration Sensing MPH	FPS	FPS/S	Lane Sensing 1 2 3	Front Sensor Distance	Front Sensor Closing Rate
CAR 1	50 60.0 70	88	0	□ □ ■	478.5	88
CAR 2	50.0 60.0 70.0	88	0	□ □ ■	54.9	-0
CAR 3	50.0 60.0 70.0	88	0	□ □ □	20.5	-0

ACTUATION

	Steering Normal	Steering Hard	Braking ON	Accelerating Down	Accelerating Up
CAR 1	■	□	□	□	□
CAR 2	■	□	□	□	□
CAR 3	■	□	□	□	□

User Input

○ Reset
● Do Normal Maneuver
○ Do Brake-Assisted Hard-Steer Maneuver
○ Drive Manually

Figure A20

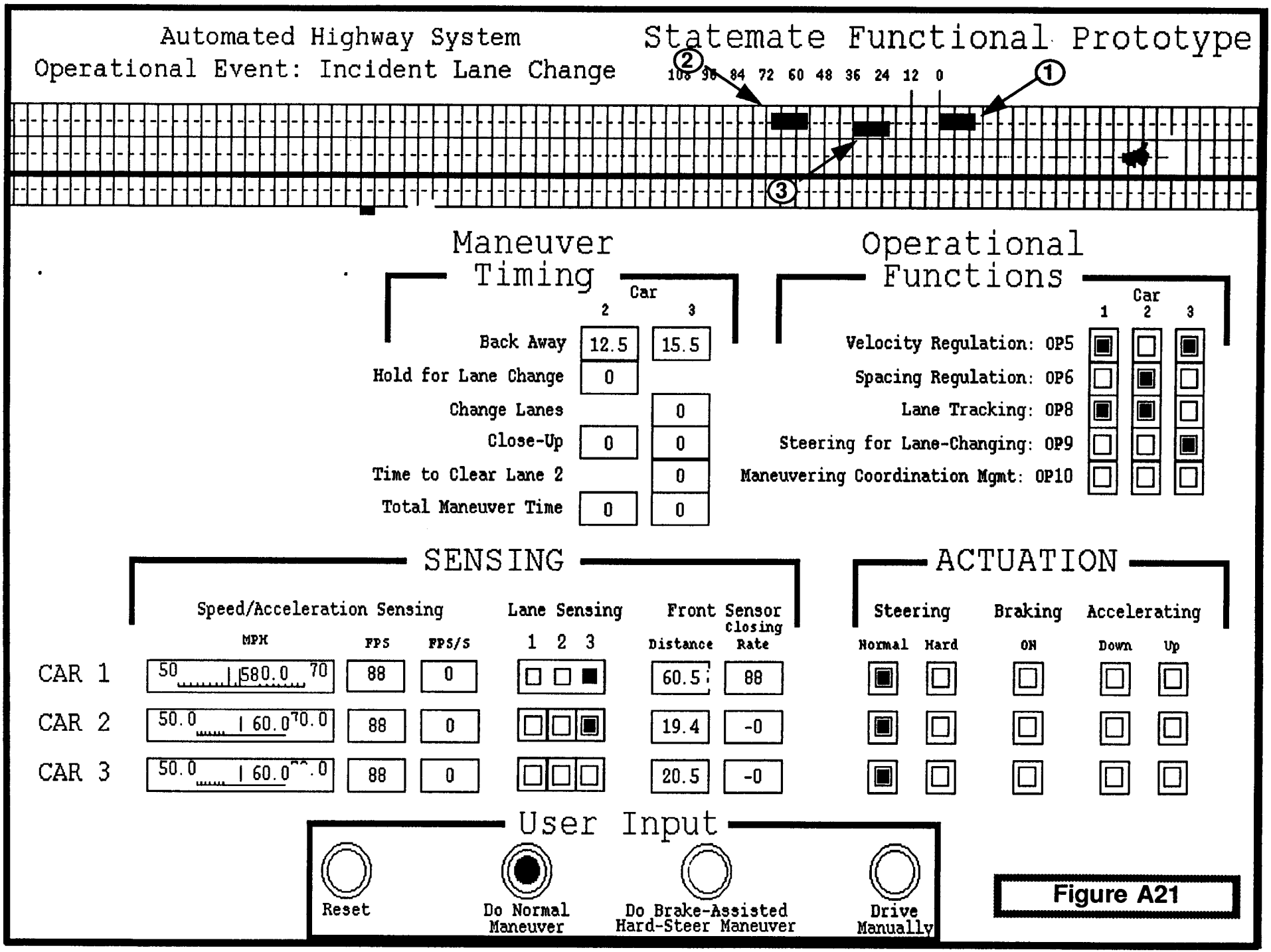

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2 3
Back Away 12.5 15.5
Hold for Lane Change 0
Change Lanes 0
Close-Up 0 0
Time to Clear Lane 2 0
Total Maneuver Time 0 0
Operational Functions
Car
1 2 3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH FPS FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance Closing Rate
ACTUATION
Steering Braking Accelerating
Normal Hard ON Down Up
CAR 1 50 58.0 70 88 0 60.5 88
CAR 2 50.0 60.0 70.0 88 0 19.4 -0
CAR 3 50.0 60.0 88 0 20.5 -0
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A21

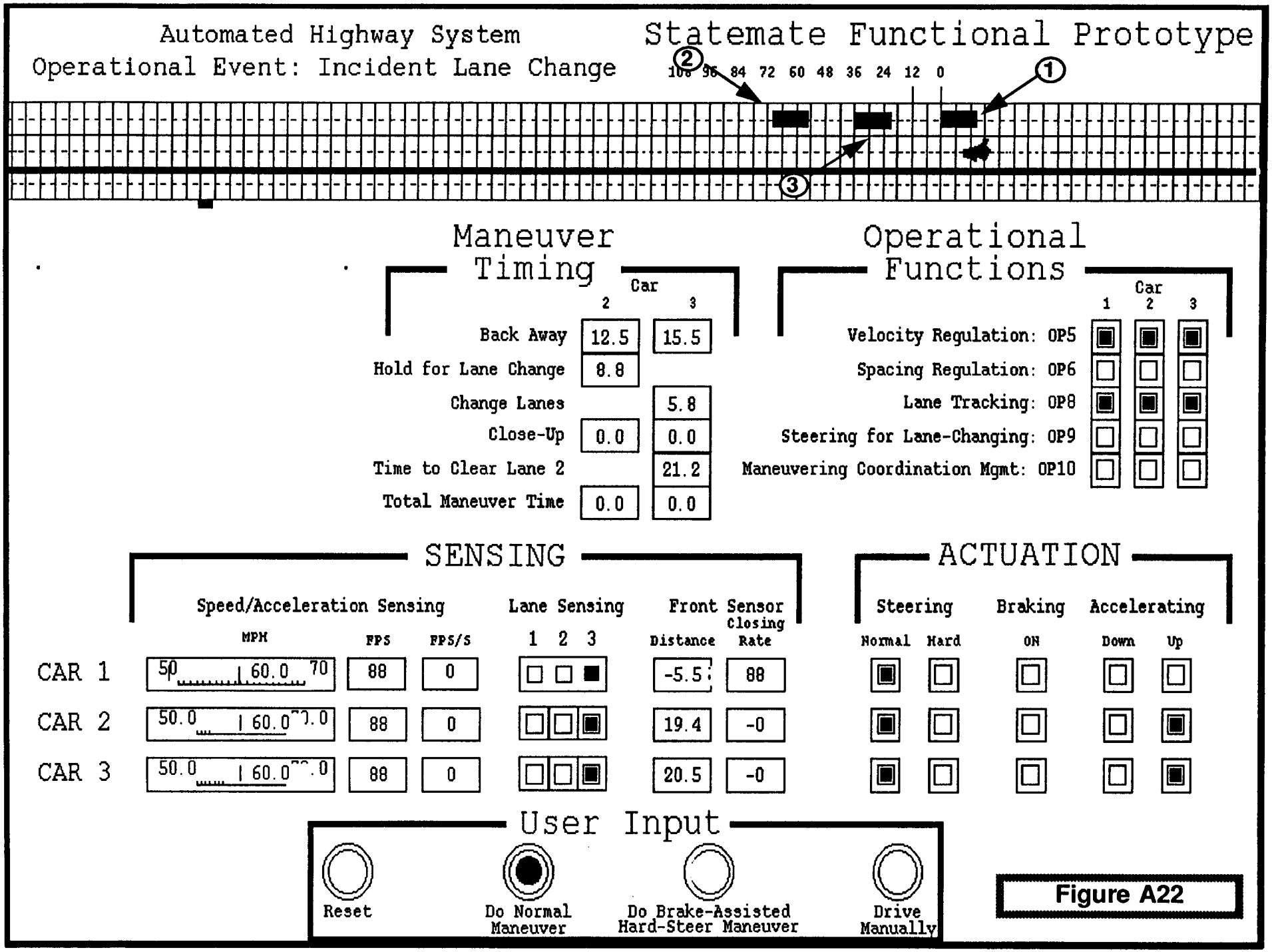

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2 3
Back Away 12.5 15.5
Hold for Lane Change 8.8
Change Lanes 5.8
Close-Up 0.0 0.0
Time to Clear Lane 2 21.2
Total Maneuver Time 0.0 0.0
Operational Functions
Car
1 2 3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
ACTUATION
Steering
Normal Hard
Braking
ON
Accelerating
Down Up
CAR 1 50 60.0 70 88 0 -5.5 88
CAR 2 50.0 60.0 70.0 88 0 19.4 -0
CAR 3 50.0 60.0 70.0 88 0 20.5 -0
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A22

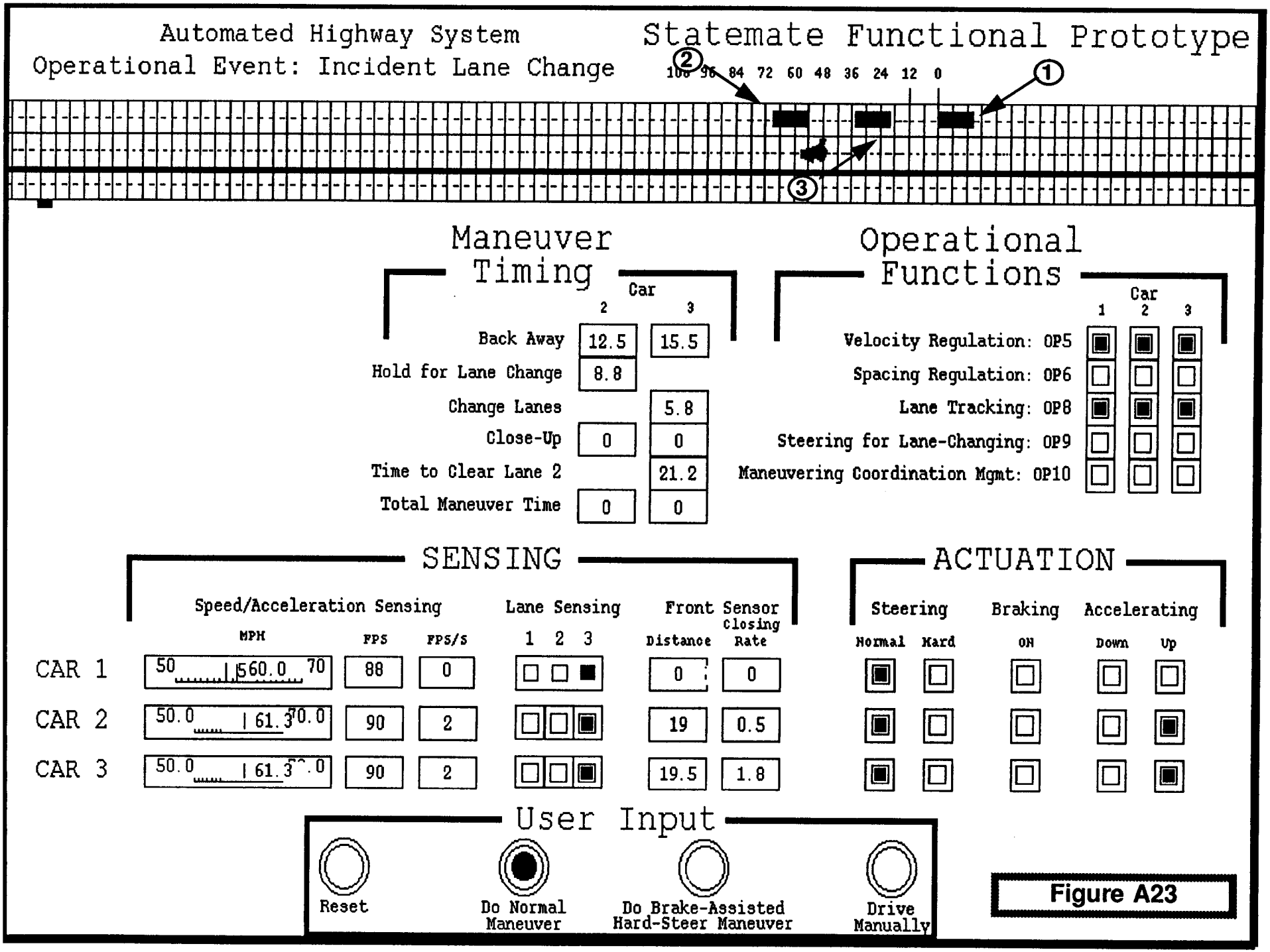

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
100 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
12.5
15.5
Hold for Lane Change
8.8
Change Lanes
5.8
Close-Up
0
0
Time to Clear Lane 2
21.2
Total Maneuver Time
0
0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50 60.0 70
88
0
0
0
CAR 2
50.0 61.3 70.0
90
2
19
0.5
CAR 3
50.0 61.3 70.0
90
2
19.5
1.8
ACTUATION
Steering
Normal
Hard
Braking
ON
Accelerating
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A23

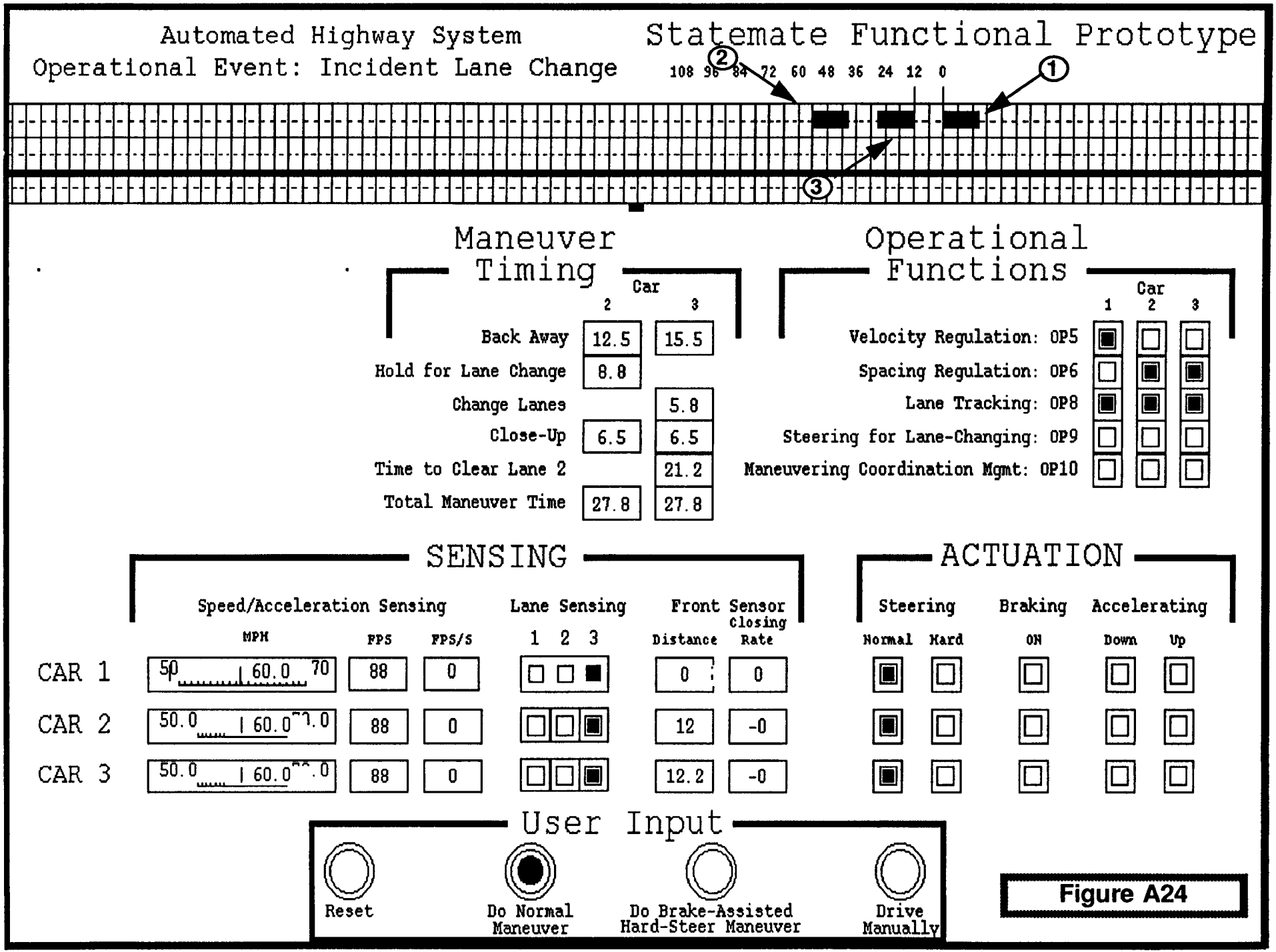

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
12.5
15.5
Hold for Lane Change
8.8
Change Lanes
5.8
Close-Up
6.5
6.5
Time to Clear Lane 2
21.2
Total Maneuver Time
27.8
27.8
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50
60.0
70
88
0
0
0
CAR 2
50.0
60.0
88
0
12
-0
CAR 3
50.0
60.0
88
0
12.2
-0
ACTUATION
Steering
Braking
Accelerating
Normal
Hard
ON
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A24

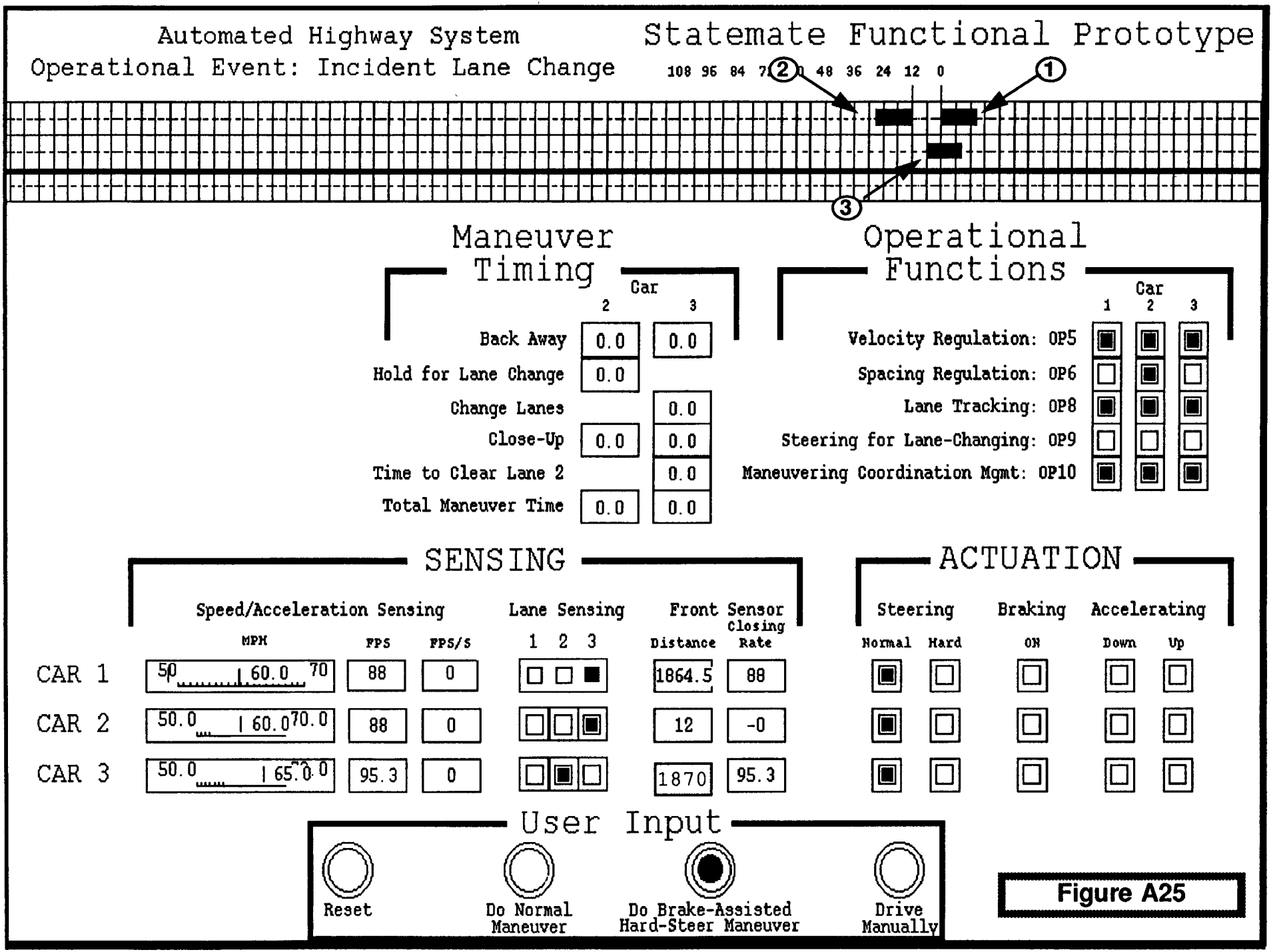

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
0.0
0.0
Hold for Lane Change
0.0
Change Lanes
0.0
Close-Up
0.0
0.0
Time to Clear Lane 2
0.0
Total Maneuver Time
0.0
0.0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50 60.0 70
88
0
1864.5
88
CAR 2
50.0 60.0 70.0
88
0
12
-0
CAR 3
50.0 65.0
95.3
0
1870
95.3
ACTUATION
Steering
Normal
Hard
Braking
ON
Accelerating
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A25

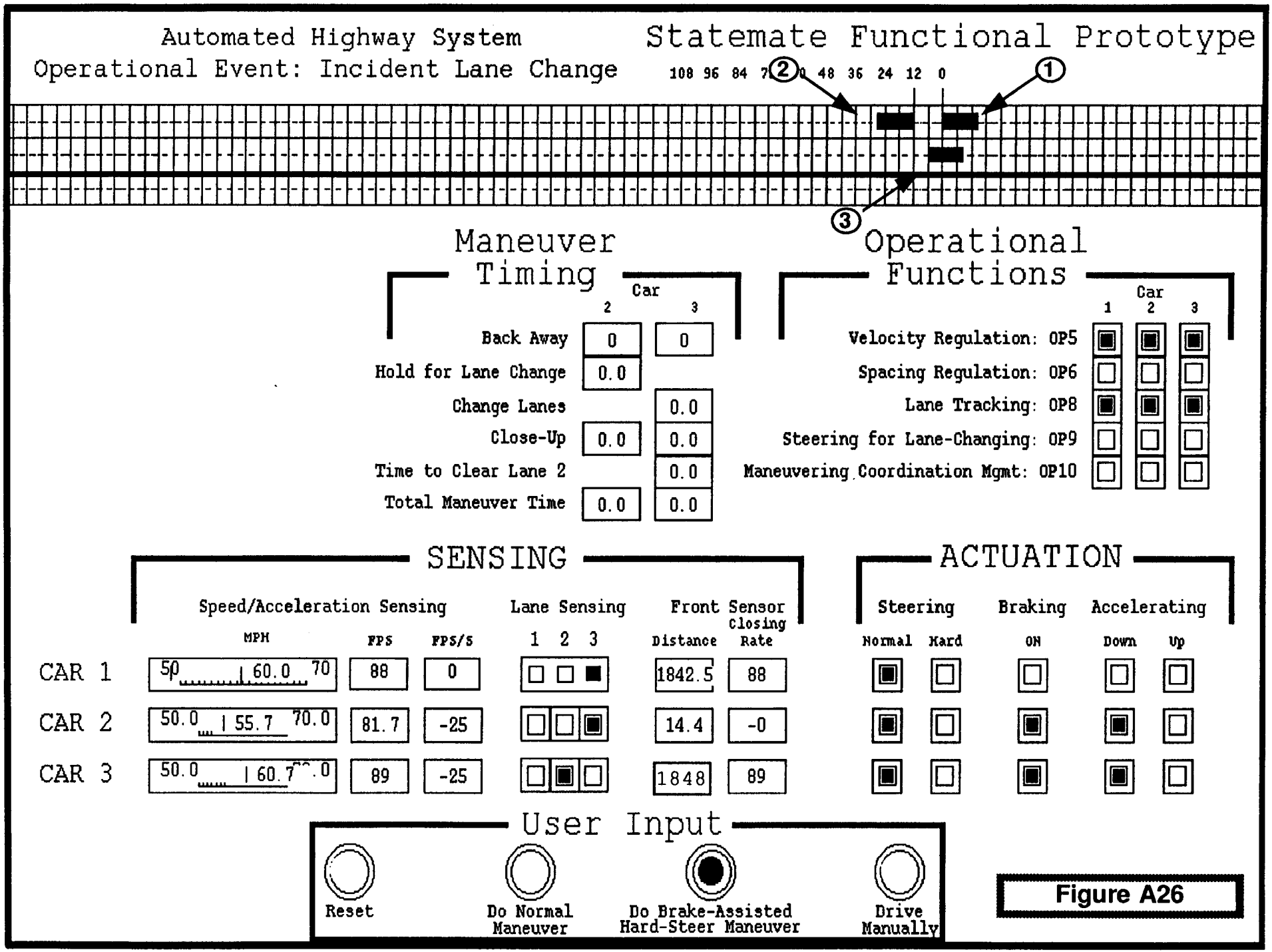
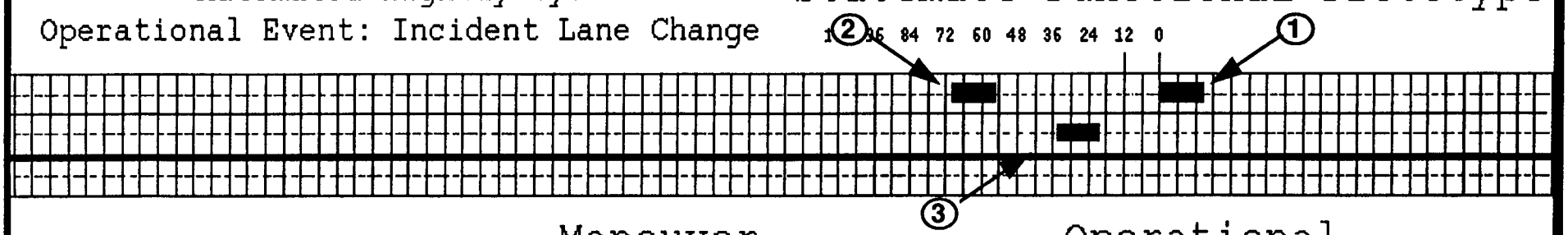

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
0
0
Hold for Lane Change
0.0
Change Lanes
0.0
Close-Up
0.0
0.0
Time to Clear Lane 2
0.0
Total Maneuver Time
0.0
0.0
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
Lane Sensing
Front Sensor
MPH
FPS
FPS/S
1 2 3
Distance
Closing Rate
CAR 1
50 60.0 70
88
0
1842.5
88
CAR 2
50.0 55.7 70.0
81.7
-25
14.4
-0
CAR 3
50.0 60.7
89
-25
1848
89
ACTUATION
Steering
Braking
Accelerating
Normal
Hard
ON
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A26

Automated Highway System
Operational Event: Incident Lane Change

Statemate Functional Prototype



Maneuver Timing

	Car 2	Car 3
Back Away	6.8	6.5
Hold for Lane Change	0.0	
Change Lanes		0.0
Close-Up	0.0	0.0
Time to Clear Lane 2		0.0
Total Maneuver Time	0.0	0.0

Operational Functions

	Car 1	Car 2	Car 3
Velocity Regulation: OP5	■	□	■
Spacing Regulation: OP6	□	■	□
Lane Tracking: OP8	■	■	□
Steering for Lane-Changing: OP9	□	□	■
Maneuvering Coordination Mgmt: OP10	□	□	□

SENSING

	Speed/Acceleration Sensing MPH	FPS	FPS/S	Lane Sensing 1 2 3	Front Sensor Distance	Front Sensor Closing Rate
CAR 1	50 | 60.0 70	88	0	□ □ ■	1270.5	88
CAR 2	50.0 | 59.9 70.0	87.9	2	□ □ ■	54.9	0.15
CAR 3	50.0 | 60.0 ^^.0	88	0.27	□ □ □	1300	88

ACTUATION

	Steering Normal	Steering Hard	Braking ON	Accelerating Down	Accelerating Up
CAR 1	■	□	□	□	□
CAR 2	■	□	□	□	■
CAR 3	□	■	□	□	□

User Input

○ Reset
○ Do Normal Maneuver
● Do Brake-Assisted Hard-Steer Maneuver
○ Drive Manually

Figure A27

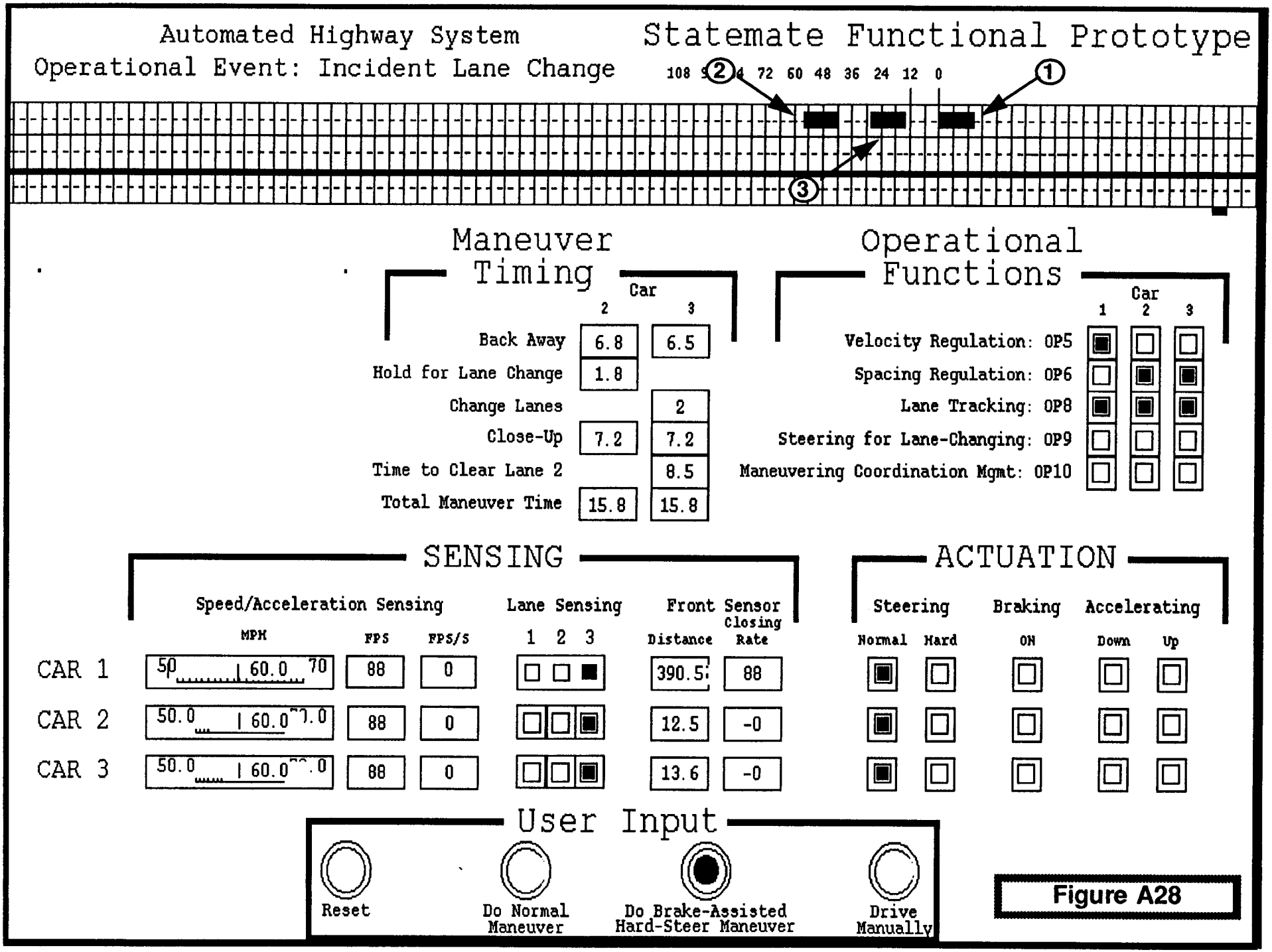

Automated Highway System
Operational Event: Incident Lane Change
Statemate Functional Prototype
108 96 84 72 60 48 36 24 12 0
1
2
3
Maneuver Timing
Car
2
3
Back Away
6.8
6.5
Hold for Lane Change
1.8
Change Lanes
2
Close-Up
7.2
7.2
Time to Clear Lane 2
8.5
Total Maneuver Time
15.8
15.8
Operational Functions
Car
1
2
3
Velocity Regulation: OP5
Spacing Regulation: OP6
Lane Tracking: OP8
Steering for Lane-Changing: OP9
Maneuvering Coordination Mgmt: OP10
SENSING
Speed/Acceleration Sensing
MPH
FPS
FPS/S
Lane Sensing
1 2 3
Front Sensor
Distance
Closing Rate
CAR 1
50 60.0 70
88
0
390.5
88
CAR 2
50.0 60.0
88
0
12.5
-0
CAR 3
50.0 60.0
88
0
13.6
-0
ACTUATION
Steering
Normal
Hard
Braking
ON
Accelerating
Down
Up
User Input
Reset
Do Normal Maneuver
Do Brake-Assisted Hard-Steer Maneuver
Drive Manually

Figure A28

APPENDIX B - SEVERITY LEVEL ASSESSMENT TABLES

B.1 STRUCTURE AND PURPOSE

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. On the basis of which elemental function and thus which major subsystem might have failed, an evaluation of the impact of the malfunction using the MOEs is performed. This appendix documents that assessment of severity levels in tabular form. Review to the technical discussion of task 4 - Assessment of Severity Levels in the main body of this report.

B.2 KEY RESULTS/CONCLUSIONS/ISSUES

Table B1a. Vehicle Check-In Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Infrastructure Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Vehicle ID assignment	No	Control center information processor	Low	Low	Control center information processor	Low	Low
Off-vehicle inspection and monitoring	Likely	Roadway sensors & instrumentation Control center information processor	Med	Med	N/A	N/A	N/A
Issuing permission/ rejection	Likely	Control center information processor	Med	Med	Vehicle information Processor	Med	Med
Vehicle condition monitoring and failure detection/ diagnosis	Likely	Vehicle internal sensor Vehicle information processor	Low	Low	Vehicle internal sensor Vehicle information processor	Med	Med
Human-machine interface	Likely	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Information link between the network layer and the link layer	Unlikely	Control center communication	Low	Low	Control center communication	Low	Low
Information exchange between the link layer and the coordination layer	Possible	Control center communication	Low	Low	Control center communication Vehicle external communication	Low	Low
Receive information	Unlikely	Driver display	Low	Low	Driver display	Low	Low
Provide information	Possible	Driver input	Low	Low	Driver input	Low	Low

Table B1b. Vehicle Check-In Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Infrastructure Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Vehicle ID assignment	Likely	Control center information processor	Med	Med	Control center information processor	Low	Low
Off-vehicle inspection and monitoring	Possible	Roadway sensors & instrumentation Control center information processor	Med	Med	N/A	N/A	N/A
Issuing permission/ rejection	Likely	Control center information processor	Med	Med	Vehicle information Processor	Med	Med
Vehicle condition monitoring and failure detection/ diagnosis	Likely	Vehicle internal sensor Vehicle information processor	Low	Low	Vehicle internal sensor Vehicle information processor	Med	Med
Human-machine interface	Likely	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Information link between the network layer and the link layer	Possible	Control center communication	Med	Med	Control center communication	Low	Low
Information exchange between the link layer and the coordination layer	Likely	Control center communication	Med	Med	Control center communication Vehicle external communication	Low	Low
Receive information	Unlikely	Driver display	Low	Low	Driver display	Low	Low
Provide information	Likely	Driver input	Low	Low	Driver input	Low	Low

Table B2a. Entering The System Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Infrastructure Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Normal maneuver coordination planning	Likely	Control center information processor	Med	Med	Vehicle information processor	Med	Med
Human-machine interface	Likely	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Information link between the coordination layer and the regulation layer	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Low	Low	Vehicle internal communication	Low	Low
Manually maneuver vehicle	Likely	Driver input	High	High	Driver input	High	High
Receive information	Possible	Driver display	Low	Low	Driver display	Low	Low

Table B2b. Entering The System Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Infrastructure Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Normal maneuver coordination planning	Likely	Control center information processor	Med	Med	Vehicle information processor	Med	Med
Human-machine interface	Likely	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Information link between coordination and regulation layers	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Low	Low	Vehicle internal communication	Low	Low
Manually maneuver vehicle	Possible	Driver input	Med	Med	Driver input	Med	Med
Receive information	Possible	Driver display	Low	Low	Driver display	Low	Low

Table B3a. Transition From Human to Automatic Control Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Infrastructure Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Normal maneuver coordination planning	Likely	Control center information processor	High	High	Vehicle information processor	High	High
Human-machine interface	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Information link between the coordination layer and the regulation layer	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Low	Low	Vehicle internal communication	Low	Low
Manually maneuver vehicle	Likely	Driver input	High	High	Driver input	High	High
Receive information	Possible	Driver display	Low	Low	Driver display	Low	Low

Table B3b. Transition From Human to Automatic Control Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Infrastructure Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Normal maneuver coordination planning	Likely	Control center information processor	High	High	Vehicle information processor	Med	Med
Human-machine interface	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Information link between the coordination layer and the regulation layer	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Low	Low	Vehicle internal communication	Low	Low
Manually maneuver vehicle	Possible	Driver input	High	High	Driver input	High	High
Receive information	Possible	Driver display	Low	Low	Driver display	Low	Low

Table B4a. Route Selection Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Monitoring traffic conditions and predicting congestion	Unlikely	Control center information processor	Low	Low	Control center information processor	Low	Low
Route recommendation	Unlikely	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Regional traffic conditions monitoring and incident management	Possible	Roadway sensor & instrumentation Control center information processor	Med	Med	Vehicle external sensor Vehicle information processor	Med	Med
Monitoring road surface conditions and weather	Possible	Roadway sensor & instrumentation Control center information processor	Low	Low	Vehicle external sensor Vehicle information processor	Low	Low
Trip progress monitoring	Unlikely	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Human-machine interface	Possible	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Information link between the network layer and the link layer	Unlikely	Control center communication	Low	Low	Control center communication	Low	Low
Information link between the link layer and the coordination layer	Likely	Control center communication	Low	Low	Control center communication Vehicle external communication	Low	Low
Information link between the coordination layer and the regulation layer	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Receive information	Possible	Driver display	Low	Low	Driver display	Low	Low
Provide information	Possible	Driver input	Low	Low	Driver input	Low	Low

Table B4b. Route Selection Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Monitoring traffic conditions and predicting congestion	Possible	Control center information processor	Med	Med	Control center information processor	Med	Med
Route recommendation	Likely	Control center information processor	Med	Med	Vehicle information processor	Low	Low
Regional traffic conditions monitoring and incident management	Likely	Roadway sensor & instrumentation Control center information processor	Med	Med	Vehicle external sensor Vehicle information processor	Low	Low
Monitoring road surface conditions and weather	Possible	Roadway sensor & instrumentation Control center information processor	Low	Low	Vehicle external sensor Vehicle information processor	Low	Low
Trip progress monitoring	Unlikely	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Human-machine interface	Possible	Vehicle information processor	Low	Low	Vehicle information processor	Low	Low
Information link between the network layer and the link layer	Possible	Control center communication	Med	Med	Control center communication	High	High
Information link between the link layer and the coordination layer	Likely	Control center communication	Low	Low	Control center communication Vehicle external communication	Low	Low
Information link between the coordination layer and the regulation layer	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Receive information	Possible	Driver display	Low	Low	Driver display	Low	Low
Provide information	Likely	Driver input	Low	Low	Driver input	Low	Low

Table B5a. Velocity Regulation Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Target speed	Possible	Control center information processor	Med	Med	Vehicle information processor	Med	Med
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Speed regulation command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Braking command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Sensing	Likely	Vehicle internal sensor Vehicle external sensor Vehicle information processor Roadway sensors & instrumentation	Med	Med	Vehicle internal sensor Vehicle external sensors	Med	Low
Actuation	Likely	Vehicle internal actuator	High	High	Vehicle internal actuator	High	High
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	High	High	Vehicle internal communication	High	High

Table B5b. Velocity Regulation Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Target speed	Likely	Control center information processor	Med	Med	Vehicle information processor	Med	Med
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Speed regulation command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Braking command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Sensing	Likely	Vehicle internal sensor Vehicle external sensor Vehicle information processor Roadway sensors & instrumentation	Med	Med	Vehicle internal sensor Vehicle external sensors	Med	Med
Actuation	Likely	Vehicle internal actuator	Med	Med	Vehicle internal actuator	Med	Med
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Med	Med	Vehicle internal communication	Med	Med

Table B6a. Spacing Regulation Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Minimal separations	Possible	Control center information processor	Low	Med	Vehicle information processor	Low	Med
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Speed regulation command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Braking command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensors & instrumentation	High	High	Vehicle internal sensor Vehicle external sensors	High	High
Actuation	Likely	Vehicle internal actuator	High	High	Vehicle internal actuator	High	High
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	High	High	Vehicle internal communication	High	High

Table B6b. Spacing Regulation Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Minimal separations	Likely	Control center information processor	High	High	Vehicle information processor	Med	Med
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Speed regulation command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Braking command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensors & instrumentation	Med	Med	Vehicle internal sensor Vehicle external sensors	Med	Med
Actuation	Likely	Vehicle internal actuator	Med	Med	Vehicle internal actuator	Med	Med
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Med	Med	Vehicle internal communication	Med	Med

Table B7a. Longitudinal Position Regulation Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Speed regulation command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Braking command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensors & instrumentation	High	High	Vehicle internal sensor Vehicle external sensors	High	High
Actuation	Likely	Vehicle internal actuator	High	High	Vehicle internal actuator	High	High
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	High	High	Vehicle internal communication	High	High

Table B7b. Longitudinal Position Regulation Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Speed regulation command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Braking command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensors & instrumentation	Med	Med	Vehicle internal sensor Vehicle external sensors	Med	Med
Actuation	Likely	Vehicle internal actuator	Med	Med	Vehicle internal actuator	Med	Med
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Med	Med	Vehicle internal communication	Med	Med

Table B8a. Lane Tracking Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Lane Assignment	Unlikely	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Steering control command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensor & instrumentation	High	High	Vehicle internal sensor Vehicle external sensors	High	High
Actuation	Likely	Vehicle internal actuator	High	High	Vehicle internal actuator	High	High
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	High	High	Vehicle internal communication	High	High

Table B8b. Lane Tracking Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Lane Assignment	Possible	Control center information processor	Med	Med	Vehicle information processor	Med	Med
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Steering control command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensor & instrumentation	Med	Med	Vehicle internal sensor Vehicle external sensors	Med	Med
Actuation	Likely	Vehicle internal actuator	Med	Med	Vehicle internal actuator	Med	Med
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Med	Med	Vehicle internal communication	Med	Med

Table B9a. Steering for Lane-Changing Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Lane assignment	Possible	Control center information processor	Med	High	Vehicle information processor	Med	Med
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Steering control command	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensor & instrumentation	High	High	Vehicle internal sensor Vehicle external sensors	High	High
Actuation	Likely	Vehicle internal actuator	High	High	Vehicle internal actuator	High	High
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	High	High	Vehicle internal communication	High	High

Table B9b. Steering for Lane-Changing Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Lane assignment	Possible	Control center information processor	High	High	Vehicle information processor	Med	Med
Supervising the sequence of the coordinated maneuvers	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Steering control command	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Sensing	Likely	Vehicle internal sensor Vehicle external sensors Vehicle information processor Roadway sensor & instrumentation	Med	Med	Vehicle internal sensor Vehicle external sensors	Med	Med
Actuation	Likely	Vehicle internal actuator	Med	Med	Vehicle internal actuator	Med	Med
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Med	Med	Vehicle internal communication	Med	Med

Table B10a. Maneuvering Coordination Management Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Monitoring traffic conditions and predicting congestion	Unlikely	Roadway sensors & instrumentation Control center information processor	Low	Low	Vehicle information processor	Low	Low
Route recommendation	Unlikely	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Lane assignment	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Maximum group size	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Prioritizing vehicle operations	Likely	Control center information processor	Med	Med	Vehicle information processor	Low	Low
Regional traffic conditions monitoring and incident management	Possible	Road sensors & instrumentation Control center information processor	Low	Low	Vehicle external sensor Vehicle information processor	Low	Low
Normal maneuver coordination planning	Likely	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Maneuvering coordination planning for hazardous conditions	Likely	Control center information processor	High	High	Vehicle information processor	High	Med
Information link between the network layer and the link layer	Unlikely	Control center communication	Low	Low	Control center communication	Low	Low
Information exchange between the link and coordination layers	Possible	Control center communication	Med	Med	Vehicle external communication Control center communication	Med	Med
Information link between the coordination layer and the regulation layer	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Low	Low	Vehicle internal communication	Low	Low
Provide information	Possible	Driver input	Low	Low	Driver input	Low	Low

Table B10b. Maneuvering Coordination Management Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Monitoring traffic conditions and predicting congestion	Possible	Roadway sensors & instrumentation Control center information processor	Med	Med	Vehicle information processor	Med	Med
Route recommendation	Unlikely	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Lane assignment	Possible	Control center information processor	Med	Med	Vehicle information processor	Low	Low
Maximum group size	Possible	Control center information processor	Low	Low	Vehicle information processor	Low	Low
Prioritizing vehicle operations	Likely	Control center information processor	Med	Med	Vehicle information processor	Low	Low
Regional traffic conditions monitoring and incident management	Likely	Road sensors & instrumentation Control center information processor	High	High	Vehicle external sensor Vehicle information processor	Med	Med
Normal maneuver coordination planning	Likely	Control center information processor	Med	Med	Vehicle information processor	Med	Med
Maneuvering coordination planning for hazardous conditions	Likely	Control center information processor	High	High	Vehicle information processor	Med	Med
Information link between the network layer and the link layer	Possible	Control center communication	Low	Low	Control center communication	Low	Low
Information exchange between the link layer and the coordination layer	Likely	Control center communication	Med	Med	Vehicle external communication Control center communication	Med	Med
Information link between the coordination layer and the regulation layer	Likely	Control center communication Vehicle external communication	Low	Low	Vehicle internal communication	Low	Low
Information link between the regulation layer and the physical layer	Likely	Vehicle internal communication	Low	Low	Vehicle internal communication	Low	Low
Provide information	Likely	Driver input	Low	Low	Driver input	Low	Low

Table B11a. Exit to a Transition Lane Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Route recommendation	Unlikely	Control center information processor	Low	N/A	Vehicle information processor	Low	N/A
Lane assignment	Possible	Control center information processor	Med	N/A	Vehicle information processor	Low	N/A
Normal maneuver coordination planning	Likely	Control center information processor	Med	N/A	Vehicle information processor	Med	N/A
Information link between the network layer and the link layer	Likely	Control center communication	Med	N/A	Control center communication	Med	N/A
Information exchange between the link layer and the coordination layer	Possible	Control center communication	Med	N/A	Vehicle external communication Control center communication	Med	N/A

Table B11b. Exit to a Transition Lane Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Route recommendation	Likely	Control center information processor	Med	N/A	Vehicle information processor	Med	N/A
Lane assignment	Possible	Control center information processor	Med	N/A	Vehicle information processor	Med	N/A
Normal maneuver coordination planning	Likely	Control center information processor	Med	N/A	Vehicle information processor	Med	N/A
Information link between the network layer and the link layer	Likely	Control center communication	Med	N/A	Control center communication	Med	N/A
Information exchange between the link layer and the coordination layer	Likely	Control center communication	Med	N/A	Vehicle external communication Control center communication	Med	N/A

Table B12a. Normal Transition from Automatic to Manual Control Malfunction Safety Severity Level.

Elemental Function	Safety Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Normal maneuver coordination planning	Likely	Control center information processor	Med	High	Vehicle information processor	Med	High
Human-machine interface	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Information link between the coordination layer and the regulation layer	Likely	Control center communication	Med	High	Control center communication Vehicle external communication	Med	High
Information link between the regulation layer and the physical layer	Likely	Vehicle information processor	Med	High	Vehicle information processor	Med	High
Manually maneuver vehicle	Likely	Driver input	High	High	Driver input	High	High
Provide information	Possible	Driver input	Med	High	Driver input	Med	High

Table B12b. Normal Transition from Automatic to Manual Control Malfunction Efficiency Severity Level.

Elemental Function	Efficiency Effect	Severity Level for Roadway Weighted RSCs			Severity Level for Vehicle Weighted RSCs		
		Primary Subsystem	BT	UE	Primary Subsystem	BT	UE
Normal maneuver coordination planning	Likely	Control center information processor	Med	Med	Vehicle information processor	Low	Low
Human-machine interface	Likely	Vehicle information processor	High	High	Vehicle information processor	High	High
Information link between the coordination and regulation layers	Likely	Control center communication	Med	Med	Control center communication Vehicle external communication	Med	Med
Information link between the regulation layer and the physical layer	Likely	Vehicle information processor	Med	Med	Vehicle information processor	Med	Med
Manually maneuver vehicle	Possible	Driver input	Low	Low	Driver input	Low	Low
Provide information	Likely	Driver input	Med	Med	Driver input	Med	Med

APPENDIX C - MALFUNCTION GROUPINGS

C.1 STRUCTURE AND PURPOSE

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.

C.2 KEY RESULTS/CONCLUSIONS/ISSUES

As a first step towards developing malfunction management strategies, categories of malfunctions by groupings with respect to RSCs are examined. Groupings by operational functions provide insight to differences between the RSCs in terms of expected malfunctions. Another grouping by elemental functions provides insight to differences of probable subsystem malfunctions in terms of RSCs. This appendix documents those groupings. Review to the technical discussion on task 5 - Malfunction Management Strategies is in the main body of this report

Table C1. Operational Function Malfunction Safety Severity Levels

		RSC			
Operational Functions	**Elemental Functions**	**IW BT**	**IW UE**	**VW BT**	**VW UE**
Vehicle check-in	Vehicle ID assignment	Low	Low	Low	Low
Vehicle check-in	Off-vehicle inspection and monitoring	Med	Med	N/A	N/A
Vehicle check-in	Issuing permission/ rejection	Med	Med	Med	Med
Vehicle check-in	Vehicle condition monitoring and failure detection/ diagnosis	Low	Low	Med	Med
Vehicle check-in	Human-machine interface	Low	Low	Low	Low
Vehicle check-in	Information link between the network layer and the link layer	Low	Low	Low	Low
Vehicle check-in	Information exchange between the link layer and the coordination layer	Low	Low	Low	Low
Vehicle check-in	Receive information	Low	Low	Low	Low
Vehicle check-in	Provide information	Low	Low	Low	Low
Entering the system	Normal maneuver coordination planning	Med	Med	Med	Med
Entering the system	Human-machine interface	Low	Low	Low	Low
Entering the system	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Entering the system	Information link between the regulation layer and the physical layer	Low	Low	Low	Low
Entering the system	Manually maneuver vehicle	High	High	High	High
Entering the system	Receive information	Low	Low	Low	Low
Transition from human to automatic control	Normal maneuver coordination planning	High	High	High	High
Transition from human to automatic control	Human-machine interface	Med	Med	Med	Med
Transition from human to automatic control	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Transition from human to automatic control	Information link between the regulation layer and the physical layer	Low	Low	Low	Low
Transition from human to automatic control	Manually maneuver vehicle	High	High	High	High
Transition from human to automatic control	Receive information	Low	Low	Low	Low
Route selection	Monitoring traffic conditions and predicting congestion	Low	Low	Low	Low

Route selection	Route recommendation	Low	Low	Low	Low
Route selection	Regional traffic conditions monitoring and incident management	Med	Med	Med	Med
Route selection	Monitoring road surface conditions and weather	Low	Low	Low	Low
Route selection	Trip progress monitoring	Low	Low	Low	Low
Route selection	Human-machine interface	Low	Low	Low	Low
Route selection	Information link between the network layer and the link layer	Low	Low	Low	Low
Route selection	Information link between the link layer and the coordination layer	Low	Low	Low	Low
Route selection	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Route selection	Receive information	Low	Low	Low	Low
Route selection	Provide information	Low	Low	Low	Low
Velocity regulation	Target speed	Med	Med	Med	Med
Velocity regulation	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Velocity regulation	Speed regulation command	High	High	High	High
Velocity regulation	Braking command	High	High	High	High
Velocity regulation	Sensing	Med	Med	Med	Low
Velocity regulation	Actuation	High	High	High	High
Velocity regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Spacing regulation	Minimal separations	Low	Med	Low	Med
Spacing regulation	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Spacing regulation	Speed regulation command	High	High	High	High
Spacing regulation	Braking command	High	High	High	High
Spacing regulation	Sensing	High	High	High	High
Spacing regulation	Actuation	High	High	High	High
Spacing regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Longitudinal position regulation	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Longitudinal position regulation	Speed regulation command	High	High	High	High
Longitudinal position regulation	Braking command	High	High	High	High
Longitudinal position regulation	Sensing	High	High	High	High
Longitudinal position regulation	Actuation	High	High	High	High
Longitudinal position regulation	Information link between the regulation layer and the physical layer	High	High	High	High
Lane tracking	Lane assignment	Low	Low	Low	Low
Lane tracking	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Lane tracking	Steering control command	High	High	High	High
Lane tracking	Sensing	High	High	High	High
Lane tracking	Actuation	High	High	High	High
Lane tracking	Information link between the regulation layer and the physical layer	High	High	High	High
Steering for lane-changing	Lane assignment	Med	High	Med	Med
Steering for lane-changing	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Steering for lane-changing	Steering control command	High	High	High	High
Steering for lane-changing	Sensing	High	High	High	High
Steering for lane-changing	Actuation	High	High	High	High
Steering for lane-changing	Information link between the regulation and physical layers	High	High	High	High

Maneuvering coordination management	Monitoring traffic conditions and predicting congestion	Low	Low	Low	Low
Maneuvering coordination management	Route recommendation	Low	Low	Low	Low
Maneuvering coordination management	Lane assignment	Low	Low	Low	Low
Maneuvering coordination management	Maximum group size	Low	Low	Low	Low
Maneuvering coordination management	Prioritizing vehicle operations	Med	Med	Low	Low
Maneuvering coordination management	Regional traffic conditions monitoring and incident management	Low	Low	Low	Low
Maneuvering coordination management	Normal maneuver coordination planning	Low	Low	Low	Low
Maneuvering coordination management	Maneuvering coordination planning for hazardous conditions	High	High	High	Med
Maneuvering coordination management	Information link between the network layer and the linklayers	Low	Low	Low	Low
Maneuvering coordination management	Information exchange between the link layer and the coordination layer	Med	Med	Med	Med
Maneuvering coordination management	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Maneuvering coordination management	Information link between the regulation layer and the physical layer	Low	Low	Low	Low
Maneuvering coordination management	Provide information	Low	Low	Low	Low
Exit to a transition lane	Route recommendation	Low	N/A	Low	N/A
Exit to a transition lane	Lane assignment	Med	N/A	Low	N/A
Exit to a transition lane	Normal maneuver coordination planning	Med	N/A	Med	N/A
Exit to a transition lane	Information link between the network layer and the link layer	Med	N/A	Med	N/A
Exit to a transition lane	Information exchange between the link layer and the coordination layer	Med	N/A	Med	N/A
Normal transition from automatic to human control	Normal maneuver coordination planning	Med	High	Med	High
Normal transition from automatic to human control	Human-machine interface	High	High	High	High
Normal transition from automatic to human control	Information link between the coordination layer and the regulation layer	Med	High	Med	High
Normal transition from automatic to human control	Information link between the regulation layer and the physical layer	Med	High	Med	High
Normal transition from automatic to human control	Manually maneuver vehicle	High	High	High	High
Normal transition from automatic to human control	Provide information	Med	High	Med	High

Table C2. Operational Function Malfunction Efficiency Severity Levels

		RSC			
Operational Functions	**Elemental Functions**	**IW BT**	**IW UE**	**VW BT**	**VW UE**
Vehicle check-in	Vehicle ID assignment	Med	Med	Low	Low
Vehicle check-in	Off-vehicle inspection and monitoring	Med	Med	N/A	N/A
Vehicle check-in	Issuing permission/ rejection	Med	Med	Med	Med
Vehicle check-in	Vehicle condition monitoring and failure detection/ diagnosis	Low	Low	Med	Med
Vehicle check-in	Human-machine interface	Low	Low	Low	Low
Vehicle check-in	Information link between the network layer and the link layer	Med	Med	Low	Low
Vehicle check-in	Information exchange between the link layer and the coordination layer	Med	Med	Low	Low
Vehicle check-in	Receive information	Low	Low	Low	Low
Vehicle check-in	Provide information	Low	Low	Low	Low
Entering the system	Normal maneuver coordination planning	Med	Med	Med	Med
Entering the system	Human-machine interface	Low	Low	Low	Low
Entering the system	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Entering the system	Information link between the regulation layer and the physical layer	Low	Low	Low	Low
Entering the system	Manually maneuver vehicle	Med	Med	Med	Med
Entering the system	Receive information	Low	Low	Low	Low
Transition from human to automatic control	Normal maneuver coordination planning	High	High	Med	Med
Transition from human to automatic control	Human-machine interface	Med	Med	Med	Med
Transition from human to automatic control	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Transition from human to automatic control	Information link between the regulation layer and the physical layer	Low	Low	Low	Low
Transition from human to automatic control	Manually maneuver vehicle	High	High	High	High
Transition from human to automatic control	Receive information	Low	Low	Low	Low
Route selection	Monitoring traffic conditions and predicting congestion	Med	Med	Med	Med
Route selection	Route recommendation	Med	Med	Low	Low
Route selection	Regional traffic conditions monitoring and incident management	Med	Med	Low	Low
Route selection	Monitoring road surface conditions and weather	Low	Low	Low	Low
Route selection	Trip progress monitoring	Low	Low	Low	Low
Route selection	Human-machine interface	Low	Low	Low	Low
Route selection	Information link between the network layer and the link layer	Med	Med	Low	Low
Route selection	Information link between the link layer and the coordination layer	Low	Low	Low	Low
Route selection	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Route selection	Receive information	Low	Low	Low	Low
Route selection	Provide information	Low	Low	Low	Low
Velocity regulation	Target speed	Med	Med	Med	Med
Velocity regulation	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Velocity regulation	Speed regulation command	Med	Med	Med	Med
Velocity regulation	Braking command	Med	Med	Med	Med
Velocity regulation	Sensing	Med	Med	Med	Med
Velocity regulation	Actuation	Med	Med	Med	Med

Velocity regulation	Information link between the regulation layer and the physical layer	Med	Med	Med	Med
Spacing regulation	Minimal separations	Med	Med	Med	Med
Spacing regulation	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Spacing regulation	Speed regulation command	Med	Med	Med	Med
Spacing regulation	Braking command	Med	Med	Med	Med
Spacing regulation	Sensing	Med	Med	Med	Med
Spacing regulation	Actuation	Med	Med	Med	Med
Spacing regulation	Information link between the regulation layer and the physical layer	Med	Med	Med	Med
Longitudinal position regulation	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Longitudinal position regulation	Speed regulation command	Med	Med	Med	Med
Longitudinal position regulation	Braking command	Med	Med	Med	Med
Longitudinal position regulation	Sensing	Med	Med	Med	Med
Longitudinal position regulation	Actuation	Med	Med	Med	Med
Longitudinal position regulation	Information link between the regulation layer and the physical layer	Med	Med	Med	Med
Lane tracking	Lane assignment	Med	Med	Med	Med
Lane tracking	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Lane tracking	Steering control command	Med	Med	Med	Med
Lane tracking	Sensing	Med	Med	Med	Med
Lane tracking	Actuation	Med	Med	Med	Med
Lane tracking	Information link between the regulation layer and the physical layer	Med	Med	Med	Med
Steering for lane-changing	Lane assignment	High	High	Med	Med
Steering for lane-changing	Supervising the sequence of the coordinated maneuvers	Low	Low	Low	Low
Steering for lane-changing	Steering control command	Med	Med	Med	Med
Steering for lane-changing	Sensing	Med	Med	Med	Med
Steering for lane-changing	Actuation	Med	Med	Med	Med
Steering for lane-changing	Information link between the regulation and physical layers	Med	Med	Med	Med
Maneuvering coordination management	Monitoring traffic conditions and predicting congestion	Med	Med	Med	Med
Maneuvering coordination management	Route recommendation	Low	Low	Low	Low
Maneuvering coordination management	Lane assignment	Med	Med	Low	Low
Maneuvering coordination management	Maximum group size	Low	Low	Low	Low
Maneuvering coordination management	Prioritizing vehicle operations	Med	Med	Low	Low
Maneuvering coordination management	Regional traffic conditions monitoring and incident management	High	High	Med	Med
Maneuvering coordination management	Normal maneuver coordination planning	Med	Med	Med	Med
Maneuvering coordination management	Maneuvering coordination planning for hazardous conditions	High	High	Med	Med
Maneuvering coordination management	Information link between the network layer and the linklayers	Low	Low	Low	Low
Maneuvering coordination management	Information exchange between the link layer and the coordination layer	Med	Med	Med	Med
Maneuvering coordination management	Information link between the coordination layer and the regulation layer	Low	Low	Low	Low
Maneuvering coordination management	Information link between the regulation layer and the physical layer	Low	Low	Low	Low
Maneuvering coordination management	Provide information	Low	Low	Low	Low
Exit to a transition lane	Route recommendation	Med	N/A	Med	N/A

Exit to a transition lane	Lane assignment	Med	N/A	Med	N/A
Exit to a transition lane	Normal maneuver coordination planning	Med	N/A	Med	N/A
Exit to a transition lane	Information link between the network layer and the link layer	Med	N/A	Med	N/A
Exit to a transition lane	Information exchange between the link layer and the coordination layer	Med	N/A	Med	N/A
Normal transition from automatic to human control	Normal maneuver coordination planning	Med	Med	Low	Low
Normal transition from automatic to human control	Human-machine interface	High	High	High	High
Normal transition from automatic to human control	Information link between the coordination layer and the regulation layer	Med	Med	Med	Med
Normal transition from automatic to human control	Information link between the regulation layer and the physical layer	Med	Med	Med	Med
Normal transition from automatic to human control	Manually maneuver vehicle	Low	Low	Low	Low
Normal transition from automatic to human control	Provide information	Med	Med	Med	Med

Table C3. Operational Function Malfunction Safety Severity Levels

Elemental Functions	Operational Functions	RSC			
		IW BT	IW UE	VW BT	VW UE
Actuation	Velocity regulation	High	High	High	High
Actuation	Spacing regulation	High	High	High	High
Actuation	Longitudinal position regulation	High	High	High	High
Actuation	Lane tracking	High	High	High	High
Actuation	Steering for lane-changing	High	High	High	High
Braking command	Velocity regulation	High	High	High	High
Braking command	Spacing regulation	High	High	High	High
Braking command	Longitudinal position regulation	High	High	High	High
Human-machine interface	Vehicle check-in	Low	Low	Low	Low
Human-machine interface	Entering the system	Low	Low	Low	Low
Human-machine interface	Transition from human to automatic control	Med	Med	Med	Med
Human-machine interface	Route selection	Low	Low	Low	Low
Human-machine interface	Normal transition from automatic to human control	High	High	High	High
Information exchange between the link layer and the coordination layer	Vehicle check-in	Low	Low	Low	Low
Information exchange between the link layer and the coordination layer	Route selection	Low	Low	Low	Low
Information exchange between the link layer and the coordination layer	Maneuvering coordination management	Med	Med	Med	Med
Information exchange between the link layer and the coordination layer	Exit to a transition lane	Med	N/A	Med	N/A
Information link between the coordination layer and the regulation layer	Entering the system	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Transition from human to automatic control	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Route selection	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Maneuvering coordination management	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Normal transition from automatic to human control	Med	High	Med	High
Information link between the network layer and the link layer	Vehicle check-in	Low	Low	Low	Low
Information link between the network layer and the link layer	Route selection	Low	Low	Low	Low
Information link between the network layer and the link layer	Maneuvering coordination management	Low	Low	Low	Low
Information link between the network layer and the link layer	Exit to a transition lane	Med	N/A	Med	N/A
Information link between the regulation layer and the physical layer	Entering the system	Low	Low	Low	Low
Information link between the regulation layer and the physical layer	Transition from human to automatic control	Low	Low	Low	Low
Information link between the regulation layer and the physical layer	Velocity regulation	High	High	High	High
Information link between the regulation layer and the physical layer	Spacing regulation	High	High	High	High
Information link between the regulation layer and the physical layer	Longitudinal position regulation	High	High	High	High
Information link between the regulation layer and the physical layer	Lane tracking	High	High	High	High

Information link between the regulation layer and the physical layer	Steering for lane-changing	High	High	High	High
Information link between the regulation layer and the physical layer	Maneuvering coordination management	Low	Low	Low	Low
Information link between the regulation layer and the physical layer	Normal transition from automatic to human control	Med	High	Med	High
Issuing permission/ rejection	Vehicle check-in	Med	Med	Med	Med
Lane assignment	Lane tracking	Low	Low	Low	Low
Lane assignment	Steering for lane-changing	Med	High	Med	Med
Lane assignment	Maneuvering coordination management	Low	Low	Low	Low
Lane assignment	Exit to a transition lane	Med	N/A	Low	N/A
Maneuvering coordination planning for hazardous conditions	Maneuvering coordination management	High	High	High	Med
Manually maneuver vehicle	Entering the system	High	High	High	High
Manually maneuver vehicle	Transition from human to automatic control	High	High	High	High
Manually maneuver vehicle	Normal transition from automatic to human control	High	High	High	High
Maximum group size	Maneuvering coordination management	Low	Low	Low	Low
Minimal separations	Spacing regulation	Low	Med	Low	Med
Monitoring road surface conditions and weather	Route selection	Low	Low	Low	Low
Monitoring traffic conditions and predicting congestion	Route selection	Low	Low	Low	Low
Monitoring traffic conditions and predicting congestion	Maneuvering coordination management	Low	Low	Low	Low
Normal maneuver coordination planning	Entering the system	Med	Med	Med	Med
Normal maneuver coordination planning	Transition from human to automatic control	High	High	High	High
Normal maneuver coordination planning	Maneuvering coordination management	Low	Low	Low	Low
Normal maneuver coordination planning	Exit to a transition lane	Med	N/A	Med	N/A
Normal maneuver coordination planning	Normal transition from automatic to human control	Med	High	Med	High
Off-vehicle inspection and monitoring	Vehicle check-in	Med	Med	N/A	N/A
Prioritizing vehicle operations	Maneuvering coordination management	Med	Med	Low	Low
Provide information	Vehicle check-in	Low	Low	Low	Low
Provide information	Route selection	Low	Low	Low	Low
Provide information	Maneuvering coordination management	Low	Low	Low	Low
Provide information	Normal transition from automatic to human control	Med	High	Med	High
Receive information	Vehicle check-in	Low	Low	Low	Low
Receive information	Entering the system	Low	Low	Low	Low
Receive information	Transition from human to automatic control	Low	Low	Low	Low
Receive information	Route selection	Low	Low	Low	Low
Regional traffic conditions monitoring and incident management	Route selection	Med	Med	Med	Med
Regional traffic conditions monitoring and incident management	Maneuvering coordination management	Low	Low	Low	Low
Route recommendation	Route selection	Low	Low	Low	Low
Route recommendation	Maneuvering coordination management	Low	Low	Low	Low
Route recommendation	Exit to a transition lane	Low	N/A	Low	N/A
Sensing	Velocity regulation	Med	Med	Med	Low
Sensing	Spacing regulation	High	High	High	High
Sensing	Longitudinal position regulation	High	High	High	High
Sensing	Lane tracking	High	High	High	High
Sensing	Steering for lane-changing	High	High	High	High
Speed regulation command	Velocity regulation	High	High	High	High
Speed regulation command	Spacing regulation	High	High	High	High

Speed regulation command	Longitudinal position regulation	High	High	High	High
Steering control command	Lane tracking	High	High	High	High
Steering control command	Steering for lane-changing	High	High	High	High
Supervising the sequence of the coordinated maneuvers	Velocity regulation	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Spacing regulation	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Longitudinal position regulation	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Lane tracking	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Steering for lane-changing	Low	Low	Low	Low
Target speed	Velocity regulation	Med	Med	Med	Med
Trip progress monitoring	Route selection	Low	Low	Low	Low
Vehicle condition monitoring and failure detection/ diagnosis	Vehicle check-in	Low	Low	Med	Med
Vehicle ID assignment	Vehicle check-in	Low	Low	Low	Low

Table C4. Elemental Function Malfunction Efficiency Severity Levels

		RSC			
Elemental Functions	**Operational Functions**	**IW BT**	**IW UE**	**VW BT**	**VW UE**
Actuation	Velocity regulation	Med	Med	Med	Med
Actuation	Spacing regulation	Med	Med	Med	Med
Actuation	Longitudinal position regulation	Med	Med	Med	Med
Actuation	Lane tracking	Med	Med	Med	Med
Actuation	Steering for lane-changing	Med	Med	Med	Med
Braking command	Velocity regulation	Med	Med	Med	Med
Braking command	Spacing regulation	Med	Med	Med	Med
Braking command	Longitudinal position regulation	Med	Med	Med	Med
Human-machine interface	Vehicle check-in	Low	Low	Low	Low
Human-machine interface	Entering the system	Low	Low	Low	Low
Human-machine interface	Transition from human to automatic control	Med	Med	Med	Med
Human-machine interface	Route selection	Low	Low	Low	Low
Human-machine interface	Normal transition from automatic to human control	High	High	High	High
Information exchange between the link layer and the coordination layer	Vehicle check-in	Med	Med	Low	Low
Information exchange between the link layer and the coordination layer	Maneuvering coordination management	Med	Med	Med	Med
Information exchange between the link layer and the coordination layer	Exit to a transition lane	Med	N/A	Med	N/A
Information link between the coordination layer and the regulation layer	Entering the system	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Transition from human to automatic control	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Route selection	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Maneuvering coordination management	Low	Low	Low	Low
Information link between the coordination layer and the regulation layer	Normal transition from automatic to human control	Med	Med	Med	Med
Information link between the link layer and the coordination layer	Route selection	Low	Low	Low	Low
Information link between the network layer and the link layer	Vehicle check-in	Med	Med	Low	Low
Information link between the network layer and the link layer	Route selection	Med	Med	Low	Low
Information link between the network layer and the link layer	Exit to a transition lane	Med	N/A	Med	N/A
Information link between the network layer and the linklayers	Maneuvering coordination management	Low	Low	Low	Low
Information link between the regulation and physical layers	Steering for lane-changing	Med	Med	Med	Med
Information link between the regulation layer and the physical layer	Entering the system	Low	Low	Low	Low
Information link between the regulation layer and the physical layer	Transition from human to automatic control	Low	Low	Low	Low
Information link between the regulation layer and the physical layer	Velocity regulation	Med	Med	Med	Med
Information link between the regulation layer and the physical layer	Spacing regulation	Med	Med	Med	Med
Information link between the regulation layer and the physical layer	Longitudinal position regulation	Med	Med	Med	Med

Information link between the regulation layer and the physical layer	Lane tracking	Med	Med	Med	Med
Information link between the regulation layer and the physical layer	Maneuvering coordination management	Low	Low	Low	Low
Information link between the regulation layer and the physical layer	Normal transition from automatic to human control	Med	Med	Med	Med
Issuing permission/ rejection	Vehicle check-in	Med	Med	Med	Med
Lane assignment	Lane tracking	Med	Med	Med	Med
Lane assignment	Steering for lane-changing	High	High	Med	Med
Lane assignment	Maneuvering coordination management	Med	Med	Low	Low
Lane assignment	Exit to a transition lane	Med	N/A	Med	N/A
Maneuvering coordination planning for hazardous conditions	Maneuvering coordination management	High	High	Med	Med
Manually maneuver vehicle	Entering the system	Med	Med	Med	Med
Manually maneuver vehicle	Transition from human to automatic control	High	High	High	High
Manually maneuver vehicle	Normal transition from automatic to human control	Low	Low	Low	Low
Maximum group size	Maneuvering coordination management	Low	Low	Low	Low
Minimal separations	Spacing regulation	Med	Med	Med	Med
Monitoring road surface conditions and weather	Route selection	Low	Low	Low	Low
Monitoring traffic conditions and predicting congestion	Route selection	Med	Med	Med	Med
Monitoring traffic conditions and predicting congestion	Maneuvering coordination management	Med	Med	Med	Med
Normal maneuver coordination planning	Entering the system	Med	Med	Med	Med
Normal maneuver coordination planning	Transition from human to automatic control	High	High	Med	Med
Normal maneuver coordination planning	Maneuvering coordination management	Med	Med	Med	Med
Normal maneuver coordination planning	Exit to a transition lane	Med	N/A	Med	N/A
Normal maneuver coordination planning	Normal transition from automatic to human control	Med	Med	Low	Low
Off-vehicle inspection and monitoring	Vehicle check-in	Med	Med	N/A	N/A
Prioritizing vehicle operations	Maneuvering coordination management	Med	Med	Low	Low
Provide information	Vehicle check-in	Low	Low	Low	Low
Provide information	Route selection	Low	Low	Low	Low
Provide information	Maneuvering coordination management	Low	Low	Low	Low
Provide information	Normal transition from automatic to human control	Med	Med	Med	Med
Receive information	Vehicle check-in	Low	Low	Low	Low
Receive information	Entering the system	Low	Low	Low	Low
Receive information	Transition from human to automatic control	Low	Low	Low	Low
Receive information	Route selection	Low	Low	Low	Low
Regional traffic conditions monitoring and incident management	Route selection	Med	Med	Low	Low
Regional traffic conditions monitoring and incident management	Maneuvering coordination management	High	High	Med	Med
Route recommendation	Route selection	Med	Med	Low	Low
Route recommendation	Maneuvering coordination management	Low	Low	Low	Low
Route recommendation	Exit to a transition lane	Med	N/A	Med	N/A
Sensing	Velocity regulation	Med	Med	Med	Med
Sensing	Spacing regulation	Med	Med	Med	Med
Sensing	Longitudinal position regulation	Med	Med	Med	Med
Sensing	Lane tracking	Med	Med	Med	Med
Sensing	Steering for lane-changing	Med	Med	Med	Med
Speed regulation command	Velocity regulation	Med	Med	Med	Med
Speed regulation command	Spacing regulation	Med	Med	Med	Med

Speed regulation command	Longitudinal position regulation	Med	Med	Med	Med
Steering control command	Lane tracking	Med	Med	Med	Med
Steering control command	Steering for lane-changing	Med	Med	Med	Med
Supervising the sequence of the coordinated maneuvers	Velocity regulation	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Spacing regulation	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Longitudinal position regulation	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Lane tracking	Low	Low	Low	Low
Supervising the sequence of the coordinated maneuvers	Steering for lane-changing	Low	Low	Low	Low
Target speed	Velocity regulation	Med	Med	Med	Med
Trip progress monitoring	Route selection	Low	Low	Low	Low
Vehicle condition monitoring and failure detection/ diagnosis	Vehicle check-in	Low	Low	Med	Med
Vehicle ID assignment	Vehicle check-in	Med	Med	Low	Low