Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Automated Check-Out

U.S. Department of Transportation
Federal Highway Administration
Publication No. FHWA-RD-95-139
November 1994

PRECURSOR SYSTEMS ANALYSES

OF

AUTOMATED HIGHWAY SYSTEMS

Activity Area C

Automated Check-Out

Results of Research

Conducted By

Delco Systems Operations

FOREWORD

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

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

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

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

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

NOTICE

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS Activity Area C Automated Check-Out		5. Report Date 6. Performing Organization Code
7. Author(s) F. Mangarelli*, A. Cochran*, D. Craig*; B. Michael**, M. Halseth, R. Schulze***		8. Performing Organization Report No.
9. Performing Organization Name and Address Delco Electronics Corporation Delco Systems Operations 6767 Hollister Avenue Goleta, CA 93117		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFH61-93-C-00194
12. Sponsoring Agency Name and Address IVHS Research Division Federal Highway Administration 6300 Georgetown Pike McLean, Virginia 22101-2296		13. Type of Report and Period Covered Final Report September 1993-November 1994 14. Sponsoring Agency Code

15. Supplementary Notes
Contracting Officer's Technical Representative (COTR) - J. Richard Bishop HSR 10
* Hughes Aircraft Company, San Diego, CA; ** PATH, Richmond, CA; *** Daniel, Mann, Johnson and Mendenhall, Phoenix, AZ

16. Abstract

This activity evaluates potential automatic-to-manual transition scenarios in terms of relative feasibility, safety, cost, and social implications. The check-out alternatives range from minimal testing of the operator and the vehicle to extensive testing of the operator and vehicle. The vehicle functions analysis presents a summary of functions that are critical to safe manual operation and proposes several options for validation. Two possible check-out processes are discussed, one intended for AHS lanes dedicated to automated traffic, and one intended for mixed mode lanes in which AHS and non-AHS vehicles are traveling. The transition to manual control will involve preparing the driver to resume manual operation prior to release of vehicle functions. Proposed tasks which could be used to determine that the driver is ready to receive control of the automated vehicle are examined.

17. Key Words	18. Distribution Statement
manual transition, operator check-out, vehicle check-out, driver validation, critical manual functions, driver alert, operator competence, depots, vehicle storage	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161

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

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

(PF V2.1, 6/30/92

TABLE OF CONTENTS

Section	Page
EXECUTIVE SUMMARY	1
INTRODUCTION	5
REPRESENTATIVE SYSTEM CONFIGURATIONS	7
TECHNICAL DISCUSSION	9
Task 1. Identify Vehicle Functions	9
Check-Out Scenario From Dedicated Lanes	10
Check-Out Scenario From Mixed Flow Lanes	11
Vehicle Function Description	11
Braking Functions	13
Engine Functions	13
Functions Associated With Tires And Wheels	14
Steering Functions	14
Vehicle Transmission And Differential	15
Fuel Quantity	15
Vehicle Longitudinal Position/Distance Sensor	16
Vehicle Lateral Position/Distance Sensor	16
Visibility Enhancement And Emergency Equipment	16
Communications Equipment	17
Task 2. Safe Vehicle Operation/Check-Out Alternatives	17
Depots	17
Task 3. Identify Operator Characteristics	19
Alerting The Driver To Resume Manual Control	20
Task 4. Operator/Driver Competence Determination	21
Driver Monitoring Systems	22
Notifying AHS Driver	22
Determine Driver Competency	23
Task 5. Evaluation Of The Acceptability Of Check-Out Alternatives	24
Operator And Vehicle Check-Out Alternatives	24
Storage Alternatives For Vehicles Which Fail Check-Out	27
Task 6. Define Check-Out Issues And Risks	29
Operator Issues And Risks	29

TABLE OF CONTENTS
(Continued)

Section	Page
Instrumentation Issues And Risks	30
Infrastructure Issues And Risks	31
Design Issues	32
Operation Issues	33
Location Issues	34
Task 7. Implications For System Configuration	34
Detailed Check-Out Protocol Logic	35
Analysis Of Check-Out Protocol For Dedicated Lanes	48
Vehicle System Decisions	48
Infrastructure Decisions	50
Driver Decisions	50
Exit Gate Attendant Decisions	51
Analysis Of Check-Out Protocol For Mixed Flow Lanes	51
Vehicle System Decisions	52
Infrastructure Decisions	54
Driver Decisions	54
Observations	56
Summary	58
CONCLUSIONS	59
BIBLIOGRAPHY	63

LIST OF FIGURES

Figure		Page
1.	Finite State Machine Representation Of Information Contained In Table 7	47
2.	Finite State Machine Representation Of Information Contained In Table 8	48

LIST OF TABLES

Table		Page
1.	Candidate Vehicle Functions For Check-Out	12
2.	Check-Out Options.	25
3.	Advantages And Disadvantages Of Check-Out Alternatives	28
4.	Summary Of Operator Issues And Risks	30
5.	Summary Of Instrumentation Issues And Risks	31
6.	Summary Of Infrastructure Issues And Risks	32
7.	Check-Out Protocol Summary For RSC's 1 and 2	36
8.	Check-Out Protocol Summary For RSC 3	41

EXECUTIVE SUMMARY

The goal of Activity C — Automated Check-Out is to evaluate potential automated-to-manual transition scenarios. The factors considered are relative feasibility, safety, cost, and social implications. The check-out alternatives range from minimal to extensive testing of the operator and the vehicle. Driver validation is often assumed to be the primary consideration during check-out; however, critical vehicle manual functions must also be validated.

The vehicle functions analysis summarizes functions that are critical to safe manual operation and proposes several options for validation. The range of testing can vary from a simple verification of continuous monitoring results to a set of dynamic tests performed by the driver as part of the check-out process. Two possible check-out processes are proposed, one for AHS lanes dedicated to automated traffic, and one for mixed-flow lanes in which AHS and non-AHS vehicles are traveling.

The proposed check-out scenario for dedicated AHS lanes assumes that the vehicle will exit the automated lanes via an offramp. Manual control of the brakes is released to the driver, and deceleration is measured against a known profile. Manual control of the throttle and the steering is released to the driver after the vehicle has come to a stop at the end of the ramp. In this scenario, the driver is responsible for control of the vehicle and management of failures when he resumes moving from the ramp. This protocol allows manual control to be resumed in isolation from the flow of automated vehicles, minimizing the risk of driver error in the transition.

The check-out scenario proposed for mixed-flow lanes assumes that the vehicle will convert to manual control in a transition lane that supports both automated and manual traffic. Vehicles exiting a mixed-flow AHS must perform check-out tests at highway speeds. This protocol suggests that the brakes remain under automatic control until all other functions have been released to reliable manual control. The vehicle is maneuvered into the transition lane while under automated control, and manual functions are transferred to the driver after the merger is completed. The check-out process releases the drive train, followed by steering, with manual braking released after functional verification of steering and throttle. The manual driving profile is monitored continually by AHS until manual steering, brake, and throttle control are verified. This protocol allows the automated system to resume control if necessary while in the automated lane. The primary disadvantage of allowing manually operated vehicles to drive in the same lane with vehicles under system control is the risk of incidents due to human error in AHS lanes.

The transition to manual control will involve preparing the driver to resume manual operation prior to release of vehicle functions. AHS may perform several tasks to determine that the driver is ready to receive control of the automated vehicle, including: 1) alert the driver that manual control of the vehicle is imminent, 2) receive acknowledgment that the driver is aware he will be taking control, 3)determine that the driver is competent to assume control of the vehicle and able to execute a safe exit from AHS, and 4) ensure that the transition from automatic to manual control minimizes driver workload and stress.

Three typical trip profiles are assumed in the analysis of driver dynamics in the automated to manual transition. The first scenario involves the home-to-work-to-home trip where the vehicle is under automatic control for a relatively short time, up to one hour. A second scenario lasting two to four hours may be typical of short out-of-town trips or day trips for business travelers. The third profile involves longer trips of over five hours. The expected interactions with the driver in each trip profile are considered, and the relative complexity of the driver transition in each scenario is addressed. The shorter trips may require little preparation of the driver to resume manual control, while the longer the automated trip, the more involved the transition process may become. A simple push-button task is recommended for trips less than one hour, while specific simulated driving tasks are proposed for longer periods of automated control.

Alternatives to operator competence validation also encompass a wide range of options. The first option is a simple check-out procedure that does not involve any testing of the driver's ability to resume control. The operator will be asked to respond to a request to assume control through an action such as pressing a button. This check-out option has the advantage of being simple, inexpensive, and reliable. The disadvantage is that it does not screen for impaired drivers.

The second option for operator testing at check-out is to require the driver to perform a few tests to verify that he or she is ready to take control. The driver's responses can be monitored by the vehicle systems, and control of the vehicle can be transferred when responses are within specified parameters. This check-out option has the advantage of providing driver tasks as part of the check-out process, combining competence verification with sufficient transition time to prepare the driver for manual driving. The disadvantage of this check-out option is that loose tolerances in driver responses may allow impaired drivers to pass the check-out tests, while tight tolerances may cause qualified drivers to be rejected.

The third option for operator check-out is to perform exhaustive tests to assure that all impaired and unqualified drivers are prevented from resuming manual control. Driver reaction time may

be verified through keypad entry of numeric sequences, for instance. Other tests, such as checking for slurred speech, retinal scanning, or testing sweat from the driver's palms can be used to check for alcohol or drug impairment. Monitoring of respiration rate, heart rate, and blood pressure is also possible. The benefit of exhaustive testing is that impaired or unqualified drivers will consistently be removed from the roadways. This option may decrease the risk of incidents due to human error in the transition lanes and arterials surrounding the AHS. The primary drawback to this approach is the added complexity and cost of implementation, which has minimal benefit to the safe operation of the automated lanes.

Another aspect of the check-out process is the potential need to divert vehicles that fail the vehicle and/or operator validation procedures. Several solutions are proposed and their relative merits debated. The first option requires parking areas, referred to as depots, to store vehicles temporarily. The acceptability of these depots depends upon their placement, cost, and the availability of services at the depot. One alternative to providing depots at exit points would be to move vehicles which are incapable of manual operation to a shoulder. This option assumes the availability of shoulders accessible to AHS lanes. Another alternative to depots is to provide storage for vehicles on the shoulder of the exit ramps from the automated lanes. Both of these storage alternatives place constraints on the use of rights-of-way compatible with AHS deployment. The issue of where to place vehicles which fail the check-out process is a key consideration in the design of the validation procedure.

The two check-out protocols suggested for dedicated and mixed-flow lanes are used to evaluate the implications of check-out alternatives to safe system design. The system design safety objective is to mitigate risk by identifying potential system hazards and addressing them through good engineering practices. The objective of this analysis is to identify some of the potential AHS hazards related to the check-out procedure. The scope of the analysis is restricted to hazards resulting from missed detections and false alarms, with respect to check-out decisions performed by the vehicle systems, infrastructure, driver, and exit function.

The assessment of tradeoffs between alternative AHS check-out protocols considers the following issues:

- Decision support: the partitioning of decision responsibilities between the vehicle system, infrastructure, and human. The check-out protocol must be consistent with the responsibilities assigned to each of these entities. The level of coordination required by a particular

check-in protocol with respect to a Representative System Configuration (RSC) is an important factor in determining the feasibility of implementation.

- Mission effectiveness: the ability of the check-out protocol to achieve the desired probability of fault detection. The system automation boundary must be drawn with regard to decision-making tasks performed as part of the check-out process. Responsibility for action in emergencies must be assigned to manual or automated processes.
- Safety: the tolerable rates of false alarms and missed detections. The effect of the check-out safety policies on such things as goodwill and liability must be considered.
- Cost: the appropriate balance between the cost of an AHS fault-detection mechanism and the corresponding rates of fault detections and false alarms. The costs associated with implementing and maintaining check-out protocols are other factors to consider.

INTRODUCTION

Check-out is the process through which a vehicle is granted permission to transition from the automated lanes of a highway onto manual lanes, an exit ramp, or other type of facility. The actual exit from the automated lanes, including any physical structures, ramps, vehicle storage areas, etc. are discussed in Activity J - AHS Entry/Exit Implementation The purpose of check-out is to determine whether the vehicle is capable of safe manual operation and that the operator is ready and able to assume control of the vehicle.

Analyses will be conducted of the vehicle and operator factors involved in the transition from AHS instrumented lanes. These analyses will focus on the variables involved in determining whether the vehicle can be manually operated and if the operator is physically capable of assuming manual control of the vehicle following transition from AHS control. The primary concern is the ability to ensure the safety of the driver and others on both the AHS and non-AHS roadways.

The check-out function for the vehicle is concerned with testing vehicle components that were disengaged during automated travel, such as steering linkages and the pedal operated braking system. Operator checks will include a readiness test to verify that the operator is prepared to take control of the vehicle and possibly tests to determine that the operator is not impaired due to drugs or alcohol. It is recommended that the Activity B - Automated Check-In report be read prior to reading this activity report since many of the check-out issues for the vehicle are discussed for check-in.

The check-out activity is organized into 7 tasks. The Identify Vehicle Functions task will address the vehicle functions which are required for manual control. This task will focus on the actions required to safely release automated control of certain vehicle functions. Vehicle systems tests and verification procedures that are required are identified and defined. The Safe Vehicle Operation/Check-Out Alternatives task examines the methodology for determining whether it is safe to operate the vehicle manually. Techniques which include self-tests and others which may require operator action are identified. The task also involves evaluating options available to vehicles that are determined unfit for manual operation. Transfer of the vehicle to a secure location and the implications of performing the transfer under AHS control are discussed. The mechanics of vehicle diversion will be addressed in Activity J - AHS Entry/Exit Implementation.

The Identify Operator Characteristics task examines the properties that qualify a driver to safely assume control of the vehicle. The properties which are important to ensure safe transition from automated to manual control will be listed. Each is discussed in terms of reasons that drivers may fail to meet the requirements for each of the characteristics. The Operator Competence Determination task examines methods which can be used to verify driver competence prior to transition to manual control. Typical methods for verifying various operator characteristics will be identified and discussed. Candidate actions for alerting drivers to driving situations so that vehicle control can safely be assumed are listed and described.

The Evaluation of the Acceptability of Check-Out Alternatives task consists of developing a list of potential options for handling vehicles and drivers which are determined incompetent for safe manual operation. A methodology for evaluating public opinion regarding acceptable checkout alternatives is presented.

The Define Issues and Risks task develops a set of design issues concerned with check-out alternatives. The risks associated with incorrectly identifying vehicles and drivers as competent or incompetent are determined.

The Discuss Implications for System Configurations task evaluates the implications of the automated checkout analyses with respect to each of the three Representative System Configurations (RSC's). Each RSC is considered in terms of cost, liability, and technological complexity. Designs which optimize safety and reduce the false alarm rate are identified.

REPRESENTATIVE SYSTEM CONFIGURATIONS

The representative system configurations (RSC's) were generated very early in this Precursor Systems Analyses of AHS program. These RSC's are used throughout the various areas of analysis whenever a diversity of system attributes is required by the analysis at hand. The RSC's identify specific alternatives for twenty AHS attributes within the context of three general RSC groups.

Since the RSC's have such general applicability to these precursor systems analyses, they are documented in the Contract Overview Report.

TECHNICAL DISCUSSION

Task 1. Identify Vehicle Functions

The check-out process includes validating the vehicle for safe exit from the AHS. The principal objectives of this task are to list the key functions involved in the check-out process, and identify the procedures which may be used to verify the function. The verification procedures vary with the vehicle function. The choice of a validation procedure for a given function depends upon the procedure cost, impact on driver safety, reliability, availability, effect on system operation, marketability, compatibility with the current system design, and appeal to those who must choose the validation method. These features will determine which approach to the check-out process is most appropriate for a particular installation. There can be several different check-out systems for specific highway configurations.

Driver validation is the primary consideration during check-out, however vehicle validation must also be performed to determine whether or not the manual functions remain viable. Certain features which are not needed on the automated highway may be important at the destination and must be verified. The check-out process may include acknowledgment of the state of the vehicle at check-in, and any non-critical loss of functionality during AHS operation which was detected by the in-vehicle monitoring system must be reported. Critical failures which occur during automated operation may result in removal of the vehicle from the system before reaching check-out.

The interaction between the driver and the vehicle and the testing of manual engine, brake, and steering functionality depend upon the physical implementation of the exit ramp design. The speed at exit, the number of check-out lanes, or the placement of a parking lot for a rejected vehicle, will impact the implementation of the check-out process. The issues involved with the exit design are discussed in detail in the Activity J - AHS Entry/Exit Implementation analysis. The major concerns with the check-out validation process are:

- Impact of a check-out test on AHS traffic.
- Cost of the check-out system.
- Safety during check-out.
- Failure to test a critical component.

- Failure to correctly test a critical component.
- Failure of the continuous in-vehicle testing.
- Association with the current vehicle system self-test methodology.
- Other methods of evaluation specific to the equipment.

The vehicle function task identifies which properties of the vehicle are important variables during check-out. This discussion includes consideration of which functions require special testing, and how check-out testing might be conducted so as to maximize safety and driver comfort. Cost of the in-vehicle equipment is not a primary consideration, since the equipment can be the same as that used during vehicle check-in.

Tests which involve visual inspection are probably not practical during check-out. The results of continuous in-vehicle monitoring while traveling in the automated lane can be read at check-out and used as part of the validation process. Dynamic testing can be performed as a part of the natural exit process as the vehicle is released into the traffic stream. The range of testing can vary from a simple verification of the results of continuous monitoring to a set of dynamic tests performed by the driver as part of the check out process. The type of testing and the complexity of the testing is related to the type of exit facility. The following paragraphs present a representative check-out process for a dedicated exit facility and a mixed flow lane exit facility.

Check-Out Scenario From Dedicated Lanes

A single generic off-ramp check-out system can be implemented for dedicated highway concepts such as RSC's 1 and 2. It is assumed in the proposed approach that the ramp does not lead to another highway, but rather to city streets or country roads. The off-ramp is terminated by a stop sign or traffic signal. A small facility similar to a toll booth is located at the ramp termination, with at least one individual in the facility to report emergencies and for visual inspection if necessary. The length of the off-ramp is determined by the standard maximum exit speed from the automated highway. A parking lot will also be at the end of the off-ramp, whose size will be based on its projected occupancy. The parking lot will function as a depot for holding vehicles which fail the vehicle/driver check-out, in addition to those who choose to park there before entering the local stream of traffic. The latter option may be used more frequently in early stages of deployment to allow users an acclimation period to readjust to manual driving.

Control of the brakes is given to the driver somewhere near the beginning of the off-ramp and the driver is allowed to stop the car manually. A profile of speed versus distance is compared to the vehicle trajectory by internal monitoring systems, and if the deviation from this profile is great enough, the system regains automatic control and directs the vehicle to the parking lot. The system will monitor for both inadequate braking rate, where there is a risk of the vehicle not stopping at the ramp terminus, and excessive braking rate, where the vehicle may stop far short of the ramp termination. This procedure serves as a test of the manual braking system and of the driver's braking response. Manual control of the throttle and the steering is released to the driver after the vehicle has come to a stop at the termination of the ramp. The driver is responsible for control of the vehicle and management of failures when he resumes moving from the ramp termination point in this scenario. The driver may indicate a system failure to the automated off-ramp control system through the user interface, which will automatically cause the vehicle to be moved to the parking lot.

Check-Out Scenario From Mixed Flow Lanes

Vehicles exiting a mixed flow AHS such as RSC 3, or exiting from any automated highway to a non-automated highway using a transition lane must perform their check-out tests at highway speeds. In order to maintain safe operation at check-out, the brakes will remain under automatic control until all other functions have come under reliable manual control. The system automatically maneuvers the vehicle into the transition lane, and control of the drive train is then provided to the driver after the merge is completed. The vehicle acceleration-deceleration profile is monitored by a longitudinal spacing sensor, and is compared to a typical profile for the current traffic flow. The driver is allowed to begin manual steering if the manual profile meets the monitoring criteria, and is notified to enter a non-automated lane when practical. The driving pattern is again matched against a reasonable profile after throttle and steering have been released. Brake functionality is given to the driver if the vehicle passes this test, and a final profile is matched to brake performance before the vehicle is completely released from AHS monitoring.

Vehicle Function Description

The categories of vehicle functions which are candidates to be tested at check-out are itemized in the list below. For those functions which should be tested at check-out, a discussion of the check-out test will be presented. Performance validation procedures for these functions generally fall into three categories: those performed during inspection; those

which are part of the continuous in-vehicle diagnostics; and those that are performed dynamically. For check-out, both the results of continuous in-vehicle diagnostics and dynamic tests performed during the transfer of control will be considered.

Dynamic tests are performed when the vehicle is under automated 'management' but not necessarily under full system control. As part of the check-out process, the driver may be given partial control of a function and then requested to perform an operation (steer into the adjacent lane, brake to slow the vehicle to a specific speed, etc.). The vehicle must successfully complete the requested actions before it is approved for exit. Diagnostic information stored in the vehicle computer is also checked prior to release from automated management in order to verify proper operation of critical vehicle functions.

The table below lists the vehicle functions, whether the function is a candidate to be tested at check-in and at check-out, and the type of testing which will be performed. Each of these functions will be discussed in detail.

Table 1. Candidate Vehicle Functions For Check-Out

Vehicle Function	**Tested At Check-in**	**Tested At Check-out**	**Dynamic Testing At Check-out**	**Continuous Monitoring**
Braking	Yes	Yes	Yes	Yes
Engine	Yes	No	No	Yes
Tire and Wheel	Yes	No	N/A	N/A
Steering	Yes	Yes	Yes	Yes
Transmission and Differential	Yes	No	N/A	N/A
Fuel Quantity	Yes	No	N/A	N/A
Electrical System	Yes	No	N/A	N/A
Vehicle Longitudinal Position/Distance Sensor	Yes	No	No	Yes
Vehicle Lateral Position/Distance Sensor	Yes	No	No	Yes

Visibility Enhancement and Emergency Equipment	Yes	No	N/A	N/A
Communications Equipment	Yes	Yes	Yes	Yes

Braking Functions

The major braking functions which are necessary and sufficient for manual operation include:

- Emergency (high g) braking.
- Routine (low g) braking.
- Antilock Brake System (ABS) and traction controllers.

Several assumptions concerning brake operation are made. It is assumed that the braking function of the vehicle has been tested during check-in. It is also assumed that the braking system is continuously monitored while under automated control. Testing of the brakes at check-out will verify that manual control has been given to the driver. It is possible that the brake pedal may be disengaged from the braking system during automatic operation. The driver will be given control of the brakes by re-engaging the brake pedal, and he will likely be requested to decelerate to a specific speed. Emergency braking capability will be verified by the continuous diagnostic checks, and not by driver action.

Many of the functions resident in the ABS and traction controllers will migrate into the engine controller microprocessor in the near future. In fact, most computer controlled vehicle functions will share a single microprocessor as the level of integration in the vehicle continues to increase. Detection of mechanical component failures in the vehicle requires expensive mechanical instrumentation. It has become common practice to use the subsystem controller as the principle means of testing for mechanical component failure by comparing subsystem performance with anticipated performance. ABS and traction control testing are typical of this trend in performance monitoring. The results of this continuous monitoring will be examined at check-out. Note that failure of the ABS or traction control system may not be classified as a critical failure. The driver may be notified of the failure, yet allowed to

complete the check-out as long as the braking system is operative and safe. Thereafter, the vehicle could be denied entry into the AHS at check-in until the failed system is repaired.

Engine Functions

There are several engine functions which can be evaluated as part of the check-out process. These engine functions are under constant evaluation as part of the engine diagnostic system. Engine diagnostics will be monitored during automated operation as well as during manual operation.

The engine controller will be expanded to include automated control functions such as throttle control, and will be coupled through a modern bus to the body control module and the on-board data base system. The controller functions required for manual operation are associated with engine management. The parameters under constant monitoring are engine temperature, oil pressure, coolant level, and performance conditions such as spark plug timing. Again, the results of the continuous monitoring of the engine properties would be summarized and transferred to the check-out station to validate the capability of the vehicle.

Continuous in-vehicle testing will identify most problems and the malfunction management system would remove the vehicle to a safe place if there was an indication that part of the switching mechanism had failed. If the transfer to manual control fails at some intermediate stage, the driver will be aware of the problem immediately when he attempts to resume driving and the system will note the failure and call for a tow truck.

A dangerous component failure such as a throttle stuck in an acceleration mode will cause the vehicle to gain speed. Provided that the brakes are still under system control, the vehicle speed can be controlled and the vehicle can be maneuvered to a safe location where it will come to rest and await a service vehicle.

Functions Associated With Tires And Wheels

It is likely that vehicles will have a Tire Inflation Monitor in the future. This monitor will notify the driver when the tire pressure drops below a certain value. The tire pressure will be tested during check-in for the purpose of minimizing the risk that a blowout would occur on the automated highway. The Tire Inflation Monitor operates continuously and can initiate

notification to the driver of any hazardous condition. No specific check-out tests are anticipated for tires and wheels.

Steering Functions

Currently, the steering system is a continuous physical linkage from the steering wheel to the front tires. In the future, there will likely be automated steering using a steer by wire system, and it's performance will be monitored just as the ABS and the power train controller are currently monitored in existing vehicles. If electronic steering is in use, then the continuous in-vehicle testing of the automated steering system may be sufficient to test the electronic manual steering control. If not, the manual steering function must be tested at check-out before steering control is returned to the driver. The act of transferring from automatic to manual steering control will require careful monitoring if the vehicle is not at rest when the transfer is made.

The transfer from automatic steering to manual steering is critically dependent on the type of hardware that will be in the vehicle. If the manual steering system is hydraulic, then there must be some mechanical method of engaging and disengaging the steering wheel from the steering system. At the time that steering control is transferred back to the driver at check-out, the hardware used to engage the steering wheel must be tested to make certain that manual steering is engaged. In the case of manual electronic steering, the steering function may quickly shift to commands generated by the driver's hand motions on the steering wheel from commands produced by a steering algorithm which receives inputs from vehicle position sensors and off-road intelligence.

Successful manual operation, such as the driver switching lanes as part of the check-out process will demonstrate that the automatic-to-manual steering switch has correctly functioned. If the lane change fails, then the situation again becomes a malfunction consideration. The system will revert to automatic control, the driver will be notified, and the vehicle driven to a breakdown lane for service and removal.

Vehicle Transmission And Differential

The vehicle transmission and differential operate identically in both manual and automated mode. No special controller operation or shift commands are required when under automatic

control. Therefore, no testing of the operation of the transmission and differential is required at check-out.

Fuel Quantity

The driver should be notified when the fuel level drops below a certain value, whether in manual or automatic operation. The fuel level is examined at check-in and the vehicle may not be allowed onto the automated lanes if it does not have sufficient fuel to get to its destination. At check-out, the driver could be alerted if his fuel level is low, and he may be given the location of the nearest fuel stations for convenience. The vehicle will be allowed to check-out of the automated lanes regardless of his fuel level.

Vehicle Longitudinal Position/Distance Sensor

The collision avoidance controller, which is the only component of the longitudinal sensor system that will be used on the non-AHS roadway, will monitor the sensor information and identify threatening situations. If there is a threat, it will first send a warning signal to the driver and then, if necessary, initiate evasive action involving the engine, the brakes, and the steering system. Self-test diagnostics could be used during automated vehicle operation and could be stored for verification at check-out. Failure of this system will not prevent the vehicle from completing check-out. The driver will be warned of the failure to the collision avoidance system.

Vehicle Lateral Position/Distance Sensor

Lateral position determination will be relevant only if it is used on the non-AHS roadway. In that case, the readout of the latest self-diagnostic tests would enable the system to determine whether or not the vehicle could rely on its lateral position sensor. Failure of this system will not prevent the vehicle from completing check-out. The driver will be notified if a failure is detected in the lateral position sensing system.

Visibility Enhancement And Emergency Equipment

Visibility enhancement and emergency equipment are not required during normal AHS operations, however they are required for operation on a non-AHS roadway. Equipment which improves manual driving visibility includes windshield wipers and defroster,

headlights, and rear window defogger. Standard emergency equipment includes a spare tire or equivalent tire inflation device. Other vehicle features which enhance safety include tail lights and brake lights, snow chains and emergency flares. This equipment may be characterized by the fact that virtually none of it can be inspected automatically. Tests of lighting and windshield wiper functionality are not currently available and the cost for development and deployment may not be justified by their limited utility on the automated roadway. The justification for implementing tests for equipment specific to operation on conventional highways is questionable. The responsibility for safe operation of the vehicle while under manual control is the driver's, and it can be argued that the driver should be held liable for correct operation of the vehicle functions discussed in this section.

Communications Equipment

Communications equipment which is used primarily during automated control will not be tested at check-out since that equipment is not necessary for manual operation. Similarly, communications equipment used during manual operation, but not necessary for safety reasons (such as communications associated with route guidance) will not be tested at check-out. If the vehicle has a communications function which is safety related during manual operation, that equipment will be tested either by an exchange of test messages with the roadside system or by examining the self-contained diagnostics.

Vehicle to vehicle communications is envisioned for vehicle based platoons. This communications system is used primarily to send distance, velocity and acceleration information to vehicles within a platoon. Since the vehicle to vehicle communications system is not necessary for manual operation, no testing of this system is required at check-out. A vehicle to roadside communications system could be used both for check-out and for infrastructure based platoon control. This communications system must be operating in order to complete the check-out process, and therefore is tested as part of the process. A specific check-out test of vehicle to roadside communications is not planned.

The check-out function will require the proper operation of the communications equipment since there must be an exchange of information between the vehicle and the check-out station. A failure in the communications system during check-out will be treated as a malfunction and will cause the vehicle to autonomously steer to the shoulder and stop.

Task 2. Safe Vehicle Operation/Check-Out Alternatives

The Automated Check-Out activity has much in common with and is inextricably linked to Activity J - AHS Entry / Exit Implementation. The general approach to these two research activities is to treat entry/exit issues which are predominately volume-related in the entry/exit activity. Safety issues and risks, as well as issues related to vehicles not ready for resumption of manual control, are addressed in automated check-out.

Depots

The issue of the potential need for depots at check-out points was raised early in the project. The line of reasoning that leads to consideration of depots is as follows:

If the AHS is capable of total control of vehicles, and detects some defect (mechanical or driver-related) which would preclude safe manual operation of the vehicle, then the system is obligated to ensure that the vehicle does not re-enter the manually controlled traffic stream.

Mechanical conditions could conceivably trigger the need for such system operation, although the automated systems would most likely work even if the manual interfaces were defective. Of greater concern is the possibility that a driver who passed the check-in test becomes impaired, unable, or unwilling to resume control during the automated trip. Possible causes for such a scenario include drug or alcohol use during the trip, deep sleep, onset of acute or disabling illness, or mental conditions.

Assuming such scenarios justify the use of depots, two extreme designs for depots can be visualized. At one extreme is a depot with lighting, emergency medical staffing, communications, and enforcement personnel standing by. At the other extreme is the simple provision of parking spaces with call boxes nearby. In either case, the depot would be designed in conjunction with the AHS exit facility.

The researchers tend to favor the latter choice based on the following logic: Most, or at least many, of the incidents that could warrant a depot should be detectable in real time, given the level of communication and sensing expected to be on board AHS vehicles. If this is the case, the vehicle should be able to detect an incident soon after its onset rather than waiting for the check-out process to begin. An appropriate response to such a detected incident includes notification (by vehicle - infrastructure communication) of the AHS control center

and/or the appropriate emergency response agency (fire, repair, medical, or enforcement.) This use of the detection and communication capability of equipped vehicles may reduce the need for depots, or allow them to have minimal amenities.

The implications of the presence or absence of AHS shoulders is discussed in Activity K - AHS Roadway Operational Analysis. Shoulders reduce the requirement for depots even further, by providing a place at which “not ready” vehicles could be safely parked and emergency action taken. It is not difficult to envision a scenario in which a defect is detected and the vehicle is kept moving until the appropriate response staffing and equipment are in place at a predetermined location on the AHS shoulder, at which time the system would stop the vehicle on the shoulder. Once the vehicle is safely stopped on the AHS shoulder, the appropriate action would take place.

Task 3. Identify Operator Characteristics

Under automatic control in AHS, drivers will require notification in sufficient time to resume manual vehicle control from automatic control prior to reaching an exit point. AHS will need to perform several tasks in this process to determine that the driver is ready to receive control of the automated vehicle. Generally, AHS will need to:

- Alert the driver that manual control of the vehicle is imminent.
- Receive acknowledgment that the driver is aware he will be taking control.
- Determine that the driver is competent to assume control of the vehicle and able to execute a safe exit from AHS.
- Ensure that the transition from automatic to manual control is done comfortably and without stress.

At some point prior to exiting the AHS, the driver will be notified that his vehicle will be exiting the AHS. How the driver is alerted and how AHS determines that the driver is competent to assume control is discussed in detail later in this section. Assuming that transition from automatic to manual control is executed under normal or non emergency situations, and the driver has acknowledged he will be assuming control, and AHS has determined that the driver is capable of assuming control, there are several approaches as to how this hand-off might occur. If the driver has been monitoring his progress along the AHS via a navigation/route guidance display system, he is well aware of his position relative to his exit point and could cue AHS that he is awaiting manual control instructions. Navigation

systems such as TravTek, which is discussed in Activity G — Comparable Systems Analysis, provide the driver with distance to an upcoming action or event. This information is provided graphically on a map display and/or by voice/audio transmission. The TravTek system presents drivers with a heads up, scale selectable street map that shows the vehicle location and the intended or planned route. TravTek provided the driver with route guidance information required to complete the route in the form of step by step instructions such as "Turn Right at Elm Street, 4.2 miles." This information could be provided via audio/voice transmission. The AHS driver could be notified on a map display or by audio of route status corresponding to upcoming events, such as "7 miles (7 minutes)", until the driver will move into the transition lane to resume manual control, and exit point on XYZ avenue is approximately 2 miles (3 minutes) beyond the manual control release point. Additional information that would also be helpful and perhaps required by the driver would be a count down "10 to 0" to the manual release point. He may be reminded that manual control will be returned at 96 km/h, and that his foot should be on the accelerator, (which would be partially depressed) like a cruise control prior to release. AHS may need to verify that the driver has his hands on the steering wheel, and the steering wheel should have the slight motion play caused by the roadway as experienced in manual driving. If a map display is available, the driver may want to see a planned view of his vehicle position (blinking) relative to other vehicles that are in front, behind, and in the adjacent transition lane and his insertion slot into the transition lane. The driver may be notified of the speed he needs to maintain as his vehicle moves into the transition lane.

Alerting The Driver To Resume Manual Control

AHS will need to alert the driver of pending return of vehicle to manual control. Prior to determining driver competence to assume control, AHS needs to establish contact with the driver. The driver could be asleep or out of the drivers seat. Different procedures and multiple alerts might be required prior to establishing contact with the driver. For example, if the driver were asleep and it were nighttime, the interior vehicle lights may be turned on by AHS. The radio may be activated and/or the volume increased. Windows could be lowered to allow outside air or noise into the vehicle. The HVAC system could be altered. Seats may be moved from a reclined position or seats may be vibrated to ensure that the driver responds to some stimuli. Seatbelts could be slightly tightened to alert or awaken the driver. At anytime during this alerting process the driver could acknowledge and terminate these alerts. Acknowledgment by the driver might include having the driver place his hands on the steering wheel, activate a response button on the steering column, or give a voice input

which would be validated by an on board voice recognition system. The driver may have to respond to a random number that AHS presents on a display by entering the displayed number on a dashboard mounted keypad.

The AHS driver will also need to be alerted regarding any changes to his planned or assumed trip route. Prior to the driver checking into the AHS, his route would have been either pre-planned by him or AHS would provide an optimum route based on AHS knowledge. This route information would be available to the driver on his route guidance/navigation display system. Additional information that the driver would require would be related to any change in the assumed travel scenario once enroute. For example, drivers would need to be warned of the existence of an accident or condition along his route that alters the assumed route or abruptly causes an unexpected lane change. Information regarding road conditions that would require adjusting automated speeds, there by changing estimated time of arrival or the route used.

Task 4. Operator/Driver Competence Determination

At some point while operating in the automatic mode of AHS the driver will be notified that he is nearing an exit point and he will be required to resume manual control. The method or procedures for alerting the driver and methods for confirming that the driver is competent to resume control will be discussed. A number of driving scenarios may define the sophistication of systems/sensors required to assess driver competence in assuming manual control. The use or complexity of any sensor or system may vary as a function of the type trip being executed.

In one AHS driving scenario, the home-to-work-to-home trip where the vehicle is under automatic control for a relatively short period of time the driver would probably be continuously aware of his trip position, surroundings, and approximate exit time for AHS departure. Driving statistics for the to-and-from work trip is approximately 16-24 km commuting one-way in urban areas and up to 40-48 km in and from rural areas. For this type of trip lasting 15 to 30 minutes to 1 hour, and occurring mostly during daytime, the driver would probably be totally alert not only of his surroundings but to where he is in terms of arrival time at his exit point. In this scenario, the driver could query AHS that he is awaiting instructions prior to resumption of manual control. This may involve a simple task such as pushing a button on the steering wheel, placement of hands on steering wheel or responding to a chime at some 3 to 5 minutes prior to assuming manual control. For the short trip the

AHS may not need to determine the driver is competent to resume control. If the driver was preoccupied (working, reading the paper) and had not cued AHS for instructions, a chime could be sounded to alert the driver that he will be receiving instructions to resume control.

In a another scenario lasting perhaps 2 to 4 hours, where the driver is leaving or returning home from out of town may involve more sophisticated methods to confirm that the driver is competent to resume control. In this scenario, (leaving town for the mountains, sea shore on Friday night), the driver may initially be more fatigued beginning this trip versus the short to-and-from daytime work trip. For the longer drive, the driver may wish to go to sleep, close his eyes while enjoying an on-board entertainment system, or put himself at risk by drinking. In this scenario AHS would have to confirm perhaps as early as 20-30 minutes prior to AHS departure that the driver is alert and competent to resume control.

A third scenario involves a longer trip, up to 8-10 hours. In this scenario, AHS could also begin cueing the driver as early as 20-30 minutes prior to return to manual driving control. AHS could also cue the driver periodically as to his status for resuming control. For this length trip, the vehicle would probably need to be refueled one or more times, therefore the driver would be notified to assume control for fueling stops. In the longer driving scenario the driver would have a greater opportunity to relax, sleep or become preoccupied with non-driving or trip status tasks. The driver may also become intoxicated at anytime during the trip, thereby requiring AHS to monitor the vehicle or driver more frequently than for a short to and from work type trip. Driver complacency must also be addressed. After several hours of non-driving the driver may be tasked with a simulated vehicle control, steering or braking task to bring the driver to an alert driving state.

In any of the above scenarios the driver may want to interact with AHS for the purpose of altering trip plans, i.e., a rest room or eating stop or to change his destination. In this case, AHS will have to verify in a short period of time that the driver is competent to resume control. In another case where AHS might need to determine driver competency quickly is the scenario where AHS operation is degrading or the possibility of a complete AHS system failure which would require near immediate driver interaction.

Driver Monitoring Systems

The goals of a Driver Monitoring System (DMS) are to detect driver impairment, driver competency (drowsiness, fatigue, intoxication, etc.) that would not permit the driver to

resume manual driving control. DMS systems will need to alert the driver to the detected condition, and/or AHS will need to retain vehicle control until the vehicle can be moved into a safe area.

The process of alerting the driver that he will be exiting AHS may require various sensors, methodologies and procedures that determines the driver is competent to assume manual vehicle control.

Notifying AHS Driver

If the driver has not queued AHS for instructions prior to departure, AHS will need to determine the drivers state. Several possible techniques might be used to alert the driver. AHS can notify the driver by sounding a chime, increasing/decreasing ventilation in the vehicle, open windows, move or vibrate the drivers seat, tighten a seat belt, increase volume of the radio, etc. The alerted driver will need to respond, by acknowledging the AHS alert. The driver will acknowledge the alert by extinguishing the alert(s). AHS now needs to determine that the driver is competent to assume manual control.

Determine Driver Competency

Any or all of the cueing devices may be required to get the attention of the driver. Once alerted, the driver may be asked to perform specific tasks in order to ensure that he is capable of resuming control. For example, the driver may be required to perform an artificial steering task. The driver may be asked to steer towards a steering target or track a vertical line displayed on the forward windscreen. The word “Brake” could be displayed on the windscreen, requiring the driver to make contact with the brake and apply full brake pressure. These actions would have no effect with the actual vehicle, i.e., brake lights would not come on to confuse a vehicle/driver in a following mode, nor would the vehicle begin to slow or stop with brake activation. These driver inputs and reaction times could be compared with a stored driver data bank information residing within AHS that would be used to determine driver competency. Another method to determine driver competence could be to display simple instructions on the forward windscreen. A message on the display might tell the driver, “Turn On Headlights”, “activate Left Turn Signal”, Turn Off Headlights”. Drivers would be required to respond within certain limits.

Other on-board sensors could monitor Blood Alcohol Count (BAC). A relatively new technology (laser diode spectrophotometry) holds the promise of a non-invasive, non-intrusive detection of alcohol level. This sensor could be positioned in the hub of the steering wheel and monitor presence of alcohol in the driver's breath. The advantage of a such a system is that it could detect blood alcohol level directly without a tedious alcohol interlock system needing some behavioral measurement to be performed. If the system detected a BAC level above a certain threshold, automatic release to manual control would not occur and the driver would be notified he was not capable of manual control and that his vehicle would be moved to a safe area.

Another technology being developed by small company in Savannah Ga., analyzes perspiration from the driver's hands to determine blood alcohol levels. This system is designed to prevent operation of the vehicle and gives the driver visible and audible warnings. While under AHS automatic control the driver could be instructed to place his hands on the steering wheel prior to assuming manual control. BAC could be measured at this time and AHS could determine if the driver were under the influence and AHS would retain control until the vehicle was removed from AHS. Secretion from the skin gives an accurate representation of blood chemical content. This system can also measure glucose, cholesterol and blood pressure.

Speech recognition systems are on the brink of substantial advances in capability. The technology is advancing rapidly. Sprint Corporation is using voice activated phone cards where Sprint's computer compares a stored voice print with the user placing a call. Voice prints are very unique and possibly very useful for AHS applications. Voice recognition systems can detect a change in the inflection of an intoxicated driver's voice. Comparing the drivers voice input with his/her stored voice print could be used to determine capability of the driver to resume manual control.

There have been several proposed systems to detect alcohol, fatigue and drug use by collecting driving control performance measures such as steering, driving speed, and acceleration. Typical driving performance data might be a prerequisite prior to entry to the AHS. Under automatic vehicle control, AHS would not be able to collect and store driving performance unless an artificial driving task (while under automatic control) were administered to the driver.

In an emergency medical situation, AHS might be equipped with a “Panic Emergency Button” that the driver could activate if capable. In the event where the driver was unable to notify AHS of an emergency, AHS through its normal alerting sequence would determine that it was not receiving any response from the driver and would thereby move the vehicle to a safe area.

Task 5. Evaluation Of The Acceptability Of Check-Out Alternatives

Operator And Vehicle Check-Out Alternatives

The potential check-out alternatives range from very little testing of the operator and the vehicle to extensive testing of the operator and vehicle. The amount of testing which must be performed before manual control of the vehicle is returned to the operator will be strongly influenced by safety considerations. The acceptability of potential check-out alternatives will be discussed to provide guidance in those instances where alternatives can be implemented safely. Table 2 lists three options for operator testing and three options for vehicle testing. Hindrances to acceptability and benefits are discussed for each of these options.

The first option is a simple check-out procedure for the operator which does not involve any testing of the operators ability to resume control. Instead of testing, the operator will be asked to respond to a request to assume control by pressing a button, grabbing the steering wheel, depressing the throttle, etc. When the operator takes the proper action, he will regain control of the vehicle. This check-out option has the advantage of being simple, inexpensive, and reliable.

Table 2. Check-Out Options

Check-out Option	Advantages	Disadvantages
Operator test consists of simple action only (e.g. push a button).	Operator is never refused control of vehicle if response is proper. Driver accepts liability by positive action.	System may allow drug or alcohol impaired driver to assume control.
Operator test includes simple tests of ability to take control of vehicle.	As drivers become familiar with tests, they will have confidence of passing. Tests will help prepare the operator for manual control.	Potential to reject a qualified driver. Test may miss a large portion of impaired drivers.
Operator test includes a complete check of the operator.	Operator test consistently removes impaired drivers from the system.	False rejection of an qualified driver will discourage driver from using AHS.
No test of vehicle functions.	Monitoring of most functions may be common. Cost effective if manual controls are reliable and preventive maintenance is performed.	Vehicle may not operate properly when control is given to operator
Simple test of vehicle functions.	Driver has some confidence that manual controls are functional.	Functions not tested may be inoperative.
Complete test of vehicle functions.	Driver has complete confidence in the manual controls.	False rejection of a properly operating vehicle will discourage operator from using AHS.

The operator will know with certainty that he can regain control of the vehicle at check-out. The disadvantage of this simple check-out is that it does not take advantage of an opportunity to increase driver safety inherent in a system that removes impaired drivers.

The second option for operator testing at check-out is to perform a small number of tests to verify that the operator is ready to take control of the vehicle. These test could include a check to determine if the operator is in the driver seat and has his seatbelt properly fastened. Other simple tests include a series of requests to the operator, such as move the steering wheel, depress the brake pedal, turn on the directional signal, or shift the transmission. The responses by the operator to these requests can be monitored by the automated system in the vehicle, and control of the vehicle can be given to the operator if his responses are correct and executed in a timely manner. This check-out option has the advantages of being simple,

thus giving the operator the confidence of being able to pass on a regular basis. The driver will also be alerted to take over manual control of the vehicle by performing natural driving tasks. The disadvantages of this check-out option is that impaired drivers could pass the check-out tests if they are too easy and if too much time is allowed for the operator to respond. On the other hand, if not enough time is given to the operator to respond, or if the sequence of actions requested is too complicated, qualified drivers may be falsely rejected, and as a result the acceptance of the candidate check-out process will be hindered.

The last option for operator check-out is to perform as complete a set of tests as possible in order to assure that all impaired and unqualified drivers are removed from the system. Tests of the drivers reactions such as asking the operator to input a displayed number sequence on a keypad could be performed. If the operator took too long, or if the number sequence was input with errors, the operator could be rejected. Other tests, such as checking for slurred speech, retinal scanning, or testing sweat from the palm of the driver can be used to check for alcohol or drug impairment. Medical testing can also be performed to aid in determining if the driver is capable of manual control. These tests include monitoring of respiration rate, heart rate, and blood pressure. The operator's license can be scanned electronically to search for unpaid traffic violations or the expiration of the operator's license. The benefits of this type of exhaustive testing is that impaired or unqualified drivers will consistently be removed from the roadways. This will have a long term effect on accidents, since it can virtually eliminate impaired drivers from exiting the AHS. Unfortunately, drivers who do not use the automated lanes will not be tested. Another hindrance to acceptance of such a system is the rate of false rejection of a driver. The public will quickly grow tired of a system that periodically rejects qualified drivers.

One option for vehicle check-out is to forgo test of any of the manual functions. This option is feasible if the manual systems have sufficient reliability. All current vehicle systems which are computer controlled, such as antilock brakes and drive train controller, have continuous diagnostics running in the background. This trend will likely continue with any computer controlled AHS equipment. If the manual control systems for AHS capable vehicles contain sufficient diagnostics, then a simple check of the status could be sufficient to verify that the manual systems are operational. The benefit of this type of check-out is that no additional vehicle cost is incurred to complete check-out. In order for this type of check-out to be acceptable, it must be reliable. Any instances of the manual system failing when control is given to the driver would negatively affect the acceptability of the system.

If built-in diagnostics is not sufficient for a reliable and safe check-out, dynamic check-out tests must be performed. Dynamic tests may be performed on a limited number of manual vehicle functions if most of the vehicle functions can be effectively checked with the diagnostics. If diagnostics prove unsuitable to assure that the manual functions work properly, the complete set of manual functions may be subject to dynamic testing at check-out. As the vehicle tests become more strict, the likelihood of a false rejection of a vehicle at check-out increases. If vehicles which are capable of manual operation fail check-out, the acceptability of the system will decrease. A benefit of a stringent check-out which consistently removes vehicles incapable of manual operation is high user confidence in the AHS.

Storage Alternatives For Vehicles Which Fail Check-Out

AHS must provide storage for vehicles which fail check-out. The type and placement of the storage facilities will have an impact on the acceptability of the automated system. Table 3 lists three vehicle storage options along with the benefits of each and corresponding impediments to acceptability.

The acceptability of depots as a storage option for vehicles and operators depends upon their placement, cost, and the availability of services at the depot. Depots could be placed at every exit. This would provide the greatest convenience, since the vehicle that failed check-out would be directed to a depot at the normal point of exit for the vehicle. Placing depots at every exit would be most costly and excessive costs could negatively impact AHS acceptance. If depots were placed at longer intervals, the vehicles (or operators) which fail check-out would be diverted to the nearest depot, which may be miles from their normal exit point. Diverting a vehicle miles from the intended exit point would also have a negative impact on the acceptability of check-out. An advantage of depots for check-out would be the availability of emergency services. The AHS could alert the proper authorities of a medical emergency or alert authorized vehicle repair services of a vehicle breakdown during the check-out process. Prompt response to an emergency would greatly enhance the acceptability of check-out. Alternately, the depots could be manned with emergency service personnel, providing immediate response and aiding in public acceptance of AHS.

Table 3. Advantages And Disadvantages Of Check-Out Alternatives

Check-out Vehicle Storage Option	Advantages	Disadvantages
Depots	Emergency services (tow truck, paramedics, etc.) may be readily available at depots.	Vehicles may be diverted 10 miles or more from requested exit. Expensive to build depots if closely spaced.
Shoulder	Vehicle is stopped close to normal exit.	May create a traffic hazard. May add requirement for shoulder.
Park on ramp	Vehicle is stopped close to normal exit. Vehicle is out of the flow of traffic.	Adequate storage for vehicles must be provided at ramps.

One alternative to providing depots at exit points would be to move vehicles which are incapable of manual operation to a shoulder on the AHS lanes. This alternative would be suitable only if the AHS lane design included shoulders. The advantage of using the shoulder to store vehicles which fail check-out is that the vehicles could be stopped near their exit, saving the driver the frustration of being diverted past his normal exit point. The major hindrances to the acceptance of this alternative are the potential of the vehicle creating a traffic hazard, the danger associated with the driver leaving the vehicle and walking on the AHS roadway, and the time that it would take for emergency services to get to the vehicle.

Another alternative to depots is to provide storage for vehicles on the shoulder of the exit ramps from the automated lanes. Note that shoulders would not necessarily have to be provided along the entire exit ramp, but only in those areas where vehicle storage is required. The advantage to this option is that vehicle storage could be provided at the normal exit point. Emergency services could be provided in a similar manner to the services provided at depots. Also, the vehicle is stored out of the flow of traffic. The disadvantage of storing vehicles on exit ramps is if adequate storage is not available at each exit. The AHS would then be forced to divert the vehicle to the next exit.

Task 6. Define Check-Out Issues And Risks

The check-out process is composed of three primary components: verification of manual vehicle functions, validation of operator competence, and transfer of the vehicle from automated to manual control. The system configuration is also an important factor in the ability to ensure a safe transition to manual operation. A primary issue concerns where the transfer of control takes place. The potential for human error exists if vehicles are allowed to enter or exit the AHS under manual control and the transition is made within the AHS lane. Similarly, if the vehicle is under AHS control in the non-AHS lane during a merge maneuver for check-out, then the AHS vehicle is susceptible to human error occurring among vehicles operating manually in the non-AHS lane. One option to minimizing these risks is to dedicate entry/exit facilities to eliminate the possibility of collisions in transition lanes caused by vehicles under manual control.

The check-out procedure is also responsible for providing coordination among vehicles in the automated lanes and vehicles in mixed mode lanes in non-dedicated configurations. The vehicle must be released to manual control in a position that provides a safe following distance from the preceding vehicle, and controls the relative speed to adjacent vehicles to ensure safe operation when manual control is resumed. These safety considerations are essential to minimize the risk of high differential velocity collisions when transfer of control takes place at freeway speeds in transition lanes. The issues involved in each of the functional areas are addressed in the following paragraphs.

Operator Issues And Risks

Deployment of AHS-related technologies has the potential to raise concerns with privacy advocates. Privacy issues are generally raised in regard to the data collected in conjunction with the check-in and check-out process. There is concern that an exhaustive check-out screening will be perceived as invasive if it involves monitoring of such attributes as sobriety or reaction time to verify driver’s ability to regain manual control. The objections to gathering this type of data include fear that drivers with medical problems will suffer discrimination, and overall discomfort with the modern trend toward routine collection of personal data. Recent media attention to the Clipper chip proposed by the Clinton administration to standardize government communications has highlighted this fear. This technology includes a provision for accessing private data by government agents with proper

court warrants. This issue can be resolved by ensuring that data collected for purposes of AHS authorization must be kept to a minimum, and providing guarantees that the data will not be accessible for purposes such as employee or insurance screening.

The gathering and use of personal information, such as blood alcohol or drug content, may invite user objection to the process. Obtaining this information indirectly through non invasive methods is one approach to mitigating the risk of potential litigation concerning first amendment rights. Successful objections could result in voiding the legality of the driver check-out procedure for all AHS drivers. The possibility of this scenario should be considered in the operation and design of the check-out process. Arguments and complaints can be expected from falsely impounded drivers or marginally not-ready drivers, even if the check-out process is never challenged, or if it is declared legal by the courts. The issues and risks associated with the rang of potential operator validation procedures are summarized in table 4.

Table 4. Summary Of Operator Issues And Risks

Issue	Risk
Exhaustive performance monitoring to ensure driver competence.	False rejection of a qualified driver will discourage driver from using AHS.
	Privacy concerns may invite litigation.
Moderate driver verification tasks consisting of tasks such as steering and response performance.	Potential to reject a qualified driver.
	Test may miss a large portion of impaired drivers.
	Liability involved with incidents following release to manual control unclear.
Eliminate driver testing and require driver to manually activate check-out process.	System may allow drug or alcohol impaired driver to assume control.

Instrumentation Issues And Risks

The instrumentation required to perform the check-out procedure must provide assurance that critical vehicle functions are operational while maintaining a balance between cost and complexity. The range of testing can vary from an exhaustive dynamic testing process to simple monitoring of self-test functions. Table 5 presents the issues and risks corresponding to the potential levels of functional verification. Exhaustive testing of systems which are not critical to safe check-out can increase the cost and complexity of the system out of

proportion to benefits obtained. Failure to sufficiently test safety critical systems prior to check-out can increase the risk of transferring unsafe vehicles to manual control. Limited testing of vehicle systems should strike a balance between the two extremes in order to ensure safe transition to manually controlled vehicle functions without compromising safety. The most cost effective approach to implementing check-out testing of vehicle functions will take advantage of instrumentation associated with existing vehicle monitoring such as traction control systems and ABS, or systems associated with AHS specific continuous monitoring of safe vehicle operation, discussed in Activity B - Automated Check-In.

Table 5. Summary Of Instrumentation Issues And Risks

Issue	Risk
Exhaustive test of vehicle functions required for manual operation.	Complexity and cost effectiveness highly dependent on current state of manual function technology.
Limited test of vehicle functions, including manual steering and braking.	Low probability failures are possible. Risk must be evaluated in terms of impact to user acceptance and implementation cost.
No test of manual vehicle functions.	Failure of manual steering or brakes could cause accidents in the mixed traffic stream.
Verification of vehicle-roadside communications associated with the check-out process.	Increased load of data rate on overall communications system capacity. Value may be limited if ability to continuously monitor is present.

Infrastructure Issues And Risks

Depots, if used, are subject to several design alternatives, each of which have their own sets of issues and risks. Issues related to depots can be grouped as follows: Design, Operation, and Location. Table 6 places the issues and risks into a matrix organization.

Check-out issues and risks are felt to be largely RSC-independent, and the discussion does not address each RSC independently. Likewise, passenger car and commercial/transit issues are not given separate treatment. Rural versus urban issues are primarily related to the numerous issues involving travel time, travel distance, and incident response time.

Table 6. Summary Of Infrastructure Issues And Risks

Issue	Risk
Do not provide depots.	Agencies could sustain liability due to accidents resulting from not-ready drivers and/or vehicles.
Provide depots that are too small.	Back-ups could extend from depots into the AHS traffic stream, degrading operations or possibly causing accidents. Spillover traffic could be diverted into mixed traffic, resulting in accident liability.
Provide depots that are too elaborate.	High construction and operation cost.
	Non-use or under-use of depots could result in a public perception that resources are wasted.
System design sets probability of detecting not ready vehicles and/or drivers too low.	Not-ready drivers/vehicles could cause accidents in the mixed traffic stream.
System design sets probability of detecting not ready vehicles and/or drivers too high.	Depots could overflow due to false alarms.
	Diversion of not-ready drivers due to depot at capacity with falsely impounded vehicles could cause negative user perception.
Depots too far apart.	Excessive travel times and distances for emergency response teams and equipment.
	Excessive travel time between incident detection and arrival at depot.
Depots too close together.	Excessive construction and operation cost.
	Under utilization may cause perception of wasted resources.
Depots unmanned.	Possibility of criminal activity.
Depots manned.	Possibility of under-utilization of manpower may cause perception of wasted budget.
	Cost of amenities and payroll for staff.

Design Issues

A range of possible depot configurations is presented in task 2, Safe Vehicle Operation/Check-Out Alternatives. An important attribute of depots is size. Depots should be designed based on the expected number of users, the duration of use, etc., with a reasonable

confidence that the capacity will not be exceeded. If capacity is exceeded the design should tolerate overflows. An overflow which backed up into an AHS through lane is not tolerable, while an overflow that backed up onto a shoulder may be considered tolerable.

Depots with excessive size would be costly to construct and operate and if under-utilized could result in complaints from the public.

Task 2 mentions a range of amenities that could be designed for depots, ranging from none or very few, to a site with emergency response personnel standing by. While an elaborately equipped site would have a rapid response time and would provide the highest level of service to users, it would also provide a burden to the operating agency and in fact such a design could result in the overall AHS program being perceived in bad light.

Depots could be designed to independently detect the entry of an in-need vehicle and send a signal to a response entity, or the depot could depend on the vehicle's, or the AHS's communications system for notification. The former alternative would add redundancy to the overall system but would require instrumentation of the depot. The latter alternative could allow non-detection of the presence of vehicles with failed communications.

Reliability and accuracy of detection of conditions that would route vehicles to depots is very important. False positive detections (resulting of impounding of non-defective vehicles) would result in complaints and overload the depots. False negative detections would place not-ready vehicles in the manual traffic stream, partially defeating the purpose of the check-out process, and resulting in liability exposure if accidents result.

Operation Issues

Operation issues are important for any check-out process involving depots. Whether or not staffing is provided at depots is probably the most important issue from the point of view of the operating agency. Staffed depots could be perceived as safer than unmanned ones, especially in high crime areas. Any staffed depot design requires far higher operating costs due to the requirement for housing the operating staff. With a highly reliable AHS, the expected number of impoundments would be low, especially during off-peak hours. Effective means of detection and short response times for impounded vehicles at depots would reduce or eliminate the need for staffing.

Given the assumption of depots as an amenity for AHS users, various methods are available to fund their use. They can be lumped into the overall cost of the AHS and funded by whatever means of funding (tolls, property tax, etc.) is used for the AHS. In this scenario the depot service is “free” for its users.

An agency may consider direct charges for use of the depot, recognizing that the driver is accountable for failures in his vehicle that resulted in impoundment. This could be considered somewhat analogous to towing and storage charges for parking violators.

Regardless of whether users are charged for use of the depot space, at least some of the response services (wreckers, for example) could be contracted out, reducing the requirement for government growth. Other services (police and ambulance) can be provided by existing agencies without the need for duplication.

It is likely that a depot would be an area where automated and non-automated activities would be mixed. It is important that these areas be designed and operated to preclude or minimize possibilities of unauthorized use. Methods to achieve this goal include security methods to detect unauthorized use and penalties to deter such use.

Location Issues

No logical reason for depots more closely spaced than AHS exit facilities can be envisioned, so one depot at each exit is considered the minimum depot spacing. This scenario also has the highest cost, regardless of individual depot design and operating parameters.

Greater spacing between depots increases travel time from emergency response center to depot. Exiting vehicles failing the check-out process at the desired (but non-depoted) exit would have to continue the trip until a depot is reached. In the case of medical-related driver disability, the added travel plus possibly increased emergency response time could be important.

False positive impoundments could be even more of a nuisance with cars not only falsely impounded, but forced to sustain added travel time.

Task 7. Implications For System Configuration

The implications of check-out procedures on AHS configurations are analyzed in this task. The objective of the analysis is to identify some of the potential AHS hazards related to the check-out phase of vehicle travel. The scope of this analysis is restricted to hazards resulting from missed detections and false alarms, with respect to check-out decisions performed by the (i) vehicle systems, (ii) infrastructure, (iii) drivers, and (iv) exit gate attendants.

Protocol verification and translation of check-out protocols into specific system designs are both system design activity and therefore outside the scope of this analysis. Moreover, what it means to "optimize system safety" is not clear, since it is generally recognized by the system safety community that the best we can do to make a system safe is to mitigate risk by identifying system hazards and applying good engineering practice to address system hazards.

Detailed Check-Out Protocol Logic

As a basis for analyzing the implications of check-out procedures on the AHS configuration, the two check-out scenarios described as scenarios in task 1 are considered. The scenarios may be restated in terms of AHS states, with preconditions and postconditions on the transitions between AHS states. This is presented in table 7 for the case of RSC's 1 and 2 which involve dedicated lanes, and in table 8 for the case of RSC 3 which involves the use of mixed flow lanes. Figures 1 and 2 are finite state machine representations of the information contained in tables 7 and 8, respectively. Circles represent system states and are labeled with unique state identifiers (S_i) corresponding to those labels used in the respective tables. Arcs represent state transitions and are labeled with unique identifiers representing the corresponding preconditions and postconditions (P_j).

Table 7. Check-Out Protocol Summary For RSC's 1 and 2

Current Vehicle State	**Preconditions On Transition to Next Vehicle State**	**Next Vehicle State**	**Postconditions On Transition to Next Vehicle State**
(S_1) Traveling on automated highway lane Automatic control of steering, braking, and acceleration	(P_1) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No exit request received from driver	(S_1) Traveling on automated highway lane Automatic control of steering, braking, and acceleration	(P_1) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No exit request received from driver
(S_1) Traveling on automated highway lane Automatic control of steering, braking, and throttle	(P_2) (i) No vehicle failure detected by automatic monitoring devices AND (ii) Exit request received from driver AND (iii) Vehicle is within a pre-defined distance of the exit ramp	(S_2) Traveling on automated highway lane Automatic control of steering and acceleration Driver performing the braking task Vehicle-based monitoring of speed-distance profile with respect to vehicle trajectory	(P_2) (i) Driver acknowledges hand-off of braking control AND (ii) No vehicle failure detected by automatic monitoring devices AND (iii) Exit request received from driver AND (iv) Vehicle is within a pre-defined distance of the exit ramp
(S_2) Traveling on automated highway lane Automatic control of steering and throttle Driver performing the braking task Vehicle-based monitoring of speed-distance profile with respect to vehicle trajectory	(P_3) (i) No vehicle failure detected by automatic monitoring devices AND (ii) Deviation of vehicle profile less than a pre-defined threshold value AND (iii) No change of exit request received from driver AND (iv) Vehicle is within a pre-defined distance of the exit ramp	(S_3) Vehicle merging onto exit ramp Automatic control of steering and acceleration Driver applying brakes Vehicle-based monitoring of braking rate	(P_3) (i) Driver acknowledges entry onto exit ramp via manual application of brakes AND (ii) No vehicle failure detected by automatic monitoring devices AND (iii) Deviation of vehicle profile less than a pre-defined threshold value AND (iv) No change of exit request received from driver

Table 7. Check-Out Protocol Summary For RSC's 1 and 2 (continued)

Current Vehicle State	Preconditions On Transition to Next Vehicle State	Next Vehicle State	Postconditions On Transition to Next Vehicle State
(S_2) Traveling on automated highway lane Automatic control of steering and acceleration Driver performing the braking task Vehicle-based monitoring of speed-distance profile with respect to vehicle trajectory	(P_4) [(i) Vehicle failure detected by automatic monitoring devices OR (ii) Deviation of vehicle profile greater than a predefined threshold value OR (iii) Change of exit request received from driver] AND (iv) Vehicle is within a pre-defined distance of the exit ramp	(S_4) Traveling on automated highway lane System reassumes automatic control of braking	(P_4) (i) Vehicle acknowledges request to reassume automatic control of braking AND [(ii) Vehicle failure detected by automatic monitoring devices OR (iii) Deviation of vehicle profile greater than a predefined threshold value OR (iv) Change of exit request received from driver] AND (v) Vehicle is within a pre-defined distance of the exit ramp
(S_4) Traveling on automated highway lane System reassumes automatic control of braking	(P_5) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No detection of collision with infrastructure or another vehicle AND (iii) No report of failure received from driver	(S_5) Merging into dormitory Automatic control of steering, braking, and throttle	(P_5) (i) Vehicle system acknowledges merge request AND (ii) No vehicle failure detected by automatic monitoring devices AND (iii) No detection of collision with infrastrue ture or another vehicle AND (iv) No report of failure received from driver

Table 7. Check-Out Protocol Summary For RSC's 1 and 2 (continued)

Current Vehicle State	Preconditions On Transition to Next Vehicle State	Next Vehicle State	Postconditions On Transition to Next Vehicle State
(S_5) Merging into dormitory Automatic control of steering, braking, and acceleration	(P_6) (i) No crash detected during maneuver AND (ii) Vehicle does not experience braking, steering, or throttle failure	(S_6) Vehicle at rest in dormitory Manual and automated vehicle control systems disabled Driver and passengers in vehicle	(P_6) (i) Vehicle system acknowledges request to shut system down AND (ii) No crash detected during maneuver AND (iii) Vehicle does not experience braking, steering, or throttle failure
(S_3) Vehicle merging onto exit ramp Automatic control of steering and acceleration Driver applying brakes Vehicle-based monitoring of braking rate	(P_7) (i) No vehicle failure detected by automatic monitoring devices AND (ii) Braking rate is neither excessive nor inadequate AND (iii) No detection of collision with infrastructure or another vehicle	(S_7) Vehicle stopping at termination of exit ramp Automatic control of steering and acceleration Driver applying brakes Vehicle-based monitoring of braking rate	(P_7) (i) Driver acknowledges entry onto exit ramp via manual application of brakes AND (ii) No vehicle failure detected by automatic monitoring devices AND (iii) Braking rate is neither excessive nor inadequate AND (iv) No detection of collision with infrastructure or another vehicle

Table 7. Check-Out Protocol Summary For RSC's 1 and 2 (continued)

Current Vehicle State	Preconditions On Transition to Next Vehicle State	Next Vehicle State	Postconditions On Transition to Next Vehicle State
(S_3) Vehicle merging onto exit ramp Automatic control of steering and acceleration Driver applying brakes Vehicle-based monitoring of braking rate	(P_8) (i) Vehicle failure detected by automatic monitoring devices OR (ii) Braking rate is either excessive or inadequate OR (iii) Detection of collision with infrastructure or another vehicle	(S_4) Traveling on automated highway lane System reassumes automatic control of braking	(P_8) (i) Automatic control system acknowledges request for resumption of automatic control of braking AND [(i) Vehicle failure detected by automatic monitoring devices OR (ii) Braking rate is either excessive or inadequate OR (iii) Detection of collision with infrastructure or another vehicle]
(S_7) Vehicle stopping at termination of exit ramp Automatic control of steering and acceleration Driver applying brakes Vehicle-based monitoring of braking rate	(P_9) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No vehicle failure reported by driver or exit gate attendant AND (iii) Vehicle is at rest (i.e., neither accelerating nor decelerating)	(S_8) Vehicle stopped at termination of the exit ramp Automatic vehicle control system disengaged	(P_9) (i) Driver acknowledges hand-off of steering and throttle control AND (ii) Driver continues to manually apply brakes AND (iii) No vehicle failure detected by automatic monitoring devices AND (iv) No vehicle failure reported by driver or exit gate attendant AND (v) Vehicle is at rest (i.e., neither accelerating nor decelerating)

Table 7. Check-Out Protocol Summary For RSC's 1 and 2 (continued)

Current Vehicle State	Preconditions On Transition to Next Vehicle State	Next Vehicle State	Postconditions On Transition to Next Vehicle State
(S_7) Vehicle stopping at termination of exit ramp Automatic control of steering and acceleration Driver applying brakes Vehicle-based monitoring of braking rate	(P_{10}) (i) Vehicle failure detected by automatic monitoring devices OR (ii) Vehicle failure reported by driver or exit gate attendant OR (iii) Vehicle moves forward or backward	(S_9) Merging onto roadway shoulder Automatic control of braking	(P_{10}) (i) Vehicle system acknowledges requests to resume automatic braking and steer vehicle onto roadway shoulder AND [(ii) Vehicle failure detected by automatic monitoring devices OR (iii) Vehicle failure reported by driver or exit gate attendant OR (iv) Vehicle moves forward or backward]
(S_9) Merging onto roadway shoulder Automatic control of braking	(P_{11}) (i) Sufficient braking applied AND (ii) No failure experienced in steering and throttle	(S_{10}) Vehicle at rest on roadway shoulder Manual and automated vehicle control systems disabled Driver and passengers in vehicle	(P_{11}) (i) Vehicle system acknowledges system shutdown command AND (ii) Sufficient braking applied AND (iii) No failure experienced in steering and throttle

Table 8. Check-Out Protocol Summary For RSC 3

Current Vehicle State	Preconditions on Transition to Next Vehicle State	Next Vehicle State	Postconditions on Transition to Next Vehicle State
(S_1) Traveling on automated highway lane Automatic control of steering, braking, and acceleration	(P_1) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No exit request received from driver	(S_1) Traveling on automated highway lane Automatic control of steering, braking, and acceleration	(P_1) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No exit request received from driver
(S_1) Traveling on automated highway lane Automatic control of steering, braking, and acceleration	(P_2) (i) No vehicle failure detected by automatic monitoring devices AND (ii) Exit request received from driver AND (iii) Space available to merge onto transition lane	(S_2) Merging onto transition lane Automatic control of steering, braking, and acceleration	(P_2) (i) Vehicle system acknowledges request to initiate merge maneuver AND (ii) No vehicle failure detected by automatic monitoring devices AND (iii) Exit request received from driver AND (iv) Space available to merge onto transition lane
(S_2) Merging onto transition lane Automatic control of steering, braking, and throttle	(P_3) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No detection of collision with infrastructure or another vehicle AND (iii) No report of failure received from driver	(S_3) Traveling on transition lane Automatic control of steering, braking, and throttle	(P_3) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No detection of collision with infrastructure or another vehicle AND (iii) No report of failure received from driver

Table 8. Check-Out Protocol Summary For RSC 3 (continued)

Current Vehicle State	Preconditions on Transition to Next Vehicle State	Next Vehicle State	Postconditions on Transition to Next Vehicle State
(S_3) Traveling on transition lane Automatic control of steering, braking, and throttle	(P_4) (i) Vehicle control system receives automated sensor input on vehicle acceleration-deceleration profile AND (ii) Vehicle profile satisfies observed traffic flow	(S_4) Traveling on transition lane Driver performing steering task Automatic control of brakes and throttle	(P_4) (i) Driver acknowledges request to begin manually steering vehicle AND (ii) Receive automated sensor input on vehicle acceleration-deceleration profile AND (iii) Vehicle profile satisfies observed traffic flow
(S_2) Traveling on transition lane Automatic control of steering, braking, and acceleration	(P_5) (i) Automated sensor input on vehicle acceleration-deceleration profile is not received OR (ii) Vehicle profile does not satisfy observed traffic flow	(S_5) Merging into dormitory Automatic control of steering, braking, and throttle	(P_5) (i) Vehicle system acknowledges request to perform merge maneuver AND [(i) Automated sensor input on vehicle acceleration-deceleration profile is not received OR (ii) Vehicle profile does not satisfy observed traffic flow]
(S_5) Merging into dormitory Automatic control of steering, braking, and acceleration	(P_6) (i) Continued application of brakes by automated control system AND (ii) No failure experienced in steering and throttle AND (iii) No collision between vehicle and either the infrastructure or another vehicle	(S_6) Vehicle at rest in dormitory Manual and automated vehicle control systems disabled Driver and passengers in vehicle	(P_6) (i) Vehicle responds to system shutdown request (ii) Continued application of brakes by automated control system AND (iii) No failure experienced in steering and throttle AND (iv) No collision between vehicle and either the infrastructure or another vehicle

Table 8. Check-Out Protocol Summary For RSC 3 (continued)

Current Vehicle State	Preconditions on Transition to Next Vehicle State	Next Vehicle State	Postconditions on Transition to Next Vehicle State
(S_4) Traveling on transition lane Driver performing steering task Automatic control of brakes and throttle	(P_7) (i) Automatic throttle and steering continue to function properly AND (ii) Receive notification to enter non-automated highway lane AND (iii) Opening in traffic	(S_7) Vehicle entering non-automated lane	(P_7) (i) Automatic throttle and steering continue to function properly AND (ii) Receive notification to enter non-automated highway lane AND (iii) Opening in traffic
(S_7) Vehicle entering non-automated lane	(P_8) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No detection of collision with infrastructure or another vehicle AND (iii) No report of failure received from driver	(S_8) Vehicle traveling on non-automated lane	(P_8) (i) Driver acknowledges receipt of manual control of throttle AND (ii) No vehicle failure detected by automatic monitoring devices AND (iii) No detection of collision with infrastructure or another vehicle AND (iv) No report of failure received from driver
(S_7) Vehicle entering non-automated lane	(P_9) (i) Automatic throttle or steering fails OR (ii) Notification to enter non-automated highway lane is revoked OR (iii) There is no opening in traffic	(S_9) Vehicle aborting entering non-automated lane	(P_9) (i) Vehicle system acknowledges abort maneuver request AND [(ii) Automatic throttle or steering fails OR (iii) Notification to enter non-automated highway lane is revoked OR (iv) There is no opening in traffic]

Table 8. Check-Out Protocol Summary For RSC 3 (continued)

Current Vehicle State	**Preconditions on Transition to Next Vehicle State**	**Next Vehicle State**	**Postconditions on Transition to Next Vehicle State**
(S_9) Vehicle aborting entering non-automated lane	(P_{10}) (i) No vehicle failure detected by automatic monitoring devices AND (ii) No detection of collision with infrastructure or another vehicle AND (iii) No report of failure received from driver	(S_4) Traveling on transition lane Driver performing steering task Automatic control of braking and throttle	(P_{10}) (i) Vehicle system acknowledges abort-maneuver request AND (ii) No vehicle failure detected by automatic monitoring devices AND (iii) No detection of collision with infrastructure or another vehicle AND (iv) No report of failure received from driver
(S_9) Vehicle aborting merging onto non-automated lane	(P_{11}) (i) Vehicle failure detected by automatic monitoring devices OR (ii) Detection of collision with infrastructure or another vehicle OR (iii) Report of failure received from driver	(S_5) Merging into depot Automatic control of steering, braking, and throttle	(P_{11}) (i) Vehicle acknowledges abort-maneuver request AND [(ii) Vehicle failure detected by automatic monitoring devices OR (iii) Detection of collision with infrastructure or another vehicle OR (iv) Report of failure received from driver]

Table 8. Check-Out Protocol Summary For RSC 3 (continued)

Current Vehicle State	Preconditions on Transition to Next Vehicle State	Next Vehicle State	Postconditions on Transition to Next Vehicle State
(S_8) Vehicle traveling on non-automated lane	(P_{12}) (i) No vehicle failure detected by automatic monitoring devices OR (ii) No detection of collision with infrastructure or another vehicle OR (iii) No report of failure received from driver	(S_{10}) Releasing vehicle from automated highway system	(P_{12}) (i) Vehicle and driver initiate handshake to initiate transfer of control AND [(ii) No vehicle failure detected by automatic monitoring devices OR (iii) No detection of collision with infrastructure or another vehicle OR (iv) No report of failure received from driver]
(S_8) Vehicle traveling on non-automated lane	(P_{13}) (i) Vehicle failure detected by automatic monitoring devices OR (ii) Detection of collision with infrastructure or another vehicle OR (iii) Report of failure received from driver	(S_{11}) Merging onto roadway shoulder Automatic control of braking	(P_{13}) (i) Vehicle system acknowledges request to commence automatic braking AND (ii) Vehicle system acknowledges merge request AND [(iii) Vehicle failure detected by automatic monitoring devices OR (iv) Detection of collision with infrastructure or another vehicle OR (v) Report of failure received from driver]

Table 8. Check-Out Protocol Summary For RSC 3 (continued)

Current Vehicle State	**Preconditions on Transition to Next Vehicle State**	**Next Vehicle State**	**Postconditions on Transition to Next Vehicle State**
(S_{10}) Releasing vehicle from automated highway system	(P_{14}) (i) No vehicle braking failure detected by automatic monitoring devices AND (ii) No detection of collision with infrastructure or another vehicle AND (iii) No report of failure received from driver	(S_{12}) Vehicle released from automated highway system Vehicle under full-manual control	(P_{14}) (i) Driver acknowledges hand-off of braking control AND (i) No vehicle braking failure detected by automatic monitoring devices AND (ii) No detection of collision with infrastructure or another vehicle AND (iii) No report of failure received from driver
(S_{10}) Releasing vehicle from automated highway system	(P_{15}) (i) Vehicle braking failure detected by automatic monitoring devices OR (ii) Detection of collision with infrastructure or another vehicle OR (iii) Report of failure received from driver	(S_{11}) Merging onto roadway shoulder Automatic control of braking	(P_{15}) (i) Vehicle system acknowledges merge-maneuver request and braking request AND [(i) Vehicle braking failure detected by automatic monitoring devices OR (ii) Detection of collision with infrastructure or another vehicle OR (iii) Report of failure received from driver]

Table 8. Check-Out Protocol Summary For RSC 3 (continued)

Current Vehicle State	**Preconditions on Transition to Next Vehicle State**	**Next Vehicle State**	**Postconditions on Transition to Next Vehicle State**
(S_{11}) Merging onto roadway shoulder Automatic control of braking	(P_{16}) (i) Continued application of brakes by automated control system AND (ii) No failure experienced in steering and throttle AND (iii) No collision between vehicle and either the infrastructure or another vehicle	(S_{13}) Vehicle at rest on roadway shoulder Manual and automated vehicle control systems disabled Driver and passengers in vehicle	(P_{16}) (i) Vehicle system acknowledges system shutdown command AND (ii) Continued application of brakes by automated control system AND (iii) No failure experienced in steering and throttle AND (iv) No collision between vehicle and either the infrastructure or another vehicle

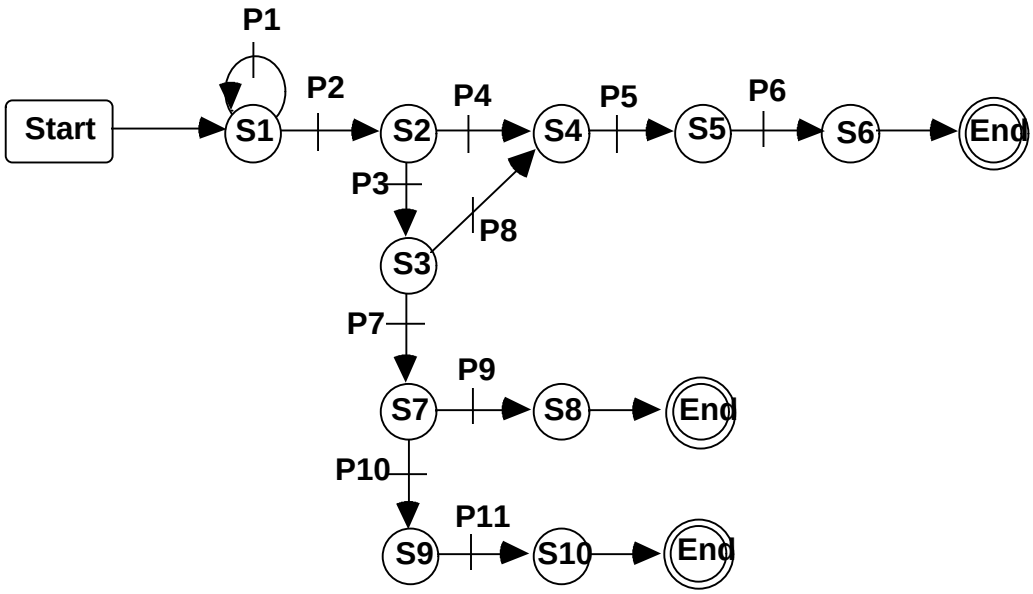

Figure 1. Finite State Machine Representation Of Information Contained In Table 7

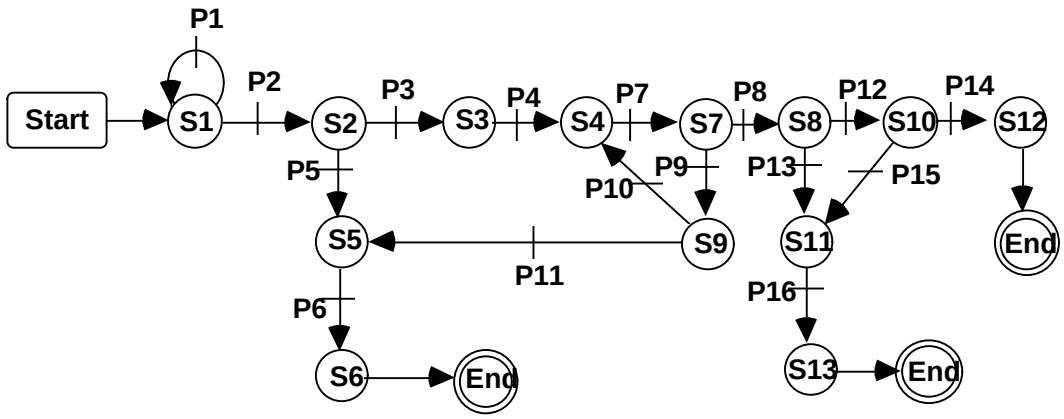

Figure 2. Finite State Machine Representation Of Information Contained In Table 8

Analysis Of Check-Out Protocol For Dedicated Lanes

Although RSC's 1 and 2 both involve dedicated lanes for all aspects of AHS operation, the two RSC's vary as to the location at which various decisions are made. Thus the following analysis will distinguish between RSC 1 and RSC 2.

Vehicle System Decisions

This section is specific to RSC 2 in which check-out decisions are made onboard the vehicles rather than the infrastructure, with a gradual transfer of decision making responsibility to the driver over the course of the check-out process. Note that a vehicle system is not responsible for making any check-out decisions in S_6 (shutdown mode), S_8 (full manual control), and S_{10} (shutdown mode).

S_1: The vehicle system is responsible for monitoring and controlling the steering, braking, and throttle systems. On receipt of a request from the driver to commence an exit maneuver from the automated highway, the vehicle system must decide whether to transfer control of the braking system to the driver. The decision to begin the exit maneuver is based on information about the current status of the vehicle control system, in terms of the detection of faults, and the acknowledgment by the driver that he or she accepts control of the braking function. If the vehicle system receives a false alarm regarding a vehicle system fault, then the vehicle will deny the exit request and take actions to maneuver the vehicle off of the automated lane, either onto the roadway shoulder or into a depot. This can expose the vehicle occupants and other AHS users to unnecessary levels of risk. The abort maneuver is

hazardous in its own right, and in combination with environment conditions (e.g., wet pavement or debris on the shoulder), can result in an accident. On the other hand, a missed detection can result in the vehicle system granting the exit request, placing the AHS in a hazardous state. In this scenario, the level of risk is a function of the severity of the fault and the impact on check-out decisions made on incomplete information, rather than on incorrect information.

S_2: The vehicle system is responsible for monitoring and controlling the steering and throttle systems. Although braking is being performed by the driver, the vehicle system retains responsibility for monitoring braking behavior. In the case of a false alarm, the vehicle system will abort the planned maneuver onto exit ramp. A missed detection will result in the vehicle system deciding to follow through the lane change maneuver. The consequences of these two scenarios are analogous to those discussed for S_1.

S_3: The vehicle system is responsible for monitoring and controlling the steering and throttle systems. The vehicle system also must decide whether or not to resume automatic control of braking. All of these decisions are made in parallel, and require some level of coordination between the individual vehicle control systems (e.g., lateral, longitudinal, and lane change maneuver planner). No coordination is required with the driver. A false alarm or missed detection can have consequences analogous to those discussed for S_1 and S_2.

S_4: The vehicle system is responsible for monitoring and controlling the steering and throttle systems. The vehicle system also must decide whether or not to merge into a depot. As in S3, all of these decisions must be made in parallel with some level of coordination between the components of the vehicle control system.

S_5: Unlike S3 and S4, the vehicle system must retake responsible for monitoring and controlling the braking system, as well as decide at what instant to shut down the vehicle system.

S_7: The vehicle system is responsible for monitoring and controlling the steering and throttle systems. The vehicle system must also decide whether to abort the exit maneuver and steer the vehicle to the roadway shoulder, or continue to the exit gate while disengaging the automatic vehicle controls. In this state there needs to be some coordination between the vehicle system and the driver during the hand-off of controls. A missed detection can have adverse effects on the controllability of the vehicle, either under manual or automated

control, with no warning given to the driver. A false alarm can cause the vehicle system to unnecessarily abort the exit manuever.

S_9: The vehicle system is responsible for monitoring and controlling the steering and throttle systems, and must decide when to disable the manual and automatic vehicle system. Certain types of sensor data can be ignored in this state since the vehicle is being brought to a halt. However, some types sensor data is critical to vehicle control until the vehicle is brought to rest. Thus, missed detections and false alarms cannot be disregarded even in this state.

Infrastructure Decisions

In RSC 1, the decisions described above will be carried out by the infrastructure. One of the important concerns here is the potentially large number of sensors and high communications bandwidth required to effect vehicle control, with additional capacity needed to process check-out decision rules. Whether such an AHS configuration is technically feasible or economically justified needs to be studied further.

There is a requirement for low-level coordination between the infrastructure and the vehicle, but essentially no coordination between the infrastructure and the driver except in states S_1, S_7, and S_8.

Driver Decisions

For this analysis we assume that the driver is responsible for providing the AHS with an exit request at some point in time after successfully checking into the AHS. Note that the driver is not responsible for making any vehicle control decisions in S_2 through S_6, S_9, and S_{10} (shutdown mode). In S_2 through S_7, the driver performs the braking function, but either the vehicle (in RSC 2) or infrastructure (in RSC 1) is responsible for making vehicle control decisions based on the monitoring of brake system performance and the driver's application of the brakes during the check-out process.

S_1: The driver is responsible for providing the vehicle (in RSC 2) or infrastructure (in RSC 1) with the an exit maneuver request. No prior coordination with the vehicle or infrastructure is required. A false alarm or missed detection is handled by the vehicle or infrastructure, unless the vehicle or infrastructure experiences a catastrophic failure. However, from a safety and human factors perspective, the driver is probably not prepared to retake complete or even partial control of the vehicle, even if the automatic control system actuators can be disabled

(i.e., the actuators can also fail). The rate at which decisions need to be made is probably greater than the driver can handle. However, if the AHS configuration provides for some form of degraded mode of operation in which only some of the check-out decisions need to be made by the driver, then the driver may be able to respond to sensory input in time to avoid a crash or minimize the severity of a crash.

S_7: The driver must either accept or reject the hand-off of manual control of the vehicle. This is the only state in which the driver must explicit coordinate with the vehicle system or infrastructure. The driver must respond in a predefined amount of time, or the vehicle system will unilaterally decide to abort the hand-off of control. The driver must also concurrently generate a plan to maneuver the vehicle to the exit gate. If the driver has received too many false alarms in the past, he or she may ignoring the fault warnings or become dissatisfied with the service provided by the AHS. Missed detections put the driver at risk, as described in S_1.

S_8: The driver must decide whether to proceed through the exit gate onto the manual highway. At this point, the driver can make decisions in a serial manner since his or her vehicle is not moving. There is no coordination with the vehicle or infrastructure. However, he or she is under some soft time constraint in that the vehicle must not be permitted to remain in at the gate for an indefinite period of time. Thus, there must be some means for a driver to move his or her vehicle to a resting area before proceeding on the manual highway. Otherwise the exit ramp can experience congestion and cause other vehicles to experience delay in exiting the automated highway.

Exit Gate Attendant Decisions

The driver is not responsible for making any vehicle control decisions in S_1 through S_6, S_9 , and S_{10}. In S_7 and S_8, he or she is responsible for reporting instances of vehicle/infrastructure failure, or driver error. Missed detections can occur due to poor visibility (e.g., fog), inattention (e.g., falling asleep due to boredom), and so on. If the exit gate attendant has generated false alarms in the past, this can affect his or her decision to report perceived or actual faults in the future, thus increasing the missed detection rate. Also, the velocity of the vehicle should be commensurate with the ability of the exit gate attendant to both make observations he or she is responsible for conducting and decide whether the vehicle should proceed to the exit gate or abort the exit. An AHS configuration can include

electromechanical devices to assist the attendant in making timely and accurate observations of approaching vehicles, in support of the decision making process.

Analysis Of Check-Out Protocol For Mixed Flow Lanes

One of the ways in which this protocol differs from that for dedicated lanes is that there is no exit gate per se, but rather transition and non-automated lanes which vehicles use during the check-out process. Hence, there is no provision for an exit gate attendant.

Vehicle System Decisions

No check-out decisions are made by the vehicle in S_6 (shutdown mode), S_{12} (full manual control), and S_{13} (shutdown mode). Thus, there is no coordination necessary with the driver or infrastructure in these states, except in S_{12} if the driver tries to re-engage the automatic vehicle control system, which should be denied unless the vehicle goes through the check-in process again; that is, there is only one possible decision outcome in that particular scenario.

S_1: The vehicle system is responsible for monitoring and controlling the steering, braking, and throttle systems. The decisions are made in parallel and under real-time constraints, and the consequences are essentially the same as those described for the dedicated lanes check-out protocol in the case of missed detections and false alarms.

S_2: The vehicle system is responsible for monitoring and controlling the steering, braking, and throttle systems. The system must also decide whether to abort the exit and steer the vehicle into the depot. No coordination is required between the vehicle system and the user.

S_3: The vehicle system is responsible for monitoring and controlling the steering, braking, and throttle systems. The vehicle system is responsible for deciding whether to transferring control of the steering to the driver. The hazards associated with missed detections and false alarms are similar to those discussed for the vehicle in the analysis of the protocol for dedicated lanes.

S_4: The vehicle system is responsible for monitoring and controlling the braking and throttle systems. It is also responsible for deciding whether to maneuver the vehicle into the non-automated lane. The AHS hazardous associated with the outcome of this decision differ from that of the dedicated lanes check-in protocol in that there is some coordination required

between the vehicle system and that of other vehicles already traveling in the non-automated lane. Thus a missed detection can result in a crash or near miss. Similarly, a false alarm will cause the vehicle to abort the exit maneuver, but still require the vehicle to eventually merge into the non-automated lane and eventually into a depot or the roadside. If one of the degraded modes involves the release of vehicle control to the driver while the vehicle is still on the automated lane, this can be viewed as placing the driver and other AHS users at unnecessary risk. That is, the driver will have to execute potentially complex decision rules and possibly at high rates in order to safely maneuver his or her vehicle off of the high-performance automated lane.

*S*5: The vehicle system is responsible for monitoring and controlling the steering, braking, and throttle systems. A unilateral decision is made by the vehicle as to when to shut down the automatic and manual vehicle controls.

*S*7: The vehicle system is responsible for monitoring and controlling the braking and throttle systems. The vehicle is also responsible for decide whether to release the throttle task to the driver, or to abort the maneuver to enter the non-automated lane. The risks are similar to those previously discussed for the vehicle system in the dedicated lanes analysis. However, a notable difference in the decision-making process is that the locus of decision making is gradually shifting to the driver. At this state, a portion of the monitoring and control are no longer the responsibility of the vehicle system. However, the complexity of control and planning functions has actually increased due to the need for coordination between the vehicle system and driver in making decisions, specifically plans for executing various types of maneuvers.

*S*8: The vehicle system is responsible for monitoring and controlling the braking system and deciding whether to release the vehicle from AHS.

*S*9: The vehicle system is responsible for monitoring and controlling the braking and throttle systems. It is also responsible for deciding whether to merge into a depot in order to aborted an exit maneuver. The decision rules processed during this state can be complex, since entry into a depot will involve consideration of factors such as:

- Whether or not the depot full.

- Whether or not the vehicle can continue to operate in a degraded mode until it reaches the depot without posing unacceptable risks with respect to the safety of other AHS users.

In addition to coordination between the vehicle system and the driver, some level of coordination between drivers or vehicle system to negotiate the use of the depot or lane space for a maneuver (e.g., two or more vehicle systems detect internal faults).

S_{10}: This state is similar to that of S9; only the decisions are slightly different: the vehicle system is responsible for monitoring and controlling the braking system, and the vehicle system is responsible for deciding whether to hand-off control of the braking task to the driver or deny the request and maneuvering vehicle to the shoulder of the roadway. The difference here is that the vehicle must retake control of the steering function from the driver in order to abort the exit maneuver, resulting in a sudden increase in the computing necessary to perform the data sensor fusion task.

S_{11}: The vehicle system is responsible for monitoring and controlling the braking system, and for deciding when to shut down the vehicle system. These decisions are made unilaterally by the vehicle system.

Infrastructure Decisions

As described in the analysis of protocol for dedicated lanes, one of the important concerns here is the potentially large number of sensors and high communications bandwidth required to effect vehicle control, with additional capacity needed to process check-out decision rules. Whether such an AHS configuration is technically feasible or economically justified needs to be studied further.

Driver Decisions

For this analysis we assume that the driver is responsible for providing the AHS with an exit request at some point in time after successfully checking into the AHS. Note that the driver is not responsible for making any vehicle control decisions in S_2, S_5, S_6 (shutdown mode), and S_{13} (shutdown mode).

S_1: The driver must decide whether to issue an exit request. As in the analysis relating to dedicated lanes, the driver need not coordinate with the vehicle or infrastructure prior to

making an exit request. A false alarm or missed detection is handled by the vehicle or infrastructure, unless the vehicle or infrastructure experiences a catastrophic failure. However, from a safety and human factors perspective, the driver is probably not prepared to retake complete or even partial control of the vehicle, even if the automatic control system actuators can be disabled (i.e., the actuators can also fail). The rate at which decisions need to be made is probably greater than the driver can handle. However, if the AHS configuration provides for some form of degraded mode of operation in which only some of the check-out decisions need to be made by the driver, then the driver may be able to respond to sensory input in time to avoid a crash or minimize the severity of a crash.

S_3: The driver is responsible for deciding whether to accept control of the steering task. If the driver decides to do so, he or she is responsible for making steering control decisions (i.e., S_4, S_7, S_8, S_9, S_{10}, S_{11}, and S_{12}) as well as coordinating with the vehicle control system and/or infrastructure in making future decisions.

S_7: This state involves three distinct decisions:

- Whether to report observed or inferred vehicle or infrastructure failures, the driver is part of the control loop in this protocol. The problem of false alarms faced by the exit gate attendant in the dedicated lanes check-out protocol are similar to those for the driver in this AHS state. Too many false alarms can result in other drivers ignoring fault warnings.
- Steering decisions.
- Whether to accept control of the throttle system - this adds to the number of concurrent decisions the driver must make in future states during the check-out process.

Missed detections put the driver and other AHS users at risk since they, possibly in combination with false alarms, complicate the decision-making process.

S_8: In this state the driver must make steering and throttle decisions and report observed or inferred vehicle or infrastructure failures. The hazards and decision-making environment are similar to those described in S_7.

S_9: The driver is responsible for monitoring and controlling vehicle steering.

S_{10}: The driver is responsible for monitoring and controlling vehicle steering and throttle. The driver is also responsible for making a decision as to whether to accept control of the braking task. The hazards and decision-making environment are similar to those described in S_7.

S_{11}: The driver is responsible for monitoring and controlling the steering and throttle systems, but this differs from the situation in S_{10} in that the driver is responsible for coordinating with the vehicle control system the actions necessary to safely abort the exit maneuver. The complexity of the coordination task is a function of rate at which these decisions need to be made and the complexity of the decisions rules. Missed detections of vehicle control system faults can result in the driver making coordination decisions resulting in system hazards, such as the steering too hard to the right while the automatic control of the braking system has experienced a fault. Alternatively, given a false alarm about the status of the brakes, the driver can make decisions that result in an under or over steering or application of the throttle.

S_{12}: The driver is responsible for monitoring and controlling the steering, throttle, and braking systems. This involves the decisions performed by drivers on existing highways under normal driving conditions.

Observations

There is an implicit safety policy embedded in these protocols that requires a vehicle to abort an exit maneuver if a fault is detected, regardless of whether the fault detection represents a false alarm. It can be perceived to be a prudent strategy to always err on the side of safety rather than permitting the vehicle, infrastructure, driver, or exit gate attendant to further expose themselves to potential or actual hazards. However, there are hazards involved in aborting an exit maneuver which in turn raise liability issues, and costs associated with handling detained vehicles and closed segments of the infrastructure, including the potential for loss of goodwill resulting from user dissatisfaction with the AHS.

The impact of the check-out protocols on the RSCs can be viewed from the perspective of the coordination of decision-making tasks among the vehicle system, infrastructure, driver, and exit gate attendant. Check-out decisions are tightly coupled with vehicle control decisions in all three RSC’s, however, the level of coordination required among the humans

and the AHS varies from one RSC to another, and from state to state within an RSC. This is exemplified by the following:

- Transfer of decision-making tasks, in terms of check-out roles and responsibilities, from one party to another.
- Interdependencies between roles and responsibilities, in terms of information exchange supporting decision making, for executing check-out plans (including plans for aborting an exit maneuver).

From the perspective of RSC 2 and RSC 1, the dedicated lanes protocol places most of the burden for decision-making and coordination on the vehicle and infrastructure, respectively. In contrast, the driver is assigned more decision-making tasks under the mixed flow lanes protocol than under the dedicated lanes protocol. From this fact we can infer that the level of coordination required among the vehicle system, infrastructure, and driver is greater in the mixed flow lanes protocol than for the dedicated lanes protocol. We can also infer that the volume and rate of communication will differ between these two protocols with regard to coordination, all other things being equal.

The complexity of the check-out decision rules and the rate at which these rules must be executed should be congruent with the abilities of the decision maker. The vehicle system and infrastructure are in general more efficient than drivers and exit gate attendants at the following:

- Processing sensor data and complex decision rules.
- Transmitting the results of processing.
- Performing multiple decision-making tasks currently.

Thus, relying primarily on the human to make check-out decisions can result in the driver or gate attendant not being able to make or coordinate check-out decisions within real-time constraints. The need for parallel execution and strict timing of check-out decisions is related to such factors as the velocity of the vehicle with respect to the characteristics of the exit ramp (in the dedicated lanes check-out protocol), transition and non-automated lanes (in the mixed flow lanes check-out protocol), and roadway shoulders and dormitories.

The division of check-out roles and responsibilities between the human and AHS also have implications on the man-machine interface. The design of the man-machine interface can

affect the efficiency and effectiveness of the check-out decision-making process, with regards to the driver viewing, interpreting, and responding to input provided by interface via, for example, a head-up display.

It is hard to say what the weakest link is for either of the protocols. From a decision-making perspective, it can be argued that the sensor represents a weak system link. If a sensor fails to detect a vehicle fault or human error, raises false alarms, or completely fails, the human and AHS will have to rely on other sources of information for making decisions. Therefore, fault tolerance can be an important issue in the design of the sensor system with respect to check-out policies and requirements. Other examples of weak links in the context of check-out activities include the following:

- Human: The driver or exit gate attendant can be incapacitated (i.e., ill, drunk, or frightened) and therefore unable, unwilling, or not ready to carry out a decision-making task, or alternatively, intentionally, or unintentionally make bad decisions.
- Vehicle System: The vehicle system can experience catastrophic faults, in some cases requiring the driver to make check-out decisions with incomplete or incorrect information and potentially little or no experience driving under high-performance conditions.
- Infrastructure: Some part of the infrastructure that is critical to the check-out process can fail, requiring either the vehicle system or human to take over responsibility for making check-out decisions.

Based on our observations of the distribution of check-in decision-making tasks among the human, vehicle system, and infrastructure, the mixed lane check-in protocol is much easier to redesign than the dedicated lanes check-in protocol in terms of providing for the transfer of decision-making tasks. In RSC 1 and RSC 2, if the infrastructure or vehicle experiences faults, then there is only the human to rely on to make check-out decisions, whereas these responsibilities are already shared in by these three parties in RSC 3.

Summary

Assessment of tradeoffs between alternative AHS check-out protocols will involve consideration of issues involving

- Decision support: What will be the partitioning of decision responsibilities between the vehicle system, infrastructure, and human? Is the check-out protocol congruent with the

responsibilities assigned to each of these entities? What level of coordination is necessitated by a particular check-in protocol with respect to a specific RSC?

- Mission effectiveness: Can the check-out protocol be used to achieve the desired probability of fault detection? Where should the system automation boundary be drawn with regard to decision making tasks performed as part of the check-out process?
- Safety: What are the tolerable rates of false alarms and missed detections? What affect will the check-out safety policies have on such things as goodwill and liability?
- Cost: What is the appropriate balance between the cost of an AHS fault detection mechanism and the corresponding rates of fault detections and false alarms? What are the costs associated with implementing and maintaining check-out protocols?

Further study is required to address these issues. In addition, experimentation with AHS technology is necessary in order to obtain estimates of fault detection performance probabilities and a more in-depth understanding of the relationship between check-out decision-making tasks and AHS configurations.

CONCLUSIONS

The transition from automated control to manual driving must follow a progression of steps that ensures the safety of the driver and surrounding vehicles in the AHS and non-AHS lanes. Potential check-out protocols must be capable of maintaining safety in a cost effective manner while considering the technical feasibility and user appeal of the procedure. The check-in process used to validate the transition from manual to automated control has often been considered to be a vehicle-intensive task, while the check-out process used to validate the transition to manual from automatic has been considered as operator intensive. This assumption focuses on the functionality of the automated control systems as the vehicle enters the AHS, and the qualifications of the driver to regain manual control as the vehicle exits the automated lanes. This study has determined that vehicle functional verification is also required to ensure a safe transition to manual control. It is recommended that the manual braking and steering functions be exercised prior to termination of automated control as a minimum. These two functions are critical to safe operation at the time that control of the vehicle is given to the driver.

The impact of a specific check-out procedure on the system configuration can be viewed from the perspective of coordinating decision-making tasks among the vehicle system, infrastructure, driver, and exit facility. The dedicated lanes protocol places most of the burden for decision-making and coordination on the vehicle and infrastructure. In contrast, the driver is assigned more decision-making tasks under the mixed flow lanes protocol. The level of coordination required among the vehicle system, infrastructure, and driver is greater in the mixed flow lanes protocol than for the dedicated lanes protocol. The complexity of the check-out decision rules and the rate at which these rules must be executed should be consistent with the abilities of the decision maker. The vehicle system and infrastructure are typically more efficient than humans at processing sensor data and complex decision rules, transmitting the results of processing, and performing multiple decision-making tasks currently.

The result of reliance on the human to make check-out decisions may be inability of the driver or gate attendant to make or coordinate check-out decisions within real-time constraints. The need for parallel execution and strict timing of check-out decisions is related to such factors as the velocity of the vehicle with respect to the characteristics of the exit ramp (in the dedicated lanes check-out protocol), transition and non-automated lanes (in the mixed flow lanes check-out protocol), and roadway shoulders and depots. The division of check-out roles and responsibilities between the human and AHS also affects design of the man-machine

interface. The efficiency and effectiveness of the check-out decision-making process depends on the ability of the driver to view, interpret, and respond to inputs.

The check-out protocols proposed for dedicated and non-dedicated exit scenarios assume that the exit maneuver is aborted if a fault is detected, regardless of whether the fault detection represents a false alarm. A conservative check-out policy may ensure safety at the risk of introducing liability issues, and will increase costs associated with handling detained vehicles and closed segments of the infrastructure. The potential for loss of goodwill resulting from user dissatisfaction with the AHS must also be considered.

The topic of storing vehicles which fail vehicle or operator validation procedures has extensive implications in terms of roadway deployment. There are multiple design issues associated with the use of depots or shoulders to temporarily store vehicles. The storage system design is based on the expected number of users and the duration of use. Construction and operational costs and land use issues are primary considerations in determining the effectiveness of storage areas. Vehicle diversion to centralized storage facilities is an option which may alleviate design issues concerning land usage, occupancy levels, and operating costs at the risk of causing poor user acceptance. The disposition of vehicles disqualified from manual operation will be a key consideration in the design of the check-out procedure.

The issue of driver readiness to resume manual control is related to issues of privacy and liability. There is a broad range of tests available to verify driver capabilities, including sensors to detect the presence of substances in the driver's blood, prompts to gauge reaction times, or scanning of eye movement to evaluate alertness. The invasiveness of certain tests may cause concerns among privacy advocates and have an adverse effect on user acceptance. The assignment of liability in the event of an incident following the transition to manual control is a concern as well. Extensive tests may create the impression that the AHS is responsible for ensuring that no impaired drivers are allowed to have manual control. It is recommended that the driver check-out consist of a simplified routine that places the responsibility for assuming manual control completely with the driver. The check-out process might follow a screening of manual brake and steering functionality with a prompt to the driver. The driver will then respond with a positive action such as pressing a push-button to indicate readiness to assume control. Legislation may be required to clearly delineate the responsibility for accidents following transition from the automated lanes.

Eliminating complex operator verification tests and placing responsibility with the driver for accepting the manual driving task is one way to simplify the issue and reduce the risk of AHS being held liable for accidents caused by improper driving immediately following travel in the automated lanes. This approach is based on the premise that the AHS is not responsible for verifying driver readiness to safely operate the car prior to entering the AHS, and returning control to the driver following automated travel should not carry a burden beyond that of ensuring that the vehicle is functioning properly.

BIBLIOGRAPHY

1. Delco Systems Operations, Activity B Report: “Automated Check-In, AHS Precursor Systems Analysis,” November 1994.

2. Delco Systems Operations, Activity J Report: “AHS Entry/Exit Implementation, AHS Precursor Systems Analysis,” November 1994.

3. “Entrepreneur Seeks Funding to Manufacture DWI Warning System,” Inside IVHS, 14 March 1994.

4. S. Stahl and M. E. Thyfault, “About-Face on Clipper?,” Information Week, 8 August 1994.