Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Vehicle Operational Analysis

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-95-099
December 1994

FOREWORD

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

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

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

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

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

NOTICE

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

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

EXECUTIVE SUMMARY

This report is part of the Precursor Systems Analysis study sponsored by the Federal Highway Administration. The contractor is Raytheon Company with a subcontract to SSC Systems (formerly PI Controls) who is solely responsible for performing the work on activity area L, entitled Vehicle Operational Analysis, by working together with Ford Motor Company researchers. The Principal Investigator is Dr. Petros Ioannou, who is assisted by the investigators Mr. Alex Kanaris, Dr. Tom Xu, Mr. Humair Raza, and Ford Motor Company researchers Dr. Michael Shulman and Dr. Steven Eckert.

The report deals with the analysis of the issues and risks associated with the development, operation and deployment of vehicles for five representative system configurations (RSCs) of automated highway systems (AHS).

The RSCs are chosen so that they follow an evolutionary path with respect to automated vehicle and roadway functions. For this reason the RSCs are referred to as evolutionary representative system configurations (ERSCs). ERSC 1 employs a dedicated lane where vehicles have the capability to maintain speed and headway and the vehicle speed is dictated by the roadway. The driver is responsible for steering and collision avoidance. In ERSC 2 the vehicle takes over the responsibility of rear-end collision avoidance leading to a full authority longitudinal controller with the driver still responsible for steering. The driver function to keep the vehicle in the center of the lane is given to the vehicle in ERSC 3 while the driver is still responsible for lane changing. In ERSC 4 the lane changing function is automated and the vehicle is fully automated with self-guiding and navigation capabilities. Multiple lanes are introduced in ERSC 4. In ERSC 5 the roadway is responsible for vehicle guidance and navigation by issuing lane change, check-out and exit commands to each vehicle in order to optimize the traffic flow. One can also view the proposed ERSCs as degraded modes of operation of a fully automated vehicle roadway system. Such degraded modes of operation could be unavoidable because no system could work with optimum performance all the time and under all environmental and roadway conditions. For each ERSC, we assume that each vehicle is autonomous with respect to safety. In other words the vehicle does not rely on the roadway or other vehicles to guarantee its safety but rather uses its on board sensors and intelligence to protect itself from colliding with other vehicles or obstacles. The vehicle functions for each ERSC are designed to provide collision free vehicle following operation under normal conditions. Since no small DV collisions are allowed, the organization of vehicles in platoons of specified size with very short headways is considered to be unnecessary and has not been studied.

The emphasis of the report is on the analysis of issues for each ERSC that are associated with reliability and safety, maintainability, vehicle and driver diagnostics, retrofitting of vehicles that were produced before the vehicles for AHS were developed and deployment scenarios.

An operational scenario for each ERSC is developed and used to identify the vehicle functions and interface with the driver and roadway and specify the functional requirements. A distinction is drawn between faults, the inability of a component to perform its mission, and failures, the inability of a system to perform its mission. For each ERSC, a set of functional and reliability requirements is developed; the system should be designed to employ sufficient redundancy to always satisfy these requirements, even in the presence of faults. From these requirements, a preliminary system level design is developed. A system level failure modes and effects analysis (FMEA) is used to identify the potential failure modes, their potential causes and effects and their severity and occurrence ratings for each ERSC. The FMEA represents a list of design requirements and recommendations that can be used to reduce the severity and occurrence rating of failure modes by using redundancies, on board diagnostics and by redesigning certain vehicle and roadway functions.

The key results of this study are:

- The vehicle reliability requirements increase considerably as the level of vehicle automation increases from one ERSC to the next. In order to meet these requirements a considerable number of redundancies and diagnostics need to be introduced that will make the vehicle highly complex.

- A large number of technical issues need to be resolved before deploying a full authority longitudinal controller or an automated lane keeping controller or a full authority lateral controller.

- Despite the availability of several sensors for intelligent cruise control, sensor technology is still not mature enough to meet the functional and reliability requirements involved in the implementation of a full authority longitudinal control.

- Automated lane keeping shall keep the vehicle in the center of the lane under all highway speeds, environmental and traffic conditions and roadway configurations. This requirement cannot be met with today's "affordable" sensor technology despite the reported success of several lane keeping experiments.

- Automated lane changing is one of the most difficult functions due to the tremendous sensor requirements involved. The sensors have to cover a wide field of view, process information fast and distinguish between threatening and non threatening situations. Emulating the human driver's senses in this case is a challenging technical problem that needs to be resolved. Vehicle to vehicle communications may be necessary in addition to all other sensor requirements in order to resolve the problem at least theoretically. The use of a large bandwidth communication system may be necessary in order to meet all the functionality requirements.

- Collision avoidance is another important function that involves serious issues and risks. In ERSC 4, 5 where vehicles change lanes automatically calculating the time to collision and distinguish between threatening and non threatening vehicles or obstacles is a difficult if not impossible task. In such an environment any vehicle in the vicinity could be classified as threatening. The use of vehicle to vehicle communications may help alleviate some of the problems but it is not clear whether all the reliability requirements can be met.

- The routing and navigation of each vehicle by the roadway in ERSC5 requires the processing of a large amount of data that calls for large and fast computers. The optimization of traffic flow by controlling the motion of each vehicle in the dynamic environment of ERSC5 could prove to be an intractable problem. Suboptimal and decentralized control techniques may be more feasible and need to be studied.

- The choice of a safe headway to be used for vehicle following so that no rear-end collision takes place when the preceding vehicle applies its brakes during emergencies depends on a lot of factors that include the braking capabilities of the vehicles involved, sensor/actuator characteristics, the friction coefficient between tires and the road etc. The reliable on-line measurement of these factors is an issue that needs to be resolved. A conservative choice may lead to a large headway that will affect capacity and efficiency whereas a short headway will have a negative impact on safety. For ERSC 2 to ERSC 5 we assume that the vehicle selects the headway by taking into account all relevant factors obtained through measurements and vehicle to vehicle communication. This raises several liability issues that need to be resolved.

- Due to the overwhelming technical issues involved in the development and deployment of fully automated vehicles, vehicle control will follow an evolutionary path. The vehicle for ERSC 1 is a natural evolution of the current vehicles and could be used in a first deployment stage of AHS. For such a deployment to be possible the government has to work closely with the automobile manufacturers in order to establish standards and resolve potential liability issues.

- The evolution of vehicle functions from ERSC 1 to ERSC 5 does not imply that vehicles built for a lower ERSC can be upgraded to be used at a higher ERSC. The design and reliability requirements differ from one ERSC to another considerably. As a result each ERSC calls for new designs, vehicle functions, subsystems, and components.

- Every vehicle function that affects the motion of the vehicle and/or has an impact on safety has to be designed so that it never puts the driver in a situation he/she cannot handle. Such situations were identified in ERSC 2 and ERSC 3 and modification of the vehicle and roadway functions were proposed to eliminate them.

- Every vehicle function that affects the motion of the vehicle has to be protected with redundancies and on board diagnostics. As a result elaborate and time consuming check-in tests at the entrance to AHS may not be necessary.

- Current vehicle electronics are designed to be maintenance free for most of the life of the vehicle e.g. 10 years or 150,000 miles. This trend is expected to continue with vehicles for AHS where the number of electronic components will be considerably higher.

- The retrofitting to vehicles that were produced before vehicles for each ERSC were developed even though technically feasible is going to be expensive. It is unlikely that it will be acceptable to users and automobile manufacturers.

- All the ERSCs call for an integration of the vehicle automated functions with the roadway functions in order to improve traffic flow efficiency. For such an integration to be possible the government has to work closely with the automobile manufacturers.

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Symbols

ABS	Anti-lock Braking System
A.C.	Air Conditioning
AHS	Automated Highway Systems
BSW	Blind Spot Warning
DV	Relative velocity at point of rear-end collision
E/D	Enable/Disable
ERSC	Evolutionary Representative System Configuration
ERSCs	Evolutionary Representative System Configurations
FMEA	Failure Modes and Effects Analyses
HOV	High Occupancy Vehicles
LCW	Lateral Collision Warning
LDW	Lane Departure Warning
LK	Lane Keeping
MTTF	Mean Time To Failure
O	Occurrence rating
RECA	Rear-End Collision Avoidance
RECW	Rear-End Collision Warning
RPN	Risk Priority Number
RSCs	Representative System Configurations
S	Severity rating
SHM	Speed and Headway Maintenance
SPD	Speed Position Destination
TLC	Time to Lane Crossing
TTC	Time To Collision
VOA	Vehicle Operational Analyses
W	Warning

SECTION 1 INTRODUCTION

Vehicle operation analysis deals with the study and analysis of the operational issues and risks associated with the development, operation and deployment of vehicles for the chosen representative system configurations (RSCs) of automated highway systems (AHS). The study includes issues related to reliability, maintainability, vehicle and driver diagnostics, retrofitting of vehicles that were produced before vehicles for AHS were developed and the evolution of vehicles to fully automated ones for AHS.

The purpose of this effort is to study and analyze the operational issues and risks associated with the development, operation and deployment of vehicles for five different RSCs. The RSCs are chosen so that they follow an evolutionary path with respect to automated vehicle and roadway functions. For this reason we refer to them as evolutionary representative system configurations (ERSCs). The ERSCs allow us to study the vehicle operational issues associated with AHS in an incremental fashion starting from partial automation, close to today's driving, and building towards a fully automated vehicle/roadway system. The ERSCs could also represent stages of implementation of AHS. For this reason, each ERSC is chosen based on the complexity of the issues involved, the feasibility of technology, and expected benefits in terms of efficiency and safety. The sequence of the ERSCs is chosen so that as we go from one ERSC to the next we automate additional driving functions until we end up with a fully automated vehicle whose route is dictated by the roadway. Figure 1 shows the primary automatic functions of the vehicle for each ERSC.

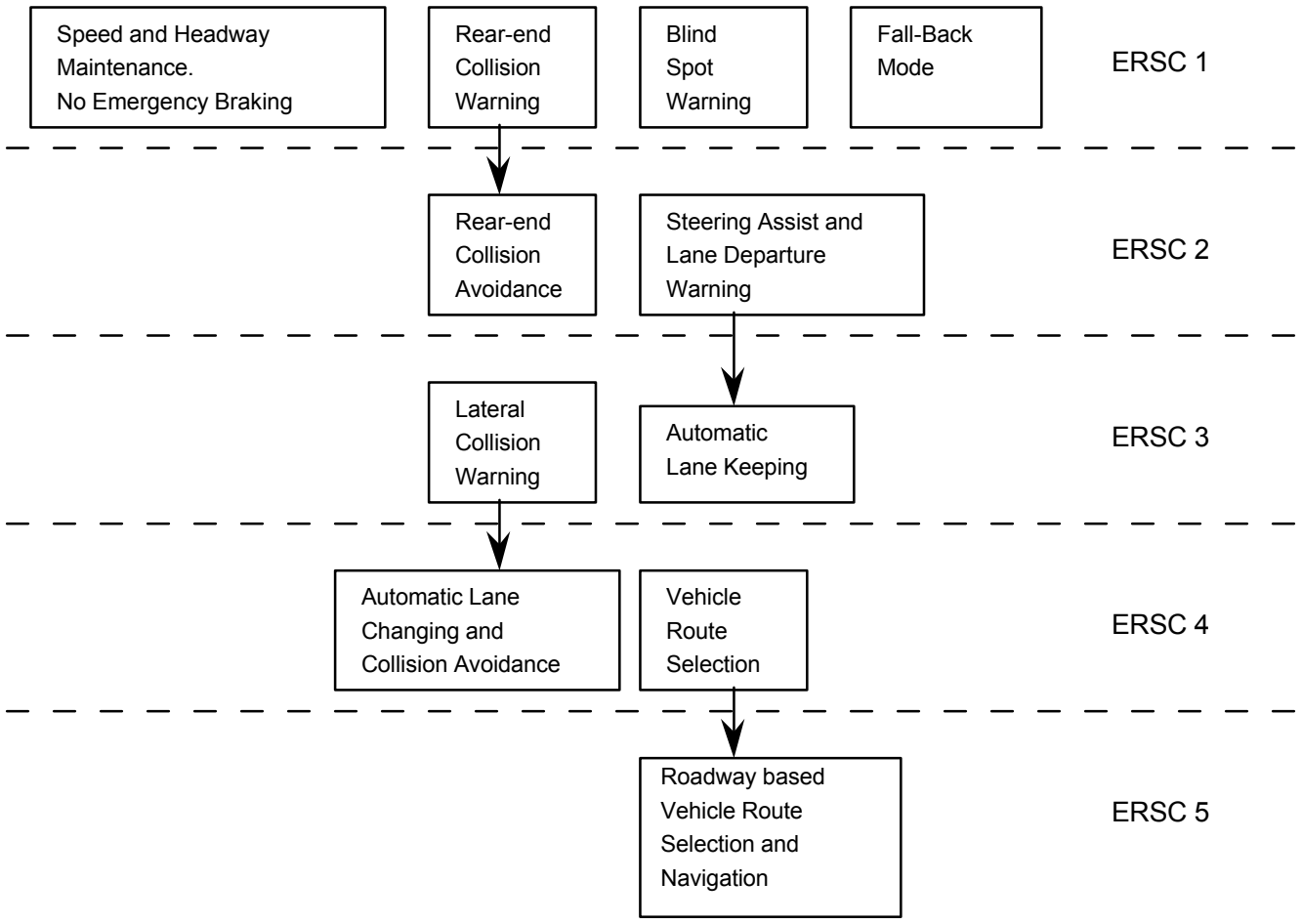

Figure 1: Main automatic vehicle functions for each ERSC. The arrow indicates the introduction of a new fully automated vehicle function.

In our study we concentrate on the issues associated with reliability and safety, maintenance, retrofitting, vehicle and driver diagnostics, evolutionary deployment and customer acceptance. We address these issues for each ERSC.

Our overall approach is based on the concept of evolution of vehicle control that is captured by the proposed ERSCs. We study each ERSC separately. We first specify the vehicle functions and interface with driver and roadway and present the functional and reliability requirements that need to be met. We perform a system level failure modes and effects analyses (FMEA) whose result is a list of potential failure modes, their potential causes and effects and a list of design requirements and recommendations.[1,2] The severity and occurrence ratings of the failure modes are presented and used to classify the criticality of the various vehicle functions. The design requirements and recommendations include the need for redundancies, diagnostics, changes in the system design, the feasibility of retrofitting etc. The results of the FMEA form the core of our analysis and allow us to study the increase in complexity and number of issues and risks associated with vehicle operation as we move from one ERSC to the next one.

Our guiding assumptions in the FMEA and in our analysis in general are the past history and current trends in vehicle control and automation and the current sensor, and actuator technology.[3,4,5] These assumptions lead us to the concept of evolution of vehicle control that is reflected in the proposed ERSCs. The evolution of vehicle control towards a fully automated one has already started with the introduction of cruise control, ABS and more recently intelligent cruise control.[5,6] The concept of evolution and the proposed ERSCs allow us to deal with each automated vehicle function separately without being overwhelmed with the complexity of a fully automated vehicle. Furthermore, one can also view the proposed ERSCs as degraded modes of operation of a fully automated vehicle roadway system. Such degraded modes of operation could be unavoidable because no system could work with optimum performance all the time and under all environmental and roadway conditions. For each ERSC we assume that each vehicle is treated as autonomous with respect to safety. In other words the vehicle does not rely on the roadway or other vehicles to guarantee its safety but rather it uses its on board sensors and intelligence to protect itself from colliding with other vehicles or obstacles. The vehicle functions for each ERSC are designed to provide collision free vehicle following and operation under normal operating conditions.[7,8] Since no low DV collisions are allowed the organization of vehicles in platoons of specified size and very short headways is considered to be unnecessary and has not been studied.

SECTION 2 ERSC 1 ANALYSIS

In this section we analyze and discuss the vehicle operational issues and results associated with ERSC 1. We first develop a detailed description of the vehicle functions and sub functions and interface with the roadway and driver and develop the functional and reliability requirements that we use to perform a preliminary system level failure mode and effects analysis (FMEA).[1] The results of the FMEA are used to discuss reliability, fault-tolerance and maintenance. The vehicle functional requirements also allow us to discuss the necessary vehicle and driver diagnostics and the feasibility of retrofitting for each ERSC. The motivation behind each ERSC is evolution and deployment at stages. We present possible scenarios for implementing ERSC 1. We conclude the discussion and analysis of ERSC 1 with a summary of key findings and conclusions.

Vehicle Functions and Interface with Roadway and Driver

We first present the specific functions and sub functions of the vehicle and interface with the roadway and driver that we analyze for ERSC 1. In order to develop these functions we need to define precisely

the role of the roadway, vehicle and driver from the point the driver decides to enter the dedicated lane of AHS to the point that he/she is back to the manual lane. The following operational scenario serves this purpose.

Operational Scenario.

The on-board vehicle diagnostics notify the driver whether the vehicle is fit to operate on the dedicated lane well before reaching the AHS facility. If the vehicle is fit, the driver drives and merges the vehicle into the dedicated lane with the aid of a blind-spot warning. The configuration of the dedicated lane and of the points of entry could be any one of the configurations shown in figure 2. Once in the lane, the driver accelerates to a desired speed and/or headway and switches on the speed headway maintenance (SHM) function and rear-end collision warning (RECW). The SHM function responds to driver commands for changing the headway and speed as follows: If there is no target within a certain range the SHM function operates as cruise control by maintaining the current speed, the speed selected by the driver. If there is a target the SHM function maintains a default headway and responds to subsequent driver commands for increasing or decreasing the headway within an upper and a lower bound. The lower bound is determined by safety considerations and the upper bound is determined by capacity considerations. If a target appears at a certain range near the vehicle, while the SHM is on the cruise control mode, the SHM switches to the follow mode and maintains the default headway. The default headway may be selected by the driver and cannot be changed below a certain preset value. The default headway is chosen a priori based on the stopping time to avoid collision under a worst case scenario.[7,8] If a target disappears from the sensing range of the vehicle the SHM follows the next valid target. A valid target is a moving vehicle or an obstacle in the same lane within a certain range (which depends on vehicle speed). In the absence of a target the SHM switches to cruise control mode and maintains the current speed. Once the SHM function is switched on, a communication link is attempted between the roadway and SHM. This communication, once established, allows the roadway to send target speed commands to the SHM and minimum headway recommendations to the RECW. The SHM function responds to roadway speed commands as follows: If the roadway target speed is larger than the current vehicle speed the SHM speeds up the vehicle to the target speed in a smooth manner provided the headway selected by the driver is not violated. If the target speed is smaller than the current vehicle speed the SHM slows down the vehicle to the target speed in a smooth manner. The driver can override the roadway commanded target speed if he/she does not feel comfortable at such speed by disabling the SHM function. In such case the driver is required to exit the lane.

The RECW warns the driver of a potential rear-end collision. The RECW estimates the time to collision (TTC)[8] and warns the driver if the TTC is smaller than a default value that is calculated a priori. The accuracy of the TTC calculations is enhanced by the use of vehicle to vehicle communication where braking capabilities and deceleration intentions are communicated to the vehicle by the preceding vehicle. The RECW receives headway recommendations from the roadway, developed using environmental and roadway conditions, and takes them into account in calculating TTC. The threshold of the RECW can be adjusted by the driver.

The functions of the communication system on board of the vehicle are to establish roadway to vehicle, vehicle to trailing vehicle and preceding vehicle to vehicle communication. The vehicle to trailing vehicle and preceding vehicle to vehicle communications allow the communication of the braking capabilities and braking intentions to be used by the vehicles' RECW to improve its accuracy and reduce false alarms. The communication between vehicles is attempted as soon as the vehicle is in the dedicated lane and the RECW function is switched on.

The blind spot warning warns the driver of the presence of an obstacle in the blind spot on either side of the vehicle. It aids the driver during entry and exit maneuvers from the dedicated lane. The driver is

responsible for driving the vehicle out of the dedicated lane at the end of the trip or when the SHM and/or RECW stop functioning. The exit from the dedicated lane is done by first disabling the SHM function. The roadway exit configurations considered for ERSC 1 are shown in figure 3.

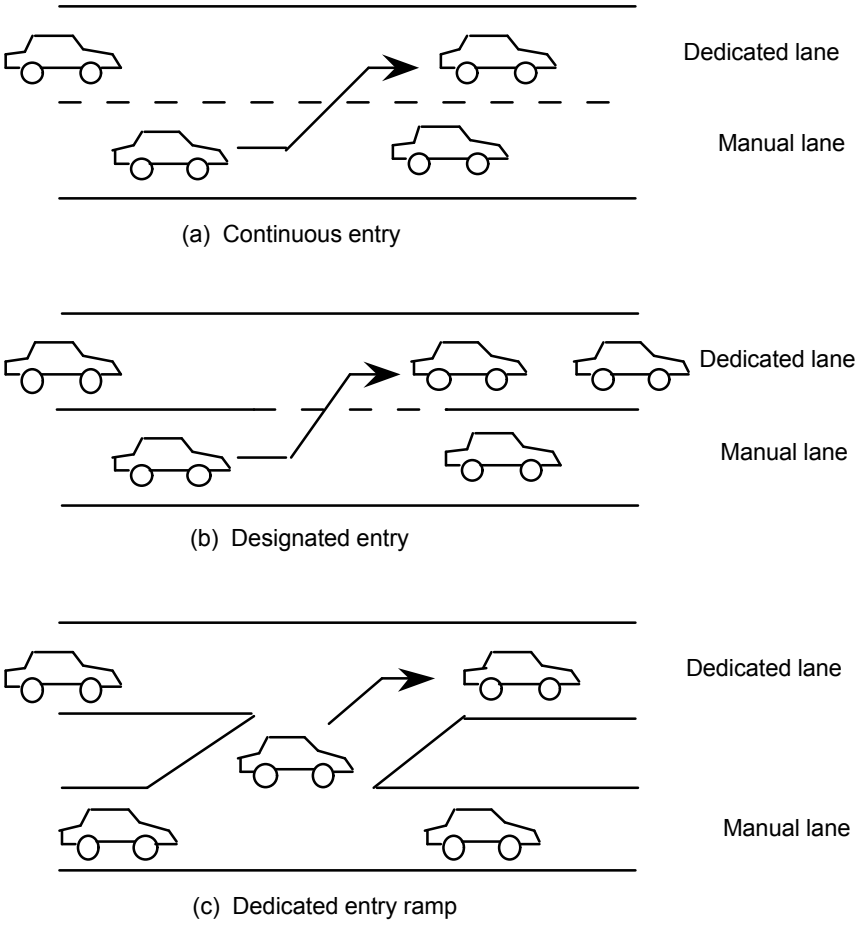

Figure 2: Entry configurations to dedicated lane.

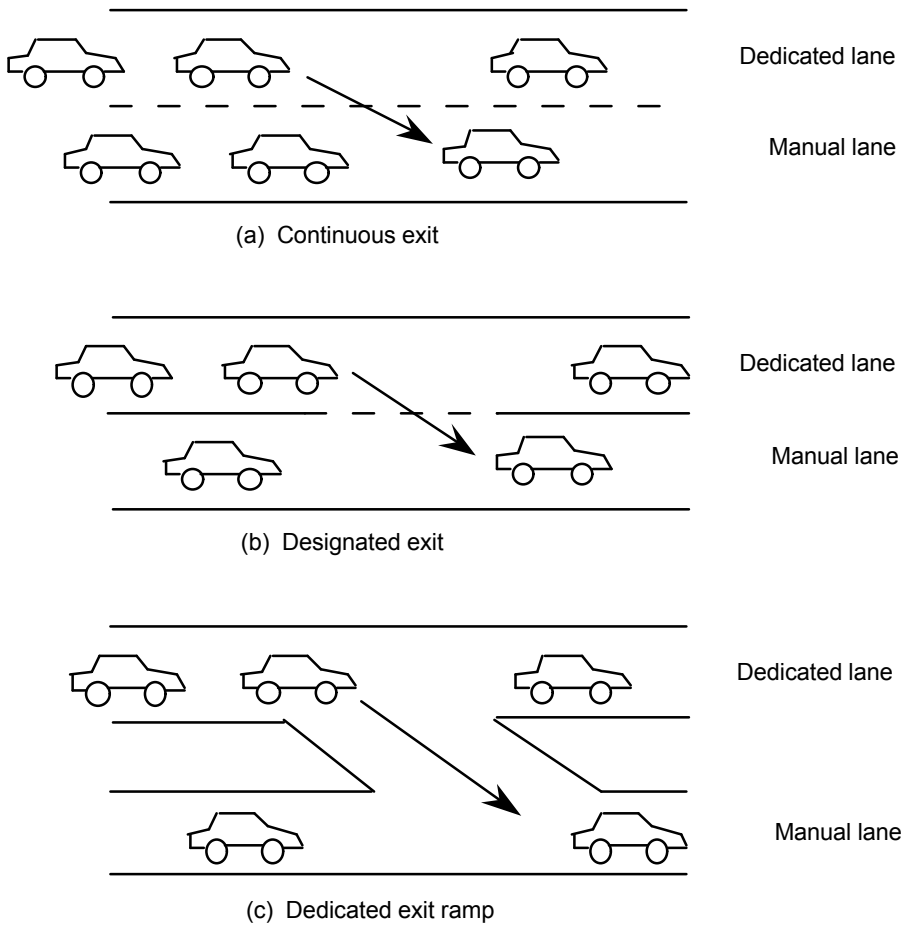

Figure 3: Exit configurations from dedicated lane.

For the activity area under consideration we are mainly concerned with the vehicle functions as well as with roadway and driver functions that affect the functionality of the vehicle during entry, operation on the dedicated lane and exit. The development of these functions is achieved by starting with the high level functions described in the above operational scenario. These are:

H1.1 Speed and Headway Maintenance
H1.2 Rear-end Collision Warning
H1.3 Blind-spot Warning
H1.4 Vehicle Driver, Roadway Interface

H1.1 Speed and Headway Maintenance

Figure 4 shows the main components of the SHM function and its interface with the driver and roadway.

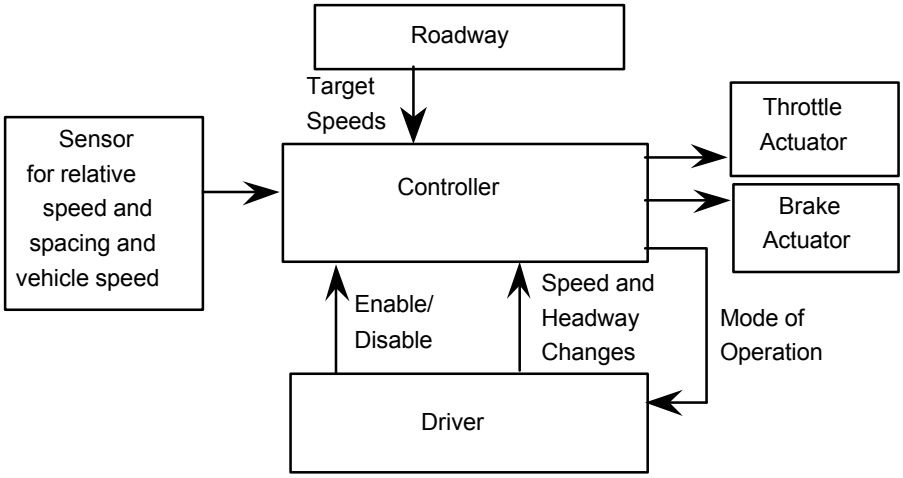

Figure 4: The speed and headway maintenance.

Inputs:

Vehicle speed from speed sensor
Relative speed and spacing from ranging sensor
Driver commands: enable, disable, speed and headway changes
Roadway commands: target speed

Outputs:

Throttle actuator command
Brake actuator command
Mode of operation

Functional specifications:

The SHM responds to driver and roadway commands for maintaining vehicle speed and headway under all freeway speeds, environmental conditions and roadway configurations by providing the appropriate commands to the throttle and brake actuators. It responds to driver commands for disabling, enabling and for changing speed and headway by taking the appropriate actions. It informs the driver of its status i.e., whether it is in the "on" or "off" mode and whether it is in the cruise or target speed or headway maintenance mode and whether there is a malfunction.

The specific functions of SHM and the functional and reliability requirements are listed below:

F1.1 Maintain cruise speed
The vehicle shall maintain a driver selected speed when no moving or stationary obstacles are within a certain range under all environmental conditions and freeway speeds.

F1.2 Maintain target speed
The vehicle shall track and maintain the roadway commanded speed, when no moving or stationary obstacles are within a certain range under all environmental conditions and freeway speeds.

F1.3 Maintain headway
The vehicle shall maintain the driver selected headway that is greater than a default value under all environmental conditions, road geometry and freeway speeds.

F1.4 Switch from maintaining speed to maintaining headway
When the system senses a valid target in the lane that is within a certain range it shall switch to the headway maintenance mode and be ready to respond to subsequent commands of the driver for changing the headway . The switching shall be smooth and on time and shall not put the driver in a situation he/she cannot handle.

F1.5 Switch from maintaining headway to maintaining speed
When the target is no longer within the default headway the system shall switch to the speed maintenance mode by maintaining the current cruise speed.

F1.6 Switch from maintaining cruise speed to maintaining target speed commanded by the roadway. When the system receives a target speed command from the roadway it shall respond by changing the current cruise speed to the target speed in a smooth manner provided no obstacle is within a certain range.

F1.7 Enable SHM
Upon driver command the SHM shall switch on.

F1.8 Disable SHM
Upon driver command the SHM shall disable itself.

The function associated with the mode of operation is considered as part of the driver vehicle roadway interface.

H1.2 Rear-end Collision Warning

Figure 5 shows the main components of the rear-end collision warning (RECW) function and its interface with the driver and roadway.

Inputs:

Vehicle speed from speed sensor
Relative speed and spacing from ranging sensor
Braking capabilities of vehicle obtained using on board sensors
Braking capabilities and intentions of preceding (target vehicle) obtained via communication.
Driver commands: enable, disable and threshold adjustment
Roadway commands: headway recommendations based on road conditions, traffic status and environmental conditions.

Outputs:

Warning to the driver
Mode of operation
Braking capabilities and intentions to trailing vehicle

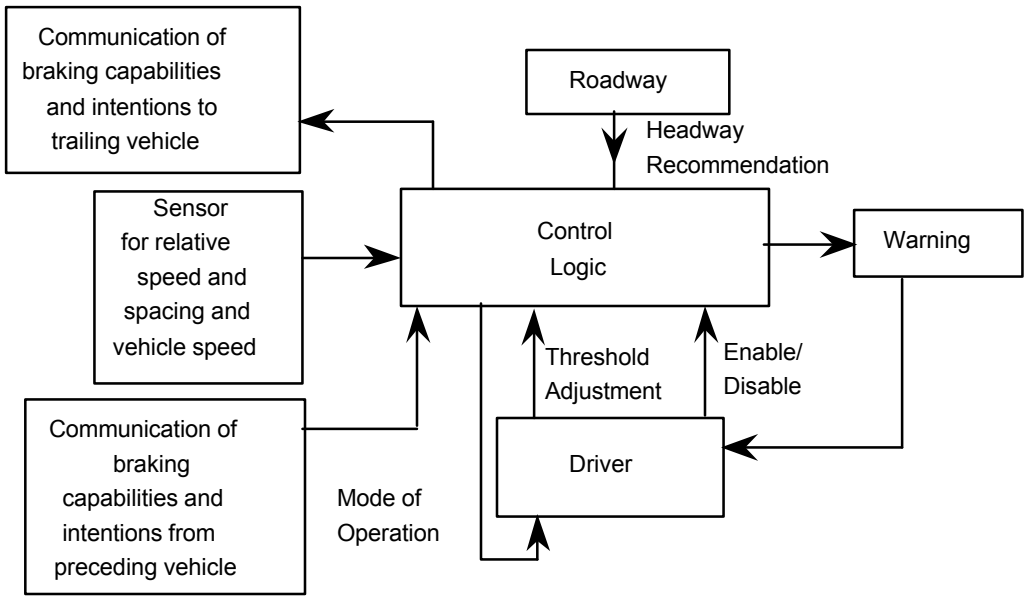

Figure 5: The rear-end collision warning system.

Functional specifications:

The RECW calculates the time to collision (TTC)[8] in the longitudinal direction by using the braking capabilities of the vehicle and of the preceding vehicle, the current speed and headway, the roadway headway recommendations and the driver's reaction time to start braking[9] and provides a warning to the driver if the TTC is less than an a priori selected TTC default value. It informs the driver whether it is in the on or off mode and responds to driver commands for disabling, enabling and changing the default value for the TTC. The TTC default value cannot be adjusted to be less than a certain level that corresponds to the minimum allowable by the system headway. The RECW communicates the braking capabilities and intentions of the vehicle to the trailing vehicle.

The main functions of the RECW and functional and reliability requirements are given below :

F1.9 Warn the driver

The system shall warn the driver when the calculated TTC is less than the TTC default value without false alarms under all freeway and environmental conditions. The TTC is calculated using speed/headway measurements from on-board sensors, braking data from preceding vehicle obtained via communication, headway recommendations provided by the roadway and the vehicle's own braking capabilities obtained using on board sensors.

F1.10 Enable RECW

Upon driver command the RECW shall switch on.

F1.11 Disable RECW

Upon driver command the RECW shall disable itself provided the SHM is disabled.

F1.12 Adjust Threshold

Upon driver command the system shall adjust the safe headway threshold of the RECW provided it doesn't exceed a certain limit.

F1.13 Communication of braking capabilities and intentions to trailing vehicle

The system shall communicate the vehicle's braking capabilities and intentions to the trailing vehicle in the same lane under all freeway conditions.

The function associated with the mode of operation is considered to be part of the driver vehicle roadway interface.

H1.3 Blind-spot Warning

The main components of a blind-spot warning (BSW) function are shown in figure 6.

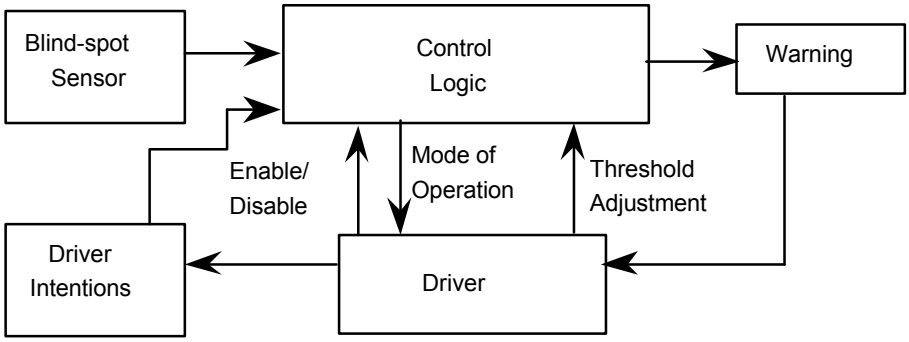

Figure 6: The blind-spot warning

Inputs:

Presence of vehicle in blind spot on either side of the vehicle detected by the blind spot sensor.
Driver's intentions used for activation of the system
Driver commands: enable, disable, threshold adjustment.

Outputs:

Warning to the driver
Mode of operation: on, off, malfunction

Functional specifications:

The BSW provides a warning to the driver when a moving or stationary obstacle is in the blind spot region on either side of the vehicle. The BSW is activated by sensing the intentions of the driver to change lanes. It responds to driver commands for enabling, disabling and adjusting the threshold. The system informs the driver whether it is on or off and when a malfunction is detected by the on board diagnostics.

The specific functions of the BSW and functional and reliability requirements are listed below :

F1.14 Warn Driver

The system shall sense the intentions of the driver to change lanes and provide an early warning if an obstacle is present in the blind spot region on either side of the vehicle without false alarms and under all roadway and environmental conditions.

F1.15 Enable BSW

Upon driver command the BSW shall switch on.

F1.16 Disable BSW

Upon driver command the BSW shall disable itself.

F1.17 Adjust Threshold

Upon driver command the size of the blind spot region sensed shall be adjusted as long as it does not exceed a certain minimum threshold.

The function associated with the mode of operation is considered to be part of the driver vehicle roadway interface.

H1.4 Driver Vehicle Roadway Interface

The block diagram in figure 7 shows the interface of the driver with the BSW, RECW, SHM and roadway during entry, normal operation and exit from dedicated lane.

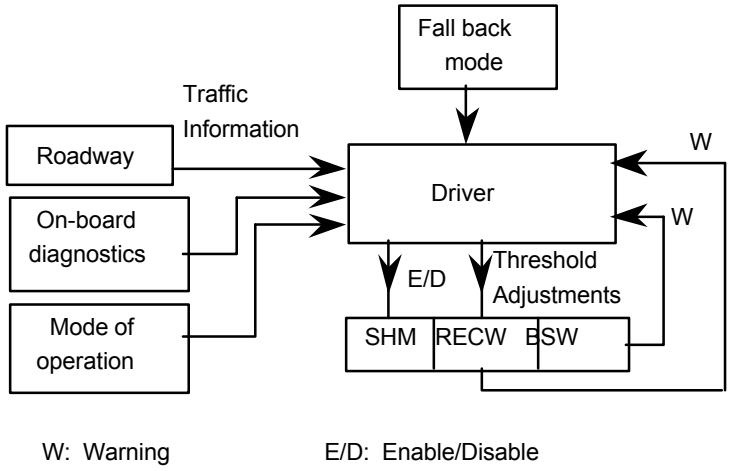

Figure 7: Driver interface with vehicle functions and roadway.

Inputs:

Traffic information from the roadway
Information from on board diagnostics and mode of operation
Warnings
Fall back mode instructions

Outputs:

Enable/Disable, Threshold adjustments
Route selection
Manual control

The interface of the driver with the vehicle functions and roadway involves the following functions:

F1.18 Check-in

The driver responds to the on-board vehicle diagnostics and verifies whether his/her vehicle is fit to operate on the dedicated lane.

F1.19 Enter the lane

The driver looks for a safe gap and drives the vehicle in the dedicated lane. Once in the lane he/she synchronizes the vehicle's speed and switches on the automated vehicle functions.

F1.20 Response to BSW and RECW

The driver responds to BSW and RECW by steering or braking in order to avoid collisions.

F1.21 Response to traffic information

Driver processes roadway traffic information in order to make routing decisions and/or assume full manual control if necessary.

F1.22 Exit the lane

The driver switches off the SHM and RECW functions and exits the lane.

F1.23 Fall back to manual control

The vehicle warns the driver to assume full manual control by slowing down, providing a warning and disabling the SHM function.

F1.24 Mode of operation

The system shall notify the driver of the mode of operation of the SHM, BSW, RECW i.e.: on, off, malfunction and status of operation.

Failure Modes and Effects Analysis

A system level FMEA [1,2] is performed for the vehicle functions F1.1 to F1.24 listed above. Appendix A gives a description of the FMEA used and the rating adopted to indicate the level of severity and occurrence rate of the possible failure modes. The purpose of the FMEA is to identify all or at least the majority of the potential failure modes, their relative probability of occurrence and the severity of their effects. This process helps identify critical characteristics and potential design deficiencies.

One of the results of the FMEA is a list of design requirements and recommendations. These are the system design approaches that need to be taken to reduce the severity or the occurrence rating or both. The intent is to eliminate system design deficiencies and eliminate potential system failure modes. The recommended actions will generally seek to eliminate or reduce the causes of system failure modes, to control or manage system failure modes and mitigate their effects by modifying the design and introducing redundancies and diagnostics.

The FMEA tables for ERSC 1 are presented in table 12 of Appendix B. Since in ERSC 1 the driver is fully responsible for emergencies he/she can be considered as a backup or a redundancy for the partially automated vehicle functions. Despite the presence of the driver as a backup and despite the fact that the driver is responsible for all the collision avoidance functions the FMEA reveals several failure modes of the partially automated functions that could lead to rear-end collisions.

We present the results of the FMEA for each high level function as follows: We list the identified failure modes, discuss their causes and effects and present the redundancy, diagnostics and malfunction requirements that have to be met for reliable operation. The failure modes and requirements are identified by the same letter and number as in the FMEA table 12 in Appendix B. Severity is a rating of the seriousness of the effect of the potential system failure mode. Severity applies only to the effect of a failure mode. The occurrence is a rating corresponding to the rate at which a cause and its resultant failure mode could occur over the lifetime of the system. Assuming single point failures and assuming

that the causes of a failure mode are independent leads to that if a cause occurs a failure mode will occur. The occurrence rating is not affected by the ability to detect and correct a failure mode.

In the following discussion, the severity (S) and occurrence (O) ratings are presented in parentheses for each one of the causes of the failure modes. The significance of these ratings is explained in Appendix A and in tables 1 and 2.

Table 1: Severity rating for system level FMEA

Effect	Rating	Criteria
Negligible	1	Negligible Effect
Very Slight	2	Very slight effect on vehicle or System performance
Slight	3	Slight effect on vehicle or System performance
Minor	4	Minor effect on vehicle or System performance
Moderate	5	Moderate effect on vehicle or System performance
Significant	6	Vehicle performance degraded but operable and safe Partial loss of System function, but operable
Major	7	Vehicle performance severely affected but drivable and safe. System function impaired
Serious	8	Vehicle inoperable, but safe. System inoperable
Very Serious	9	Potential safety related vehicle failure Able to stop without mishap. Gradual failure.
Hazardous	10	Potentially hazardous failure. Safety related, sudden failure

Table 2: Occurrence rating for system level FMEA

Occurrence	Rating	Criteria	Failure Rate
Almost impossible	1	Failure unlikely. History of similar designs shows no failures	< 1 in 1500000
Remote	2	Very few failures likely	1 in 150000
Very Slight	3	Few failures likely	1 in 2000
Slight	4	Infrequent failures likely	
Low	5	Some failures likely	1 in 400
Medium	6	Regular failures likely	1 in 80
Moderately	7	Frequent failures likely	1 in 20
High	8	Many failures likely	1 in 7
Very High	9	Failures very likely	1 in 3
Almost Certain	10	Failures almost certain to occur. History of similar designs shows many failures.	> 1 in 3

H1.1 Speed and Headway Maintenance

Potential Failure Mode : F1.1.1 Loss of speed maintenance.

The SHM may lose its ability to maintain a constant cruise speed if any one of the following components fails to perform as designed:

(F1.1.1.1) The speed sensor gives erroneous readings (S=6, O=2)
(F1.1.1.2) The controller electronics or software fail (S=6, O=2)
(F1.1.1.3) The throttle actuator fails (S=6, O=3)
(F1.1.1.4) The brake actuator fails (S=8, O=3)

The possible effects of these failures are for the vehicle to accelerate and decelerate above or below the desired speed or maintain an incorrect constant speed. Such vehicle response may lead to the violation of traffic rules. The driver may get annoyed and his/her steering performance may be affected.[10]

The severity of these failures is fairly low (S=6) and the occurrence rating varies from O=2 to O=3. The exception is the failure of the brake actuator that is given a severity S=8. The use of the brake is essential in maintaining constant speed during some downhill cruising situations. Failure of the brake actuator may cause the vehicle speed to exceed the speed limit or decelerate rapidly, when not expected, possibly causing panic to the driver.

The speed maintenance function is part of the current cruise control system which employs only throttle actuation. As a result the current cruise control system cannot maintain speed during some downhill driving situations. The use of brake control for speed maintenance will eliminate this problem.

The design requirements and recommendations associated with failure mode F1.1.1 generated by the FMEA are listed as follows:

(F1.1.1.1) Diagnostics and built in tests must perform a test for reasonableness on speed sensor data. When sensor malfunction is detected, system shall return to manual control and provide warning to the driver.

(F1.1.1.2) The system must have supervisory elements (in hardware and software) or adequate redundancies for the controller electronics and software. When a controller malfunction is detected, system shall return to manual control and provide warning to the driver.

(F1.1.1.3) The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.

(F1.1.1.4) The system must use sensors and diagnostic programs to monitor the brake actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.

Based on past experience with cruise control[3,11] the requirements listed above can be met and therefore no significant issues or risks are associated with failure mode F1.1.1.

Potential Failure Mode F1.1.2 System switches to headway maintenance (instead of maintaining cruise speed) in the absence of valid target.

This failure will take place when:

> (F1.1.2.1) The ranging sensor detects an invalid target within certain range of the vehicle while the vehicle is at constant cruise speed. (S=8, O=6)

The potential effect of the failure is for the vehicle to change its speed using engine torque and braking for no apparent reason to the driver. The RECW may also get activated. The driver may get annoyed, panic and his/her steering performance may be affected.[10] The severity of this failure is rated as S=8 . Based on current ranging sensor technology the occurrence of such failure is very likely and is given a rating of O=6. The failure may take place around curves, going under bridges and under other road configurations and traffic conditions. The failure may also be the result of interference with signals from other ranging sensors or similar devices.

The design requirements and recommendations for reducing the severity and occurrence of failure mode F1.1.2 generated by the FMEA are:

(F1.1.2.1) The system must be able to discriminate between valid and invalid targets.

The design requirement will be easier to meet if two ranging sensors that are not subject to common mode failures are used together with the appropriate logic and diagnostics. The outputs of the two sensors should be continuously monitored and checked for reasonableness and consistency. A higher level controller should be used to decide which of the two outputs is the correct one when the two outputs are different. If the controller cannot decide the system shall follow the output that indicates the closer target and shall revert to manual control. The use of three ranging sensors that are based on different principles of operation and not subject to common mode failures may be a better way of improving the reliability of the ranging measurements. In this case the three outputs of the sensors are compared and the majority rule is used to choose the output to be used for control purposes.

Potential Failure Mode : F1.2.1 Vehicle cannot maintain target speed as commanded by the roadway

The vehicle may lose its ability to maintain the roadway commanded target speed if any one of the following components fails to perform as designed:

(F1.2.1.1) The speed sensor gives erroneous readings (S=6, O=2)
(F1.2.1.2) The controller electronics or software fail (S=6, O=2)
(F1.2.1.3) The throttle actuator fails (S=6, O=3)
(F1.2.1.4) The brake actuator fails (S=8, O=3)
(F1.2.1.5) Vehicle doesn't receive target speed due to loss of communication or noise corruption(S=6, O=3)
(F1.2.1.6) Receiver malfunction (S=6, O=3)

The potential effects of the vehicle not maintaining the target speed commanded by the roadway are degradation of safety and efficiency. The vehicle may be cruising at a speed that is unsafe for the existing traffic conditions. In another situation the vehicle may be cruising at a lower speed holding traffic and causing reduction in capacity and efficiency. The severity of the failures is rated as S=6 with the exception of F1.2.1.4 that is rated as S=8 due to the higher impact the brake actuator may have on safety. The occurrence rating is also very low due to the availability of mature technology that has already been tested in current cruise control systems and short range communication systems.[12] The design requirements for reducing the severity and occurrence of failure mode F1.2.1 are the same as those generated for failure mode F1.1.1 with the addition of the following:

(F1.2.1.5) The system must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. The system must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). When a communication malfunction is detected the driver shall be notified.

(F1.2.1.6) The system must have supervisory elements in the controller software and receiver to detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.

Based on current communication technology [12,13] the above requirements can be met and therefore the severity and occurrence ratings of the failure can be drastically reduced.

Potential Failure Mode F1.3: System cannot maintain desired headway

The system may fail to maintain the desired headway due to the following causes:

(F1.3.1) Ranging sensor fails to provide signal (S=10, O=6)
(F1.3.2) Ranging sensor loses target due to road curvature or insufficient target discrimination (S=10, O=7)
(F1.3.3) Ranging sensor has locked on unintended target (S=9, O=7)
(F 1.3.4) Brake actuator failure (S=9, O=3)
(F1.3.5) Throttle actuator failure (S=6, O=3)
(F1.3.6) Controller electronics or software failure (S=9, O=2)
(F1.3.7) Ranging sensor gives erroneous readings (S=10, O=6)

The effects of the failures of the above components to perform as designed are severe and the occurrence rate is high, especially in the case of a ranging sensor that fails to provide correct measurements in the presence of a valid target or fails to detect a target within the default headway. Since the RECW also relies on the same sensor the system may put the driver that relies on the system too much, without warning, in a situation of a very short headway that he/she cannot handle. Such a situation may lead to a rear-end collision. Based on current sensor technology the probability of missing valid targets, having incorrect measurements due to interference are fairly high.[14,15,16] Problematic cases are: maintaining track of the target around curves, under bridges and during lane changes where switching from one target to another is necessary. The failure resulting from the sensor locking on invalid targets is less severe but also crucial. In this case the RECW may get activated, the driver may get annoyed and possibly panic since the vehicle is behaving in a way not expected by the driver. In addition his/her steering performance may be affected. The failure of the brake actuator may result in the activation of the RECW due to the inability of the system to maintain the desired headway with engine torque alone. If the driver relies on the system too much for initial soft braking, he/she may delay his/her action to apply the brakes leading to a possible rear-end collision.[17] The failure of the throttle actuator doesn't pose any serious safety concerns provided the system is designed so that the brakes kick in when the throttle alone fails to maintain the desired headway. The failure of the controller or electronics may lead to a potential rear-end collision if the driver is not attentive and not aware of the failure taking place.

The design requirements and recommendations for reducing the severity and occurrence ratings of failure mode F1.3 generated by the FMEA are:

(F1.3.1) The system must be able to detect and accommodate intermittent sensor failures. The system software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and the driver shall be asked to resume control. Redundant ranging sensors, not subject to common mode failures, with appropriate logic may be required.

(F1.3.2) The ranging sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target.[14,18] The driver must be notified when a target is ambiguous and cannot be followed reliably and possibly be given the option to resume manual control. Sensor redundancy might be needed.

(F1.3.3) The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. The system must distinguish vehicles moving to adjacent lanes and around curves in the same lane. A redundant ranging sensor not subject to common failure modes with the appropriate logic may be required.

(F1.3.4) The system must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. When an actuator malfunction is detected, the system shall return to manual control and provide warning to the driver.

(F1.3.5) The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, the system shall return to manual control and provide warning to the driver.

(F1.3.6) The system must have supervisory elements (in hardware and software) or adequate redundancies for controller electronics and software. When a controller malfunction is detected, the system shall return to manual control and provide warning to the driver.

(F1.3.7) The system must be able to discriminate against gross errors from the ranging sensor. The sensor and the controller must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. System shall provide warning and return control to the driver in case of a detected sensor failure. Sensor redundancy and appropriate logic may be needed to totally eliminate the possibility of undetected errors.

The ranging sensor requirements can be met if redundant sensors that are not subject to common mode failures are employed with the appropriate logic. Two redundant sensors with proper diagnostics that have the capability of distinguishing which of the two sensors has the correct reading when their readings differ may be sufficient. The reliability and accuracy of the ranging sensor measurements can be improved further if three ranging sensors based on different principles of operation and not subject to common mode failures are used and the majority rule is employed for selecting the appropriate sensor output. The question whether two or three redundant sensors are necessary is a design issue that needs to be resolved.

Potential Failure Mode F1.4 : The system fails to switch from maintaining speed to maintaining headway despite the presence of a valid target within the default headway

The causes of the above failure mode are the results of the following components failing to performed as designed:

(F1.4.1) Ranging sensor fails to detect a valid target (S=10, O=6)
(F1.4.2) Hardware or software failure of the SHM (S=9, O=2)

The effect of the failure of the ranging sensor to detect a target within the default headway may lead to a rear-end collision despite the fact that the driver is responsible for rear-end collision avoidance. The collision could take place if the driver delays his/her actions or simply doesn't pay attention since he/she expects the system to provide an initial soft braking and a RECW when the headway becomes too small. Based on current sensor technology the occurrence rating of such a failure is relatively high. The effect of the hardware or software failure of the SHM may lead to a small headway and activation of the RECW. The severity of this failure could be high in situations where the driver relies too much on the system and delays his/her braking actions by expecting the system to provide soft braking. On the other hand if the driver doesn't rely on the RECW very much he/she may again delay his/her response thinking that the warning is a false one.

The design requirements and recommendations for reducing the severity and occurrence rating of the failure of the above components are:

(F1.4.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics.

(F1.4.2) The system must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware and software) or adequate redundancies. The system shall provide warning and return control to the driver in case of failure.

As with the previous failure modes the reliability of the ranging sensor is the most crucial one. The type of redundancies mentioned earlier can be used to improve the reliability of the ranging measurements.

Potential Failure Mode F1.5 : Failure to switch to speed maintenance mode when the target moves out of the lane and becomes unsuitable to follow.

The above failure mode will take place when:

(F1.5.1) The ranging sensor locks on the original target even though it is no longer a valid one due to lane changing or the sensor locks on another target that is not a valid one (S=8, O=6).
(F1.5.2) The hardware or software of the SHM fails (S=5, O=2)

The failure (F1.5.1) of the ranging sensor may arise under certain road configurations such as curves where the neighboring lane is in the field of view of the sensor. Also roadway structures such as bridges or signs may appear to the sensor as valid targets. The potential effects of this failure are for the vehicle to behave in a way not expected by the driver, such as unnecessary deceleration, RECW activation. The driver may get annoyed, panic and his/her steering performance may be affected. The severity of the failure is S=8. Based on today's technology and on the use of the radar as the most likely accepted ranging sensor the occurrence rating (O=6) is fairly high.[14] The failure (F1.5.2) of the SHM is less severe with a much lower occurrence rating. The reason is that failure of the SHM will cause the vehicle to revert to the manual mode by disabling the SHM and slowing down the vehicle. Even though the driver may get annoyed his/her safety may not be affected. The failure, however, will cause a disturbance in the traffic flow and may affect the efficiency of the dedicated lane. Based on the reliability of similar hardware and software components the occurrence rating is expected to be low.

The design requirements for reducing the severity and occurrence rating of the failures of the above components are:

(F1.5.1) The system must be able to discriminate between valid and invalid targets. It may or may not be possible to design a ranging sensor to meet this requirement. If not, two redundant sensors not subject to common mode failures must be used together with the appropriate diagnostics.

(F1.5.2) The system must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware and software) or adequate redundancies. System shall provide warning and return control to the driver in case of a detected failure.

Potential Failure Mode F1.6.1 : Failure to switch from maintaining cruise speed to maintaining roadway commanded target speed

The causes of the above failure mode are due to:

(F1.6.1.1) Loss of target speed information due to receiver malfunction(S=6, O=4)

(F1.6.1.2) Vehicle does not receive target speed information due to loss of communication or target speed is corrupted during communication(S=6, O=3)

The above failing components will affect safety and the efficiency of the dedicated lane. Safety is affected by the vehicle operating at a speed that is not considered safe based on the current road and traffic conditions. Efficiency is affected by the vehicle not operating at a speed that is optimal or near optimal based on the traffic conditions. The severity of the failures is not that critical assuming all the other vehicle functions are healthy. The occurrence rating is fairly low due to the availability of reliable short range communication devices.[12,13]

The design requirements and recommendations for reducing the effects of the above failures are:

(F1.6.1.1) The system must have supervisory elements in the controller software and receiver to detect any receiver malfunction. The roadway must assist in testing receiver functionality. The driver shall be notified that the vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.

(F1.6.1.2) The system must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. The system must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). When a communication malfunction is detected, the system shall notify the driver.

Potential Failure Mode F1.6.2: The system switches to headway maintenance in the absence of valid target instead of switching from cruise control speed to maintaining target speed.

The possible cause of this failure is due to the following:

(F1.6.2.1) Ranging sensor detects an invalid target within the default headway (S=6, O=6)

The failure may lead to unnecessary deceleration and activation of the RECW. The driver may get annoyed, panic and his/her steering performance may be affected.

The design requirements and recommendations are:

(F1.6.2.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics.

Potential Failure Mode F1.7: The SHM cannot be enabled

The driver may not be able to enable or switch on the SHM due to:

(F1.7.1) Electronic malfunction. (S=6, O=2)

The result of this failure is that the vehicle can only be operated in the manual mode and the driver may have to exit the dedicated lane. The failure will affect safety by annoying the driver and taking his/her attention away from driving. In addition the vehicle has to rely on the driver to adjust to the speed of the dedicated lane and will therefore introduce a disturbance in the traffic flow that will affect the efficiency

of the dedicated lane. Due to the reliability of current electronics the occurrence rating of this failure is fairly low.
The design requirements and recommendations are:

(F1.7.1) The controller electronics must be sufficiently reliable. Diagnostics must be performed even when the SHM is in the standby mode. The driver shall be notified if there is any malfunction detected.

Potential Failure Mode F1.8: The SHM cannot be disabled

The driver may not be able to disable the SHM due to:

(F1.8.1) Electronic or software malfunction (S=9, O=2)

With this failure the driver may have to apply braking in an effort to put the vehicle under control. He/she may feel out of control of the vehicle for at least a short period of time which may cause annoyance, panic and his/her steering performance and vigilance may be affected leading to a possible collision.

The design requirements and recommendations are:

(F1.8.1) The controller electronics must be sufficiently reliable. There must be redundant means of disabling the SHM.

Based on current technology and similar systems the use of redundant means of disabling the SHM is essential and feasible to implement. The most suitable method of disabling the SHM is a human factors issue and needs to be studied.

H1.2 Rear-End Collision Warning

Potential Failure Mode F1.9.1: The system fails to provide rear-end collision warning

The RECW will fail to provide a warning to the driver if any one of the following failures take place:

(F1.9.1.1) The ranging sensor provides incorrect readings (S=9, O=6)
(F1.9.1.2) Incorrect calculation of time to collision (TTC) due to a wrong estimate of the braking capabilities of the vehicle and/or of the preceding one (S=9, O=6)
(F1.9.1.3) The threshold of the warning is set too high (S=9, O=5).
(F1.9.1.4) Warning device failure (S=9, O=3)
(F1.9.1.5) Preceding vehicle's braking information is corrupted or lost during communication, due to noise, interference or blocking of communication (S=9, O=3)
F1.9.1.6) The preceding vehicle is unable to communicate its braking capabilities and intentions (S=9, O=3)

The potential effect of the above failures is for the headway to be too small and unsafe without the driver being aware of it since he/she expects to receive a warning if he/she is in the unsafe region. If the driver relies on the warning too much a rear-end collision is possible. Failure of the ranging sensor and incorrect calculation of the TTC are the most severe failures with the higher occurrence rating. These ratings are estimated based on today's technology and available ranging sensors. The calculation of the correct TTC relies very much on the correct estimate of the braking capabilities of the vehicle and of the preceding one. These capabilities depend on a lot of factors including the friction between tires and road

that can only be estimated with an approximation error. Slippery spots on the road may lead to a large variation of the friction coefficient that is difficult to estimate on time. It is therefore very likely that the estimate of the braking capabilities of the vehicles will have a large approximation error that will affect the accuracy of the calculated TTC. The system will also fail to provide warning if the threshold of the device is set high. Since the driver is the one that adjusts the threshold the failure may be due to human error or decision. Lack of communication of the braking intentions of the preceding vehicle may lead to a delayed warning and a headway that is unsafe. If the driver relies too much on the warning and he/she is not attentive a rear-end collision is possible.

The design requirements and recommendations are:

(F1.9.1.1) The ranging sensor and the controller must be very reliable. Redundant ranging sensors not subject to common mode failures together with the appropriate logic may be necessary.

(F1.9.1.2) The system must perform tests of reasonableness of the estimated braking capabilities. The system must be designed to tolerate some inaccuracies in the estimates of braking capabilities

(F1.9.1.3) The driver shall be able to select a headway that he/she is comfortable with. The default threshold must be set to a low level.

(F1.9.1.4) The warning device must be reliable. Redundant warning delivery methods must be used.

(F1.9.1.5) The system must have diagnostic programs to test for reasonableness on received braking information data and monitor the operation of communication devices. The system must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.)

(F1.9.1.6) The system must have diagnostic programs to monitor and detect the lack of information from preceding vehicle. The system must be able to accommodate temporary loss of communication. When a malfunction is detected, the system shall take that into account in calculating the TTC.

Potential Failure Mode F1.9.2 : System gives false warnings

The system may give false rear-end collision warnings due to the failure of the following components:

(F1.9.2.1) Ranging sensor provides incorrect information (S=5, O=6).
(F1.9.2.2) Incorrect calculation of TTC due to wrong estimate of braking capabilities of vehicle and/or preceding vehicle (S=5, O=6)
(F1.9.2.3) The threshold of warning is set too low (S=5, O=5)
(F1.9.2.4) Preceding vehicle's braking information is corrupted or lost during communication, due to noise, interference or blocking of communication (S=5, O=3)

The effect of false alarms or warnings on safety is less severe than no warnings. Too many false warnings may annoy the driver, distract him/her from other driving tasks and reduce his/her confidence level. The design requirements and recommendations that could be used to reduce the number of false alarms are:

(F1.9.2.1) The ranging sensor must be very reliable. Redundant ranging sensors not subject to common mode failures together with the appropriate logic may be necessary.

(F1.9.2.2) The system must perform tests of reasonableness of the estimated braking capabilities. The system must be designed to tolerate some inaccuracies in the estimates of braking capabilities.

(F1.9.2.3) The driver shall be able to select a headway that he/she is comfortable with. The default threshold shall be set to a low level.

(F1.9.2.4) The system must have diagnostic programs to test for reasonableness on received braking information data and monitor the operation of communication devices. The system must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.)

Potential Failure Mode F1.10: The RECW cannot be enabled

The driver may not be able to switch the RECW on due to:

(F1.10.1) Electronics failure (S=6, O=2)

The effect of such failure is that the driver may have to exit the dedicated lane and he/she will not receive a warning when a rear-end collision is imminent. The occurrence rating of such failure is low due to the reliability of current electronics. The design requirements and recommendations are:

(F1.10.1) The controller electronics must be sufficiently reliable and must have supervisory elements in hardware. The driver shall be notified about the RECW operating mode.

Potential Failure Mode F1.11: The RECW cannot be disabled

The driver may fail to disable the RECW due to:

(F1.11.1) Electronics failure (S=3, O=2)

The effect of this failure is not severe and could only annoy some drivers. It will be annoying and distractive, however, when the system has a high false alarm rate and the driver cannot disable it.

The design requirements and recommendations are:

(F1.11.1) The system electronics must be sufficiently reliable and must have supervisory elements in hardware. The warning device shall be such that the driver can turn it off easily in case he/she cannot disable the RECW.

Potential Failure Mode F1.12: The threshold of the RECW cannot be adjusted

This failure mode may be due to:

(F1.12.1) Electronics failure (S=7, O=2)

The effect is that the driver may get annoyed and uncomfortable with the system if the default threshold is set too low leading to many unnecessary warnings. If the threshold cannot be adjusted from a high value to a lower one the driver may no longer receive warnings when rear-end collisions are imminent.

The design requirements and recommendations are:

(F1.12.1) The controller electronics must be sufficiently reliable. The threshold shall default to a low level when the RECW is enabled for the first time.

Potential Failure Mode F1.13: The correct braking capabilities and intentions are not communicated to the trailing vehicle.

The above failure mode may be the result of:

(F1.13.1) Failure or inaccuracies of sensors estimating braking capabilities and/or diagnostics failure (S=9, O=6)
(F1.13.2) Transmitter failure (S=9, O=3)

The effect of these failures is a delayed response of the RECW of the trailing vehicle and the possibility of a rear-end collision if the driver of the trailing vehicle is not attentive. The difficulty in estimating accurately the braking capabilities of the vehicle accounts for the fairly high occurrence rating. The design requirements and recommendations are:

(F1.13.1) The vehicle must have reliable sensors and diagnostics for estimating braking capabilities and braking levels. The system must have diagnostics to monitor the performance of sensors and detect malfunctions. The trailing vehicle shall be notified of the inability of vehicle to accurately estimate braking capabilities and intentions. The driver shall be notified and possibly asked to exit the lane.

(F1.13.2) The system must be able to detect transmitter failures, by employing supervisory elements in hardware. The driver shall be notified and possibly asked to exit lane.

The accurate estimate of the braking capabilities of the vehicle is an issue that needs further research. Multiple sensors may be necessary to measure all the variables that affect braking.

H1.3 Blind-spot warning

Potential Failure Mode F1.14.1: The system is unable to provide warning

The system may fail to give a warning due to any one of the following factors:

(F1.14.1.1) Blind spot sensor failure (S=7, O=5)
(F1.14.1.2) Electronics failure or software failure (S=7, O=2)
(F1.14.1.3) Threshold has been set too high (S=7, O=4)
(F1.14.1.4) Warning delivery device failure (S=7, O=2)

The effect of these component failures is that safety will be compromised during lane changing if the driver relies too much on the warning. The design requirements and recommendations are:

(F1.14.1.1) Supervisory elements must monitor the output of the sensor for reasonableness and consistency. The driver shall be notified when a malfunction is detected.

(F1.14.1.2) Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.

(F1.14.1.3) The default threshold must be set to a low level. The driver shall be aware of the lack of warnings due to the high threshold setting.

(F1.14.1.4) The warning device must be reliable. Redundant warning delivery methods shall be used.

Potential Failure Mode F1.14.2: The system gives false alarms

False alarms may be given by the system due to the following failures:

(F1.14.2.1) Blind spot sensor gives incorrect reading (S=5, O=5)
(F1.14.2.2) Electronics failure or software failure (S=5, O=2)
(F1.14.2.3) Threshold has been set too low (S=5, O=4)
(F1.14.2.4) System misinterprets driver intention to change lanes (S=5, O=7)

The above failures may lead to many false alarms that may distract the driver and reduce his/her confidence level in the system. The design requirements and recommendations are:

(F1.14.2.1) Supervisory elements in hardware and software must be used to monitor the sensor. The driver shall be notified when a malfunction is detected.

(F1.14.2.2) Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.

(F1.14.2.3) The driver shall be able to select a threshold level that he/she is comfortable with. The default threshold must be set to a level appropriate for typical conditions.

(F1.14.2.4) A reliable method must be used to sense the intentions of the driver to change lanes or the system must be redesigned to eliminate the necessity of sensing the driver's intentions.

If the system is on all the time the false alarm rate will be high due to the detection of vehicles in the next lane that are not threatening. If the warning is audible a high false alarm rate may be very undesirable to the driver. If the warning is visual such as a head up display indicating the presence of an obstacle in the blind spot a high "false" alarm rate may be acceptable but the warning may not be as effective. The BSW must be active and ready to operate before the driver initiates lane changing. A method must be developed that meets this requirement without introducing false alarms. Sensing the turn signal and steering wheel angle is another method of detecting the intentions of the driver to change lanes and activating the BSW. This method , however, may lead to a delayed warning that may not be effective. Further research is needed in order to develop a method for activating the BSW.[19]

Potential Failure Mode F1.15 : The BSW cannot be enabled

The driver may not be able to switch the BSW on due to:

(F1.15.1) Electronics failure (S=6, O=2)

The effect of this failure is not safety critical provided the driver is aware that the BSW is not on.

The design requirements and recommendations are:

(F1.15.1) The controller electronics must be sufficiently reliable and must have supervisory elements in hardware and software. The driver shall be notified of the BSW operating mode i.e.: on, off, malfunction.

Potential Failure Mode F1.16: The BSW cannot be disabled

The driver may not be able to disable the BSW due to :

(F1.16.1) Electronics failure (S=3, O=2)

The design requirements and recommendations are:

(F1.16.1) The controller electronics must be sufficiently reliable. There shall be redundant methods to disable the BSW.

Potential Failure Mode F1.17: The threshold of the BSW cannot be adjusted

The threshold of the BSW is adjusted by the driver. This adjustment may not be possible due to:

(F1.17.1) Electronics failure (S=6, O=2)

The effect of such failure is that the driver may feel uncomfortable with the current threshold. If the threshold is high the driver may not receive warnings when he/she should and if it is low the driver may receive many unnecessary warnings. Such response will be annoying and will reduce the level of confidence in the system.

The design requirements and recommendations are:

(F1.17.1) The controller electronics must be sufficiently reliable. The threshold setting shall default to a low level when the BSW is enabled for the first time. The driver shall be able to read and verify the selected threshold setting.

H1.4 Driver Vehicle Roadway Interface

Potential Failure Mode F1.18: Failure of the check-in function

The check-in function may failed to perform as designed due the following:

(F1.18.1) On-board diagnostics failed to detect a fault in major functions of the vehicle (S=8, O=3)
(F1.18.2) Driver ignores the results of on-board diagnostics (S=8, O=3)
(F1.18.3) On-board diagnostics made a wrong decision about a component or function that was not at fault (S=5, O=2)

The effect of the first two failures is that the vehicle will enter and operate in the dedicated lane without being fit. The last failure will stop the vehicle from entering the dedicated lane even though it is fit. The

severity of the first two failures is fairly high . It will affect safety and efficiency especially if the vehicle stays in the lane for a long time. The design requirements and recommendations are:

(F1.18.1) The diagnostic algorithms must be robust and highly reliable.

(F1.18.2) The roadway must be able to identify an unfit vehicle operating in the dedicated lane. Traffic rules and regulations must be used to deter the driver from violating the rules.

(F1.18.3) On board diagnostics must be highly reliable. Redundancies and supervisory elements must be considered for improving reliability.

Potential Failure Mode F1.19: Vehicle fails to enter the dedicated lane

The driver may fail to merge into the dedicated lane due to the following:

> (F1.19.1) Dedicated lane is congested or driver is not able to merge due to high speed and/or small headways in dedicated lane or driver doesn't have the required skills (S=5, O=4)

The effect of this failure is that the vehicle is restricted from or delayed in entering the dedicated lane. This will lead to possible congestion in the transition lane or entrance to the lane.

The design requirements and recommendations are:

(F1.19.1) The roadway must be able to enforce lower speeds and larger headway near the entry points. Driver skills for lane merging shall be tested as part of the licensing procedure.

Potential Failure Mode F1.20: Driver fails to respond to BSW and RECW

The driver may fail to respond to the BSW or RECW or both due to the following:

> (F1.20.1) Driver ignores warning unintentionally or becomes confused (S=9, O=6)
> (F1.20.2) Driver ignores warning intentionally due to high false alarm rate (S=8, O=6)

The potential effects of these failures are driver confusion that may lead to panic and/or inappropriate response that in turn may lead to collisions. Of particular importance is the situation where both the BSW and RECW are sending warnings at the same time. The severity and occurrence ratings of these effects may be reduced by using the following design requirements and recommendations:

(F1.20.1) The warnings shall be very clear and unambiguous to the driver. Driver interface shall be as simple as possible

(F1.20.2) False alarm rate must be very low. Warning signals shall be easily distinguishable from each other. Warning threshold shall be adjustable by the driver.

Potential Failure Mode F1.21: Driver fails to respond to traffic information

The driver may fail to respond to traffic information provided by the roadway due to the following:

(F1.21.1) Driver capability is impaired or traffic information is unclear or confusing (S=4, O=5)

The effect of the failure is that the efficiency of the dedicated lane may be affected. Under some circumstances safety may be affected if the driver ignores the advice from the roadway. The design requirement is that:

(F1.21.1) The roadway traffic information shall be clear and brief.

Potential Failure Mode F1.22.1: Driver cannot exit the dedicated lane

The driver may not be able to exit the lane due to:

(F1.22.1) Congestion in the manual lane or the transition lane (S=4, O=5)

The effect is that the vehicle will remain in the dedicated lane. If the vehicle is exiting due to malfunction of the automated functions, then the efficiency of the dedicated lane may be degraded. The design requirement is that:

(F1.22.1) A dedicated transition lane or some form of regulation such as "yield to auto lane" must be implemented to ensure easy exit even when traffic congestion exists in the manual lane. The roadway must warn the driver of congestion ahead of time via traffic information communication.

Potential Failure Mode F1.22.2: Driver doesn't exit the dedicated lane and operates in manual mode

In this case the driver misses the exit by failing to:

(F1.22.2) Perform the necessary steering action (S=4, O=5)

Since the driver remains in the lane and operates in manual mode the efficiency of the lane will be affected. The recommendation is that:

(F1.22.2) Law enforcement must be used when traffic rules are violated. If a vehicle operates in the manual mode and skips exits intentionally it will constitute a violation of the traffic laws.

Potential Failure Mode F1.23.1: System doesn't switch to manual control

The system may fail to revert to manual mode due to:

(F1.23.1) Hardware or software failure (S=6, O=4)

The effect of such failure is that the vehicle will remain in the automated mode under conditions that may not be safe. For example the system may have to operate in the manual mode if road and/or environmental conditions are such that the operation of sensors and communication devices is unreliable. By remaining in the automated mode safety may be affected. The design requirements and recommendations are:

(F1.23.1) The system shall have two independent ways to disable itself. The driver must be notified whenever the mode of operation changes. The driver shall have more than one way of disabling the system.

Potential Failure Mode F1.24: The system fails to notify the driver of current mode of operation.

The system may fail to notify the driver of the current mode of operation due to:

(F1.24.1) Electronic or software malfunction (S=9, O=2)

Such failure may confuse the driver, since the vehicle may be doing something different that is unknown to the driver, cause annoyance, panic and loss of confidence to the system that will have negative consequences on safety. The occurrence rating of the failure is very low due to the reliability of current electronics and software.

The design requirements and recommendations are:

(F1.24.1) The electronics and software of the SHM and interface with driver must be very reliable. Redundancies and diagnostics must be used to improve reliability.

Vehicle, Driver Diagnostics and Maintenance

Vehicle Diagnostics

To guarantee an acceptable performance and reliability level for a future Automated Highway System (AHS) architecture, without over-designing its components and without introducing unnecessary redundancies, we will have to design and install a thorough network of self testing capabilities and diagnostics. This is the approach already taken by every vehicle manufacturer today,[3,4] when they introduce complex electronic systems on the car such as Electronic Fuel Injection, Electronic Engine Management, Anti-Lock Brakes, and Air-bag deployment circuits. These systems have significant responsibility for the handling and safety of the vehicle, yet it is not economical to over-design them with multiple redundancies. The alternative approach taken is to design a sufficient number of tests and diagnostics so that if there is failure or malfunction, it will be diagnosed and isolated as early as possible.

The level of diagnostic tests on the vehicle has been in a constantly increasing pattern since the advances of electronic technology and integrated circuit technology allow the complexity of the electronic subsystems of the vehicle to increase and cost to decrease, year after year. Since cost remains a factor though, we tend to see more comprehensive self tests and diagnostics in more expensive and luxury type car lines, regardless of manufacturer or country of origin.

One of the results of the FMEA is a list of recommended diagnostics for each function of component that affects the SHM, RECW and the BSW. The need for these diagnostics follows the trend of adding diagnostics in most electronic and subsystems as well as crucial mechanical and hydraulic parts for most of the new vehicles.[3,4] These diagnostics monitor performance, detect failures and keep the driver informed about their operating status and the need for maintenance.

The most crucial diagnostics are those that affect safety. In ERSC 1 the diagnostics for the ranging sensor, brake actuator, braking path and associated electronics and software are the most essential ones.

The diagnostics for the reasonableness and accuracy of the ranging measurements are the most difficult to develop especially in the case where only one ranging sensor is available. The sensor may have all the self-tests and diagnostics, but it may have unreliable measurements due to curved roads, interference from sensors in other vehicles etc.[14] The requirement for two ranging sensors not subject to common mode failures may help the development of reliable diagnostics. In this case the outputs of the two sensors can be compared for consistency and a certain criterion be used to choose the one with the correct response when the two responses are different. The development of such criterion using vehicle models and expert techniques is an issue for further research.

The use of three ranging sensors not subject to common mode failures is a better alternative even though more costly. In this case the majority rule can be used to select the correct measurement when one sensor output differs from the others. When all three sensor outputs differ, a case of multiple failures, a criterion could be used for the selection of the correct output or the system should stop relying on the sensors. An executive controller could be used to monitor the actions of SHM and RECW as shown in figure 8. The Controller is based on a vehicle model whose outputs are compared with those of the vehicle for consistency.

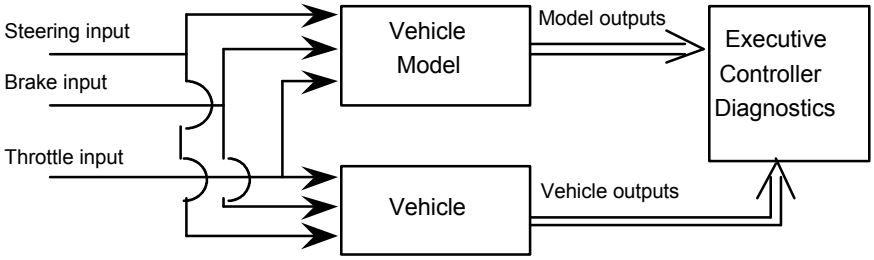

Figure 8: Overall diagnostics system.

The executive controller can make decisions about the consistency of sensor measurements, actuator response etc. Due to the availability of accurate vehicle models that have been validated with real data the above method is quite feasible. The details of the executive controller and the level of accuracy and reliability that can be achieved are issues that need further research.

Driver Diagnostics

In ERSC 1 there are no special demands for driver diagnostics that go beyond those that are researched for manual driving.[20,21,22] The availability of the ranging sensor(s) and RECW, however, may be used to monitor driver behavior for braking even during manual driving. The driver's reaction time for rear-end collision avoidance could be estimated and used to improve the reliability of RECW.

Techniques such as neural networks [23] may be used to model driver's behavior in braking. The driver will be identified with an identification number that some recent vehicles already use for automatic adjustment of mirrors, seats etc.[24] The driver's model could be used in connection with diagnostics to monitor driver's behavior in braking as shown in figure 9.

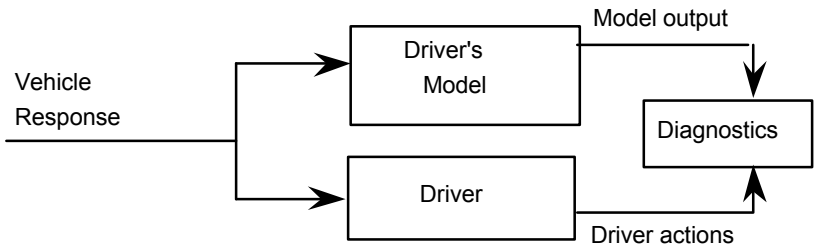

Figure 9: Overall diagnostics system for driver.

The system may be able to assess the driver's reaction time to braking and use that for the minimum value of the TTC or warn the driver when his/her behavior is unsafe. More research is required to develop and evaluate the effectiveness of such a system.

Maintenance Requirements

The automotive industry has the goal of continuously improving product reliability, because it has been proven to be a strong customer desire and a fundamental product characterizing attribute. Therefore the manufacturers make efforts to design and build most vehicle components that are subjected to wear, so that their expected lifetime will match or exceed the expected lifetime of the entire vehicle.[25] This is not always possible though because designing every component to this requirement would require over-designing certain components to the point of overburdening their cost. So it has become an accepted practice that certain components like brake friction materials, clutch friction material and engine and transmission lubricants will have to be replaced at certain periodic intervals.

The mean expected life or the Mean Time To Failure (MTTF) of electronic components is typically very high, because the wear-out mechanism of electronic components are almost insignificant compared to that of mechanical components subjected to loads.[2,26] Wear-out mechanisms for electronic components do exist, however. They affect mostly circuit areas that carry high current densities. Careful design of such susceptible areas can minimize the consequences and bring the reliability of those areas to the same level as the rest of the system. With the proper design, wear-out effects on electronic circuits and systems take very long to manifest. The current trend in most automobile companies is for the electronic components to be free of maintenance for at least 10 years or 150,000 miles.[25] This trend is expected to continue with the vehicles for ERSC 1. One particular area that may affect maintenance is the alignment of ranging sensors. Following the trend of low maintenance the ranging sensor(s) should be mounted so that no frequent alignments are required.

Retrofitting

Retrofitting existing vehicles with the appropriate hardware to enable them to operate on automated lanes is going to be a challenging task. Normally a car is never subjected to any major modifications during its lifetime. Most service stations, both dealer owned and independent, prefer to repair faulty parts using either original parts or parts that are fully compatible. They rarely perform any kind of retrofitting of major subsystems.

One notable exception, the retrofitting of an air conditioning (A.C.) unit in a vehicle that is not already equipped with one is usually facilitated by the fact that most vehicles have been designed for the option of having an air conditioner, but that option may have not been installed at the factory. Even though it is relatively easy, retrofitting an air conditioner is quite expensive. Certain vehicle manufacturers were

building cars with the option to be easily retrofitted with air-conditioning, but after the market analysis showed them that this was an option that most customers wanted anyway, they decided it was more economical to produce the vehicles with factory installed A.C.[25]

Retrofitting vehicles with components that affect the control and motion of the vehicle, which is the case for ERSC 1, will be even a more challenging and costly proposition when compared with the retrofitting of A.C.

Retrofitting a system of sensors, actuators computers and communication transceivers on an existing vehicle may be a prohibitively expensive proposition. Practically all vehicles manufactured until today have not been designed to accommodate the addition of so many new components. Furthermore each make and each model poses a unique problem especially on the issue of retrofitting it with actuators for throttle and brake control, by the fact that each model has adopted a different layout and arrangement of critical engine components and driver controls. The retrofitting of the various components that affect the control of the vehicle cannot be complete without several time consuming road tests. Such tests will drive the cost even higher and make retrofitting a non feasible proposition.

An alternative strategy that stands to reason is that manufacturers might choose to build vehicles that are "AHS ready by retrofitting" and provide all the mounting points and electrical connections for the sensors actuators and computers except the AHS equipment itself. This might be a very desirable strategy for the manufacturers in the early years of AHS when they are not certain of what the market demand for AHS will be. This way, a customer who does not want or need AHS capability is not burdened with the cost of these components but he has the assurance that his vehicle will not be obsolete if in the near future he decides to participate in AHS. Retrofitting in this case may be less costly but road testing may still be necessary and will drive up the cost. Most likely, vehicles built to be "AHS ready for retrofitting" will be more expensive than those without this feature. As a result people will buy such vehicles if they are absolutely sure they will use AHS in the future although they cannot buy or use now for various reasons such as cost, relocation etc.

Another possible category of vehicles that could be candidates for retrofitting for ERSC 1 are those that are built independently of AHS but have features that are common to AHS. For example vehicles with intelligent cruise control capability and a rear-end collision warning, developed independently of ERSC 1, that are capable of performing most of the functions of ERSC 1, could be retrofitted with roadway to vehicle communication devices and blind spot warning sensors. Such retrofitting will require software and possibly hardware changes as well as road testing and could also drive the cost high. The following table summarizes the result of retrofitting for ERSC 1.

Table 3: Retrofitting for ERSC 1.

Category of Vehicles	Technically Feasible	Cost	Expected Consumer Acceptance
Vehicle with no ERSC 1 capabilities	Yes	Very High	Unlikely
Vehicle built for easy retrofit	Yes	High	Unlikely
Vehicle built independent of ERSC 1 but have some capabilities for ERSC 1	Yes	Moderate to high depending on the extent of retrofitting	Questionable

The retrofitting of small electronics components such as communication devices may be feasible and acceptable provided it is not costly and serves a good purpose.

Deployment Scenarios

ERSC 1 could become the first deployment stage of AHS if the reliability problems addressed in the FMEA as well as the associated liability problem[27] are resolved and the car manufacturers and federal, state and local governments come together to make such a system work by dedicating lanes and agreeing on standards and protocols.

The car manufacturers both in USA, Europe and Japan are moving in the direction of developing vehicles that can perform several of the important vehicle functions of ERSC 1. A system known as intelligent cruise control with the capability of maintaining cruise speed and headway will soon be available as an option in a number of vehicles. Rear-end collision warnings and blind spot warnings have also been developed and tested.[15,19] On the other hand, short range vehicle to roadside communication technologies developed and tested during the past few years[12,13] make the roadway to vehicle communication function easy to implement.

The deployment of these technologies independent of ERSC 1 will improve the understanding of the technical and human factors issues involved and will test customer acceptance and popularity. The driving force behind customer acceptance will most likely be safety and driver comfort.

The development, maturity and customer acceptance of the technologies relevant for ERSC 1 technologies will motivate the implementation of ERSC 1 in order to obtain benefits in terms of congestion management, capacity and safety. The implementation of ERSC 1 may take place under two different scenarios.

In the first scenario almost all the vehicle, roadway and driver functions essential for ERSC 1 are already developed to be used in the same lanes with manually driven vehicles. As the number of the equipped vehicles increases and the potential benefits are well understood and accepted it may make sense to the federal, state and local governments to dedicate lanes to such vehicles in order to realize these benefits.

In the second scenario ERSC 1 forms the first stage of AHS implementation that is developed by the cooperation of government and automobile manufacturers. The government provides the dedicated lanes and roadway instrumentation and automobile manufacturers produce the specially equipped vehicles.

ERSC 1 may not necessarily be implemented the way it is described in this report. For example for liability reasons the roadway target speed command could be made to be an advisory for the driver rather

than followed directly by the vehicle at the expense of reduced benefits of course. Another possible modification is to have multiple dedicated lanes for ERSC 1.

In summary, the current and near term emerging technologies make it technically feasible to deploy ERSC 1 as the first stage of AHS. Some of the difficulties of making it happen is the possible inability to dedicate a lane for AHS and the failure of the government and automobile manufacturers to work together and make it happen. The experience and problems associated with the dedication of HOV lanes could be used as a comparison.[28]

Key Results and Conclusions

1. Despite the fact that the driver is fully responsible for all emergencies and is a back-up to all partially or fully automated functions a rear-end collision may still take place if certain functions fail to perform as designed. In particular the ranging sensor measurements are the most susceptible ones to errors and the most critical ones with respect to safety. Our design requirements and recommendations call for two to three redundant ranging measurements that are not subject to common mode failures with the appropriate diagnostics that allow the system to select the correct measurement. The ranging sensors must have a wide field of view and easily distinguish between valid and invalid targets.

2. The brake actuator and braking path also needs to be highly reliable. The driver's expectation that the system will apply soft braking in a potential rear-end collision situation may delay the driver's response for rear-end collision avoidance.[17]

3. The accurate estimate of the braking capabilities of the vehicle is an issue that needs further research. One of the most important factors of braking capability is the friction coefficient between tires and the road. It depends on many factors such as the type of tire, the tire pressure, the condition of the road, etc. An accurate estimate of friction coefficient [29,30] will help reduce the false alarm rate of the RECW and improve its effectiveness.

4. The communication of the braking intentions of the preceding vehicle to the following one plays the role of the red brake lights in manual driving. It is an important feature that improves the reliability and accuracy of the RECW. The best method of communication in this case that is not susceptible to interference is a technical issue that needs to be addressed.[31]

5. The use of the blind spot warning in ERSC 1 is supposed to assist the driver during lane changing. The effectiveness of the warning will depend on how and when it is given to the driver. Human factor studies are required to resolve the above issue.[19]

6. The purpose of the rear-end collision warning (RECW) in ERSC 1 is to warn the driver to take action and avoid a rear-end collision. The RECW relies on the ranging sensor measurements that need to be highly reliable. A non-reliable RECW system may give the driver a false sense of security and be responsible for rear-end collisions.[32] Redundant ranging sensors with a wide field of view and with the capability of distinguishing between valid and invalid targets and between threatening and non threatening objects are essential. Further research is required to develop such reliable sensing systems.

7. All automated or partially automated functions and warnings shall have on board diagnostics that monitor their performance and functionality. These diagnostics could be used even when the vehicle is in the manual mode. As a result the driver will be notified if his/her vehicle is not fit to operate in the

dedicated lane before he/she approaches the lane. Therefore no elaborate and time consuming check-in procedures may be required at the entrance to the dedicated lane.

8. For ERSC 1 no special driver diagnostics are essential. The on-board ranging sensors, however, and the associated software and hardware tools may be used to monitor and assess the performance of the driver during manual driving and use the results to warn the driver in case of inappropriate behavior.

9. The driver interface with the vehicle functions and roadway should be clear and simple. Human factor studies are required to understand the interface of the driver with the vehicle and roadway functions of ERSC 1. Current human factors studies on intelligent cruise control systems may provide considerable knowledge that is relevant to ERSC 1.

10. The trend of low maintenance vehicles is expected to continue with the vehicles for ERSC 1.

11. Retrofitting is expected to be an expensive proposition. It is unlikely that it will be accepted by the users. Retrofitting of small electronic components that do not affect the motion and safety of the vehicle may be feasible.

12. The deployment of AHS is likely to take place in stages by following an evolutionary path. Each stage of deployment should provide to the user obvious benefits that will include effective congestion control, lower accident rates, shorter travel time, higher capacity and lower pollution. For ERSC 1 to form the first deployment stage of AHS the reliability problems identified by the FMEA should be resolved. Furthermore, the state and/or federal government have to allocate a dedicated lane to AHS and provide the required support by working together with automobile manufacturers. In addition, further research is required on legal, liability and social issues associated with such deployment.

SECTION 3 ERSC 2 ANALYSIS

As with ERSC 1 we analyze the vehicle operational issues and risks associated with ERSC 2 by first developing a detailed description of the vehicle functions and interface with the roadway and driver that we use to perform a system level FMEA. The results of the FMEA are used to discuss reliability, redundancies, diagnostics, fault-tolerant designs, maintenance and the feasibility for deploying ERSC 2. The issue of retrofitting vehicles that are not originally build for ERSC 2 for operation in ERSC 2 is discussed. The section is concluded with a list of key findings and conclusions.

Vehicle Functions and Interface with Roadway and Driver

We present the specific functions and sub functions of the roadway vehicle and driver that we will analyze for ERSC 2.

Operational Scenario

On-board vehicle diagnostics notify the driver whether the vehicle is fit to operate on the dedicated lane well before reaching the lane. Once the vehicle is close to the dedicated lane it establishes communication with the roadway and presents its fitness status and identification to the roadway. If the vehicle is fit the roadway gives permission to enter the lane. The driver drives the vehicle to the entrance of the dedicated lane and looks for a safe gap for merging the vehicle. The roadway coordinates the

traffic and assists vehicles to merge into the lane by creating appropriate gaps. Once in the lane, the driver accelerates to a desired speed and switches on the SHM and the rear-end collision avoidance (RECA) functions, the blind spot warning, the lane departure warning and steering assist function. If there is no vehicle or obstacle within a certain range the SHM function maintains the current speed and responds to driver commands for increasing it or decreasing it. If another vehicle is within the range of the vehicle then the SHM establishes communication with that vehicle and calculates a safe headway to be used for vehicle following. The safe headway is calculated based on the braking capabilities of the vehicle, the information about the braking capabilities of the preceding vehicle obtained via communications and any headway recommendation received from the roadway. The SHM adjusts the vehicle speed in order to reach and maintain the calculated headway. The SHM responds to roadway target speed commands provided the response does not lead to a reduction of the selected headway. The switching from headway to speed maintenance is the same as in ERSC 1. The SHM uses engine torque and soft braking to control the speed and headway. Hard braking is the responsibility of the RECA function.

The RECA function monitors the actions and responses of the SHM and calculates the minimum time to collision (TTC). If the TTC becomes less or equal to the time required for bringing the vehicle to a full stop without collision, the RECA provides the appropriate commands to the brake actuator by overriding the actions of the SHM.

The driver cannot intervene in the operation of the SHM and RECA functions by overriding the actions of the throttle and brake. The driver, however, can initiate a disabling procedure during which the SHM function reduces the speed and increases the headway to some default values that are compatible with driver skills and reaction times and warns the driver to resume control.

The function of the blind spot warning is the same as in ERSC 1. The lane departure warning senses the position of the vehicle in the lane and warns the driver if the lateral deviation exceeds a certain threshold that is adjusted by the driver. For this function to work the roadway provides lane identification aids. The steering assist function helps the driver with steering by correcting his/her steering inputs for better stability of the lateral motion of the vehicle.[34,35,36]

At the end of the trip the driver initiates a check-out procedure by starting the disabling of the SHM and RECA functions, that put him/her in a position that he/she can handle, and exits the lane. The driver may be required to initiate a check-out procedure when any one of the functions such as the SHM or the RECA and/or the lane departure warning are malfunctioning. A possible fall-back mode that may allow the driver to remain in the lane for a period of time operating as in ERSC 1 is if the lane departure warning is not working and/or the RECA can only operate as a RECW. In all other cases of malfunctions the driver may be required to exit the lane as soon as possible using the next available exit.

The entry and exit configuration for ERSC 2 are the same as those for ERSC 1 and are shown in Figures 2, 3.

The development of the vehicle functions is achieved by starting with the high level functions described in the above operational scenario. These are:

H2.1 Speed and Headway Maintenance and Rear-end Collision Avoidance
H2.2 Blind Spot Warning
H2.3 Lane Departure Warning
H2.4 Steering Assist
H2.5 Driver Vehicle Roadway Interface

The main functions for ERSC 2 are presented below:

H2.1. Speed and Headway Maintenance and Rear-end Collision Avoidance.

The SHM and RECA functions interact with each other in order to provide a full-authority longitudinal control. The functional block diagram of these two functions is shown in figure 10.

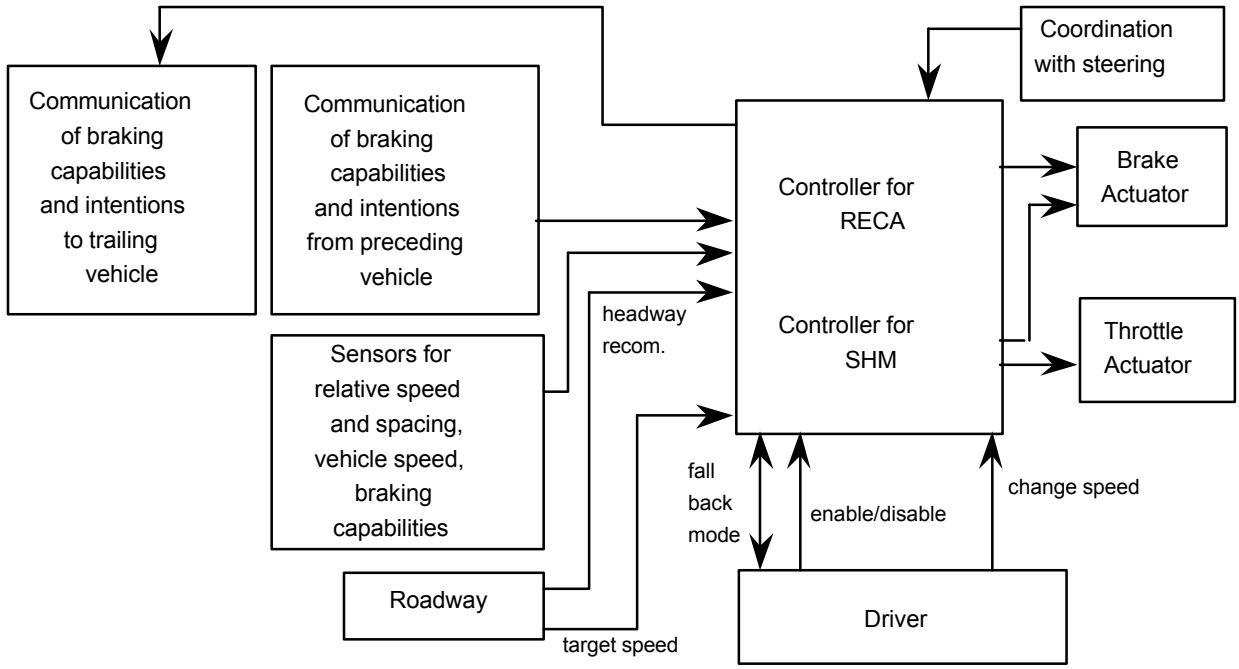

Figure 10: Speed and headway maintenance and rear-end collision avoidance.

Inputs:

Vehicle speed from speed sensor
Relative speed and spacing from ranging sensor
Braking capabilities of vehicle obtained using on board sensors
Braking capabilities and intentions of preceding (target vehicle) obtained via communications
Driver commands: enable, disable and speed/headway changes
Roadway commands: target speed, headway recommendations based on road conditions, traffic status and environmental conditions.
Steering angle and preview road data.

Outputs:

Throttle actuator command
Brake actuator command
Mode of operation
Braking capabilities and intentions to trailing vehicle

Functional specifications:

The system calculates the safe headway based on the braking capabilities of the vehicle, the information about the braking capabilities of the preceding vehicle obtained via communications and any headway recommendation received from the roadway. The SHM adjusts the vehicle speed in order to reach and

maintain the calculated headway. The SHM responds to roadway target speed commands provided the response does not lead to a reduction of the selected headway. The switching from headway to speed maintenance is the same as in ERSC 1. The SHM uses engine torque and soft braking to control the speed and headway. Hard braking is the responsibility of the RECA function.

The RECA function monitors the actions and responses of the SHM and calculates the minimum time to collision (TTC). If the TTC becomes less or equal to the time required for bringing the vehicle to a full stop without collision the RECA provides the appropriate commands to the brake actuator by overriding the actions of the SHM.

The driver cannot intervene with the operation of the SHM and RECA functions by overriding the actions of the throttle and brake. He/she can initiate a disabling procedure during which the SHM function reduces the speed and increases the headway to some default value that is compatible with driver skills and reaction times[9,19] and warns the driver to resume control.

The system uses steering angle data and preview road information to adjust speed around curves.

The main functions of the SHM and RECA and the functional and reliability requirements are:

F2.1 Calculate safe headway
The SHM uses information from on-board sensors that sense the vehicle's braking capabilities, the braking capabilities of the preceding vehicle obtained via communication and headway recommendations from the roadway to calculate a safe headway for vehicle following. The calculation of the safe headway shall take into account all factors and worst case stopping scenarios.

F2.2 Maintain cruise speed
The vehicle shall maintain a driver selected speed when no moving or stationary obstacles are within a certain range. It shall respond to driver commands for changing the speed if there is no target speed from the roadway.

F2.3 Track and maintain roadway commanded target speed
The vehicle shall track and maintain the roadway commanded speed as long as no moving or stationary obstacles are within a certain range.

F2.4 Maintain headway
The vehicle shall maintain the headway selected by the vehicle or the driver under all environmental conditions, road geometry and freeway speeds.

F2.5 Switch from maintaining cruise speed to maintaining headway
When the system senses a valid target in the same lane that is within the calculated certain range it shall switch to the following mode by maintaining a safe headway calculated by the vehicle.

F2.6 Switch from maintaining headway to maintaining cruise speed
When the target is no longer within the calculated default headway the system shall switch to maintaining the current cruise speed.

F2.7 Switch from maintaining cruise speed to maintaining the roadway commanded
target speed. The system shall respond to roadway target speed commands by changing current cruise speed to the target speed in a smooth manner provided no obstacle is within a certain range

F2.8 Hard braking for rear-end collision avoidance
The system shall calculate the time to collision (TTC) continuously by monitoring the actions and response of the SHM function, the status of the vehicle and of the preceding one. If the TTC becomes less or equal to the time required for stopping without collision then it shall send the appropriate command to the brake actuator to avoid a rear-end collision.

F2.9 Enable the SHM and RECA
Upon driver command the SHM and RECA shall both be switched on at the same time.

F2.10 Disable the SHM and RECA
Upon driver command the SHM and RECA functions shall be disabled by first reducing the speed and increasing the headway to levels that are considered to be safe for manual driving.

F2.11 Communication of braking capabilities and intentions to the trailing vehicle
The system shall communicate the vehicle's braking capabilities and intentions to the trailing vehicle in the same lane under all freeway conditions.

F2.12 Speed control around curves
The system shall maintain vehicle stability and driving comfort around curves by adjusting vehicle speed and headway under all environmental and road conditions. The system may use preview road information from the roadway and steering angle information to generate the appropriate commands for the throttle and brake actuators.

H2.2 Blind Spot Warning

The functional block diagram of the blind spot warning is shown in figure 11.

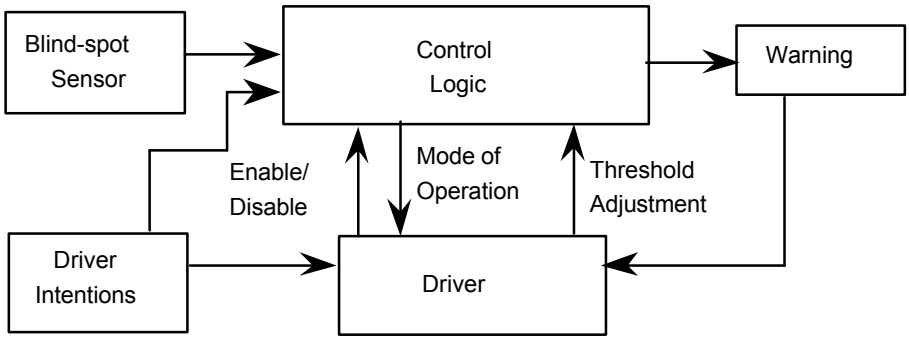

Figure 11: Blind-spot warning.

Inputs:
Presence of vehicle in blind spot on either side of the vehicle detected by the blind spot sensor.
Driver's intentions used for activation of the system
Driver commands: enable, disable, threshold adjustment.

Outputs:
Warning to the driver
Mode of operation: on, off, malfunction

Functional specifications:

The BSW provides a warning to the driver when a moving or stationary obstacle is in the blind spot region on the side of the vehicle where the vehicle is turning. The BSW is activated by sensing the intentions of the driver to change lanes. It responds to driver commands for enabling, disabling and adjusting the threshold. The system informs the driver whether it is on or off and when a malfunction is detected by the on board diagnostics.

The specific functions of the BSW and reliability functional requirements are listed below:

F2.13 Warn Driver

The system shall sense the intentions of the driver to change lanes and provide an early warning if an obstacle is present in the blind spot region on the side of the vehicle where the vehicle is turning without false alarms.

F2.14 Enable BSW

Upon driver command the BSW shall switch on.

F2.15 Disable BSW

Upon driver command the BSW shall disable itself.

F2.16 Adjust Threshold

Upon driver command the size of the blind spot region sensed shall be adjusted as long as it does not exceed a certain minimum threshold.

The function associated with the mode of operation is considered to be part of the driver vehicle roadway interface.

H2.3. Lane Departure Warning

The functional block diagram of the lane departure warning (LDW) is shown in figure 12 below:

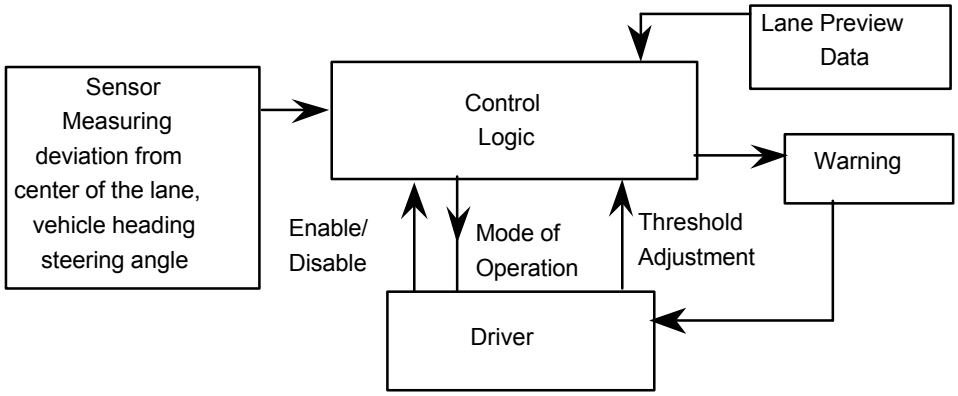

Figure 12: Lane Departure Warning.

Inputs:

Deviation from center of the lane and vehicle heading data
Steering angle, turn signal status
Preview information about the geometry of the roadway
Driver commands: enable, disable, threshold adjustment

Outputs:

Warning to the driver
Mode of operation: on, off, malfunction

Functional specifications:

The system estimates the time-to-lane crossing (TLC). The TLC is the time necessary for the vehicle to reach either edge of the lane. If the TLC is less than a certain default value the system provides a warning to the driver. The default value is adjusted by the driver by changing the threshold of the LDW. The system responds to driver commands for enabling and disabling itself and notifies the driver of its mode of operation: on, off, malfunction.

The specific functions of the LDW and the functional requirements are listed below:

F2.17 Warn the driver

The system shall calculate the TLC continuously and provide a warning to the driver when the TLC is less than a certain default value adjusted by the driver. The default value shall be greater than an a priori selected minimum value that takes into account the driver's reaction time to lane departure warnings.

F2.18 Enable LDW

Upon driver command the LDW shall be switched on.

F2.19 Disable LDW

Upon driver command the LDW shall be disabled.

F2.20 Adjust threshold

Upon driver command the default value of the TLC shall be adjusted

H2.4. Steering Assist

The functional block diagram of the steering assist system is shown in figure 13 below:

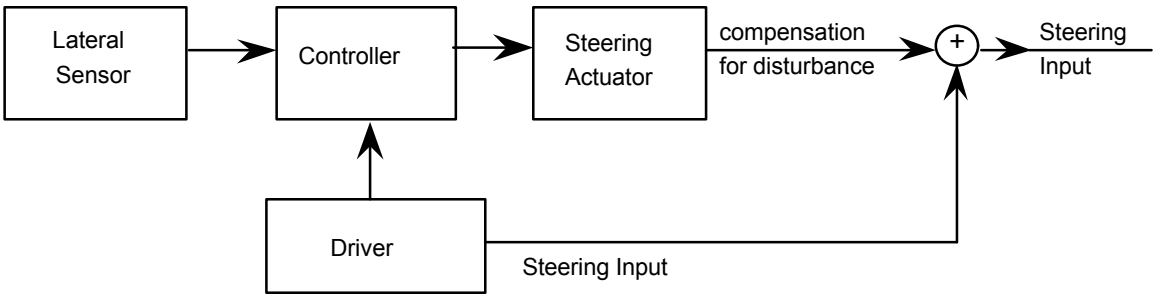

Figure 13: Steering Assist.

Inputs:

Lateral sensor measurements
Driver steering command

Outputs:

Steering input to steering subsystem

Functional Specifications:

The steering assist system augments the driver's steering inputs in an effort to improve the vehicle's lane keeping and lane changing performance and compensate for disturbances due to wind gust, road geometry etc.

The main function and functional and reliability requirements of the steering assist system is:

F2.21 Assist steering

The system shall attenuate the effect of high frequency disturbances by properly augmenting the driver's steering inputs.

H2.5. Driver, Vehicle, Roadway Interface

Figure 14 shows the block diagram of the driver interface with the vehicle and roadway.

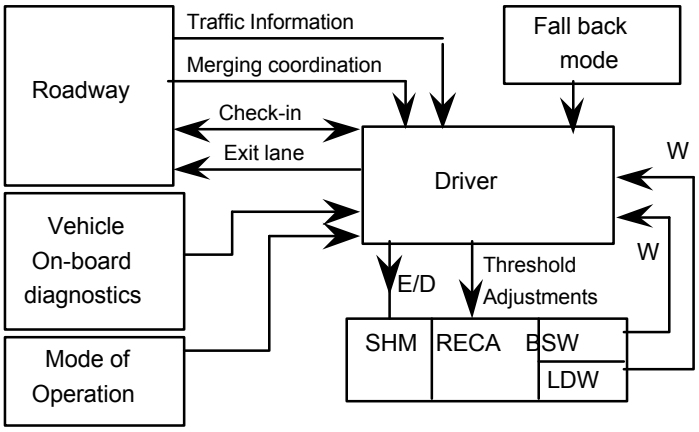

Figure 14: Driver interface with vehicle functions and roadway.

Inputs:

Traffic information from the roadway
Information from on board diagnostics and mode of operation
Warnings
Fall back mode instructions

Outputs:

Enable/Disable
Route selection
Manual control

The interface of the driver with the vehicle functions and roadway involve the following functions:

F2.22 Check-in

The driver responds to the on-board vehicle diagnostics and acknowledgment from roadway and verifies whether his/her vehicle is fit to operate on the dedicated lane.

F2.23 Enter the lane

The driver responds to the merging coordination and directions provided by the roadway, looks for a safe gap and drives the vehicle into the dedicated lane. Once in the lane he/she synchronizes the vehicle's speed and switches on the automated vehicle functions.

F2.24 Response to BSW and LDW

The driver responds to BSW and LDW by steering when the SHM and RECA functions are on and by steering and braking when the RECA function is off.

F2.25 Response to traffic information

The driver processes roadway traffic information in order to make routing decisions and/or assume full manual control if necessary.

F2.26 Exit the lane

The driver initiates check-out by starting a disabling procedure of the SHM and RECA functions. The SHM reduces speed and increases headway and notifies roadway of the driver's intention to exit the lane. The driver drives the vehicle out of the dedicated lane . The system sends a notification to the roadway.

F2.27 Fall back to ERSC 1

The vehicle functions revert to those of ERSC 1 in case of malfunctioning of the RECA function or when roadway conditions are such that headway calculation by the SHM is not possible. The system notifies the driver and reduces speed and increases headway to levels that the driver feels comfortable with. It warns the driver to assume the responsibility of rear-end collision avoidance.

F2.28 Fall-back to manual control

During malfunction of any of the automatic functions or during exiting from the lane the vehicle returns to the manual mode by reducing speed and increasing headway to comfortable levels and by warning the driver to assume manual control.

F2.29 Notify driver of mode of operation

The system shall notify the driver of its mode of operation, of malfunctions and provide clear instructions to the driver for changes in the mode of operation.

Failure Modes and Effects Analysis

The results of the FMEA for ERSC 2 are presented in table 13 of Appendix B. Below we present the identified failure modes and their potential causes together with their severity and occurrence ratings. We discuss their potential effects and give a list of design requirements and recommendations that could be used to reduce the severity and occurrence ratings. The Severity (S) and Occurrence (O) ratings are given in parentheses together with the potential causes of the failure modes. The significance and explanation of these rating are discussed in Appendix A and are summarized in tables 1 and 2.

H2.1 Speed and Headway Maintenance and Rear-end Collision Avoidance.

Potential Failure Mode F2.1: Loss of ability to calculate correct value of safe headway

The calculation of a safe headway to be used in vehicle following is one of the most critical functions in AHS. It has an impact on safety and capacity. The safe headway depends on a lot of factors that include the braking capabilities of the vehicle and those of the preceding vehicle, the friction coefficient between the tires and the road, the delays and accuracy of brake actuators and sensors, the current speed, computational delays etc.[8] In ERSC2 we assume that the vehicle is equipped with the appropriate sensors and diagnostics that make the necessary measurements and estimation of the factors that affect the safe headway. In addition the preceding vehicle communicates its braking capabilities and braking intentions which are essential in calculating the safe headway. The braking intentions of the preceding vehicle help in minimizing the computational delay and therefore reduce the value of the safe headway. The safe headway should be calculated based on a worst case stopping scenario.[8]

The system may fail to calculate the safe headway to be used by the vehicle due to lack of information from sensors and communication. It may also calculate an incorrect headway due to inaccurate information and undetected faults of sensors. The following are potential causes that may lead to incorrect or conservative estimates of the safe headway.

(F2.1.1) Detected malfunction or inability of the sensors to estimate the braking capabilities and intentions of the preceding vehicle and/or vehicle (S=6, O=6)
(F2.1.2) Detected malfunction or loss of communication with preceding vehicle (S=6, O=6)
(F2.1.3) Faulty or inaccurate measurements of braking capabilities of vehicle and/or preceding vehicle (S=10, O=6)
(F2.1.4) Incorrect braking capabilities and intentions are received through communication due to interference or noise corruption (S=10, O=6)
(F2.1.5) Loss of communication with roadway and/or lack of headway recommendation (S=6, O=4)
(F2.1.6) Loss of braking data information from preceding vehicle due to receiver malfunction (S=6, O=4).

The effect of on time detected failures, such as (F2.1.1), (F2.1.2), is that the lack of information due to the failures can be taken into account leading to a larger headway. A large headway has a negative impact on capacity and efficiency of the lane.

The effect of undetected failures, such as (F2.1.3), (F2.1.4), on safety is severe. Such failures may lead to short and unsafe headways with a high possibility of rear-end collision. They may also lead to larger than necessary headways. In this case safety is not affected but the efficiency of the lane is.

The lack of roadway headway recommendation and/or loss of information about the braking intentions of the preceding vehicle (Failures F2.1.5, F2.1.6) are considered to be detectable failures and therefore can be taken into account in calculating the safe headway. In this case a larger headway may be used, which may have a negative effect on the efficiency of the lane.

The design requirements and recommendations generated by the FMEA are:

(F2.1.1) The malfunction of sensors or gross inaccuracies in the estimation of the braking capabilities must be detected fast. The system must fall back to the default headway that takes into account the inaccuracies or malfunction of the sensors.

(F2.1.2) Diagnostics and built-in self tests must be used to guarantee a fast detection of the communication failures. When a malfunction occurs the headway must be automatically increased to the default safe level that takes into account the failure.

(F2.1.3) The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements must be monitored and taken into account in the calculation of the safe headway.

(F2.1.4) The measurements of braking capabilities of all vehicles must be accurate. The system must check the reasonableness of preceding vehicle's braking capabilities and take into account possible inaccuracies and inconsistencies in calculating the safe headway.

(F2.1.5) The system must be able to accommodate the lack of headway recommendation from roadway .

(F2.1.6) The system must have supervisory elements and diagnostics that monitor the functionality of the receiver and detect malfunctions. The malfunction of the receiver must be taken into account in calculating the safe headway.

The accurate estimation and measurements of all the factors that affect the minimum safe headway is a challenging problem that requires further research. One of the most important factors is the friction coefficient between the tires and the road. There are methods for estimating its value on line [29,30] but slippery spots along the lane due to snow or rain have to be detected a priori. The large variation of the friction coefficient introduces a high variation in the value of the safe headway. As a result the use of a conservative estimate of the friction coefficient by assuming a slippery road and vehicles with "bad" tires will lead to a large and undesirable, from the point of view of capacity, headway. The issue of the friction coefficient and the estimate of braking capabilities of the vehicles is an important safety and capacity issue and needs further research.

Potential Failure Mode F2.2.1: Loss of speed maintenance function.

The SHM may lose its ability to maintain a constant cruise speed if any one of the following components fails to perform as designed:

(F2.2.1.1) The speed sensor gives erroneous readings (S=6, O=2)
(F2.2.1.2) The controller electronics or software fail (S=6, O=2)
(F2.2.1.3) The throttle actuator fails (S=6, O=3)
(F2.2.1.4) The brake actuator fails (S=10, O=3)

The possible effects of these failures are for the vehicle to accelerate and decelerate above or below the desired speed or maintain an incorrect constant speed. Such vehicle response may lead to the violation of traffic rules. The driver may get annoyed and his/her steering performance may be affected.

The severity of these failures is fairly low (S=6) and the occurrence rating varies from O=2 to O=3. The exception is the failure of the brake actuator that is given a severity S=10. The use of the brake is essential in maintaining constant speed during steep downhill cruising situations. Failure of the brake actuator may cause the vehicle speed to exceed the speed limit or decelerate rapidly when not expected, causing possible panic to the driver. Failure of the brake actuator also implies that the RECA function is not operational and therefore a rear-end collision is possible if an obstacle appears in the lane. For the failure of the speed sensor we assume that it will have no effect on the RECA function because the RECA relies on relative distance and speed measurements more than on absolute speed measurements otherwise the severity rating of the failure (F2.2.1.1) has to be modified.

The design requirements and recommendations associated with failure mode F2.2.1 generated by the FMEA are listed as follows:

(F2.2.1.1) Diagnostics and built in tests must perform a test for reasonableness on speed sensor data. When a sensor malfunction is detected, the system shall return to manual control and provide warning to the driver.

(F2.2.1.2) The system must have supervisory elements (in hardware and software) or adequate redundancies for the controller electronics and software. When a controller malfunction is detected, the system shall return to manual control and provide warning to the driver.

(F2.2.1.3) The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, the system shall return to manual control and provide warning to the driver.

(F2.2.1.4) The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failure must be employed together with the appropriate logic and diagnostics that allow automatic switching from a failed actuator to a healthy one. When an actuator malfunction is detected, the system shall return to ERSC 1 or manual control by using the redundant healthy actuator to increase headway and reduce speed to some default values that are comfortable for the driver. The driver shall be warned of the transition and given directions to assume control.

Potential Failure Mode F2.2.2: System switches to headway maintenance (instead of maintaining cruise speed) in the absence of valid target.

This failure will take place when:

(F2.2.2.1) The ranging sensor detects an invalid target within a certain range of the vehicle while the vehicle was at constant cruise speed. (S=8, O=6)

The potential effect of the failure is for the vehicle to change its speed using engine torque and braking for no apparent to the driver reason. The RECA may also get activated. The driver may get annoyed, panic and his/her steering performance may be affected. The severity of this failure is rated as S=8 . Based on current ranging sensor technology the occurrence of such failure is very likely and is given a rating of O=6. The failure may take place around curves, going under bridges and under other road configurations and traffic conditions. The failure may also be the result of interference with signals from other ranging sensors or similar devices.

The design requirements and recommendations for reducing the severity and occurrence of failure mode F2.2.2.1 generated by the FMEA are:

(F2.2.2.1) The system must be able to discriminate between valid and invalid targets.
The design requirement will be easier to meet if two ranging sensors that are not based on the same principle of operation and are not subject to common mode failures are used together with the appropriate logic and diagnostics. The outputs of the two sensors should be continuously monitored and checked for reasonableness and consistency. A higher level controller should be used to decide which of the two outputs is the correct one when the two outputs are different. If the controller cannot decide the system shall follow the output that indicates the closer target and shall revert to manual control. The use of three ranging sensors that are based on different principles of operation and not subject to common mode failures may be a better way of improving the reliability of the ranging measurements. In this case

the three outputs of the sensors are compared and the majority rule could be used to choose the output to be used for control purposes.

Potential Failure Mode F2.3.1.1: Vehicle cannot maintain target speed as commanded by the roadway

The vehicle may lose its ability to maintain the roadway commanded target speed if any one of the following components fails to perform as designed:

(F2.3.1.1) The speed sensor gives erroneous readings (S=6, O=2)
(F2.3.1.2) The controller electronics or software fail (S=6, O=2)
(F2.3.1.3) The throttle actuator fails (S=6, O=3)
(F2.3.1.4) The brake actuator fails (S=10, O=3)
(F2.2.1.5) Vehicle doesn't receive target speed due to loss of communication or noise corruption (S=6, O=3)
(F2.3.1.6) Receiver malfunction (S=6, O=3)

The potential effects of the vehicle not maintaining the target speed commanded by the roadway are degradation of safety and efficiency. The vehicle may be cruising at a speed that is unsafe for the existing traffic conditions. In another situation the vehicle may be cruising at a lower speed holding traffic and causing reduction in capacity and efficiency. The severity of these failures is rated as S=6 with the exception of F2.3.1.4 that is rated as S=10 due to the higher impact the brake actuator may have on safety. Failure of the brake actuator implies that the RECA function is not operational which in turn implies that a rear-end collision is possible if an obstacle appears in the lane. The occurrence rating is very low due to the availability of mature technology that has already been tested in current cruise control systems and short range communication systems .

The design requirements for reducing the severity and occurrence of failure mode F2.3.1 are the same as those generated for failure mode F2.2.1 with the addition of the following:

(F2.3.1.5) The system must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. The system must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). When a communication malfunction is detected the driver shall be notified.

(F2.3.1.6) The system must have supervisory elements in controller software and receiver to detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.

Based on current communication technology the above requirements can be met and therefore the severity and occurrence ratings of the failure can be drastically reduced.

Potential Failure Mode F2.4: The system cannot maintain desired headway

The SHM may fail to maintain the desired headway selected by the system due to the following:

(F2.4.1) Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability. (S=10, O=6)

(F2.4.2) Ranging sensor loses target due to road curvature or insufficient target reflectiveness (S=10, O=7)
(F2.4.3) Ranging sensor has locked on an invalid target (S=9, O=7)
(F2.4.4) Brake actuator failure. (Or intermittent failure to respond) (S=10, O=3)
(F2.4.5) Throttle actuator failure. (S=7, O=3)
(F2.4.6) Controller electronics or software failure. (S=9, O=2)
(F2.4.7) Ranging sensor gives erroneous readings (S=10, O=4).

The most serious effect of the above failures is a rear-end collision. Failure of the ranging sensor and/or brake actuator implies that the RECA function is also ineffective and therefore a rear-end collision may be unavoidable. The most serious failure associated with the ranging sensor is the one where the sensor fails to detect an obstacle within a certain range or provides a larger range reading due to interference and/or malfunction. The case where the sensor provides a shorter range reading by locking on an invalid target is less serious. In this case the RECA may be activated and the driver may get annoyed or panic since the system is not performing as expected. His/her steering performance may be affected. A similar effect may be caused by the failure of controller electronics and/or software. The failure of the throttle actuator will not pose any safety concerns since the RECA will kick in when the TTC reaches a certain value.

The design requirements and recommendations generated by the FMEA are:

(F2.4.1) The system must be able to detect and accommodate an intermittent sensor failure. The system software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle should slow down and the driver should be given a warning to resume control. Redundant ranging sensors, not subject to common mode failures, with appropriate logic must be used.

(F2.4.2) The sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Vehicle shall slow down and the driver must be notified when target is ambiguous and cannot be followed reliably and possibly be given the option to resume manual control. Sensor redundancy must be used to track targets around curves and minimize the possibility of interference.

(F2.4.3) The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. The system must distinguish vehicles moving to adjacent lanes and around curves in the same lane. Redundant ranging sensors not subject to common failure modes with appropriate logic are required.

(F2.4.4) The system must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators that are not subject to common mode failures with appropriate logic that allows automatic switching from a failed actuator to a healthy one are essential.

(F2.4.5) The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, the system shall return to manual control and provide warning to the driver.

(F2.4.6) The system must have supervisory elements (in hardware and software) or adequate redundancies. The system shall return control to the driver in case of failure by slowing down the vehicle and increasing headway.

(F2.4.7) The system must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. The system must provide warning and return control to the driver in case of a detected sensor failure by reducing speed. Sensor redundancy may be needed to totally eliminate the possibility of undetected errors.

The above requirements suggest redundancies for the ranging sensor and brake actuator. Two or even three ranging sensors may be needed to meet the above requirements. The redundant sensors must not be susceptible to common mode failures. Their outputs must be processed using appropriate logic in order to select the correct one. Three ranging measurements may be necessary in order to select the correct measurement by using the majority rule. If all three measurements are different, the one that gives the shorter range for a target shall be selected.

Two or three redundant brake actuators and paths are essential in improving the reliability of braking. The redundancies shall include the appropriate logic and diagnostics that allow automatic switching from a faulty to a healthy brake actuator without affecting the performance of the SHM and RECA functions.

When a redundant sensor or brake actuator fails the vehicle shall be considered unfit to operate in the lane and shall exit as soon as possible. The driver shall be notified in case of failure and be given the appropriate instructions.

Based on today's sensor technology developed for intelligent cruise control applications and vehicle following experiments more research in ranging sensors is required in order to meet the design requirements described above.

Potential Failure Mode F2.5: Failure to switch to maintaining headway even when a valid target exists.

The system is supposed to switch from maintaining cruise speed to maintaining headway when a target appears within a certain range. The system may fail to do so due to the following:

(F2.5.1) Ranging sensor fails to detect a valid target (S=10, O=5)
(F2.5.2) Hardware or software failure of the SHM (S=7, O=2)

The effect of failure (F2.5.1) is a possible rear-end collision since the RECA function is also affected by the same failure. The effect of failure (F2.5.2) is less severe but also crucial since it may affect the steering performance of the driver due to the unpredictable and irrational behavior of the system caused by the failure.

The design requirements and recommendations are:

(F2.5.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics. In case of sensor failure the system shall return control to the driver by slowing down the vehicle and providing warning.

(F2.5.2) The system must have supervisory elements (in hardware or software) or adequate redundancies. The system shall provide warning and return control to the driver in case of a detected failure by reducing speed and increasing headway to levels that are comfortable for the driver.

Potential Failure Mode F2.6 : Failure to switch to speed maintenance mode when the original target moves out of the lane and becomes unsuitable to follow, and no other valid target exists.

When the target moves out of the sensing range or changes lane the system is supposed to switch to the speed maintenance mode and maintain the current speed. The system may fail to switch due to the following:

(F2.6.1) Ranging sensor locks on the original target or locks on another target which is invalid when the original target becomes unsuitable to follow (S=7, O=6)
(F2.6.2) Hardware or software failure of the SHM (S=7, O=2)

The worst possible effect of the above failures is for the RECA function to be activated when it should not. The driver may be annoyed, panic and his/her steering performance may be affected.

The design requirements and recommendations generated by the FMEA are:

(F2.6.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics.

(F2.6.2) The system must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. The system shall provide warning and return control to the driver in case of a detected failure.

Potential Failure Mode F2.7.1: Failure to switch from maintaining constant speed to maintaining roadway commanded target speed.

The system is supposed to switch from cruising at current speed to maintaining the roadway commanded target speed. Failure to do so may be due to the following:

(F2.7.1.1) Loss of target speed information input due to receiver malfunction (S=7, O=3).
(F2.7.1.2) Loss of roadway transmission capability or target speed is corrupted during communication (S=7, O=3)

The above failures may affect safety and efficiency. The effect on safety is due to the vehicle operating at a cruise speed that is unsafe according to the roadway and traffic conditions. The efficiency may also be affected by the vehicle operating with a non-optimal speed.

The design requirements and recommendations are:

(F2.7.1.1) The system must have supervisory elements in the receiver and the controller software to detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified when the vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.

(F2.7.1.2) The system must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). The system must be able to accommodate momentary loss of roadway target speed command. When a communication malfunction is detected, the system shall notify the driver and return to a default cruise speed.

Potential Failure Mode F2.7.2: Instead of switching from cruise speed control to maintaining the roadway commanded target speed it switches to headway maintenance.

The main cause of the above failure is due to:

(F2.7.2) Ranging sensor detects an invalid target. (S=7, O=6)

The above failure may cause unnecessary acceleration or deceleration and activation of the RECA, confuse the driver and affect his/her steering performance.

The design requirements and recommendations are:

(F2.7.2) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures may be used.

Potential Failure Mode F2.8.1: Failure to take action on time for reducing the possibility of rear-end collision.

The system may fail to apply hard braking in order to avoid or reduce the possibility of rear-end collision due to the following:

(F2.8.1.1) The ranging sensor fails to provide signal or provides incorrect signal (S=10, O=5).
(F2.8.1.2) Loss of communication of braking intentions of preceding vehicle (S=10, O=5).
(F2.8.1.3) Controller electronics or software failure (S=10, O=2).
(F2.8.1.4) Brake actuator failure (S=10, O=3).
(F2.8.1.5) The calculated time to collision (TTC) is larger than the actual TTC due to incorrect measurement of braking capabilities (S=10, O=6).
(F2.8.1.6) Ranging sensor switches from a valid target to another one with completely different operating status and braking capabilities e.g. preceding vehicle exits lane and next vehicle in lane is disabled (S=10, O=3).

All of the above failures have the maximum severity rate of S=10. Their effect is a highly probable rear-end collision. Basically the above failures render the RECA function ineffective. Since the driver is not expected to serve as a back-up to the system a rear-end collision cannot be avoided. The following design requirements and recommendations call for adequate redundancies for all the components hardware and software that affect the functionality of the RECA function:

(F2.8.1) The system must have redundant sensing inputs to reduce the probability of missing a target to essentially zero . If redundancy is lost, the system shall increase headway and reduce speed, warn the driver and revert to ERSC1 or to manual mode.

(F2.8.1.2) A redundant method must be used to communicate the preceding vehicle's braking intention. The calculated safe headway must take into account momentary loss of vehicle to vehicle communication. If loss of communication is permanent, system shall take that into account in calculating the safe headway.

(F2.8.1.3) The system must have supervisory elements in software and hardware and adequate redundancies. When a redundancy is lost, the system shall increase headway and reduce speed to comfortable levels and warn the driver to operate as in ERSC1 or manual mode.

(F2.8.1.4) The system must have redundant braking actuators that are not subject to common mode failures and appropriate diagnostics that allow the fast detection and accommodation of failures without degrading the performance of the RECA function. When a redundant braking path fails the system shall return to ERSC1 or manual mode and warn the driver appropriately. The transition to ERSC1 or manual mode shall be done by first reducing speed and increasing headway to levels that are comfortable for the driver.

(F2.8.1.5) The TTC must be accurate and conservative in order to accommodate possible inaccuracies in measurements. Independent estimates of TTC based on independent measurements must be used.

(F2.8.1.6) The system must be designed to account for the situations described in the failure cause (F2.8.1.6). Vehicle to vehicle communication may be used to notify the trailing vehicle of condition ahead or the system is designed so that exiting from the lane is possible only at designated points where larger headways are imposed.

Requirements (F2.8.1.2) to (F2.8.1.5) call for substantial redundancies in all hardware and software components. The most significant ones are the redundancies in the ranging sensors, brake actuators and sensors estimating braking capabilities. Despite these redundancies failure (F2.8.1.6) cannot be avoided without redesigning the system. The failure is not due to any malfunctioning of the components but rather is the result of the proposed design. The failure may arise in the following situation. The preceding vehicle, which has been followed, changes lane due to an obstacle such as a disabled vehicle in the lane. That is the driver of the preceding vehicle was capable of avoiding a rear-end collision by using steering. The following vehicle changes targets but finds itself within a short headway that is not large enough for the RECA function to bring the vehicle to stop without collision. It is also not large enough for the driver to act on time by steering the vehicle safely away from the obstacle. This failure mode has therefore several implications:

(i) The RECA function may have to be introduced together with lateral collision avoidance leading to a fully automated vehicle.

(ii) The dedicated lane may have to exclude continuous entry exit configurations and use designated entry and exit points where headways are large and speeds are low close to those points so that failure (F2.8.16) cannot take place.

(iii) A more extensive communication network may have to be implemented with vehicle to vehicle and roadway to vehicle communication. In such an environment the roadway should be able to detect disabled vehicles and notify other vehicles. Vehicles should also notify the following vehicles of their intentions to change lanes and of the status of their preceding vehicle.

The new potential failure modes associated with the above modifications, their causes and effects need further research.

Potential Failure Mode F2.8.2: The RECA is activated unnecessarily.

The incorrect activation of the RECA may be due to following causes:

(F2.8.2) Incorrect range is sensed or incorrect TTC is calculated. (S=6, O=4)

The unnecessary activation of the RECA may annoy the driver, cause panic and affect his/her steering performance. The design requirements are:

(F2.8.2.2) The system must minimize the number of faulty activations of the RECA function as much as possible. Independent ranging measurements and calculations of the TTC must be used.

Potential Failure Mode F2.9: SHM and RECA cannot be enabled

The possible cause of the above failure is:

(F2.9.1) Electronic malfunction. (S=7, O=2)

The effect is that the vehicle may fail the check-in test if the failure is detected by the on-board diagnostics or the vehicle will have to exit the dedicated lane causing a disturbance to the traffic flow and affecting efficiency.

The design requirements and recommendations are:

(F2.9.1) The controller electronics must be sufficiently reliable.
Diagnostics must be performed even when the SHM and RECA are in the standby mode. The driver shall be notified of any detected malfunctions.

Potential Failure Mode F2.10.1: SHM and RECA cannot be disabled

The potential cause of the above failure is:

(F2.10.1) Electronic malfunction. (S=10, O=2)

The effect of the above failure is serious since the driver may feel out of control that could cause panic and affect his/her performance for steering and other driving tasks.

The design requirements and recommendations are:

(F2.10.1) The controller electronics must be sufficiently reliable. The driver shall have redundant means of turning off the SHM and RECA. The switching off of the functions must follow the disabling procedure so that the driver is not put in a situation he/she cannot handle.

Potential Failure Mode F2.10.2: SHM and RECA are disabled without first reducing speed and increasing headway.

This malfunction may be caused by:

(F2.10.2) Software failure or failure of the brake actuator. (S=10, O=3)

The effect of the failure is serious and may lead to collision. In this case the driver may be put in a situation of a short headway and high speed and be expected to assume manual control of the throttle and brake. Most drivers may consider such situations dangerous and may not have enough time to act to maintain full control of the vehicle.

The design requirements and recommendations are:

(F2.10.2) The system must have redundancies in software and redundant braking actuator paths. The system must be designed to fall back to a default speed and headway in a reliable manner when a failure is detected before the SHM and RECA are disabled. The driver shall be notified.

Potential Failure Mode F2.11.1: Loss of communication of braking capabilities and intentions to trailing vehicle

The potential cause of the above failure mode is due to:

(F2.11.1) Failure of transmitter. (S=10, O=3)

If the failure is detected fast enough the trailing vehicle will take that into account and increase its headway. In this case efficiency will be affected. If undetected or detected late the calculated TTC of the trailing vehicle may be large or incorrect leading to a possible rear-end collision.

The design requirements and recommendations are:

(F2.11.1) The system must have supervisory elements to monitor the transmitter. A redundant transmitter may be necessary. If the transmitter fails permanently, the vehicle shall exit the lane.

Potential Failure Mode F2.11.2: The vehicle transmits incorrect braking capabilities or braking intention to trailing vehicle.

The potential cause of the failure is due to:

(F2.11.2) Faulty or inaccurate measurements of braking capabilities and or braking intentions. (S=10, O=6)

The effect of the above failure is a possible rear-end collision with the trailing vehicle due to the inaccurate calculation of the TTC by the trailing vehicle.

The design requirement and recommendations are:

(F2.11.2) The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements shall be monitored. Independent means for calculating braking capabilities must be employed.

Potential Failure Mode F2.12.: The system fails to adjust speed around curves.

The system is designed to coordinate with steering and adjust speed around curves in order to maintain stability and driving comfort. Failure to do so may be due to the following:

(F2.12.1) Incorrect preview road data or incorrect steering angle information. (S=10, O=3)
(F2.12.2) Throttle and/or brake actuator failure. (S=10, O=3)
(F2.12.3) Controller electronics and/or software failure. (S=10, O=2)

The potential effect of the above failures is for the vehicle to go out of control and cause a major accident or cause a considerable discomfort to the driver and passengers. The following design requirements and recommendations are generated by the FMEA.

(F2.12.1) There must be more than one source of preview data and steering angle information not subject to common mode failures.

(F2.12.2) The system must use sensor and diagnostic programs to monitor the throttle and brake actuators. When a malfunction is detected the system shall slow down the vehicle and notify the driver.

(F2.12.3) The system must have supervisory elements or adequate redundancies for the controller electronics and software. When a malfunction is detected the system shall slow down the vehicle and notify the driver.

H2.2 Blind-spot warning

The failure modes, causes and effects as well as the design requirements and recommendations for the BSW are the same as in ERSC1 and are repeated here for the sake of completeness.

Potential Failure Mode F2.13.1: The system is unable to provide warning

The system may fail to give a warning due to any one of the following factors:

(F2.13.1.1) Blind spot sensor failure (S=7, O=5)
(F2.13.1.2) Electronics failure or software failure (S=7, O=2)
(F2.13.1.3) Threshold has been set too high (S=7, O=4)
(F2.13.1.4) Warning delivery device failures (S=7, O=2)

The effect of these component failures is that safety will be compromised during lane changing if the driver relies too much on the warning. The design requirements and recommendations are:

(F2.13.1.1) Supervisory elements must monitor the output of the sensor for reasonableness and consistency. The driver shall be notified when a malfunction is detected.

(F2.13.1.2) Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.

(F2.13.1.3) The default threshold must be set to a low level. The driver shall be aware of the lack of warnings due to the high threshold setting.

(F2.13.1.4) The warning device must be reliable. Redundant warning delivery methods shall be used.

Potential Failure Mode F2.13.2: The system gives false BSW alarms

False alarms may be given by the system due to the following failures:

(F2.13.2.1) Blind spot sensor gives incorrect reading (S=5, O=5)
(F2.13.2.2) Electronics failure or software failure (S=5, O=2)

(F2.13.2.3) Threshold has been set too low (S=5, O=4)
(F2.13.2.4) System misinterprets driver intention to change lanes (S=5, O=7)

The above failures may lead to many false alarms that may distract the driver and reduce his/her confidence level on the system. The design requirements and recommendations are:

(F2.13.2.1) Supervisory elements in hardware and software must be used to monitor the sensor. The driver shall be notified when a malfunction is detected.

(F2.13.2.2) Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.

(F2.13.2.3) The driver shall be able to select a threshold level that he/she is comfortable with. The default threshold must be set to a level appropriate for typical conditions.

(F2.13.2.4) A reliable method must be used to sense the intentions of the driver to change lanes or the system must be redesigned to eliminate the necessity of sensing driver's intentions.

If the system is on all the time the false alarm rate will be high due to the detection of vehicles in the next lane that are not threatening. If the warning is audible a high false alarm rate may be very undesirable to the driver. If the warning is visual such as a head up display indicating the presence of an obstacle in the blind spot a high "false" alarm rate may be acceptable but the warning may not be as effective. The BSW must be active and ready to operate before the driver initiates lane changing. A method must be developed that meets this requirement without introducing false alarms. Sensing the turn signal and steering wheel angle is another method of detecting the intentions of the driver to change lanes and activating the BSW. This method, however, may lead to a delayed warning that may not be effective. Further research is needed in order to develop a method for activating the BSW.[19]

Potential Failure Mode F2.14 : The BSW cannot be enabled

The driver may not be able to switch the BSW on due to:

(F2.14.1) Electronics failure (S=6, O=2)

The effect of this failure is not safety critical provided the driver is aware that the BSW is not on.

The design requirements and recommendations are:

(F2.14.1) The controller electronics must be sufficiently reliable and must have supervisory elements in hardware and software. The driver shall be notified about changes in the BSW operating mode i.e.: on, off, malfunction.

Potential Failure Mode F2.15: The BSW cannot be disabled

The driver may not be able to disable the BSW due to :

(F2.15.1) Electronics failure (S=3, O=2)

The design requirements and recommendations are:

(F2.15.1) The controller electronics must be sufficiently reliable. There shall be redundant methods to disable the BSW.

Potential Failure Mode F2.16: The threshold of the BSW cannot be adjusted

The threshold of the BSW is adjusted by the driver. This adjustment may not be possible due to:

(F2.16.1) Electronics failure (S=6, O=2)

The effect of such failure is that the driver may feel uncomfortable with the current threshold. If the threshold is high the driver may not receive warnings when he/she should and if it is low the driver may receive many unnecessary warnings. Such response will be annoying and will reduce the level of confidence on the system.

The design requirements and recommendations are:

(F2.16.1) The controller electronics must be sufficiently reliable. The threshold setting shall default to a low level when the BSW is enabled for the first time. The driver shall be able to read and verify the selected threshold setting.

H2.3 Lane Departure Warning

Potential Failure Mode F2.17.1: Loss of lane departure warning function

The system may fail to provide a lane departure warning due to the following causes:

(F2.17.1.1) Loss of lane reference position due to damage or loss of roadway reference aids. (S=9, O=5)
(F2.17.1.2) Lateral reference sensor fails or gives erroneous readings. (S=9, O=4)
(F2.17.1.3) Controller electronics or software failure. (S=9, O=2)
(F2.17.1.4) Warning delivery device failure. (S=9, O=2)

The effect of these failures is a departure of the vehicle from the center of the lane when the driver relies too much on the warning and he/she is not very attentive.

(F2.17.1.1) Supervisory elements in lateral sensor processor (in software) must be able to detect the loss of reference. The driver shall be notified when roadway lane reference aids are lost. Redundant reference aids may be necessary.

(F2.17.1.2) Supervisory elements must be used to monitor the response of the lateral reference sensor. The driver must be notified if a malfunction is detected. A redundant lateral sensor with the appropriate logic may be essential.

(F2.17.1.3) The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall notify the driver.

(F2.17.1.4) The warning device must be reliable. Redundant warning delivery methods shall be used.

Potential Failure Mode F2.17.2: The system gives unnecessary warning.

The system may give false warnings due to the following causes:

(F2.17.2.1) Lateral reference reading sensor gives erroneous readings. (S=5, O=5)
(F2.17.2.2) Controller electronics or software failure. (S=5, O=2)

The effects of these failures are not serious. They may distract and annoy the driver and reduce confidence in the system. In some cases they may make the driver more attentive.

The design requirements and recommendations are:

(F2.17.2.1) The system must check the reasonableness of lateral sensor data by using an appropriate vehicle dynamics model. Redundant lateral sensors may be necessary. If a malfunction is detected, the driver shall be notified.

(F2.17.2.2) The system must have supervisory elements (in hardware and software). When a controller malfunction is detected, the system shall notify the driver.

Potential Failure Mode F2.18: LDW cannot be enabled

The potential cause of the failure is:

(F2.18) Electronics malfunction failure. (S=6, O=2)

The effect is that the driver has to operate the vehicle without the LDW. Safety is compromised.

The design requirements and recommendations are:

(F2.18) The controller electronics must be sufficiently reliable. The driver shall be notified about the change in LDW operating mode.

Potential Failure Mode F2.19: LDW cannot be disabled

The potential cause of the failure is due to:

(F2.19) Electronics malfunction. (S=3, O=2)

The driver may get annoyed by receiving unwanted warnings.

The design requirements and recommendations are:

(F2.19) The driver shall have a redundant way of turning the system off.

Potential Failure Mode F2.20: Threshold cannot be adjusted.

The potential cause of the failure may be due to:

(F2.20) Electronics malfunction in the controller or the driver interface. (S=6, O=2)

The effect of the failure is that the driver may be uncomfortable with the current threshold and he/she may disable the system.

The design requirements and recommendations are:

(F2.20) The electronics must be sufficiently reliable. The default threshold must be at a high level when the LDW is first enabled. Driver shall be able to read and verify the selected threshold setting.

H2.4 Steering assist

Potential Failure Mode F2.21: Can not assist driver in steering

The steering assist may fail to assist the driver due to the following:

(F2.21.1) Lateral sensor failure. (S=5, O=5)
(F2.21.2) Erratic steering actuator response or failure of steering actuator. (S=5, O=3)
(F2.21.3) Controller electronics or software failure. (S=5, O=2)

The effect of the above failures are not serious. They may affect ride quality and increase driver workload.

The design requirements and recommendations are:

(F2.21.1) The system must employ supervisory elements to detect sensor failures. Driver shall be notified when a sensor malfunction is detected. Redundant lateral sensor and appropriate logic may be necessary.

(F2.21.2) The system must employ supervisory elements and self diagnostics to monitor the steering actuator. The system must be designed to accommodate steering actuator failures without causing the vehicle to depart from the lane. When a failure is detected the system shall accommodate it or the steering assist system shall be disconnected and the driver shall be notified.

(F2.21.3) The controller must be sufficiently reliable. If a failure is detected, the steering actuator must be disconnected and the driver be notified. Controller and software redundancies may be necessary.

H2.5 Driver Vehicle Roadway Interface

Potential Failure Mode F2.22: Failure of check-in function.

The check-in function may fail to perform as designed due to the following:

(F2.22.1) On-board diagnostics fail to detect a fault in major functions of the vehicle. (S=9, O=3)
(F2.22.2) Driver ignores the results of the on-board diagnostics. (S=9, O=3)
(F2.22.3) On-board diagnostics makes a wrong decision about a component or function that was not at fault. (S=6, O=2)

The effect of the first two failures is that the vehicle will enter and operate in the dedicated lane without being fit. The last failure will stop the vehicle from entering the dedicated lane even though it is fit. The severity of the first two failures is fairly high . It will affect safety and efficiency especially if the vehicle stays in the lane for long time. The design requirements and recommendations are:

(F2.22.1) Diagnostics algorithms must be robust and highly reliable. Roadway shall be able to detect an unfit vehicle operating in the dedicated lane. Law enforcement can be used to deal with the violators.

(F2.22.2) The roadway shall be able to identify an unfit vehicle operating in the dedicated lane. Traffic rules and regulations must be used to deter the driver from violating the rules.

(F2.22.3) On board diagnostics must be highly reliable. Redundancies and supervisory elements must be considered for improving reliability

Potential Failure Mode F2.23: The driver fails to enter the lane or he/she enters the lane improperly

The driver may fail to merge into the dedicated lane due to the following:

> (F2.23) Dedicated lane is congested or driver is not able to merge due to high speed and/or small gap in dedicated lane or driver doesn't have the required skills. (S=7, O=4)

The effect of the failure is that the vehicle is restricted from or delayed in entering the dedicated lane. This will lead to possible congestion in the transition lane or entrance to the lane.

The design requirements and recommendations are:

(F2.23) The roadway must enforce lower speeds and larger headways near the entry points. Driver skills for merging into the dedicated lane should be tested as part of the licensing procedure.

Potential Failure Mode F2.24: Driver fails to respond to BSW and/or LDW

The driver may fail to respond to the BSW and/or LDW due to the following:

> (F2.24.1) Driver ignores warning unintentionally or becomes confused. (S=10, O=4)
> (F2.24.2) Driver ignores warning intentionally due to high false alarm rate. (S=10, O=4)

The above failures have a serious impact on safety and in some cases may lead to collision. The failures may be the result of human error. The system shall be designed so that it does not induce human errors. The following design requirements and recommendations are generated:

(F2.24.1) The warnings shall be very clear and unambiguous to the driver. Driver interface shall be as simple as possible.

(F2.24.2) False alarm rate must be very low. The warning signals must be easily distinguishable from each other. The warning threshold shall be adjustable by the driver. The driver interface with the warning devices shall be as simple as possible.

Potential Failure Mode F2.25: Driver fails to respond to traffic information

The driver may fail to respond to traffic information provided by the roadway due to the following:

(F2.25.1) Driver capability is impaired. (S=4, O=5)

The effect of the failure is that the efficiency of the dedicated lane may be affected. Under some circumstances safety may be affected if the driver ignores the advice from the roadway. The design requirement is that:

(F2.25.1) Roadway traffic information must be clear and brief.

Potential Failure Mode F2.26: The driver can not exit the lane.

The driver may not be able to exit the lane due to:

(F2.26.1) Congestion in manual lane or the transition lane. (S=6, O=5)

The effect is that the vehicle will remain in the dedicated lane. If the vehicle is exiting due to malfunction of the automated functions, then the efficiency of the dedicated lane may be degraded.

The design requirements and recommendations are:

(F2.26.1) A dedicated transition lane or some form of regulation such as "yield to auto lane" must be implemented to ensure easy exit even when traffic congestion exists in the manual lane. The system must warn the driver of congestion, ahead of time, via traffic information communication.

Potential Failure Mode F2.27.1: System does not fall back to ERSC1

The system may fail to revert to ERSC 1 operating mode due to:

(F2.27.1) Software failure. (S=10, O=2)

The failure may affect safety depending on the situation.

The design requirements and recommendations are:

(F2.27.1) Reliable supervisory and diagnostics programs must be implemented. Redundant means for returning to the ERSC 1 mode must be used.

Potential Failure Mode F2.27.2: Driver fails to assume role for ERSC 1.

The driver may fail to assume his/her role for ERSC 1 due to the following:

(F2.27.2.1) Warning delivery device failure. (S=10, O=2)
(F2.26.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The effect of these failures is a possible collision. If the vehicle reverts to ERSC 1 and the driver operates as if the vehicle is in ERSC2 a collision is possible. The design requirements and recommendations are:

(F2.27.2.1) The warning device must be reliable. Redundant warning delivery methods must be used.

(F2.27.2.2) The warnings and instructions to the driver must be clear and understandable and shall not impose a heavy workload on the driver.

The question whether a driver can switch from one mode of operation to another within a short time by following the warnings and instructions given by the vehicle is a human factors issue that requires further research. The issue is more crucial when the two often used modes of operation are manual and ERSC 2. The driver may gain experience and be able to handle these two modes and the transition between them but he/she may have little or no experience with ERSC 1. Another issue is whether the driver can understand the different modes of operation and adjust to them fast enough.

Potential Failure Mode F2.28.1: System does not fall back to manual control

The system may fail to revert to manual control due to:

(F2.28.1) Controller software failure. (S=10, O=2)

Due to the above failure the vehicle may continue to be under automatic control when it should be under manual control. The driver may try to disable the RECA and SHM functions. He/she may also get confused, panic and cause an accident.

The design requirements and recommendations are:

(F2.28.1) Reliable supervisory and diagnostics programs must be used. Redundancies in hardware and software may be necessary.

Potential Failure Mode F2.28.2: Driver fails to assume full manual control

The above failure may be caused by any one of the following factors:

(F2.28.2.1) Warning delivery device failure. (S=10, O=2)
(F2.28.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

Due to the above failure the vehicle may continue to be under automatic control when it should be under manual control. Safety will be affected and collision is possible. The design requirements and recommendations are:

(F2.28.2.1) The warning device must be reliable. Redundant warning delivery methods must be used.

(F2.28.2.2) The warnings and instructions must be clear and understandable. Driver workload must be manageable.

According to the above requirements the system must be designed so that it does not induce human errors. The method of instructing the driver to switch modes of operation when the vehicle is at

relatively high speed and short headway is an important human factors issue. Slowing down the vehicle and increasing headway may reduce the workload of the driver but may have an adverse effect on efficiency. Further research is required in order to find an optimum way in terms of efficiency and safety to switch from ERSC 2 to the manual mode.

Potential Failure Mode F2.29: The system fails to notify the driver of correct mode of operation

The system is designed so that it notifies the driver of its mode of operation. For example whether the SHM and RECA, BSW, LDW and steering assist functions are on, off or there is a malfunction. Failure of the system to do so may be due to:

(F2.29.1) Electronics or software failure. (S=8, O=3)

Failure of the system to notify the driver of its correct mode of operation may lead to confusion. As a result the driver may decide to initiate a check-out procedure and exit the lane. The driver may also panic under some situations where the wrong mode is displayed and cause an accident.

The design requirements and recommendations are:

(F2.29.1) The electronics and software must be very reliable. Redundancies and on board diagnostics must be used to improve reliability.

How much information the driver should be given about the operational status of the vehicle is an issue that needs further research. The workload of the driver shall be low and manageable. Any information given to the driver shall be clear, brief and easy to process at all speeds and headways.[37,38]

Vehicle, Driver Diagnostics and Maintenance

Vehicle Diagnostics

The FMEA for ERSC2 gives an extensive list of design requirements and recommendations that involve the use of diagnostics for almost all components, sensors, actuators and software that are used for the functions of SHM, RECA, steering assist, BSW and lane departure warning. The use of diagnostics is essential in avoiding over designing the system with redundancies. Even though diagnostics may be less costly than redundancies they still increase the cost as the number of the AHS functions increases.

The most crucial diagnostics for ERSC2 are those covering safety functions. These are the diagnostics used for the RECA and SHM. In particular the functions associated with the calculation of the safe headway, the ranging measurements and the brake subsystem need to be protected with redundancies and on board diagnostics.

As in ERSC1 the monitoring of the overall motion of the vehicle using an executive controller with diagnostics that is based on a validated vehicle model as shown in figure 8, could be an essential feature of the vehicle of ERSC2. These overall diagnostics will add an additional layer of safety by detecting and accommodating failures that cannot be easily detected at the local component level.

Driver Diagnostics

In ERSC2 the driver is responsible for steering and he/she is expected to be alert. Driving, however, in a single straight lane for a long period of time such as in rural areas without having to pay attention to the

longitudinal motion of the vehicle may cause drowsiness.[22] The situation also exists in today's driving in rural areas when the traffic is very light and the vehicle is on cruise control. In ERSC2, however, these situations will appear more often due to the fully automated longitudinal motion of the vehicle and need to be studied.

Another important issue is the effect of the fully automated longitudinal function on the steering performance of the driver. His/her reaction time to lateral collision avoidance may increase. The question whether on board driver diagnostics are essential in order to continuously monitor and assess the status of the driver at ERSC2 is a human factors issue that needs to be addressed. Since in this situation the driver is not performing any driving tasks the assessment of his/her alertness has to be done by checking physical responses such as eye lid movement etc.[33]

In ERSC2 the system is designed so that the transition from the fully automated longitudinal control function to the manual one is done by reducing speed and increasing headway to default levels that are considered to be comfortable for the driver. The level of comfortable speed and headway will differ depending on the status of the driver, i.e., how drowsy he/she is etc. An effective method for assessing the status and capability of the driver to resume manual control is needed since it will help in selecting levels of speed and headway for the transitions in order to optimize safety and efficiency.

Maintenance

The trend of low maintenance that exists in today's vehicle is expected to continue and apply to the AHS vehicles. This trend calls for very reliable components with long mean time to failure values and extensive use of sensors and diagnostics. There is no doubt that the price of a low maintenance vehicle is the high initial cost of the vehicle. The specific maintenance requirements for the various components of ERSC2 are technology and equipment dependent and are difficult to develop at this stage. There is no doubt that the automobile manufacturers will choose components and designs that do not require frequent maintenance. For example the use of an optical method for sensing range where the driver is required to clean the lens every time he/she drives the vehicle or whenever the lens gets dust will not be accepted. Also the need for frequent alignment of a ranging sensor may be a reason for rejecting the sensor for the proposed application.

Since electronic components have lower maintenance needs than mechanical and hydraulic components that are more susceptible to wear, the increase in the number of electronics in the vehicles for ERSC 2 is not expected to increase the frequency of maintenance.

The addition of redundant braking paths and the impact the braking capabilities of the vehicles have on safety may call for more frequent maintenance for things like brake fluids, and brake pads, tires etc.

The use of diagnostics to monitor the state of mechanical parts together with improvement of materials will help minimize the need for frequent maintenance.

Retrofitting

As in ERSC1, retrofitting of vehicles for ERSC2 is going to be costly and unacceptable to users and automobile manufacturers. The question whether vehicles developed for ERSC1 can be upgraded to be used for ERSC2 is worth raising. The answer is that technically such upgrading is feasible but is going to be costly. The reason is that the design requirements for the ERSC2 vehicles are very different from those for ERSC1 vehicles. For example an ERSC1 vehicle has to go through major changes and tests in

order to meet the required reliability levels for components such as brake actuators, ranging sensors and the additional diagnostics that are essential for ERSC2. Table 4 summarizes the results of retrofitting for ERSC2.

Table 4 Retrofitting for ERSC 2.

Category of Vehicles	**Technically Feasible**	**Cost**	**User Acceptance**
Vehicles with no ERSC 1, 2 capabilities	Yes	Very High	Unlikely
Vehicles with ERSC 1 but not ERSC 2 capability	Yes	High	Unlikely
Vehicles built for easy retrofit	Yes	High	Unlikely
Vehicles built independent of ERSC2 but have similar capabilities for ERSC2	Yes	Moderate to high depending on the extent of retrofitting	Questionable

Deployment Scenarios

ERSC2 can be considered as an upgrade of ERSC1 and could form a second deployment stage of AHS provided the reliability problems addressed earlier are resolved.

ERSC2 will increase the capacity of the dedicated lane considerably since the headway chosen by the vehicle is much smaller than that for ERSC1 (where the driver sets the headway) and the vehicle speed commanded by the roadway could be kept above a lower limit. Two of the major problems that need to be resolved before ERSC2 is deployable are the problems of liability and human factors and safety associated with the effect of the full authority longitudinal controller on the human driving tasks that include steering and lateral collision avoidance. The problem of liability arises from the fact that the vehicle chooses the headway and is responsible for rear-end collision, and the roadway chooses the speed. One can imagine a series of accident situations where liability issues are likely to be raised with the accident cause attributed to the vehicle and/or roadway. In some of these situations it may be difficult to distinguish between the cause due to driver's error and the cause due to equipment failure or error. The effect of the full authority longitudinal controller on the steering performance of the driver especially during lateral collision avoidance situations is a human factors and safety issue that needs to be addressed. The driver for example may fail to use steering to avoid a rear end collision where braking alone is not sufficient due to the short headway relative to his/her reaction time. One possible scenario is to modify ERSC2 so that steering for lane changing is restricted to designated points where a different headway and speed are selected and the vehicle and roadway functions are modified so that rear-end collision avoidance using steering is not necessary along the lane. Such modifications may demand more vehicle to vehicle and roadway to vehicle communications as well as roadway sensors to sense disabled or unfit vehicles and obstacles along the lane and notify the vehicles upstream accordingly.

Another possible scenario is to add lateral collision avoidance and lane keeping and remove the human driver from the driving loop completely. Such a vehicle, however, becomes the same as the one used for ERSC4 to be discussed later on. Another obstacle to the deployment of ERSC2 is the increase in the cost of the vehicle due to the considerable number of redundancies and diagnostics that are required for reliable operation.

Key Results and Conclusions

1. In ERSC2 a system on the vehicle calculates the safe headway to be used in vehicle following. The size of the headway is such that the vehicle can always stop by using braking without colliding with the preceding vehicle or an obstacle in the lane. The choice of headway has an impact on safety and capacity. Safety calls for large headways. For a safe and efficient operation, a minimum safe headway that guarantees collision free vehicle following under certain worst case scenarios,[8] depends on a lot of factors that include the braking capabilities of the vehicle and those of the preceding vehicle, the friction coefficient between the tires and road, time delays and accuracy of brake actuators and sensors, current vehicle speed, computational delays etc. The accurate estimation and measurements of all the factors that affect the minimum safe headway is a challenging problem that requires further research. One of the most important factors is the friction coefficient between the tires and the road. Several methods have been proposed for estimating its value on-line [29,30] to be used for applications such as traction control. Slippery spots along the lane due to snow or rain have to be detected a priori in order to be used for headway calculations. The variation of the friction coefficient introduces a variation in the value of the minimum safe headway. The use of a conservative estimates of the friction coefficient by assuming a slippery road and vehicles with "bad" tires will lead to a large and undesirable, from the point of view of capacity, headway. The accurate estimate of the friction coefficient and of the braking capabilities of the vehicle is an important safety and capacity issue that needs further research. The communication of the braking intentions, such as braking for emergency, from the preceding vehicle to the following one plays the role of the brake lights in normal driving. It helps reduce the computational delay for detecting emergency stops and the value of the minimum safe headway. The best method of communicating the braking intentions to the following vehicle without interference is a design issue that needs to be addressed.

2. The full authority longitudinal controller for ERSC2 has to be protected from all possible failures. This requirement calls for a highly reliable system with multiple redundancies for the sensors, actuators, electronic and software components. A block diagram of the envisioned full authority controller with its redundancies is shown in figure 15.

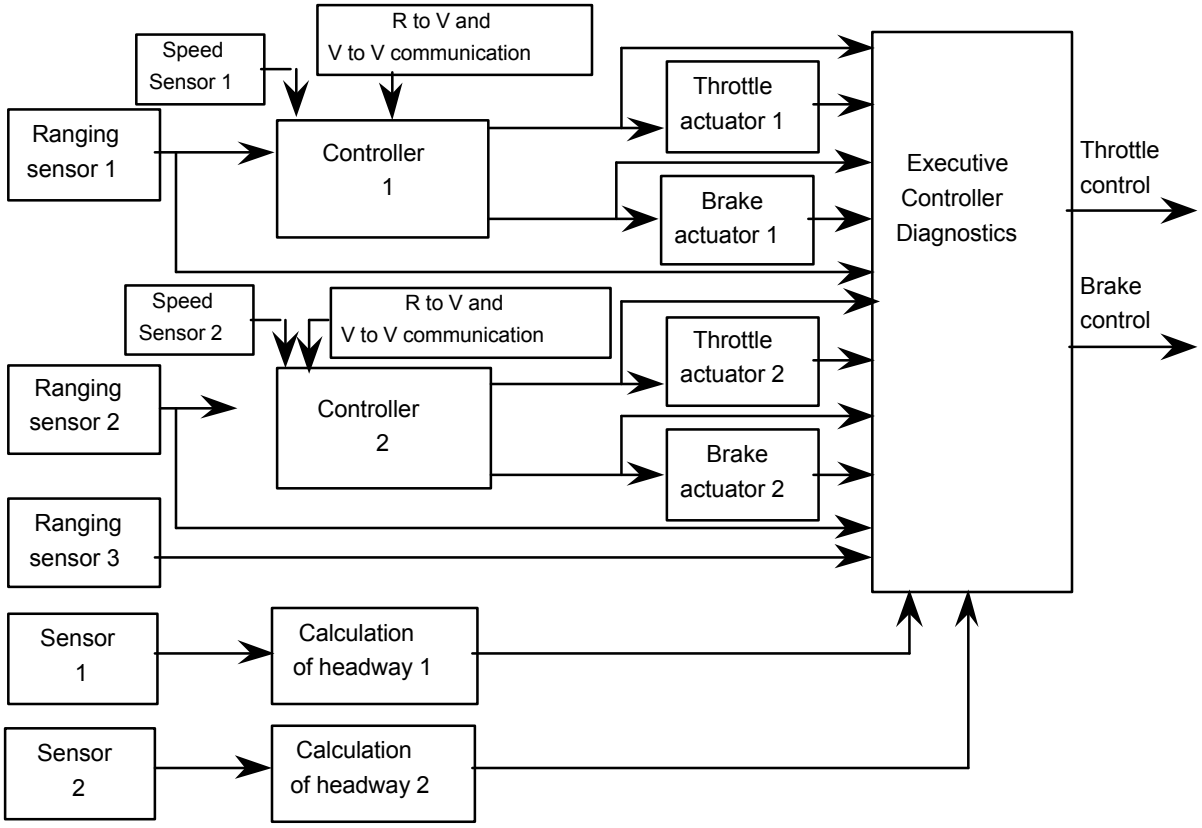

Figure 15: The block diagram of the potential design of the full authority longitudinal controller.

The proposed design has two active channels that are designed so that they are not subject to common mode failures. The executive controller and diagnostics monitor the two channels and switch from the faulty one to the healthy one in case of failure in a way that does not affect the performance of the system. The ranging measurements have a third redundancy due to the higher susceptibility of the ranging sensors to errors and inconsistencies. When one of the channels fails the vehicle shall be considered unfit to operate in the lane and shall follow a check out procedure for exiting.

The diagram indicates the level of complexity that may be required in order to meet the reliability requirements that are essential for the full authority longitudinal controller. That level of complexity is expected to increase cost. The additional cost as a percentage of the cost of the vehicle is hard to evaluate at this stage.

3. In ERSC2 the driver is responsible for steering and lateral collision avoidance. The effect of the full authority longitudinal controller on the steering performance of the driver especially during situations where steering is essential for avoiding a rear-end collision is a human factors issue that needs to be addressed. Furthermore the effect of hard braking during a rear-end collision avoidance situation on the steering performance of the driver is also a human factors issue that needs to be addressed. The above comments raise the question of whether the full authority longitudinal controller should be introduced together with the full authority lateral controller.

4. The driver in ERSC2 shall not be put in a situation of a short headway and high speed, relative to his/her reaction time, that he/she cannot handle. As a result the transition from the full authority longitudinal controller to the manual mode shall be completed after the system has increased the headway and reduced the speed to some preset levels that are comfortable for the driver. The driver shall not have a direct override of the longitudinal controller since that may put him/her in the situation of a short

headway and high speed that he/she may not be able to handle. The driver, however, shall always be able to initiate the transition from the automatic to manual mode as described above.

5. The full authority longitudinal controller reduces the workload of the driver considerably in highways with no curves in urban and even more in rural areas possibly causing drowsiness that may affect driver's performance in the normal driving tasks. This is a human factors issue that needs to be studied.

6. The use of the blind spot warning in ERSC2 is to assist the driver during lane changing. The effectiveness of the warning will depend on how and when it is given to the driver. Human factors studies are required to resolve this issue.

7. A lane departure warning assists the driver in keeping the vehicle in the center of the lane. The accuracy of the warning depends on the accuracy of the sensing the position of the vehicle relative to the center of the lane. The sensor requirements call for lane reference aids and sensors on the vehicle. These hardware requirements increase infrastructure and vehicle cost. This cost has to be traded off with the potential safety benefits offered by the warning system. This trade off analysis is an issue that needs to be resolved by further research.

8. All the automated and partially automated functions and warnings would have on board diagnostics to monitor the performance and functionality. These diagnostics could be used even when the vehicle is in the manual mode. As a result the driver will be notified if his/her vehicle is not fit to operate in the dedicated lane before he/she approaches the lane. Therefore no elaborate and time consuming check-in procedures are required at the entrance to the dedicated lane of AHS.

9. The transition from ERSC2 mode of operation to ERSC1 may take place when the RECA function is no longer reliable due to environmental conditions, component failure etc. This switching mode of operation raises several questions that need to be addressed. The main question is whether the driver can switch from one mode of operation to another within a short time by following the warnings and instructions given by the vehicle. The transition is more critical when the driver is used to operating in ERSC2 and manual mode and ERSC1 operation is rare. The driver is not expected to understand the details of the different modes of operation and adjust to them fast enough. Human factors studies need to be performed in order to examine the feasibility of switching from one ERSC to a lower one.

10. The system must be designed so that it is not inducing human errors. The operation of the system shall appear simple to the driver and the interface, instructions and warnings shall be clear, brief and understandable without overloading the driver to the point that his/her driving tasks are affected. This requirement puts a limit as to how much information the system may display to the driver. Further research is required to develop the vehicle driver interface through on board displays.

11. Retrofitting vehicles with no ERSC 2 capabilities to operate in ERSC2 is an expensive proposition that is not expected to be acceptable by users and automobile manufacturers. The upgrading of ERSC1 vehicles to ERSC2 is also going to be expensive due to the additional functions and redundancies required for ERSC2. An ERSC2 vehicle is almost a new design when compared with the vehicle for ERSC 1.

12. The low maintenance trend of today's vehicles is expected to continue for ERSC2 vehicles by the use of more electronics and on board diagnostics that monitor the equipment and provide warning for maintenance. These diagnostics will add to the acquisition cost of the vehicle. The lane reference aids, however, provided by the roadway have to be maintained and be available under almost all environmental conditions. The maintenance cost taken up by the roadway could be very high.

SECTION 4 ERSC 3 ANALYSIS

As with ERSC 1 and 2 in this section we present the details of the operation of ERSC 3 and specify the vehicle functions and interface with the driver and roadway as well as the functional and reliability requirements. We perform a system level FMEA in order to study the need for redundancies, diagnostics and identify possible deficiencies in the proposed functions of the system. The FMEA allows us to study reliability and maintenance issues and assess the potential for deploying ERSC 3 and for retrofitting. The section is concluded with a list of key findings and conclusions.

Vehicle Functions and Interface with Roadway and Driver

As with the previous ERSCs we start with a specific operating scenario for ERSC 3 that we use to develop the vehicle functions and the functions associated with the interaction of the vehicle with the roadway and driver.

Operational Scenario

The fitness of the vehicle to operate in the dedicated lane is evaluated constantly through on board vehicle diagnostics even when the vehicle is operating on manual lanes. When the vehicle approaches the dedicated lane it establishes communication with the roadway and presents its fitness status. The driver indicates his/her intention to enter the lane. If the vehicle is fit the roadway issues a permission to enter the lane. The driver looks for a safe gap and drives the vehicle into the dedicated lane. The roadway coordinates the merging of vehicles in the lane by controlling traffic via speed and headway commands for the vehicles operating in the lane and green and red signals for the merging vehicles. The lateral collision warning (LCW) is on during entry to the lane in order to assist the driver to merge safely. Once in the lane the driver switches on the automatic functions which are the SHM, RECA, and lane keeping (LK). The SHM, RECA operate as in ERSC 2. The LK function takes over steering in order to keep the vehicle in the center of the lane. The operation of the vehicle is "feet-off", "hands-off" and the driver has no direct overriding capabilities. He/she can disable the SHM, RECA and LK functions by initiating a check-out procedure. In this case the SHM function reduces speed and increases headway to a level which is comfortable for the driver and warns the driver to take over the throttle and brake. Similarly the LK system warns the driver to assume manual steering and allows him/her to start providing steering inputs. These inputs are augmented by the LK function in order to keep the lateral deviation from the center of the lane to within certain limits. The less correction the driver steering inputs require the more authority over steering is given to the driver until the LK function switches off completely and the driver is in full control of the vehicle. When the check-out procedure is complete the driver with the aid of the LCW drives the vehicle out of the dedicated lane. The roadway is informed when the vehicle intends to exit and when the exit maneuver is completed. If the driver fails the check-out procedure repeatedly the vehicle guides itself to a special ramp or shoulder lane where it stops and notifies the roadway. During operation in the dedicated lane the on-board diagnostics continuously monitor the fitness of the vehicle functions. The diagnostics may signal a check-out procedure in case of malfunctions and warn the driver appropriately. The system allows vehicles operating on fall-back modes in the dedicated lane at least for short periods of time, without affecting the safety of the fit vehicles. The fall-back modes include: operation as in ERSC 2, operation as in ERSC 1 and manual operation. The entry and exit configurations for ERSC 3 are the same as those for ERSC 1, 2 and are shown in figures 2, 3.

As with the previous ERSCs we start with the following high level vehicle functions that we use to generate the vehicle functions associated with ERSC 3.

H3.1 Speed and Headway Maintenance and Rear-End Collision Avoidance
H3.2 Lane Keeping
H3.3 Lateral Collision Warning
H3.4 Driver, Vehicle, Roadway Interface

H3.1 Speed and Headway Maintenance and Rear-End Collision Avoidance.

The block diagram of the SHM and RECA is shown in figure 16.

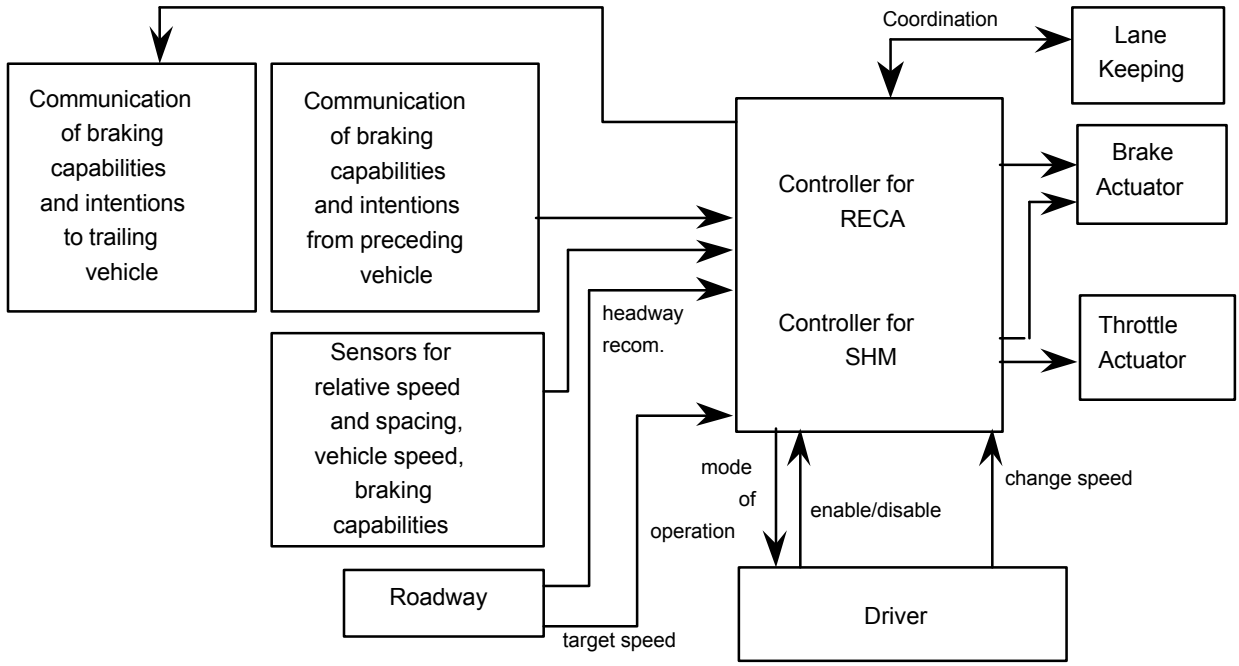

Figure 16: Speed and headway maintenance and rear-end collision avoidance.

Inputs:

Vehicle speed from speed sensor
Relative speed and spacing from ranging sensor
Braking capabilities of vehicle obtained using on board sensors
Braking capabilities and intentions of preceding (target vehicle) obtained via communications
Driver commands: enable, disable and speed/headway changes
Roadway commands: target speed, headway recommendations based on road conditions, traffic status and environmental conditions.
Steering angle and preview road data.

Outputs:

Throttle actuator command
Brake actuator command
Mode of operation displayed to the driver
Braking capabilities and intentions to trailing vehicle

Functional specifications:

The system calculates the safe headway based on the braking capabilities of the vehicle, the information about the braking capabilities of the preceding vehicle obtained via communication and any headway recommendation received from the roadway. The SHM adjusts the vehicle speed in order to reach and maintain the calculated headway. The SHM responds to roadway target speed commands provided the response does not lead to a reduction of the selected headway. The switching from headway to speed maintenance is the same as in ERSC 1, 2. The SHM uses engine torque and soft braking for controlling the speed and headway. Hard braking is the responsibility of the RECA function.

The RECA function monitors the actions and responses of the SHM and calculates the minimum time to collision (TTC). If the TTC becomes less or equal to the time required for bringing the vehicle to a full stop without collision the RECA provides the appropriate commands to the brake actuator overriding the actions of the SHM.

The driver cannot intervene in the operation of the SHM and RECA functions by overriding the actions of the throttle and brake. He/she can initiate a disabling procedure during which the SHM function reduces the speed and increases the headway to some preset values that are compatible with driver skills and reaction times and warns the driver to resume control.

The system interacts with the lane keeping function in order to adjust speed and maintain stability and riding comfort around curves.

The main functions of the SHM and RECA and the functional and reliability requirements are:

F3.1 Calculate safe headway
The SHM uses information from on-board sensors that sense vehicle's braking capabilities, the braking capabilities of the preceding vehicle obtained via communication and headway recommendations from the roadway to calculate a safe headway for vehicle following. The calculation of the safe headway shall take into account all factors and worst case stopping scenarios.

F3.2 Maintain cruise speed
The vehicle shall maintain a driver selected speed when no moving or stationary obstacles are within a calculated certain range. It shall respond to driver commands for changing the speed.

F3.3 Track and maintain roadway commanded target speed
The vehicle shall track and maintain the roadway commanded speed when no moving or stationary obstacles are within a calculated certain range, as long as the driver selected headway or the minimum safe headway is not violated.

F3.4 Maintain headway
The vehicle shall maintain the headway selected by the vehicle under all environmental conditions, road geometry and freeway speeds.

F3.5 Switch from maintaining cruise speed to maintaining headway
When the system senses a valid target in the same lane within a certain range it shall switch to the following mode and maintain a safe headway calculated by the vehicle.

F3.6 Switch from maintaining headway to maintaining cruise speed

When the target is no longer valid (or within range) the system shall switch to maintaining the current cruise speed.

F3.7 Switch from maintaining cruise speed to maintaining the roadway commanded target speed
The system shall respond to roadway target speed commands by changing current cruise speed to the target speed in a smooth manner provided no obstacle is within a certain range

F3.8 Hard braking for rear-end collision avoidance
The system shall calculate the time to collision (TTC) continuously by monitoring the actions and response of the SHM function, the status of the vehicle and of the preceding one. If the TTC becomes less or equal to the time required for stopping without collision then it shall send the appropriate command to the brake actuator to avoid a rear-end collision.

F3.9 Enable the SHM and RECA
Upon driver command the SHM and RECA shall both be switched on at the same time.

F3.10 Disable the SHM and RECA
Upon driver command the SHM and RECA functions shall be disabled by first reducing the speed and increasing the headway to levels that are safe for manual driving.

F3.11 Communication of braking capabilities and intentions to the trailing vehicle
The system shall communicate the vehicle's braking capabilities and intentions to the trailing vehicle in the same lane under all freeway conditions.

F3.12 Coordination with lane keeping and steering
The SHM and RECA shall coordinate with lane keeping and steering in order to adjust speed and maintain vehicle stability and riding comfort around curves.

H3.2 Lane Keeping

The functional block diagram of lane keeping is shown in figure 17.

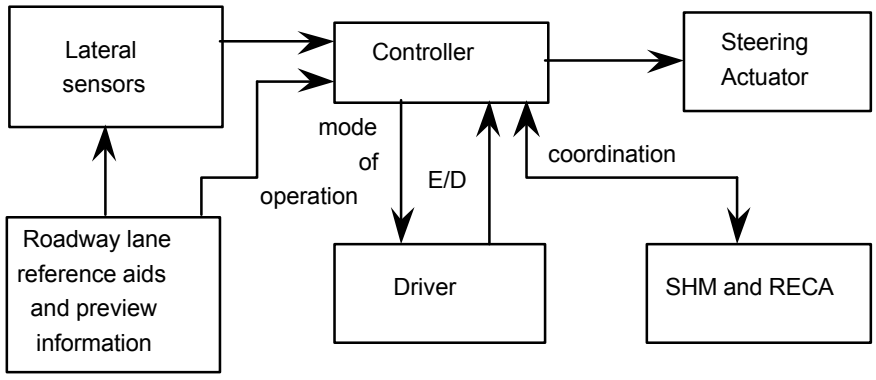

Figure 17: Lane keeping.

Inputs:
Deviation from center of the lane
Vehicle heading data (yaw rate, slip angle)

Preview information about the geometry of the roadway
Driver commands: enable, disable
Vehicle speed, brake actuator position from SHM and RECA

Outputs:
Command to steering actuator
Mode of operation displayed to the driver
Steering angle and steering intentions to SHM and RECA

Functional specifications:

The system uses inputs from lateral sensors that sense the position of the vehicle relative to the center of the lane, the yaw rate and the slip angle and preview information about the geometry of the road ahead. It calculates and sends the appropriate control commands to the steering actuator so that the vehicle remains in the center of the lane while traveling at highway speed. The system interacts with the SHM and RECA so that steering around curves is coordinated with speed in order to maintain vehicle stability and riding comfort. The system is switched on by the driver during entry to the dedicated lane provided the lane has the appropriate reference aids required by the on board lateral sensors. The driver cannot override the system while in the dedicated lane but he/she can initiate a check-out procedure that gradually disables the system provided the driver is fit to take over steering. The fitness of the driver is assessed by the system by allowing the driver some authority over steering. The driver's inputs are augmented by the system so that the performance of the vehicle is within certain bounds. The driver's authority over steering is increased gradually depending on his/her performance until the driver is in full control. The system notifies the driver of its mode of operation i.e., on, off, stand by, malfunction.

The specific functions of lane keeping and functional and reliability requirements are listed below:

F3.13 Keep vehicle in the center of lane
The system shall keep the vehicle in the center of the lane at all highway speeds, under all roadway and environmental conditions and during all modes of operation of the SHM and RECA functions.

F3.14 Enable LK
Upon driver command the LK function shall switch on.

F3.15 Disable LK
Upon driver command the LK function shall initiate a check-out procedure (see check-out function F3.24) and disable itself when the driver assumes full authority of steering for lane keeping.

H3.3 Lateral Collision Warning

The functional block diagram of the LCW is shown in figure 18.

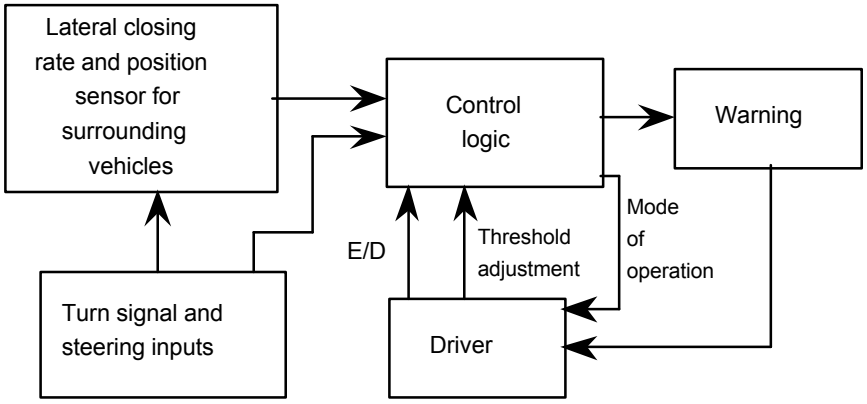

Figure 18: Lateral collision warning.

Inputs:

Lateral sensor measurements: lateral closing rate and position of surrounding vehicles
Intentions of driver to change lanes by sensing steering inputs, turn signal
Driver commands: enable, disable, threshold adjustment

Outputs:

Warning
Mode of operation displayed to the driver

Functional Specifications:

The system senses the position and closing rates of vehicles in adjacent lanes and calculates the time to collision (TTC) during lane changing maneuvers.

It warns the driver when the TTC is less than his/her reaction time or below a certain default value. The activation of the warning could be done by monitoring the turn signal and steering inputs. The threshold of the system is adjusted by the driver within certain limits that have to be selected based on human factors studies and experiments. The system is switched on and off by the driver. The system notifies the driver of its mode of operation i.e., whether it is on, off or whether there is a malfunction.

The specific functions and functional and reliability requirements are listed below:

F3.16 Warn driver
The system shall use the lateral sensor information to calculate the TTC in the lateral direction for a potential lane changing maneuver. The system shall monitor the intentions of the driver to change lanes and shall provide a warning to the driver before the execution of the maneuver and when the TTC is less than a certain default or driver selected value.

F3.17 Enable LCW
Upon driver command the LCW shall switch on to the standby mode.

F3.18 Disable LCW
Upon driver command the LCW shall switch-off.

F3.19 Adjust threshold

The driver shall be able to adjust the threshold of the LCW according to his reaction times and lane changing capabilities in order to reduce the number of unnecessary warnings. The adjustment shall be done within certain limits calculated using human factors considerations.

H3.4 Driver Vehicle Roadway Interface

Figure 19 shows the interface of the driver with the vehicle and roadway

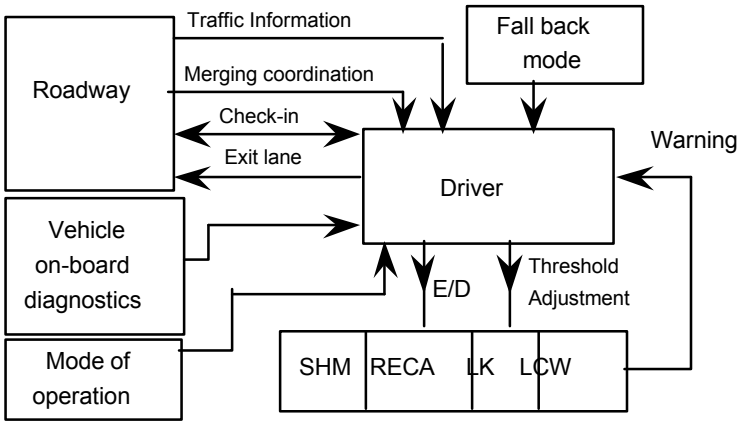

Figure 19: Driver interface with vehicle and roadway.

Inputs:

Traffic information from the roadway
Information from on board diagnostics and mode of operation
Lateral collision warning
Fall back mode instructions

Outputs:

Enable/Disable, Threshold adjustments
Route selection
Manual control for entry, exit

The interface of the driver with the vehicle functions and roadway involve the following functions and requirements:

F3.20 Check-in

On board diagnostics continuously check the fitness of the vehicle to operate on the dedicated lane and notify the driver of the fitness status of the vehicle for AHS operation. When the driver requests to check-in, the vehicle presents its fitness status and identification to the roadway via vehicle to roadway communication. If the vehicle is fit the roadway sends an acknowledgment that the vehicle passed the check-in test.

F3.21 Enter the lane

The driver responds to the merging coordination and directions provided by the roadway, looks for a safe gap and drives the vehicle into the dedicated lane. The merging of the vehicle into the dedicated lane is aided by the lateral collision warning function. Once in the lane he/she switches on the automated vehicle functions and driving becomes "hands-off", "feet-off".

F3.22 Response to LCW
The driver responds to the LCW during lane changing maneuvers by using steering, throttle and brakes.

F3.23 Response to traffic information
The driver processes roadway traffic information in order to make routing decisions and/or assume full manual control or a lower ERSC if necessary.

F3.24 Check-out
The driver initiates a check-out procedure. The SHM reduces speed and increases headway and notifies the roadway of the driver's intention to leave the lane. The driver is warned to take over lane keeping and throttle and brake control. The transition from automatic to manual control is done under the supervision of the automated functions of the vehicle as follows: After the check-out procedure initiation the driver actions are monitored and supervised by the system. The driver inputs to the throttle, brake and steering are augmented by those of the SHM, RECA and LK functions in order to maintain the stability and performance of the vehicle. If the driver's performance is acceptable the driver is gradually given more authority until the transition to manual control is fully completed. If the driver fails the check-out procedure repeatedly the vehicle guides itself to a special exit ramp or shoulder lane, stops and notifies the roadway.

F3.25 Exit the lane
When the check-out procedure is successful the driver assumes manual control and drives the vehicle out of the dedicated lane. The system sends a notification to the roadway.

F3.26 Fall back to ERSC 2
The vehicle functions revert to those of ERSC 2 in case of detected malfunctions of the LK function or in case the roadway cannot provide lane reference aids. The transition is done after the driver takes over steering successfully.

F3.27 Fall back to ERSC 1
The vehicle functions revert to those of ERSC 1 when the RECA function becomes inaccurate due to the inability of the system to assume responsibility of rear-end collisions. The driver is warned to take over steering and supervise throttle and braking. The transition of lane keeping and throttle, brake control to driver is done as in the check-out procedure.

F3.28 Fall back to manual control
During check-out or when certain vehicle functions or their redundant paths are not functioning properly the driver is required to assume manual control. The driver is given the appropriate warning to start the check-out procedure and transition to manual control.

F3.29 Notify driver of mode of operation
The system shall notify the driver of the current mode of operation of all the automated functions.

Failure Modes and Effects Analysis

The results of the FMEA for ERSC 3 are analyzed and used to identify the need for redundancies, vehicle diagnostics, human factors issues, technical issues and risks and future research items. The FMEA tables are presented in table 14 of Appendix B.

In this section we present the identified potential failure modes, list their causes and discuss their effects. We list a set of design requirements and recommendations that could be followed in order to reduce the severity and occurrence ratings and identify issues and risks as well as issues for future research.

H3.1 Speed and Headway Maintenance and Rear-End Collision Avoidance.

Potential failure Mode F3.1 : Loss of ability to calculate correct value of safe headway

As in ERSC 2 the calculation of the safe headway by the system is very critical. In ERSC 3 is even more critical due to the fact that the lane keeping function is also automated and driving is "feet-off", "hands-off". A failure in the longitudinal direction due to the incorrect calculation of the safe headway may lead to failures in the lateral direction with catastrophic consequences. As in ERSC 2 the causes for failure mode F3.1 are the same and are listed below for the sake of completeness:

(F3.1.1) Detected malfunction or inability of the sensors to estimate the braking capabilities and intentions of the preceding vehicle. (S=6, O=6)
(F3.1.2) Detected malfunction or loss of communication with preceding vehicle. (S=6, O=6)
(F3.1.3) Faulty or inaccurate measurements of braking capabilities of vehicle or the preceding vehicle. (S=10, O=6)
(F3.1.4) Incorrect braking capabilities and intentions are received through communication due to interference or noise corruption. (S=10, O=6)
(F3.1.5) Loss of communication with roadway and/or lack of headway recommendation. (S=6, O=4)
(F3.1.6) Loss of braking data information from preceding vehicle due to receiver malfunction. (S=9, O=4)

The effect of the early detected failures such as (F3.1.1), (F3.1.2), (F3.1.5) is degradation of efficiency since the lack of information, taken into account in calculating the headway, leads to a larger headway. Undetected failures and failures detected late such as (F3.1.3), (F3.1.4), (F3.1.6) may lead to an incorrect calculation of headway. If such headway is smaller than what is required to stop without a collision a rear-end collision may take place.

The design requirements and recommendations are:

(F3.1.1) The malfunction of sensors or gross inaccuracies in the estimation of the braking capabilities must be detected fast. The system must fall back to the default headway that takes into account the inaccuracy or malfunction of the sensors.

(F3.1.2) Diagnostics and built-in self tests must be used to guarantee a fast detection of any communication failure. When a malfunction occurs the headway must be automatically increased to the default safe level that takes into account the failure.

(F3.1.3) The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements must be monitored and taken into account in the calculation of the safe headway.

(F3.1.4) The measurements of braking capabilities of all vehicles must be accurate. The system must check the reasonableness of preceding vehicle's braking capability and take into account possible inaccuracies and inconsistencies in calculating the safe headway.

(F3.1.5) The system must be able to accommodate the lack of headway recommendation from roadway .

(F3.1.6) The system must have supervisory elements and diagnostics that monitor the functionality of the receiver. The malfunction of the receiver must be taken into account in calculating the safe headway.

As in ERSC2 the accurate estimation and measurements of all factors that affect headway is an issue that requires further research. A conservative estimation of the safe headway will lead to large headways that will affect capacity. The criticality of the calculation of the correct safe headway is so high that multiple methods must be used to calculate and evaluate it. The roadway may have to play a more active role in informing vehicles of the expected tire to road friction coefficients, the presence of disabled and/or unfit vehicles in the lane ahead etc.

Potential failure Mode F3.2.1: Loss of speed maintenance function.

The SHM may lose its ability to maintain a constant cruise speed if any one of the following components fails to perform as designed:

(F3.2.1.1) Speed sensor gives erroneous or variable readings. (S=9, O=2)
(F3.2.1.2) Controller electronics or software failure. (S=9, O=2)
(F3.2.1.3) Throttle actuator failure. (S=8, O=3)
(F3.2.1.4) Brake actuator failure (brake cannot be applied or brake is continuously applied). (S=10, O=3)

The potential effect of the above failures is the inability of the vehicle to obey the traffic rules for speed limits. In addition the system may not be able to adjust speed around curves. Since the driver is no longer a back-up the system may fail to maintain stability and driving comfort around curves by coordinating with the lane keeping function. In the case of failure (F3.2.1.4) the vehicle may fail to slow down around a curve and may go out of control and lead to multiple collisions.

The design requirements and recommendations are:

(F3.2.1.1) Diagnostics and built-in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.2.1.2) The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.2.1.3) The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.2.1.4) The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failures must be employed together with the appropriate logic and diagnostics that allow automatic switching from a failed actuator to a healthy one.

When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

The most severe failure is that of the brake actuator. Such failure implies that the RECA function is not effective and the system may not be able to slow down around curves. The effect of the failure of the throttle actuator is mitigated by the use of braking which can override the actions of the throttle in speed control. The design requirements call for redundancies and extensive diagnostics both in hardware and software. The most crucial redundancies are those of the brake actuator as described by requirement (F3.2.1.3).

Potential failure Mode F3.2.2: System switches to headway maintenance in the absence of valid target.

The possible cause of the above failure is due to:

(F3.2.2.1) Ranging sensor detects an invalid target within a certain range

The potential effect of the failure is unnecessary deceleration and activation of the RECA function which may lead to degradation of riding comfort and efficiency.

The design requirements and recommendations are:

(F3.2.2.1) The system must be able to discriminate between valid and invalid targets.
As with ERSC2 the design requirement will be easier to meet if two ranging sensors that are not subject to common mode failures are used together with the appropriate logic and diagnostics. The outputs of the two sensors should be continuously monitored and checked for reasonableness and consistency. A higher level controller should be used to decide which of the two outputs is the correct one when the two outputs are different. If the controller cannot decide the system shall follow the output that indicates the closer target and shall revert to manual control. The use of three ranging sensors that are based on different principles of operation and not subject to common mode failures may be a better way of improving the reliability of the ranging measurements. In this case the three outputs of the sensors are compared and the majority rule could be used to choose the output to be used for control purposes.

Potential failure Mode F3.3.1: Vehicle cannot maintain target speed as commanded by the roadway.

The vehicle may lose its ability to maintain the roadway commanded target speed if any one of the following components fails to perform as designed.

(F3.3.1.1) Speed sensor gives erroneous readings. (S=9, O=2)
(F3.3.1.2) Controller electronics or software failure. (S=9, O=2)
(F3.3.1.3) Throttle actuator failure. (S=8, O=3)
(F3.3.1.4) Brake actuator failure. (S=10, O=3)
(F3.3.1.5) Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication. (S=8, O=3)
(F3.3.1.6) Loss of target speed information due to receiver malfunction. (S=8, O=3)

The potential effects of the vehicle not maintaining the target speed commanded by the roadway are degradation of safety and efficiency. The vehicle may be cruising at a speed that is unsafe for the existing traffic conditions. In another situation the vehicle may be cruising at a lower speed holding traffic and causing reduction in capacity and efficiency. Failures (F3.3.1.1), (F3.3.1.2) may also imply that the

system may not be able to adjust speed around curves and thus affect the performance of the lane keeping function. The brake actuator failure implies that the RECA function is not effective and therefore the vehicle is no longer capable of avoiding rear-end collisions.

The design requirements and recommendations are:

(F3.3.1.1) Diagnostics and built-in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.3.1.2) The system must have supervisory elements (in hardware or software) or adequate redundancies. When a controller malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.3.1.3) The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.3.1.4) The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failures must be employed together with the appropriate diagnostics that allow automatic switching from a failed actuator to a healthy one. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.3.1.5) The system must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.) When a communication malfunction is detected the system shall fall back to a default lower speed if there is no valid target to follow. The driver shall be notified of the loss of communication.

(F3.3.1.6) The system must have supervisory elements in controller software and receiver to detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to initiate a check-out procedure and exit the lane.

Potential failure Mode F3.3.2: System switches to headway maintenance in the absence of valid target.

The cause of the above failure mode may be due to:

(F3.3.2) The ranging sensor detects an invalid target within a certain range. (S=7, O=6)

The potential effect of the failure is degradation of riding comfort and efficiency due to the unnecessary use of deceleration and possible activation of the RECA function.

The design requirements and recommendations are:

(F3.3.2) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics. As with ERSC 2 the

ranging measurements must be accurate and reliable. Redundant ranging sensors with appropriate logic and diagnostics are essential in meeting the high reliability standards.

Potential failure Mode F3.4: The system cannot maintain desired headway

The SHM may fail to maintain a desired headway selected by the system due to the following:

(F3.4.1) Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability. (S=10, O=6)
(F3.4.2) Sensor loses target due to road curvature or insufficient target reflectiveness. (S=10, O=7)
(F3.4.3) Ranging sensor has locked on an invalid target. (S=7, O=7)
(F3.4.4) Brake actuator failure. (Or intermittent failure to respond) (S=10, O=3)
(F3.4.5) Throttle actuator failure. (S=8, O=3)
(F3.4.6) Controller electronics or software failure. (S=9, O=2)
(F3.4.7) Ranging sensor gives erroneous readings. (S=10, O=4)

The most serious effect of the failures is a rear-end collision. Failure of the ranging sensors and/or the brake actuator implies that the RECA function is also ineffective and therefore a rear-end collision may be unavoidable. The most serious failure associated with the ranging sensor is the one where the sensor fails to detect an obstacle within a certain range or provides a larger range reading due to interference and/or malfunction. A rear-end collision may also cause the vehicle to depart the lane, go out of control leading to multiple collisions. Failures (F3.4.3), (F3.4.5) are less serious as far as safety is concerned but they may affect efficiency and riding comfort.

The design requirements and recommendations are:

(F3.4.1) The system must be able to detect and accommodate intermittent sensor failures. The system software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and switch to manual control by following the check-out procedure. Redundant ranging sensors, not subject to common mode failures, with appropriate logic must be used.

(F3.4.2) The sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Vehicle shall slow down and switch to manual control when target is ambiguous and cannot be followed reliably. Sensor redundancies must be used to track targets around curves and minimize the possibility of interference.

(F3.4.3) The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. The system must distinguish vehicles moving to adjacent lanes and around curves in the same lane. Redundant ranging sensors not subject to common failure modes with appropriate logic may be required.

(F3.4.4) The system must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators that are not subject to common mode failures with appropriate logic must be used. When a redundant braking path fails the system shall initiate a check-out procedure.

(F3.4.5) The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, the system shall switch to manual control by warning the driver and following the check-out procedure.

(F3.4.6) The system must have supervisory elements (in hardware and software) or adequate redundancies. The system shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.

(F3.4.7) The system must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. The system shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.

The above requirements call for significant redundancies for the ranging sensor and brake actuator. The level of required reliability for the ranging sensor and brake actuator is much higher for ERSC 3 due to the effect a rear-end collision may have on lane keeping. It is unlikely that under a severe rear-end collision the lane keeping function will manage to keep the vehicle in the lane. Since driving is "feet-off", "hands-off" the driver is not expected to play any constructive role during emergencies. As a result a rear-end collision may cause the vehicle to depart the lane, go out of control and collide with vehicles in adjacent lanes.[39] It is therefore very important that the probability of a rear-end collision be reduced to almost zero by introducing two or even three redundant paths for the brakes and two or three redundant ranging sensors with the appropriate diagnostics and logic. The system shall be considered unfit to operate in the automated mode if any one of the redundant paths fails.

A design issue associated with the redundant brake actuators that needs further research is how to design the system to switch from a failed path to a redundant healthy one without degrading the braking performance.

Another issue is how to design the lane keeping function so that it is robust with respect to disturbances that take place during a rear-end collision. It is unlikely that the lane keeping function can be designed not to be affected by any rear-end collision. This raises the question whether lane keeping and RECA can be deployed together without an automated lateral collision avoidance system.

Potential failure Mode F3.5: Failure to switch from maintaining speed to maintaining headway even when a valid target exists.

The system is supposed to switch from maintaining cruise speed to maintaining headway when a target appears within a certain range. The system may fail to do so due to the following:

(F3.5.1) Ranging sensor fails to detect a valid target. (S=10, O=5)
(F3.5.2) Hardware or software failure of the SHM. (S=9, O=2)

The effect of failure (F3.5.1) is a possible rear-end collision that may cause the vehicle to depart the lane and go out of control. The effect of failure (F3.5.2) is less severe provided the RECA function is healthy. It may affect, however, efficiency and riding comfort.

The design requirements and recommendations are:

(F3.5.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics. In case of sensor failure

the system shall switch to manual control by providing a warning to the driver, slowing down and following the check-out procedure.

(F3.5.2) The system must have supervisory elements (in hardware or software) or adequate redundancies. The system shall switch to manual control by warning driver and following a check-out procedure in case of a detected failure.

Potential failure Mode F3.6: Failure to switch to speed maintenance mode when the original target moves out of the lane and becomes unsuitable to follow, and no other valid target exists.

When the target moves out of the sensing range or changes lane, the system is supposed to switch to maintaining the current speed. The system may fail to switch due to the following:

(F3.6.1) Ranging sensor locks on the original target or locks on another target which is invalid when the original target becomes unsuitable to follow. (S=8, O=6)
(F2.6.2) Hardware or software failure of the SHM. (S=8, O=2)

The effect of the above failures is unnecessary acceleration or deceleration and activation of the RECA function that may lead to degradation of riding comfort and efficiency. The design requirements and recommendations are:

(F3.6.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics.

(F3.6.2) The system must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. System shall switch to manual control by warning the driver and following a check-out procedure in case of a detected failures.

Potential failure Mode F3.7.1: Failure to switch to maintaining roadway commanded target speed.

The system is supposed to switch from cruising at current speed to maintaining the roadway commanded target speed. Failure to do so may be due to the following:

(F3.7.1.1) Loss of target speed information input due to receiver malfunction. (S=8, O=3)
(F3.7.1.2) Loss of roadway transmission capability or target speed is corrupted during communication. (S=8, O=3)

The effect of the above failures is degradation of efficiency and safety since the vehicle does not switch to an optimal and/or safer speed based on current traffic and roadway conditions.

The design requirements and recommendations are:

(F3.7.1.1) The system must have supervisory elements in controller software and receiver to detect any receiver malfunction. The roadway must assist in testing receiver functionality. The driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to initiate a check-out procedure and exit the lane.

(F3.7.1.2) The system must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. The system must be able to accommodate

temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). The system must be able to accommodate momentary loss of roadway target speed command. When a communication malfunction is detected, the system shall fall back to a default lower speed if there is no valid target to follow. The driver shall be notified of the loss of communication.

Potential failure Mode F3.7.2: Switching to headway maintenance instead of switching from cruise control speed to maintaining the roadway target speed command..

The main cause of the above failure is due to:

(F3.7.2) Ranging sensor detects an invalid target. (S=8, O=6)

The above failure may cause unnecessary acceleration or braking and activation of the RECA function leading to a possible degradation of riding comfort and efficiency.

The design requirements and recommendations are:

(F3.7.2) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used.

Potential failure Mode F3.8.1: Failure of the RECA function to take action on time.

The system may fail to apply hard braking in order to avoid rear-end collision or reduce the possibility of one due to the following:

(F3.8.1.1) Ranging sensor fails to provide signal or provides incorrect signal. (S=10, O=5)
(F3.8.1.2) Loss of communication of braking intentions of preceding vehicle. (S=10, O=5)
(F3.8.1.3) Controller electronics or software failure. (S=10, O=2)
(F3.8.1.4) Brake actuator failure. (S=10, O=3)
(F3.8.1.5) Calculated time to collision (TTC) is larger than actual TTC due to incorrect measurement of braking capabilities. (S=10, O=6)
(F3.8.1.6) Ranging sensor switches from a valid target to another one with completely different operating status and braking capabilities e.g. preceding vehicle exits lane and next vehicle in lane is disabled. (S=10, O=3)

The effect of the above failures are catastrophic. Failure of the RECA function may easily lead to a rear-end collision that may cause the vehicle to depart the lane, go out of control and collide with additional vehicles in the same and/or other lanes.

The design requirements and recommendations are:

(F3.8.1) The system must have redundant sensing inputs to reduce the probability of missing a target to essentially zero . If redundancy is lost, the system shall increase headway and reduce speed and switch to manual control. The system and lane keeping function shall be designed so that the vehicle doesn't depart the lane during rear-end collisions.

(F3.8.1.2) A redundant method must be used to communicate the preceding vehicle's braking intention. The calculated safe headway must take into account momentary loss of vehicle to vehicle

communication. If loss of communication is permanent, system shall take that into account in calculating the safe headway.

(F3.8.1.3) The system must have supervisory elements in software and hardware and adequate redundancies. When a redundancy is lost, the system shall increase headway and reduce speed to comfortable levels and warn the driver to operate at ERSC1 or the manual mode and exit the lane as soon as possible.

(F3.8.1.4) The system must have redundant braking actuators that are not subject to common mode failures and appropriate diagnostics that allow the fast detection and accommodation of failures without degrading the performance of the RECA function. When a redundant braking path fails the system shall switch to ERSC1 or manual mode and warn the driver appropriately. The transition to ERSC1 or manual mode shall be done by first reducing speed and increasing headway to levels that are comfortable for the driver.

(F3.8.1.5) The TTC must be accurate and conservative in order to accommodate possible inaccuracies in measurements. Independent estimates of TTC based on independent measurements must be used. The system and lane keeping function shall be designed so that the vehicle doesn't depart the lane during rear-end collisions.

(F3.8.1.6) The system must be designed to account for such situations. Vehicle to vehicle communication may be used to notify the trailing vehicle of conditions ahead or the system must be designed so that exiting from the lane is possible only at designated points where larger headways are imposed.

The FMEA results raised several important safety issues that are discussed below.

The RECA function shall be highly reliable. To achieve a high level of reliability considerable redundancies for the sensors, brake actuators, hardware and software components and diagnostics are required. This requirement will increase complexity and introduce new failure modes that require further study.

A rear-end collision or even hard braking may cause the vehicle to depart the lane. Since the driver is no longer considered to be a backup for steering or braking, a lane departure may cause the lane keeping function to fail or become ineffective causing the vehicle to go out of control. This may lead to multiple collisions with vehicles in the same and/or other lanes. This safety issue raises the question whether the RECA and the lane keeping functions can operate together without a lateral collision avoidance function.

The analysis also indicates that the lane keeping function shall be designed to be robust with respect to disturbances that arise during hard braking applied by the RECA and during moderate rear-end collisions.

One of the major deficiencies of ERSC 3 is that neither the vehicle nor the driver are considered to be responsible for collision avoidance using steering. This deficiency makes ERSC 3 non deployable unless the functions of the vehicle and roadway as well as the roadway configurations are modified.

Potential failure Mode F3.8.2: The RECA is activated unnecessarily.

The incorrect activation of the RECA may be due to the following causes:

(F3.8.2) Incorrect range is sensed or incorrect TTC is calculated. (S=7, O=4)

The false activation of the RECA may affect riding comfort and efficiency.

The design requirements and recommendations are:

(F3.8.2) The system must minimize the number of faulty activations of the RECA function as much as possible. Independent ranging measurements and calculations of the TTC must be used. Activation of the RECA shall not affect the performance of the lane keeping function and shall not cause the vehicle to depart the lane.

Potential failure Mode F3.9: SHM and RECA cannot be enabled

The possible cause of the above failure is:

(F3.9) Electronic malfunction. (S=7, O=2)

The effect of the above failure is that the vehicle cannot operate in the dedicated lane. It will either fail the check-in test or the driver has to drive it away from the entrance to AHS. Failure of the SHM and RECA may cause a disturbance at the entrance to the lane or inside the lane and may affect efficiency.

The design requirements and recommendations are:

(F3.9) The controller electronics must be sufficiently reliable.
Diagnostics must be performed even when the SHM and RECA are in the standby mode. The driver shall be notified of any detected malfunctions.

Potential failure Mode F3.10.1: SHM and RECA cannot be disabled

The potential failure cause of the above failure is:

(F3.10.1) Electronic malfunction. (S=10, O=2)

The effect of the above failure is possible panic and confusion to the driver during the transition from automatic to manual mode that may affect his/her performance such as steering or taking over the lane keeping function.

The design requirements and recommendations are:

(F3.10.1) The controller electronics must be sufficiently reliable. The driver shall have redundant means of turning off the SHM and RECA. Switching off of the functions must follow the disabling procedure so that the driver is not put in a situation he/she cannot handle.

Potential failure Mode F3.10.2: SHM and RECA are disabled without first reducing speed and increasing headway.

This malfunction may be caused by:

(F3.10.2) Software failure or failure of the brake actuator. (S=10, O=3)

The effect of this failure is serious and may lead to collision. It may put the driver in a situation of high speed and short headway that he/she cannot handle.

The design requirements and recommendations are:

(F3.10.2) The system must have redundancies in software and redundant braking actuator paths. The system must be designed to fall back to a default speed and headway in a reliable manner when a failure is detected before the SHM and RECA are disabled.

Potential failure Mode F3.11.1: Loss of communication of braking capabilities and intentions to the trailing vehicle

The potential cause of the above failure mode is due to:

(F3.11.1) Failure of transmitter. (S=10, O=3)

If the failure is detected fast enough the trailing vehicle is supposed to take that into account and increase its headway. In this case efficiency will be affected. If undetected or detected late the computed TTC of the trailing vehicle may be large and incorrect leading to a possible rear-end collision that may cause both vehicles to depart the lane and go out of control.

The design requirements and recommendations are:

(F3.11.1) The system must have supervisory elements to monitor the transmitter. Redundant transmitters may be necessary. If the transmitter fails permanently, the vehicle shall exit the lane. The lane keeping function and system must be designed so that the vehicle does not go out of control due to rear end collisions.

Potential failure Mode F3.11.2: The vehicle transmits incorrect braking capabilities and/or braking intentions to trailing vehicle.

The potential cause of the failure is due to:

(F3.11.2) Faulty or inaccurate measurements of braking capabilities and/or braking intentions. (S=10, O=6)

The effect of the above failure is a possible rear-end collision with the trailing vehicle due to the inaccurate calculation of the TTC by the trailing vehicle. The rear-end collision may cause vehicles to depart the lane and go out of control.

The design requirements and recommendations are:

(F3.11.2) The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements shall be monitored. Independent means for calculating braking capabilities must be employed. The lane keeping function and system must be designed so that the vehicle doesn't go out of control due to rear end collisions.

Potential failure Mode F3.12: Loss of coordination with lane keeping and steering

The system is suppose to adjust speed depending on the steering angle by coordinating its actions with the lane keeping function. Failure to do so may be due to:

(F3.12) Electronics or Software failure. (S=10, O=3)

The effect of the failure is the possibility of the vehicle to depart the lane and go out of control.

The design requirements and recommendations are:

(F3.12) Redundancies in electronics and software must be used. When a failure is detected the vehicle shall slow down excessively around curves, increase headway and the driver shall be warned to initiate a check out procedure.

Potential failure Mode F3.13: Loss of lane keeping capability

The lane keeping function may fail to perform as designed due to the following:

(F3.13.1) Failure to detect vehicle's lateral position due to malfunction of sensor or roadway lane reference aid. (S=10, O=5)
(F3.13.2) Lane preview information is not available. (S=8, O=3)
(F3.13.3) Control software or electronics failure. (S=10, O=2)
(F3.13.4) Steering actuator failure. (S=10, O=3)

The effect of the above failures is catastrophic with the exception of (F3.13.2) where the vehicle may be able to accommodate the failure by slowing down and falling back to a lower ERSC since the detection of the failure can be fast. Loss of the lane keeping capability may automatically cause the vehicle to depart the lane and go out of control. The driver, even if alert, may not have sufficient time to react and take over steering.

The design requirements and recommendations are:

(F3.13.1) The system must have redundant measurements of the lateral position of the vehicle. Redundant sensors and reference aids may be required with the appropriate diagnostics and logic. When a redundant component fails the system shall warn the driver and switch to manual control or to a lower ERSC.

(F3.13.2) The system must have redundant means of obtaining preview information. In the absence of preview information the system shall warn the driver and switch to a lower ERSC.

(F3.13.3) All electronic components and software must have redundancies and appropriate diagnostics to detect failures. When a failure of a redundant component is detected the system shall switch to a lower ERSC and warn the driver. Detection and accommodation of failures shall be fast and shall not affect the performance of the lane keeping function.

(F3.13.4) Redundant steering actuators and components with the appropriate diagnostics and logic must be used. When a redundant component fails the system shall warn the driver to assume manual control of the steering function by following a check-out procedure.

The switching from a redundant path that failed to a healthy one must be automatic so that the lane keeping performance is not affected. Further research is needed to develop such systems using hardware and software designs and control systems techniques.

The availability of sensors and lane reference aids that can be used at all highway speeds under all road and environmental conditions is a technical issue that needs further research. Despite recent successful experiments in lane keeping[40,41,42] the design and reliability requirements generated by the FMEA cannot be met with today's sensor technology within affordable cost constraints.

Another issue is the effect of other functions such as RECA on lane keeping and the effect of lane keeping on RECA. Both functions must be designed to be robust with respect to disturbances caused by these functions.

Potential failure Mode F3.14: Lane keeping cannot be enabled.

A possible cause of the above failure is due to:

(F3.14) Controller electronic circuitry or software failure. (S=6, O=2)

This failure doesn't have any significant effect on safety. The vehicle may fail the check-in test or may have to operate at a lower ERSC if allowed into the AHS facility.

The design requirements and recommendations are:

(F3.14.1) The controller electronics and software must be sufficiently reliable. Diagnostics must be performed even when the LK is in the standby mode and the driver shall be notified of detected malfunctions.

Potential failure Mode F3.15.1: LK cannot be disabled

A possible cause of the above failure is:

(F3.15.1) Electronic and/or software malfunction. (S=8, O=2)

The effect of the failure is that the driver may panic since he/she cannot control the situation. He/she may bring the vehicle to a stop by disabling the SHM and RECA functions and therefore disturb the traffic.

The design requirements and recommendations are:

(F3.15.1) The controller electronics must be sufficiently reliable. The driver shall have redundant means of disabling the LK. The disabling of the LK function shall follow the check-out procedure.

Potential failure Mode F3.15.2: LK is disabled suddenly without following the check-out procedure.

A possible cause of the above failure is:

(F3.15.2) Electronic and/or software failure. (S=10, O=2)

The sudden disabling of the lane keeping function may put the driver in a situation he/she cannot handle. Even if the driver is alert his/her reaction time may not be short enough to take over steering and stop the vehicle from departing the lane.

The design requirements and recommendations are:

(F3.15.2) All electronic components and software must have redundancies and appropriate diagnostics to detect failures. When a failure of a redundant component is detected the system shall switch to a lower ERSC and warn the driver. Detection and accommodation of failures shall be fast and shall not affect the performance of the lane keeping function.

H3.3 Lateral Collision Warning

Potential failure Mode F3.16.1: Cannot provide LCW.

The system may fail to provide a lateral collision warning due to the following causes:

(F3.16.1.1) Sensor failure to detect lateral range and range rate of "threatening" vehicles. (S=9, O=5)
(F3.16.1.2) Control software or electronics failure. (S=9, O=2)
(F3.16.1.3) The threshold is set too high. (S=9, O=4)
(F3.16.1.4) Warning output device failure. (S=9, O=3)
(F3.16.1.5) The calculated TTC is incorrect. (S=9, O=6)

The result of the above failure could be a collision with other vehicles if the driver relies on the system too much.

The design requirements and recommendations are:

(F3.16.1.1) Supervisory elements and diagnostic programs must be used to monitor the reasonableness of the sensor measurements. Redundant sensors may be needed. The driver shall be notified of any malfunction.

(F3.16.1.2) Software and electronics must be reliable. Redundancies must be employed to improve reliability. The driver shall be notified of any malfunction.

(F3.16.1.3) Supervisory element is needed to check threshold. The default level of threshold must be low. The level of the threshold and its consequences shall be visible to the driver.

(F3.16.1.4) The warning device must be reliable. Redundant warning methods must be used.

(F3.16.1.5) There shall be independent methods of calculating the TTC. The most conservative estimate of TTC shall be used.

The most important issues in LCW are the following:

(i) When and how to give the warning. The warning must be given before the driver starts changing lanes in order to give him/her enough time to react. If the LCW is on all the time the driver may be

receiving many unnecessary warnings due to the moving vehicles in the neighboring lane. If these warnings are audible the driver may be disturbed, get annoyed and switch the system off. A visual warning using a display may be less distractive in this situation. Human factors studies are essential in determining the type of warning.[43]

(ii) The ability of the system to identify threatening vehicles and calculate the TTC is a technical issue that needs to be studied. Due to the high bandwidth of steering any vehicle in the neighboring lane could be classified as threatening.

(iii) The sensor requirements for LCW are also a technical issue that needs further study. The sensors should cover more than 180 degrees field of view, identify all moving objects, their closing rates and classify them as threatening or non-threatening.

Potential failure Mode F3.16.2: Give frequent false warnings

This failure may be due to the following causes:

(F3.16.2.1) Threshold is too low. (S=6, O=5)
(F3.16.2.2) Control software malfunction or warning device failure. (S=6, O=2)

The effect of these failures are not significant as far as safety is concerned. They may distract the driver, annoy him/her and force him/her to switch the system off.

The design requirements and recommendations are:

(F3.16.2.1) The driver shall be able to select a threshold level that he/she feels comfortable with. The default threshold must be set to a level appropriate for typical conditions.

(F3.16.2.2) The number of false alarms must be minimized by improving the reliability of hardware and software components. Redundant components and appropriate diagnostics may be used to improve reliability.

Potential failure Mode F3.17: The LCW cannot be enabled.

The potential cause is:

(F3.17) Electronic circuitry or software failure. (S=5, O=2)

The effect is that the driver has to operate the vehicle without the LCW. Safety is compromised.

The design requirements and recommendations are:

(F3.17) The system must have sufficiently reliable electronic circuitry and software. Redundancies shall be used to achieve a high level of reliability.

Potential failure Mode F3.18: LCW cannot be disabled.

The potential cause is:

(F3.18) Electronic circuitry failure. (S=3, O=2)

The effect of the failure is minor. The driver may get distracted and annoyed.

The design requirements and recommendations are:

(F3.18) The system must have very reliable electronic circuitry. The driver shall have redundant means of turning off the LCW.

Potential failure Mode F3.19: LCW Threshold cannot be adjusted.

(F3.19) Electronics or failure. (S=6, O=2)

The effect is that the driver may be uncomfortable with the currently selected threshold. He/she may get annoyed.

The design requirements and recommendations are:

(F3.19) The controller electronics and software must be sufficiently reliable. The threshold setting shall default to a low level when the LCW is enabled for the first time or when a failure is detected. Driver shall be able to read and verify the selected threshold setting.

H3.4 Driver Vehicle Roadway Interface

Potential failure Mode F3.20: Failure of check-in function.

The check-in function may fail to perform as designed due to the following:

(F3.20.1) On-board diagnostics fail to detect a fault in major functions of the vehicle. (S=9, O=3)
(F3.20.2) Driver ignores the results of the on-board diagnostics and/or roadway considers the vehicle to be fit when it is not. (S=9, O=3)
(F3.20.3) On-board diagnostics make a wrong decision about a component or function that was not at fault. (S=6, O=2)

The effect of the first two failures is that the vehicle may enter and operate in the dedicated lane without being fit. The last failure will stop the vehicle from entering the dedicated lane even though it is fit. The severity of the first two failures is fairly high . It will affect safety and efficiency especially if the vehicle stays in the lane for long time.

The design requirements and recommendations are:

(F3.20.1) Diagnostic algorithms must be robust and highly reliable. The roadway must be able to detect an unfit vehicle operating in the dedicated lane.

(F3.20.2) The roadway must be able to identify an unfit vehicle operating in the dedicated lane. Traffic rules and regulations must be used to deter the driver from violating the rules.

(F3.20.3) On board diagnostics must be highly reliable. Redundancies and supervisory elements must be considered for improving reliability.

Potential failure Mode F3.21: Driver fails to enter the lane

The driver may fail to merge into the dedicated lane due to the following:

(F3.21) Dedicated lane is congested or driver is not able to merge due to high speed and/or small headways in dedicated lane or driver doesn't have the required skills. (S=5, O=4)

The effect of this failure is that the vehicle is restricted from or delayed in entering the dedicated lane. This will lead to possible congestion in the transition lane or entrance to the lane.

The design requirements and recommendations are:

(F3.21) The roadway must be able to enforce lower speeds and larger headways near the entry points. Driver skills for lane merging shall be tested as part of the licensing procedure.

Potential failure Mode F3.22: Driver fails to respond to LCW.

The driver may fail to respond to the warning due to the following:

(F3.22.1) Driver ignores warning unintentionally or becomes confused. (S=10, O=4)
(F3.22.2) Driver ignores warning intentionally due to high false alarm rate. (S=10, O=4)

If the driver ignores the warning when he/she should not, a collision with vehicles in other lanes may take place.

The design requirements and recommendations are:

(F3.22.1) The warnings must be very clear and unambiguous to the driver.

(F3.22.2) The false alarm rate must be very low. The warning signals must be easily distinguishable from each other. The warning threshold shall be adjustable by the driver. The driver interface shall appear simple to the driver.

Potential failure Mode F3.23: Driver fails to respond to traffic information

The driver may fail to respond to traffic information provided by the roadway due to the following:

(F3.23) Driver capability is impaired. (S=5, O=5)

The roadway may provide information about traffic ahead that may influence the decision of the driver to change lanes, exit etc. Failure to respond to the roadway information may affect roadway capacity and congestion control.

The design requirements and recommendations are:

(F3.23) The roadway traffic information shall be clear and brief.

Potential failure Mode F3.24.1: Vehicle doesn't initiate or respond to a check-out request.

The above failure mode may be due to any one of the following causes:

(F3.24.1.1) Controller failed to recognize check-out initiation input. (S=9, O=2)
(F3.24.1.2) Controller software failure. (S=9, O=2)
(F3.24.1.3) Warning delivery device failure. (S=7, O=2)

The effect of the above failures is that the vehicle will continue operating in the lane. For the first two failures, where the driver is aware of the failure, the effect is more severe since the driver may feel helpless, panic or try to interfere with the automated functions of the system.

The design requirements and recommendations are:

(F3.24.1.1) The system must be sufficiently reliable. Some redundancy to initiate check-out is needed.

(F3.24.1.2) The system must have supervisory elements in hardware and software. Once a failure is detected the system shall switch to a lower ERSC and warn the driver.

(F3.24.1.3) The warning device must be reliable. Redundant warning delivery methods must be used.

Potential failure Mode F3.24.2: Driver fails to pass check-out test.

The driver is given full authority of the vehicle functions provided he/she passes the check-out test. The driver may fail the check-out test due to:

(F3.24.2) Driver's failure in handling throttle, brake, and steering properly during check-out. (S=7, O=4)

The effect of the failure is that the vehicle will either continue operating or will guide itself to a special exit ramp or shoulder of the lane, stop and notify the roadway.

The design requirements and recommendations are:

(F3.24.2) The handling of the throttle, brake, and steering during check-out must be no more difficult than in normal manual driving.

Potential failure Mode F3.25.1: The driver can not exit the lane.

The driver may not be able to exit the lane due to:

(F3.25) Congestion in manual lane or the transition lane. (S=6, O=5)

The effect is that the vehicle will remain in the dedicated lane. If the vehicle is exiting due to malfunction of the automated functions, then the efficiency of the dedicated lane may be degraded.

The design requirements and recommendations are:

(F3.25) A dedicated transition lane or some form of regulation such as "yield to auto lane" must be implemented to ensure easy exit even when traffic congestion exists in the manual lane. Must warn the driver of congestion ahead of time via traffic information communication.

Potential failure Mode F3.26.1: Vehicle doesn't fall back to ERSC2 even when it is necessary

The system is designed to fall back to ERSC 2 when the lane keeping function is no longer considered to be reliable due to environmental and/or roadway conditions. Failure to do so may be due to:

(F3.26.1.1) Software failure. (S=10, O=2)

The effect of the failure is degradation of safety and the possibility of collision due to the degradation of the reliability of the lane keeping function.

The design requirements and recommendations are:

(F3.26.1) Reliable supervisory and diagnostics program must be implemented.

Potential failure Mode F3.26.2: Driver fails to assume role for ERSC 2

The driver may fail to take over steering and operate as in ERSC due to:

(F3.26.2.1) Warning delivery device failure. (S=10, O=2)
(F3.26.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The effect of the above failures is degradation of safety and the possibility of collision due to degradation of reliability of the lane keeping function which could be the main reason for falling back to ERSC 2.

The design requirements and recommendations are:

(F3.26.2.1) The warning device must be reliable. Redundant warning delivery methods must be used.

(F3.26.2.2) The warnings must be clear and distinguishable from each other.

Potential failure Mode F3.27.1: System does not fall back to ERSC1 when it should

The system may fail to revert to ERSC 1 when the RECA function is no longer reliable due to:

(F3.27.1) Software failure. (S=10, O=2)

The effect of this failure is the possibility of rear-end collision due to the loss of reliability of the RECA function that was the probable reason for reverting to ERSC 1.

The design requirements and recommendations are:

(F3.27.1) Reliable supervisory and diagnostic programs must be implemented for reliable transition to ERSC 1.

Potential failure Mode F3.27.2: Driver fails to assume roles for ERSC 1

When the system falls back to ERSC 1 the driver is warned to assume responsibility for rear-end collision avoidance. The driver may fail to do so due to:

(F3.27.2.1) Warning delivery device failure. (S=10, O=2)
(F3.27.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The effect of the failure is the possibility of rear-end collision since the RECA function is no longer operating and the driver is not aware of it.

The design requirements and recommendations are:

(F3.27.2.1) The warning device must be reliable. Redundant warning delivery methods must be used.

(F3.27.2.2) The warnings must be clear and distinguishable from each other.

Potential failure Mode F3.28.1: System does not fall back to manual control when it should.

The system is designed to fall back to manual control when certain basic functions fail to operate. Failure to do so may be due to:

(F3.28.1) Software failure. (S=10, O=2)

The effect of the failure could be catastrophic if the vehicle functions for lane keeping and/or RECA are no longer reliable and the system does not switch to manual mode.

The design requirements and recommendations are:

(F3.28.1) Reliable supervisory and diagnostics program must be implemented.

Potential failure Mode F3.28.2: Driver fails to assume full manual control.

The driver may fail to assume responsibilities for manual control due to:

(F3.28.2.1) Warning delivery device failure. (S=10, O=2)
(F3.28.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The effects are the same as those with failure mode F3.28.1.

The design requirements and recommendations are:

(F3.28.2.1) The warning device must be reliable. Redundant warning delivery methods must be used.

(F3.28.2.2) The warnings must be clear and distinguishable from each other.

The question whether a driver can switch from one mode of operation to another within a short time by following the warnings and instructions given by the system is a human factors issue that requires further research. Another issue is whether the driver can understand the different modes of operation and adjust to them fast enough.

Potential failure Mode F3.29: Fail to notify driver of correct mode of operation

The system is designed so that it notifies the driver of its mode of operation. For example, whether the SHM, RECA, LK, and LCW are on, off or there is a malfunction. Failure of the system to do so may be due to:

(F3.29) Electronics or software failure. (S=8, O=3)

Failure of the system to notify the driver of its correct mode of operation may lead to confusion. As a result the driver may decide to initiate a check-out procedure and exit the lane. The driver may also panic under some situations where the wrong mode is displayed and cause an accident.

The design requirements and recommendations are:

(F3.29) The electronics and software must be very reliable. Redundancies and on board diagnostics may be used to improve reliability.

The amount of information the driver should be given by the system is an issue that needs further research. The workload of the driver shall be low and manageable. Any information given to the driver shall be clear, brief and easy to process at all speeds and headways.

Vehicle, Driver Diagnostics and Maintenance

Vehicle diagnostics.

The FMEA for ERSC3 gives an extensive list of design requirements and recommendations that involve an extensive list of diagnostics for the fully and partially automated vehicle functions. The most crucial diagnostics are those related to the SHM, RECA and lane keeping functions that directly affect safety.

The on board diagnostics shall continuously monitor all functions and their redundancies during manual and automated mode. The monitoring of redundant paths can be made possible by having them activated either continuously or periodically. The diagnostics for the lane keeping function may pose a problem due to the reliance of the function on the lane reference aids. While the vehicle actuators and electronic components can be monitored the sensors that sense the location of the vehicle in the lane can only be checked in the presence of lane reference aids. This is an issue that needs to be addressed. A possible solution is to equip lanes leading to the AHS lane with lane reference aids that allow the on board vehicle diagnostics to test their sensors and equipment even during manual mode and before entering the AHS lane. Another possible solution is to perform the diagnostics at the entry point during the check-in procedure. The entry point could be a dedicated ramp equipped with lane reference aids.

As in ERSC1 and 2 the overall motion of the vehicle can be monitored by an executive controller with diagnostics using a validated vehicle model as shown in figure 8. This overall controller and diagnostics

structure adds an additional layer of safety by detecting and accommodating failures that cannot be easily detected at the local component level.

Driver Diagnostics.

In ERSC3 driving on the AHS lane is "feet-off", "hands-off". As a result the driver may fall asleep, read a paper and forget about upcoming driving tasks. Since the driver is responsible for lane changing and routing, a level of alertness is required in order to avoid missing the exit or to prepare for exiting by changing lanes. This level of alertness should be constant when the vehicle is in motion because the system is not aware of the destination of the vehicle and the intentions of the driver. How to keep the driver alert is an issue that needs to be resolved. A possible solution is to develop a method that monitors the driver status and keeps him/her alert all the time. Another solution is for the system to have a navigation capability. In this case the driver needs to be alerted only when a lane change or exiting maneuver needs to be performed.

In addition to the above the driver also needs to be alerted to initiate check-out during malfunctions, transition to a lower ERSC, etc. The most effective method for alerting the driver is an issue that needs further research. During check-out the driver is given partial authority for lane keeping and longitudinal control, his/her actions are monitored and the authority is increased depending on his/her performance. This is a direct method for assessing driver's readiness to resume manual control.

A driver's behavioral model and diagnostics may be used to assess the driver's ability to take over as shown in figure 9. The feasibility, effectiveness and technical details of the method need to be researched.

Maintenance

As in previous ERSCs the trend of low maintenance will call for reliable components with long mean time to failure and low maintenance needs. These requirements will increase the initial cost of the vehicle. The use of additional electronics is not expected to increase the frequency of maintenance. The recommended use of redundant steering mechanisms may affect maintainability depending whether the mechanism is electronic or mechanical and hydraulic.

Another maintenance requirement is that of the lane reference aids. The infrastructure should be responsible for maintaining them in order to support lane keeping under all environmental conditions. The maintenance cost will depend on the type of lane reference aids used. The choice of the lane reference aids should take into account the maintenance cost in addition to reliability and technical issues.

Retrofitting

Retrofitting vehicles for ERSC3 is going to be expensive and undesirable to users and automobile manufacturers. The upgrade of vehicles built for ERSC1, ERSC2, or ERSC3 is also going to be costly due to the different design requirements, redundancies, and hardware and software components. Table 5 summarizes the results of retrofitting for ERSC3.

Table 5: Retrofitting for ERSC 3.

Category of Vehicles	Technically Feasible	Cost	User Acceptance
Vehicles with no ERSC 1, 2, 3 capabilities	Yes	Very High	Unlikely
Vehicles with ERSC 1 capability	Yes	High	Unlikely
Vehicles with ERSC 2 capability	Yes	High	Unlikely
Vehicles built for easy retrofit	Yes	High	Unlikely
Vehicles built independent of ERSC3 but with same capabilities	Yes	Moderate to high depending on the extent of retrofitting	Questionable

Deployment Scenarios

ERSC3 can be considered as an evolution of ERSC2 where the lane keeping task is automated and a lateral collision avoidance warning is introduced. The deployment of ERSC3 as an intermediate stage of AHS raises several questions. The main question is whether it is possible from the reliability and human factors point of view to deploy a full authority longitudinal controller together with an automated lane keeping controller and rely on the driver for lateral collision avoidance. Even if the equipment is 100% reliable, situations can be found in ERSC3 where a rear-end collision cannot be avoided without steering. Since driving is "feet-off", "hands-off", we can not assume that the driver is always alert and capable of acting fast enough to avoid a collision using steering especially at short headways and high speeds. Furthermore, if we give the driver such an override capability over lane keeping, problems such as accidental disabling of lane keeping by the driver will raise other safety issues. For ERSC3 to be deployable certain major functional modifications need to be introduced in order to avoid putting the driver in unsafe situations. One possible modification is to introduce lateral collision avoidance in ERSC3. Another modification is to change the roadway and the operation of the AHS lane so that the probability of using steering for collision avoidance during the automated mode is reduced to almost zero. The study of such modifications is a topic for research. Another possible scenario that is worth studying is the introduction of lane keeping without a full-authority longitudinal control. The incentive for such a system could be safety.

Key Results and Conclusions

1. The calculation of the minimum safe headway in ERSC3 is more critical than in ERSC2. The reason is that the use of an incorrect headway may lead to a rear-end collision which can cause the lane keeping function to fail, the vehicle to go out of control and collide with vehicles in other lanes. The accurate evaluation of all factors that affect the minimum safe headway is an issue that needs to be carefully researched. Multiple methods that are not subject to common mode failures, errors and inaccuracies must be used to calculate the minimum safe headway. A level of conservatism must be used in choosing the headway. The roadway may have to play a more active role in informing vehicles of the road condition such as the range of friction coefficients between vehicle tires and the road, the presence of disabled and/or unfit vehicles in the lane ahead, etc. The roadway may also have to maintain the AHS lane in good condition.

2. The reliability requirements for the SHM and RECA functions are even higher in ERSC3 since failure of the functions to perform as designed may cause failure in the lane keeping function with catastrophic consequences. In this case the vehicle may depart the lane, go out of control and cause multiple collisions. The SHM and RECA should be in continuous interaction with the lane keeping function in order to coordinate speed around curves and maintain vehicle stability. The potential design of a full authority longitudinal controller as shown in figure 15 may be improved with the addition of another redundant control channel and diagnostics for interaction with the lane keeping function. The system shall be considered unfit to operate in the AHS lane if any one of the redundant control channels has failed. The technical details and diagnostics of these designs are topics that need to be researched. There is no doubt that the reliability requirements call for complex designs both in hardware and software that will increase the cost of the vehicle considerably. A design issue associated with the redundant control channels that needs further research is how to design the system to switch from a failed control channel to a healthy one without degrading the performance of the longitudinal controller.

3. A crucial issue and risk in ERSC3 is the effect a rear-end collision may have on lane keeping. It is unlikely that under a severe rear-end collision the lane keeping function will manage to keep the vehicle in the lane. Since driving is "feet-off," "hands-off" the driver is not expected to play any constructive role during emergencies. A rear-end collision may cause the vehicle to depart the lane, go out of control and collide with vehicles in adjacent lanes. The design of the lane keeping function so that it is robust with respect to disturbances that take place during a rear-end collision is an issue that needs further research. The risk is that it is unlikely for the lane keeping function not to be affected by a severe rear-end collision.

4. The failure of the lane keeping function to keep the vehicle in the center of the lane during a rather strong rear-end collision raises the question whether lane keeping and RECA can operate together without an automated lateral collision avoidance function.

5. In ERSC3 the driver cannot be responsible for lateral collision avoidance when the vehicle is in the automated mode. The reason is that driving is "feet-off," "hands-off" and therefore the driver may not be alert to respond fast enough to a lateral collision warning. The system cannot avoid collisions in the case where steering is required for collision avoidance. Such situations may appear in ERSC3. One particular example is when a preceding vehicle avoids collision with an obstacle or disabled vehicle in the lane by changing lanes leaving the following vehicle in a situation of a short headway where a rear-end collision cannot be avoided. A possible solution is to restrict lane changing to designated sections where headways are longer and develop a roadway to vehicle and vehicle to vehicle communication system that informs vehicles of expected maneuvers, presence of unfit vehicles and/or obstacles, etc. Another possible solution is to introduce an automated lateral collision avoidance function at ERSC3.

6. The driver cannot be a back-up to a lane keeping function. It takes a much shorter time than the human reaction time for the vehicle to depart the lane during a failure. A vehicle lane departure due to the failure of the lane keeping function could be catastrophic. The vehicle may go out of control and cause multiple collisions in adjacent lanes. The lane keeping function must be highly reliable. This high level of reliability calls for considerable redundancies in sensors, actuators, components and software that will increase the complexity and the cost of the vehicle. A potential design of a reliable lane keeping controller is shown in figure 20.

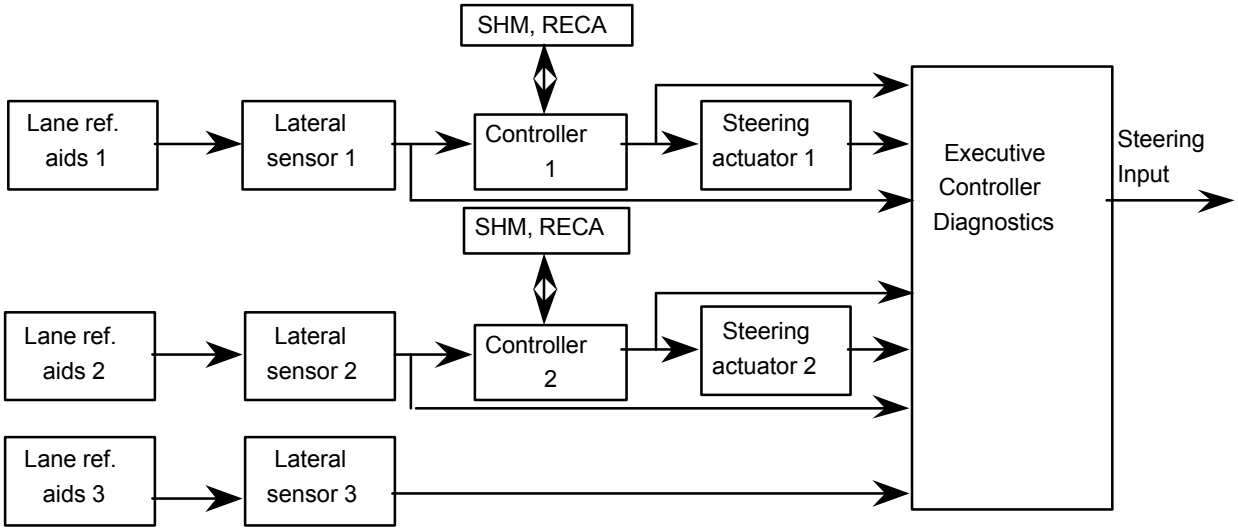

Figure 20: Block diagram of a potential lane keeping controller.

The figure shows two parallel control channels. These channels shall not be susceptible to common mode failures. The need for a third independent control channel is an issue that needs further study. The use of three different lateral sensors and lane keeping reference aids may be essential in deciding which of the three sensors give the correct measurements. An important technical issue that needs to be resolved is how to switch from a failed control channel to a healthy one without affecting the performance of the lane keeping function. The time constants involved are very short which gives a very limited time for detection and accommodation of failures. A special automatic control system may be designed to keep both channels active by weighting their outputs and allowing for automatic detection and accommodation of failures. The vehicle shall be considered unfit to operate in the AHS lane if any one of the redundant channels fails.

7. The driver shall not be allowed to override the lane keeping function while the vehicle is operating automatically in the longitudinal direction. The reason is that a sudden disabling of the lane keeping function may put the driver in a situation he/she cannot handle due to the short headway and high speed used and the short time constants involved in steering. The driver, however, shall be able to request the disabling of the lane keeping function. In such cases the disabling should be done by following a check-out procedure where the steering capabilities of the driver are assessed before a complete transition to manual control. In addition the headway and speed shall fall back to preset values that are comfortable for the driver before the driver takes over steering.

8. Despite the reported success of several lane keeping experiments today's sensor technology is not yet mature to meet the requirements for reliable lane keeping. Further research and experiments with different sensor technologies for lane keeping are essential.

9. The lateral collision warning (LCW) is designed to assist the driver during lane changing and merging. The most important issues associated with the LCW are the following:

(i) When and how to give the warning. The warning must be given before the driver starts changing lanes in order to give him/her enough time to react. If the LCW is on all the time, the driver may be receiving many unnecessary warnings due to the moving vehicles in neighboring lanes. If these warnings are audible the driver may be distracted, get annoyed and eventually switch the system off. A visual warning using a display may be less distractive in this situation. Human factors studies are essential in determining the most appropriate type of warning.

(ii) The ability of the system to identify threatening vehicles and calculate the TTC is a technical issue that needs to be studied. Due to the fast dynamics of steering any vehicle in the neighboring lane could be classified as threatening.

(iii) The sensor requirements for LCW is also a technical issue that needs further study. The sensor should cover more than 180 degree field of view, identify all moving objects, their closing rates and classify them as threatening or non-threatening. These requirements cannot be met with current sensor technology within the constraints of reasonable cost.

10. As in the previous ERSCs the fall back mode from one ERSC to a lower one is a human factors issue that needs to be studied. The principal question is whether the driver can understand the different modes of operation and adjust to them fast enough.

11. The system shall notify the driver of its main mode of operation. Such information assists the driver to understand what the system is doing. The issue here is how much information should be displayed to the driver without increasing his/her workload beyond manageable levels.

12. In ERSC3 the driver may be sleeping, reading a paper, etc. The system has to alert him/her in order to inform him/her of certain malfunctions or provide him/her with traffic information. The system, however, will not be able to alert the driver to change lanes for exiting at the end of the trip since it is not assumed to be equipped with a navigation system. This means that the driver should be continuously alert for route selection or the system should be equipped with navigation capability.

13. As in the previous ERSCs, retrofitting vehicles for ERSC3 is an expensive proposition. Upgrading vehicles for ERSC2 to ERSC3 is also going to be costly due to the extensive redundancies and different functions that are needed for ERSC3.

14. The low maintenance trend for current vehicles is expected to continue with vehicles equipped for ERSC 3.

15. For ERSC 3 to be deployable certain vehicle functions and the roadway functions and configuration need to be modified. The lack of a lateral collision avoidance function is the main deficiency of ERSC 3.

SECTION 5 ERSC 4 ANALYSIS

The analysis for ERSC 4 follows the same steps as in the previous ERSCs. We first specify the vehicle operation of ERSC 4 and the vehicle functions and interface with the driver and roadway as well as the functional requirements. We then perform a system level FMEA that provides us with a list of potential failure modes, their potential causes and effects and a list of design requirements and recommendations. The results of the FMEA are used to discuss reliability, redundancies, diagnostics, maintenance, retrofitting, and possible deployment scenarios. The section is concluded with a list of key findings and conclusions.

Vehicle and Interface with Roadway and Driver Functions

With the introduction of the lane changing capability in ERSC4 the vehicle becomes fully automated. Automatic lane changing allows the introduction of multiple dedicated automated lanes. The following

operational scenario is used to develop the vehicle functions and their interface with the roadway and driver.

Operational Scenario

The fitness of the vehicle to operate on AHS is displayed constantly through on board diagnostics when the vehicle is operating either manually or automatically. When the vehicle approaches the AHS facility it establishes communication with the roadway in order to verify its performance capabilities. The intentions of the driver to enter the AHS are communicated to the roadway together with the vehicle's fitness status and identification. If the vehicle is fit the driver is notified and instructed to drive the vehicle to the entry point or area and switch on the automated mode. The automated mode includes the SHM, LK, lane changing and collision avoidance functions, self-navigation and route selection and vehicle-to-vehicle and vehicle-to-roadway communication for maneuver coordination. The vehicle is therefore fully instrumented with full navigation capabilities that make it similar to an autonomous robot.

Once the automated mode is switched on, the vehicle uses its on-board sensors and functions to merge itself into the automated lanes. The roadway assists in merging by coordinating traffic via speed and headway control. The desired destination of the vehicle is indicated by the driver at check-in and can be changed by the driver during automated driving. The vehicle uses this information together with traffic flow information received from the roadway to navigate itself and reduce travel time. The navigation commands, such as lane changes check-out, exit, etc., are carried out by the automated lateral/longitudinal control functions of the vehicle. The lane changing is performed using the on-board sensors and actuators in order to avoid possible collisions with other vehicles. Vehicle-to-vehicle communication is used to coordinate the maneuvers of vehicles and assist lane changes by following certain "right of way" protocols.

Once the automated mode is switched-on the driver has no direct override capability. The driver, however, may initiate a check-out procedure that will allow him/her to regain manual control. The check-out procedure initiated by the driver involves the following functions:

The driver indicates his/her intention to exit AHS. The vehicle guides itself to a transition lane or special ramp and warns the driver to assume manual control. The driver's inputs i.e. steering, braking and throttle are monitored and corrected by the system in order to maintain vehicle stability and performance. If the performance of the driver is acceptable the system increases his/her level of authority until the transition to manual control is complete. If the driver's performance is not acceptable the level of authority given to the driver remains the same or is decreased and the driver is given another chance. If the driver fails the check-out test within the available time limits the vehicle guides itself to a special shoulder lane or area and stops. At the same time it notifies the roadway. The roadway is also notified when the check-out procedure completes successfully.

A check-out procedure at the end of the trip is initiated by the vehicle by first alerting the driver with a warning to assume manual control. The driver's inputs are monitored and augmented by the system and authority is gradually given to the driver depending on his/her performance as described above. If the driver cannot be alerted or fails the test for assuming manual control the vehicle guides itself to a special shoulder lane or ramp and stops.

The roadway provides target speed commands, headway recommendations and traffic information to vehicles. It coordinates merging and manages incidents.

The vehicles respond to target speed commands and headway recommendations the same way as in previous ERSCs.

The functional block diagram shown in figure 21 indicates the interaction of the vehicle's automated functions with the roadway, driver and other vehicles.

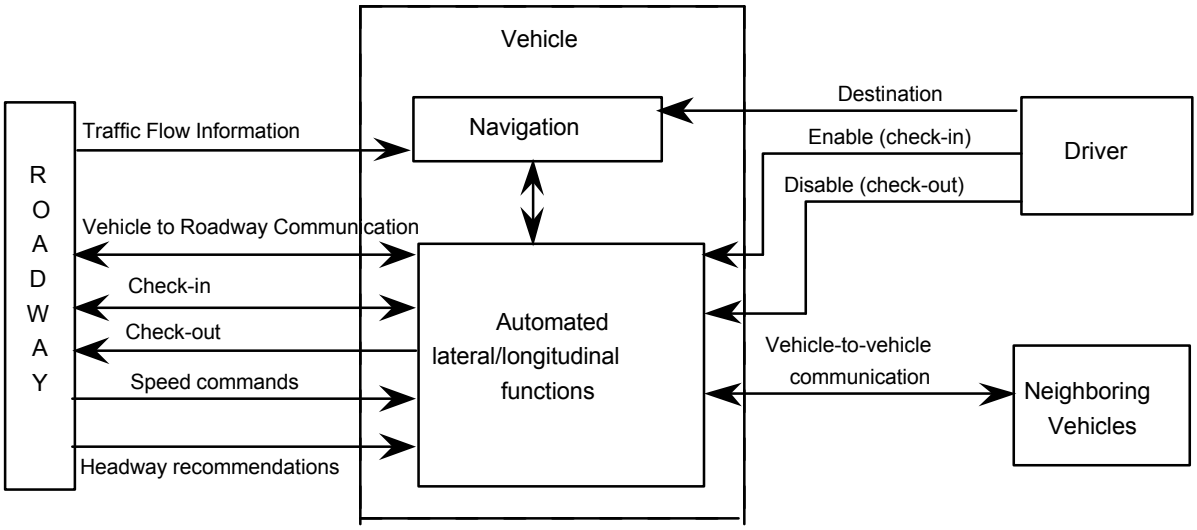

Figure 21: Functional block diagram of vehicle functions and interface with roadway, driver and neighboring vehicles.

The main high level functions associated with ERSC4 are:

H4.1 Navigation Functions
H4.2 Automated Lateral/Longitudinal Control
H4.3 Driver Vehicle Roadway Interface

The high-level function H4.2 include the SHM, lane keeping, lane changing, and collision avoidance, both in the lateral and longitudinal directions. Some of these functions are similar to those in the previous ERSCs. Since the operation of ERSC4 is different from the previous ones, the purpose of these functions and the way they interact with other functions are also different. As before we use the above high-level functions to generate the vehicle functions and sub-functions and their interaction with the driver, roadway and other vehicles for ERSC4.

H4.1 Navigation Functions

The functional block diagram of the navigation system is shown in figure 22.

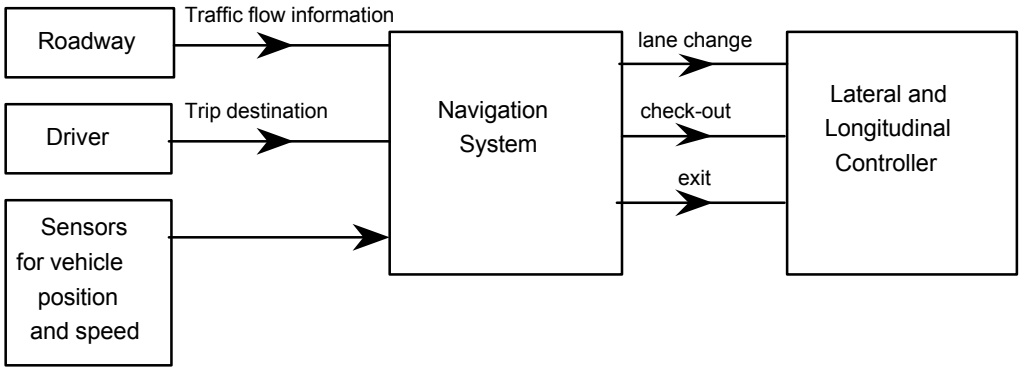

Figure 22: Functional block diagram of vehicle navigation system.

Inputs:
- Traffic flow information from roadway
- Trip destination
- Position and speed of vehicle

Outputs:
- Lane change commands
- Check-out and exit commands

Functional Specifications

The on-board navigation system computes the route for the vehicle by using real time traffic flow information in order to minimize travel time. It sends the appropriate commands such as lane change, check-out and exit to the automated lateral/longitudinal control system. The system accepts driver inputs for trip destination at check-in and at any time during traveling.

The main functions of the navigation system and the functional and reliability requirements are:

F4.1 Locate absolute position of vehicle
The system shall locate the position of the vehicle relative to the roadway at each time under all roadway and environmental conditions.

F4.2 Compute vehicle's route
The system shall use the trip destination indicated by the driver and the traffic flow information sent by the roadway to determine the optimum route for the vehicle.

F4.3 Generate commands for lateral/longitudinal control
The system shall use the selected route to issue navigational commands for the lateral/longitudinal controller. These commands include lane changing, check-out and exiting.

F4.4 Enable Navigation
Upon driver's command the navigation functions shall switch on during check-in.

F4.5 Disable Navigation
Upon driver's command the navigation functions switches off.

H4.2 Automated Lateral/Longitudinal Control

The functional block diagram of the automated lateral/longitudinal functions is shown in figure 23.

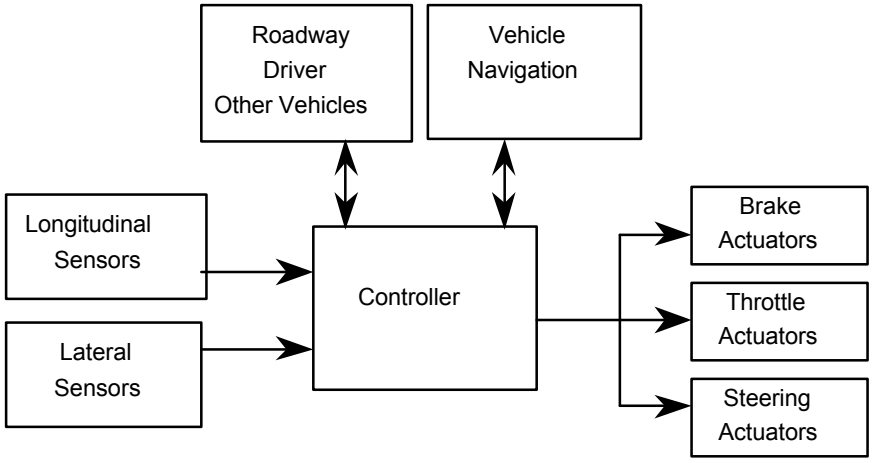

Figure 23: Functional block diagram of automated lateral/longitudinal control.

Inputs:

Longitudinal measurements: speed, relative speed and spacing, acceleration.
Lateral measurements: yaw rate, steering angle, preview, lateral acceleration.
Roadway commands: target speed, headway recommendations, merging coordination.
Navigation commands: lane change, check-out, exit.
Other vehicles: braking capabilities and intentions, lane change, and merging intentions.
Driver commands: enable at check-in, disable at check-out.

Outputs:

Commands to brake, throttle and steering actuators.
Notify driver and roadway of mode of operation.
Braking capabilities and intentions, lane change and merging intentions to other vehicles.

Functional Specifications:

The automated lateral/longitudinal control system includes the SHM, LK, lane changing functions and the combined lateral and longitudinal collision avoidance function. The system is responsible for the lateral and longitudinal motion of the vehicle and for avoiding collisions with all moving and stationary obstacles. It takes inputs from the vehicle navigation system for lane changing, check-out and exiting. It responds to target speed commands, roadway recommendations and merging coordination commands from the roadway. It communicates its braking capabilities and braking, lane changing and merging intentions to other neighboring vehicles and receives the corresponding information from the surrounding vehicles.

It responds to driver's inputs for switching on during check-in and switching off during check-out.

The main functions and functional and reliability requirements of the lateral and longitudinal control system are:

F4.6 Calculate safe headway

The system uses information from on-board sensors that sense vehicle's braking capabilities, the braking capabilities of the preceding vehicle obtained via communication and headway recommendations from the roadway to calculate a safe headway for vehicle following. The calculation of the safe headway shall take into account all factors and worst case stopping scenarios.

F4.7 Maintain speed

The vehicle shall track and maintain the roadway commanded speed as long as no valid target is present.

F4.8 Maintain headway

The vehicle shall maintain the headway selected by the vehicle under all environmental conditions, road geometry and freeway speeds.

F4.9 Switch from maintaining speed to maintaining headway

When the system senses a valid target in the same lane that is within certain range it shall switch to the following mode by maintaining a safe headway calculated by the vehicle.

F4.10 Switch from maintaining headway to maintaining cruise speed

When the target moves out of the sensing range or changes lane the system shall switch to maintaining roadway commanded speed.

F4.11 Keep vehicle in the center of lane

The system shall keep the vehicle in the center of the lane at all highway speeds, under all roadway and environmental conditions and during all modes of operation of the lateral and longitudinal controller.

F4.12 Coordinate lane change with other vehicles

The system shall coordinate a lane change maneuver with neighboring vehicles by communicating its identification, operational status and intention to change lane. The system shall also accept similar lane change information from other vehicles and assist them during lane changing by obeying the traffic rules and the established "right of way."

F4.13 Synchronize speed and headway for lane change

The system shall synchronize its speed and headway to be ready for a lane change maneuver or to assist other vehicles during lane change.

F4.14 Change lane

The system shall use its on-board sensors and controllers to change lanes after functions F4.12, F4.13 are completed.

F4.15 Switch from lane changing to longitudinal control

The system shall position the vehicle in the center of the lane after a lane change maneuver is completed and switch to the speed or headway maintenance, and lane keeping mode.

F4.16 Combined lateral and longitudinal collision avoidance.

The system shall avoid colliding with any moving or stationary obstacle by monitoring the motion of the vehicle relative to the surroundings and providing the appropriate commands to the steering, throttle and brake actuators. The system shall use on-board sensors and vehicle to vehicle communication to learn about the capabilities of the vehicles and their intentions for braking, lane changing. It shall calculate the TTC from all directions. If the TTC becomes less than a certain value then it shall send the appropriate commands to the brake, throttle and steering actuators.

F4.17 Switch from collision avoidance function to normal operation

A collision avoidance maneuver may bring the vehicle to a full stop or place it in a different lane or make it deviate from its normal operation. The purpose of this function is to bring the vehicle back to the speed or headway maintenance and lane keeping function by using its on-board sensors and vehicle-to-vehicle communications.

F4.18 Enable the lateral/longitudinal

Upon driver's command during check-in the lateral/longitudinal functions shall switch on.

F4.19 Disable the lateral/longitudinal functions

The lateral/longitudinal functions shall switch off after the driver has passed the check-out test and assumed full manual control.

H4.3 Driver Vehicle Roadway Interface

The high level functional block diagram of the driver interface with vehicle and roadway is shown in figure 24.

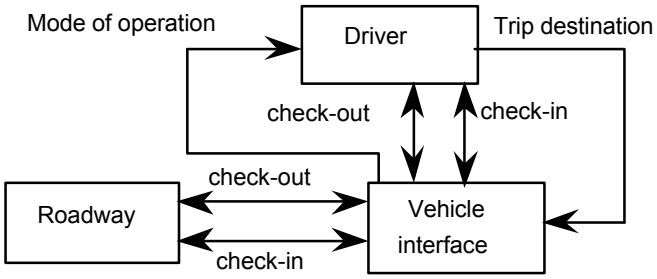

Figure 24: Functional block diagram of driver interface with vehicle and roadway.

The following functions are associated with the interface of the driver with the vehicle and roadway.

F4.20 Check-in

Driver shall use the on-board diagnostics to check the fitness of the vehicle to operate on the AHS facility. The vehicle shall establish communication with the roadway via vehicle-to-roadway communication and present its fitness status and identification to the roadway. If the vehicle is fit the roadway shall send an acknowledgment that the vehicle passed the check-in test and is ready to enter the AHS facility.

F4.21 Enter AHS

If the vehicle passes the check-in test the driver shall drive the vehicle to the entrance of the AHS facility, enter the trip destination and switch on the automated mode. The vehicle shall drive itself by using its on-board sensors and communications with the roadway and other vehicles.

F4.22 Merge into the automated lanes

The vehicle shall merge into the automated lane by communicating with other vehicles and the roadway in order to coordinate its maneuvers. Each maneuver shall be followed provided it is considered to be safe by the on-board sensors.

F4.23 Change of trip destination

The driver shall be able to change its trip destination while the vehicle is in the automated mode without interfering with the automated functions. The new trip destination input shall be fed into the navigation system that calculates the route of the vehicle based on the new destination.

F4.24 Alert driver for check-out

At the end of the trip the vehicle shall alert the driver to initiate a check-out procedure.

F4.25 Check-out

The driver shall initiate a check-out procedure after he/she has been alerted and warned by the system or after he/she has made a decision to abort the automated operation. The check-out procedure involves the gradual transition from the automated mode to the manual mode by transferring control to the driver depending on his/her driving performance. The check-out procedure starts by allowing the driver to provide small steering and throttle/brake inputs. These inputs are augmented by the system in order to maintain vehicle stability and performance. If the driver performance is acceptable he/she is given additional authority over steering, throttle and brake until the system switches to manual mode. If the driver fails the check-out procedure by not performing well enough or by not responding at all, then the vehicle guides itself to a special ramp or shoulder of a lane, brings itself to a full stop and notifies the roadway. The roadway is also notified when the check-out procedure starts and ends. The vehicle can also initiate a check-out procedure if the driver cannot be alerted by the system. In this case the vehicle guides itself to a special ramp or shoulder, stops and notifies the roadway. The check-out procedure may take place in a special transition lane or in a slow lane or special ramp.

F4.26 Exit lane

After passing the check-out test the driver assumes manual control of the vehicle and exits the AHS facility. The vehicle sends a notification to the roadway when the exit is completed.

F4.27 Fall back to ERSC 3

The vehicle functions shall switch to those of ERSC 3 when the lane changing function and/or the overall collision avoidance function become inaccurate or their redundant paths fail. The transition involves an initial warning to the driver and monitoring of his/her actions. If the driver is fit to operate as in ERSC 3 the system completes the transition. If not the system initiates a check-out procedure.

F4.28 Fall back to ERSC 2

The vehicle functions shall switch to those of ERSC 2 when the lane keeping function becomes inaccurate or when a redundant path fails. The transition involves an initial warning to the driver to assume the driving role required by ERSC 2 (i.e. steering). After the warning the system shall be monitoring the driver's performance. If the driver is alert, and his performance is acceptable then the transition is complete. If the driver cannot be alerted or he/she repeatedly fails the test the vehicle will be guided to a stop.

F4.29 Fall back to ERSC 1

The vehicle functions shall switch to those of ERSC 1 when the RECA function becomes inaccurate due to the inability of the system to assume responsibility for avoiding rear-end collisions. The transition involves an initial warning for the driver to assume the driving role required by ERSC1 (i.e. steering and collision avoidance). After the warning the system shall be monitoring the driver's performance. If the driver responds and his performance is acceptable, then the transition to ERSC 1 is complete. If the driver cannot be alerted or he/she repeatedly fails the test the system the vehicle will be guided to a stop.

F4.30 Fall back to manual control

When certain vehicle functions such as SHM are not functioning properly or the roadway and environmental conditions are inappropriate for automated operation the system shall switch to manual mode. The transition involves an initial warning for the driver to resume manual control of all vehicle functions. After the warning the system shall be monitoring the driver's performance. If the driver responds and his performance is acceptable, then the transition to manual mode is complete. If the driver cannot be alerted or he/she repeatedly fails the test the vehicle will be guided to a stop.

4.31 Mode of Operation

The system shall continuously notify the driver of its mode of operation i.e. on, off, normal, emergency, malfunction, etc.

Failure Modes and Effects Analysis

The FMEA tables for ERSC 4 are presented in table 15 of Appendix B. The results of the FMEA is a list of identified potential failure modes, their possible causes and effects, their severity (S) and occurrence (O) rating and a list of design requirements and recommendations. The design requirements and recommendations involve the need for redundancies, diagnostics, reliable sensors, actuators, electronics and software, and suggestions for modifying vehicle functions etc.

Below we present a list of the identified potential failure modes, and we discuss their potential causes and effects. We also present a list of design requirements and recommendations and discuss the issues and risks associated with ERSC 4.

H4.1 Navigation Functions

Potential Failure Mode F4.1: The on-board system cannot locate the correct absolute position of vehicle.

The navigation system of the vehicle relies on the measurement of the absolute position of the vehicle in the roadway. Failure to locate the current position of the vehicle at each time may be due to the following causes:

(F4.1.1) Absolute position sensor failure (detected) (S=5, O=4)
(F4.1.2) Absolute position sensor gives erroneous readings. (S=7, O=4)

The effect of the failure is that the navigation of the vehicle may be affected or lost leading to longer travel time and causing frustration to the driver. If the failure is detected the driver may be asked to take over navigation.

The design requirements and recommendations are:

(F4.1.1) Supervisory elements are needed to monitor the position sensor. Redundant methods shall be used to calculate the position of the vehicle. The driver shall be warned to take over navigation tasks when a failure is detected. The driver shall be able to provide navigation commands without interfering with the automated functions.

(F4.1.2) Supervisory elements are needed to monitor the reasonableness of the sensor measurements. Roadway to vehicle or vehicle to vehicle communication can help check the reasonableness of the sensor data by using other vehicles' positions.

Based on today's navigation devices [44,45] that are being developed independent of AHS the above design requirements can be met by using reference points on the roadway to obtain redundant measurements and improve accuracy. The loss of vehicle navigation capability is not considered to cause any safety hazards if all other vehicle functions are healthy.

Potential Failure Mode F4.2.1: The on-board system cannot compute vehicle's route.

The on-board system may fail to compute the route of the vehicle due to any one of the following causes:

(F4.2.1.1) Absolute position sensor failure (Detected) (S=5, O=4)
(F4.2.1.2) Traffic flow information is not available. (S=5, O=4)
(F4.2.1.3) Failure in software (S=5, O=2)

The effects of the above failures are not safety critical. They may lead to an increase in travel time, frustrate the driver and force him/her to take over navigation.

The design requirements and recommendations are:

(F4.2.1.1) Supervisory elements are needed to monitor the position sensor. In case of failure the driver shall be warned and be able to choose the route manually without interfering with the operation of the other automated functions.

(F4.2.1.2) Traffic flow information must be updated continuously. The vehicle shall be able to compute the vehicle's route in the absence of traffic flow information.

(F4.2.1.3) All the software units shall be carefully tested. Detection methods shall be used to detect failures and warn the driver to take over navigation.

Based on today's navigation devices and technology the above requirements can be met. The loss of vehicle navigation capability is not expected to cause any safety hazards.

Potential Failure Mode F4.2.2: Wrong route is computed.

The system may compute a wrong route for the vehicle due to the following causes:

(F4.2.2.1) Wrong absolute position is sensed. (S=5, O=4)
(F4.2.2.2) Failure in communication with roadway. (S=5, O=4)

The effect of the above failure is not safety critical. It may increase travel time, take the driver in the wrong destination or get the vehicle lost without been able to recover. It may frustrate the driver and eventually force him/her to take over navigation.

The design requirements and recommendations are:

(F4.2.2.1) The computed route shall be displayed to the driver .

(F4.2.2.2) The system shall be able to detect communication failures and warn the driver to take over navigation.

Potential Failure Mode F4.3: The navigation system does not generate correct commands for lateral and longitudinal control.

The navigation system may fail to generate correct commands for lane changing, check-out and exit due to the following causes:

(F4.3.1) Absolute position sensor fails or gives erroneous readings (S=5, O=4)
(F4.3.2) Navigation software failure (S=5, O=2)

The effect of the above failures is not safety critical. The travel time may increase or the vehicle may get lost, and force the driver to take over navigation.

The design requirements and recommendations are:

(F4.3.1) Supervisory elements are needed to monitor the position sensor. Redundant methods shall be used to calculate the position of the vehicle. The driver shall be warned of the failure and given the authority to take over navigation and generate the commands for lat./long. control.

(F4.3.2) All the software units shall be carefully tested. Detection methods shall be used to detect failures and warn the driver to take over navigation and generate the commands for the lat./long. control.

Potential Failure Mode F4.4: The system cannot enable navigation.

The navigation system may fail to switch on at check-in due to:

(F4.4) Electronic circuitry or software failure. (S=5, O=2)

The effect of this failure is not safety critical. The vehicle may not be allowed to operate on the AHS facility.

The design requirements and recommendations are:

(F4.4) Electronic circuitry and software shall be sufficiently reliable. The driver may have to ask for permission to operate on AHS without a navigation system.

Potential Failure Mode F4.5: The system cannot disable navigation.

The navigation system may fail to switch off due to:

(F4.5) Electronic circuitry failure (S=1, O=2)

This failure has no effect on safety. It may distract the driver if the navigation system continues to give commands and warnings to him/her that are no longer useful.

The design requirements and recommendations are:

(F4.5) The electronic circuitry shall be sufficiently reliable.

H4.2 Automated Lateral/Longitudinal Control

Potential Failure Mode F4.6: Loss of ability to calculate correct value of safe headway

As in ERSC 2 and 3 the system may fail to calculate the correct value of safe headway due to the following:

(F4.6.1) Detected malfunction or inability of the sensors to estimate the braking capabilities and intentions of the preceding vehicle. (S=6, O=6)
(F4.6.2) Detected malfunction or loss of communication with preceding vehicle (S=6, O=6)
(F4.6.3) Faulty or inaccurate measurements of braking capabilities of vehicle or preceding vehicle (S=10, O=6)
(F4.6.4) Incorrect braking capabilities and intentions from preceding vehicle are received through communication due to interference or noise corruption (S=10, O=6)
(F4.6.5) Loss of communication with roadway and/or lack of headway recommendation (S=6, O=4)
(F4.6.6) Loss of braking data information from preceding vehicle due to receiver malfunction. (S=9, O=4)

The effect of the early detected failures such as (F4.6.1), (F4.6.2), (F4.6.5) is degradation of efficiency due to the choice of a larger headway that accounts for the lack of information due to the failures. Undetected failures or failures detected late may lead to the calculation of a headway that is unsafe. Unsafe headways may be the cause of collisions.

The design requirements and recommendations are:

(F4.6.1) The malfunction of sensors or gross inaccuracies in the estimation of the braking capabilities must be detected early as possible. The system must fall back to some default headway that takes into account a worst case scenario of inaccuracy or malfunction of the sensors.

(F4.6.2) Diagnostics and built-in self tests must be used to guarantee a early detection of communication failures. When a malfunction occurs the headway must be automatically increased to some preset safe level that takes into account the failure.

(F4.6.3) The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements must be monitored and taken into account in the calculation of the safe headway.

(F4.6.4) The measurements of braking capabilities of all vehicles must be accurate. The system must check the reasonableness of preceding vehicle's braking capabilities and take into account possible inaccuracies and inconsistencies in calculating the safe headway.

(F4.6.5) The system must be able to accommodate the lack of headway recommendation from roadway.

(F4.6.6) The system must have supervisory elements and diagnostics that monitor the functionality of the receiver and detect malfunctions. The malfunction of the receiver must be taken into account in calculating the safe headway.

As in ERSC2 and 3 an accurate estimation and measurements of all factors that affect headway is an issue that requires further research. A conservative estimation of the safe headway will lead to large headways that will affect capacity. The criticality of the calculation of the correct safe headway is so high that multiple methods must be used to calculate and evaluate it. The roadway may have to play a more active role in informing vehicles of the of the expected friction coefficient, the presence of disabled and/or unfit vehicles in the lane ahead etc. Since the vehicle is equipped with a collision avoidance system, certain rear-end collisions can be avoided by steering therefore in certain cases an unsafe headway may not be as serious as in previous ERSCs without lateral collision avoidance.

Potential Failure Mode F4.7.1: Loss of speed maintenance function.

The SHM may lose its ability to maintain a constant roadway commanded speed if any one of the following components fail to perform as designed:

(F4.7.1.1) Speed sensor gives erroneous readings. (S=10, O=2)
(F4.7.1.2) Controller electronics or software failure. (S=9, O=2)
(F4.7.1.3) Throttle actuator failure. (S=10, O=3)
(F4.7.1.4) Brake actuator failure (brake cannot be applied or brake is continuously applied) (S=10, O=3)
(F4.7.1.5) Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication. (S=8, O=3)
(F4.7.1.6) Loss of target speed information due to receiver malfunction (S=8, O=3)

The potential effect of the above failures is the inability of the vehicle to obey the traffic rules for speed limits. Failures such as (F4.7.1.1), (F4.7.1.3, 4) may also imply that the collision avoidance function failed which means collisions cannot be avoided. Furthermore around curves the system may not be able to adjust speed which can lead to the vehicle going out of control and colliding with vehicles in other lanes.

The design requirements and recommendations are:

(F4.7.1.1) Diagnostics and built-in tests must perform a test for reasonableness on sensor data. Redundant speed sensors not subject to common mode failures must be used. When sensor malfunction is detected, the system shall switch to manual control by warning the driver and following the check-out procedure.

(F4.7.1.2) The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, the system shall switch to manual control by warning the driver and following the check-out procedure.

(F4.7.1.3) The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, the system shall switch to manual control by warning the driver and following the check-out procedure. Redundant throttle actuators not subject to common mode failures must be used with appropriate logic and diagnostics.

(F4.7.1.4) The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failures must be employed together with the appropriate logic and diagnostics that allow automatic switching from a failed actuator to a healthy one. When an actuator malfunction is detected, the system shall switch to manual control by warning the driver and following the check-out procedure

(F4.7.1.5) The system must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. The system must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). When a communication malfunction is detected the system shall fall back to a default lower speed if there is no valid target to follow.

(F4.7.1.6) The system must have supervisory elements in controller software and receiver to detect any receiver malfunction. The roadway must assist in testing receiver functionality. If the receiver has a malfunction the driver may be required to initiate a check-out procedure and exit the lane.

The most severe failures are those of the speed sensor, throttle and brake actuators. Such failures imply that the collision avoidance function may be ineffective and the adjustment of speed around curves may not be possible. The design requirements call for redundancies and extensive diagnostics both in hardware and software.

Potential Failure Mode F4.7.2: System switches to headway maintenance in the absence of valid target.

The possible cause of the above failure is due to:

(F4.7.2.1) Ranging sensor detects an invalid target within a certain range (S=9, O=6)

The potential effect of the failure is unnecessary acceleration, deceleration or activation of the collision avoidance function which may lead to degradation of riding comfort and efficiency.

The design requirements and recommendations are:

(F4.7.2.1) The system must be able to discriminate between valid and invalid targets.
As with ERSC2, 3 the design requirement will be easier to meet if two ranging sensors that are not subject to common mode failures are used together with the appropriate logic and diagnostics. The outputs of the two sensors should be continuously monitored and checked for reasonableness and consistency. A higher level controller should be used to decide which of the two outputs is the correct one when the two outputs are different. If the controller cannot decide, the system shall follow the output that indicates the closer target and shall switch to manual control by warning the driver and following a check-out procedure. The use of three ranging sensors that are based on different principles of operation and not subject to common mode failures may be a better way of improving the reliability of the ranging measurements. In this case the three outputs of the sensors are compared and the majority rule can be used to choose the output to be used for control purposes.

Potential Failure Mode F4.8: The system cannot maintain headway

The SHM may fail to maintain a desired headway selected by the system due to the following:

(F4.8.1) Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability. (S=10, O=6)
(F4.8.2) Sensor loses target due to road curvature or insufficient target reflectiveness. (S=10, O=7)
(F4.8.3) Ranging sensor has locked on an invalid target. (S=7, O=7)
(F4.8.4) Brake actuator failure. (Or intermittent failure to respond) (S=10, O=3)
(F4.8.5) Throttle actuator failure. (S=10, O=3)
(F4.8.6) Controller electronics or software failure. (S=10, O=2)
(F4.8.7) Ranging sensor gives erroneous readings. (S=10, O=4)

The most serious effect of the above failures is a rear-end collision. Failure of the ranging sensors and/or the brake, throttle actuator implies that the collision avoidance function is also ineffective and therefore a rear-end collision may be unavoidable. The most serious failure associated with the ranging sensor is the one where the sensor fails to detect an obstacle within the default headway or provides a larger range reading due to interference and/or malfunction. A rear-end collision may cause the vehicle to go out of control leading to multiple collisions.

The design requirements and recommendations are:

(F4.8.1) The system must be able to detect and accommodate an intermittent sensor failure. The system software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and switch to manual control by following a check-out procedure. Redundant ranging sensors, not subject to common mode failures, with appropriate logic must be used.

(F4.8.2) The ranging sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Vehicle shall slow down and switch to manual control when target is ambiguous and cannot be followed reliably. Sensor redundancies must be used to track targets around curves and minimize the possibility of interference.

(F4.8.3) The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. The system must distinguish vehicles moving to adjacent lanes and around curves in the same lane. Redundant ranging sensors not subject to same failure mode with appropriate logic must be used.

(F4.8.4) The system must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators that are not subject to common mode failures with appropriate logic must be used. When a redundant braking path fails the system shall initiate a check-out procedure.

(F4.8.5) The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. Redundant throttle actuators that are not subject to common mode failures must be used. When an actuator malfunction is detected, the system shall switch to manual control by warning the driver and following the check-out procedure.

(F4.8.6) The controller must have supervisory elements (in hardware and software) or adequate redundancies. The system shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.

(F4.8.7) The system must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. Redundant ranging sensors not subject to common mode failures must be

used. The system shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.

The above requirements call for significant redundancies for the ranging sensor, throttle, brake actuators controller electronics and software as well as diagnostics and supervisory elements. Failure of the throttle or brake actuator implies that the collision avoidance function is ineffective. A high level of reliability is therefore essential.

Potential Failure Mode F4.9: Failure to switch to maintaining headway even when a valid target exists.

The system is supposed to switch from maintaining cruise speed to maintaining headway when a target appears within a certain range. The system may fail to do so due to the following:

(F4.9.1) Ranging sensor fails to detect a valid target. (S=10, O=5)
(F4.9.2) Hardware or software failure of the SHM. (S=9, O=2)

The effect of failure (F4.9.1) is a possible rear-end collision that may cause the vehicle to depart the lane and go out of control. The effect of failure (F4.9.2) is less severe provided the collision avoidance is healthy. It may affect, however, efficiency and riding comfort.

The design requirements and recommendations are:

(F4.9.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics. In case of sensor failures the system shall switch to manual control by providing a warning to the driver, slowing down and following the check-out procedure.

(F4.9.2) The system must have supervisory elements (in hardware or software) or adequate redundancies. The system shall switch to manual control by warning the driver and following a check-out procedure in case of a detected failure.

Potential Failure Mode F4.10: Failure to switch to speed maintenance mode when the original target moves out of the lane and becomes unsuitable to follow, and no other valid target exists.

When the target moves out of the sensing range or changes lane from the sensing range the system is suppose to switch to the speed maintenance mode by maintaining the roadway command speed. The system may fail to switch due to the following:

(F4.10.1) Ranging sensor locks on the original target or locks on another target which is invalid when the original target becomes unsuitable to follow. (S=8, O=6)
(F4.10.2) Hardware or software failure of the SHM (S=8, O=2)

The effect of the above failures is unnecessary acceleration, deceleration or activation of the collision avoidance function that may lead to degradation of riding comfort and efficiency.

The design requirements and recommendations are:

(F4.10.1) The system must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics.

(F4.10.2) The system must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. The system shall switch to manual mode by warning the driver and following a check-out procedure in case of detected failures.

Potential Failure Mode F4.11: Loss of lane keeping capability

The lane keeping function may fail to perform as designed due to the following:

(F4.11.1) Failure to detect vehicle's lateral position due to malfunction of sensor or roadway lane reference aid. (S=10, O=5)
(F4.11.2) Lane preview information is not available. (S=8, O=3)
(F4.11.3) Control software or electronics failure. (s=10, O=2)
(F4.11.4) Steering actuator failure. (S=10, O=3)

The effect of the above failures is catastrophic with the exception of (F4.11.2) where the vehicle may be able to accommodate the failure by slowing down and switching to a lower ERSC since the detection of the failure is possible. Loss of the lane keeping capability may automatically cause the vehicle to depart the lane and go out of control especially in the case of failure (F4.11.4). The collision avoidance function may be activated but its effectiveness is questionable. In the case of the steering actuator failure, braking alone may not be sufficient to control the vehicle and bring it to a full stop without collision. The reason is that the failure of the steering function may leave very little time for detection and decision making. Application of the brakes when the steering function fails may cause the vehicle to spin or overturn with catastrophic consequences.

The design requirements and recommendations are:

(F4.11.1) The system must have redundant measurements of the lateral position of the vehicle. Redundant sensors and reference aids may be required with the appropriate diagnostics and logic. When a redundant component fails the system shall switch to manual control or lower ERSC and warn the driver.

(F4.11.2) The system must have redundant means of obtaining preview information. In the absence of preview information the system shall switch to a lower ERSC and warn the driver.

(F4.11.3) All electronic components and software must have redundancies and appropriate diagnostics to detect failures. When a failure of a redundant component is detected the system shall switch to a lower ERSC and warn the driver. Detection and accommodation of failures shall be fast and shall not affect the performance of the lane keeping function

(F4.11.4) Redundant steering actuators and associated components with the appropriate diagnostics and logic must be used. When a redundant component fails the system shall warn the driver to assume manual control of the steering function by following a check-out procedure.

Potential Failure Mode F4.12: Loss of coordination of lane changing with other vehicles.

The system may fail to coordinate lane changing with other vehicles due to:

(F4.12.1) Loss of vehicle to vehicle communication (S=9, O=3)
(F4.12.2) Coordination software failure (S=9, O=2)

The effect of the above failure is unnecessary disturbance in the traffic flow and degradation of efficiency. The collision avoidance function may be activated. Collision is possible if the vehicle tries to change lanes without coordination with other vehicles.

The design requirements and recommendations are:

(F4.12.1) Vehicles shall have supervisory programs to check communications. If a failure takes place either in transmitting or receiving signals, the vehicle shall be advised to check out. Roadway may be used as a backup for coordination

(F4.12.2) The system software must be tested thoroughly for all possible situations before implemented. Some redundancies in software may be necessary i.e., similar algorithms are implemented using different software tools.

Potential Failure Mode F4.13: The system cannot synchronize vehicle speed and headway during lane change.

The potential causes are:

(F4.13.1) Failure in getting position and/or velocity of vehicles in adjacent lane. (S=10, O=4)
(F4.13.2) Control software or electronics failure. (S=10, O=2)
(F4.13.3) Throttle actuator or brake actuator failure. (S=10, O=4)

The possible effect of the above failures is that the lane change may not take place. Another possible effect is that the lane change is attempted causing activation of the collision avoidance function that may fail to avoid certain collisions.

The design requirements and recommendations are:

(F4.13.1) The system shall have the capability to sense the position and velocity of multiple vehicles both in front and in adjacent lanes. Supervisory elements and adequate redundancies are needed. The system shall fall back to lower ERSCs when malfunction is detected.

(F4.13.2) The system shall have supervisory elements and adequate redundancies. The system shall warn the driver to check out when malfunction is detected.

(F4.13.3) Sensors and diagnostic programs are needed to monitor throttle and brake actuator actions. Redundant actuators must be used. Driver shall be warned to check out when failure is detected.

Potential Failure Mode F4.14: Loss of lane change function

The possible causes of this failure are:

(F4.14.1) Lateral sensor failure (S=10, O=4)
(F4.14.2) Control software or electronics failure (S=10, O=2)
(F4.14.3) Steering actuator failure (S=10, O=3)

The effect of the first two failures (F4.14.1), (F4.14.2) is that the lane change may be aborted if failures are detected early. If failures are not detected early a lane change may be attempted, the collision avoidance function may be activated and collision may take place. Failure of the steering actuator could be catastrophic due to the high bandwidth of the steering subsystem and the fact that without steering the collision avoidance function may be ineffective.

The design requirements and recommendations are:

(F4.14.1) Redundant lateral sensors must be used. Diagnostics shall be used to detect failures before the initiation of a lane change.

(F4.14.2) The system shall have supervisory programs (in hardware and software) and adequate redundancies. Diagnostics shall be used to detect failures before the initiation of a lane change.

(F4.14.3) Redundant steering actuators are required. Sensors and diagnostic program are needed to monitor steering actuator actions. Switching from one redundant path to another shall not affect steering performance. If a redundant path fails a check out procedure shall be initiated.

Potential Failure Mode F4.15: Vehicle fails to resume lane keeping and longitudinal control after moving to the new lane.

The potential causes of this failure are:

(F4.15.1) The lateral position sensor gives erroneous readings (the vehicle does not know it has reached the desired lane). (S=10, O=3)
(F4.15.2) Control software failure. (S=10, O=2)
(F4.15.3) The SHM function fails. (S=10, O=5)

The effect of the above failures is a possible disturbance of the traffic flow and activation of the collision avoidance function bringing the vehicle to a full stop. Collision with other vehicles is possible.

The design requirements and recommendations are:

(F4.15.1) Supervisory elements and adequate redundancies are needed for the lateral sensor measurements. When failure is detected the vehicle shall stop and warn the driver to assume manual control and exit AHS.

(F4.15.2) Supervisory programs shall be used. All control software units must be tested for full range of inputs before implemented. When failure is detected the vehicle shall stop and warn the driver to take over control and exit AHS.

(F4.15.3) The system shall have supervisory and redundant elements that detect and accommodate SHM function failures. In case of failure the vehicle shall stop, warn the driver to take over control and exit AHS.

Potential Failure Mode F4.16: Loss of combined lateral and longitudinal collision avoidance

The loss of the collision avoidance function may be due to the following failures:

(F4.16.1) Loss of communication with surrounding vehicles (S=10, O=3)
(F4.16.2) On-board sensors fail to detect surrounding vehicles' positions speeds and intentions. (S=10, O=4)
(F4.16.3) Control software or electronics failure (S=10, O=2)
(F4.16.4) Brake or throttle or steering actuator failure (S=10, O=4)
(F4.16.5) The calculation time to collision is incorrect (S=10, O=7)

The potential effect of the above failures is catastrophic. Multiple collisions may take place if the collision avoidance function fails to perform as designed.

The design requirements and recommendations are:

(F4.16.1) Supervisory elements are needed to monitor communications. Driver shall be warned to check out when communication capability is lost.

(F4.16.2) Redundant lateral and longitudinal sensors are needed. The system shall continuously monitor the reasonableness of sensor data. The driver shall be warned to check out when a redundant path fails.

(F4.16.3) System supervisory elements both in software and hardware must be used. All software shall be tested for full range of inputs.

(F4.16.4) Sensors and diagnostic program are needed to monitor actuator response. Redundant brake, throttle and steering actuators are needed.

(F4.16.5) All factors affecting the calculation of TTC as well as the discrepancies involved in evaluating these factors shall be taken into account. Redundant methods shall be used to calculate TTC.

Potential Failure Mode F4.17: The system cannot go back to normal operation after the activation of the collision avoidance function.

The potential cause of this failure is:

(F4.17) Control software failure in switching logic (S=8, O=2)

The effect of this failure is that the vehicle may come to a full stop unnecessarily and traffic may be disturbed. The driver may have to intervene and take over control of the vehicle.

The design requirements and recommendations are:

(F4.17) The control software must be reliable. It shall be tested under all possible conditions before implemented. Redundant software tools must be used.

Potential Failure Mode F4.18: The automatic lateral/longitudinal control functions cannot be enabled.

The potential cause of the above failure is:

(F4.18) Electronic circuitry failure (S=6, O=2)

The above failure may cause the vehicle to fail the check-in test or the driver may have to drive the vehicle manually out of the entry area of the AHS.

The design requirements and recommendations are:

(F4.18) The electronic circuitry must be sufficiently reliable. The driver shall be notified about the vehicle's operating mode.

Potential Failure Mode F4.19: The automatic lateral/longitudinal control functions cannot be disabled.

The system may fail to disable the lateral/longitudinal functions due to anyone of the following:

(F4.19.1) Electronic circuitry failure (S=8, O=2)
(F4.19.2) Driver does not handle throttle, brake, and steering properly and fails to pass the check-out test. (S=6, O=4)

The effect of the above failures is that the system may not be able to transfer control to the driver and stay in the auto lane until it reaches its destination or it runs out of gas.

The design requirements and recommendations are:

(F4.19.1) The electronic circuitry must be sufficiently reliable. Some redundancy is needed.

(F4.19.2) The handling of the throttle, brake, and steering during check-out shall be no more difficult than in normal driving. Supervisory elements are needed to monitor driver operation.

H4.3 Driver Vehicle Roadway Interface

Potential Failure Mode F4.20: Failure of check-in function.

The check-in function may fail to perform as designed due to the following:

(F4.20.1) On-board diagnostics fail to detect a fault in major functions of the vehicle. (S=9, O=3)
(F4.20.2) Roadway failed to detect that vehicle is not fit for AHS. (S=9, O=3)
(F4.20.3) On-board diagnostics make a wrong decision about a component or function that was not at fault. (S=6, O=2)

The effect of the first two failures is that the vehicle may enter and operate in the auto lanes without being fit. The last failure will stop the vehicle from entering the dedicated lane even though it is fit. The severity of the first two failures is fairly high . It will affect safety and efficiency especially if the vehicle stays in the lane for long time.

The design requirements and recommendations are:

(F4.20.1) The diagnostic algorithms shall be robust and highly reliable. The roadway shall be able to detect an unfit vehicle operating in the auto-lane.

(F4.20.2) The roadway shall be able to identify unfit vehicles at check-in.

(F4.20.3) The diagnostic algorithms shall be highly reliable. The system shall repeat the diagnostic checking if the vehicle is rejected.

Potential Failure Mode F4.21: The vehicle cannot enter AHS.

The potential cause of the failure is the following:

(F4.21.1) There is not enough gap at the entry point or entry area. (S=4, O=2)

The effect of the failure is that the driver has to drive the vehicle away from the area.

The design requirements and recommendations are:

(F4.21.1) The entry area to AHS shall have enough space to accommodate the vehicles. Vehicles shall be notified in advance of the availability of space.

Potential Failure Mode F4.22: The vehicle cannot merge into the auto lane.

The vehicle may fail to merge into the automated lanes due to the following:

(F4.22.1) Roadway fails to coordinate a gap. (S=4, O=4)
(F4.22.2) On board sensors give incorrect measurements. (S=4, O=6)

The effect of the failure is a possible delay of the vehicle at the entry area causing frustration to the driver.

The design requirements and recommendations are:

(F4.22.1) The roadway shall have redundant algorithms and back-up modes for coordination of vehicle speeds and headway.

(F4.22.2) Check-in tests shall be able to test correctness and functionality of on-board sensors.

Potential Failure Mode F4.23.1: Driver inputs wrong destination to the navigation system.

This failure may be due to:

(F4.23.1) Driver error (S=5, O=4)

The effect is that the driver may not get to the desired destination. Travel time may be increased.

The design requirements and recommendations are:

(F4.23.1) The destination and the computed route shall be displayed to the driver. Driver's attention shall be called whenever a new route is calculated.

Potential Failure Mode F4.23.2: Driver cannot change the trip destination.

The driver may not be able to change the trip destination due to:

(F4.23.2) Input device failure. (S=5, O=2)

The potential effect of this failure is that the navigation system cannot be used and the driver may be required to take over navigation or check-out.

The design requirement is:

(F4.23.2) The input device shall be sufficiently reliable.

Potential Failure Mode F4.24: System does not alert driver to check out when necessary.

The system may fail to alert the driver for check-out due to:

(F4.24) Software failure (S=10, O=2)
(F4.24) Warning delivery device failure (S=10, O=3)

Due to the above failures the vehicle may stay under automatic control and miss the destination exit. If the reason for check-out is malfunction collision may be possible.

The design requirements and recommendations are:

(F4.24.1) The system shall have reliable diagnostic algorithms.

(F4.24.2) Adequate redundant warning delivery devices are needed.

Potential Failure Mode F4.25.1: Vehicle does not initiate or respond to a check out request.

The above failure mode may be due to any one of the following causes:

(F4.25.1.1) Controller failed to recognize check-out initiation input. (S=7, O=2)
(F4.25.1.2) Controller software failure. (S=7, O=2)
(F4.25.1.3) Warning delivery device failure. (S=6, O=2)

The effect of the above failures is that the vehicle will continue operating in the auto lane. For the first two failures where the driver is aware of the failure the effect is more severe since the driver may feel helpless, panic or try to interfere with the automated functions of the system.

The design requirements and recommendations are:

(F4.25.1.1) The system shall be sufficiently reliable. Some redundancy to initiate check-out is needed

(F4.25.1.2) The system shall have supervisory elements in software. Once a failure is detected the vehicle shall automatically slow down and stop, and warn the driver to take over.

(F4.25.1.3) Warning device shall be reliable. Redundant warning delivery methods shall be used.

Potential Failure Mode F4.25.2: Driver fails to pass check-out test.

The driver is given full authority of the vehicle functions provided he/she passes the check-out test. The driver may fail the test due to:

(F4.25.2) Driver's failure in handling throttle, brake, and steering properly during check-out. (S=7, O=6)

The effect of the failure is that the vehicle will either continue operating or will guide itself to a special exit ramp or shoulder of the lane, stop and notify the roadway.

The design requirements and recommendations are:

(F4.25.2) The system shall employ driver status diagnostics. Supervisory programs are needed to monitor driver's response. The handling of throttle, brake, and steering during check-out shall be no more difficult than in normal manual driving.

Potential Failure Mode F4.26: Driver cannot drive the vehicle to the exit of the auto lane.

The driver may not be able to exit the auto lane due to:

(F4.26) Not enough gap in manual lane. (S=7, O=6)

The effect is that the vehicle will remain in the auto lane. If the vehicle is exiting due to malfunction of the automated functions, then the efficiency and safety of the system may be degraded.

The design requirements and recommendations are:

(F4.26) A dedicated transition lane or some form of regulation such as "yield to auto lane" shall be implemented to ensure easy exit even when traffic congestion exists in the manual lane. The system and driver shall be warned of congestion ahead of time via traffic information communication.

Potential Failure Mode F4.27.1: The system does not fall back to ERSC3 even when it is necessary.

The system is designed to fall back to ERSC 3 when the automatic lane changing function or lateral collision avoidance is no longer reliable. Failure of the system to fall back to ERSC 3 may be due to:

(F4.27.1) Software failure (S=10, O=2)

The failure may cause the system to operate as in ERSC 4 even though it should not. The operation may therefore be unreliable leading to possible collisions.

The design requirement is:

(F4.27.1) Reliable supervisory and diagnostics program shall be implemented.

Potential Failure Mode F4.27.2: Driver fails to assume responsibility for lane changing and navigation when lane change function or overall collision avoidance function become inaccurate or their redundant paths fail.

The possible causes are:

(F4.27.2.1) Warning delivery device failure. (S=10, O=2)
(F4.27.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The failure may cause the system to operate as in ERSC 4 even though it should not. The operation may therefore be unreliable leading to possible collisions.

The design requirements and recommendations are:

(F4.27.2.1) The warning device shall be reliable. Redundant warning delivery methods shall be used.

(F4.27.2.2) The warnings shall be clear and distinguishable from each other. The warning shall be very effective in exercising driver's attention.

Potential Failure Mode F4.28.1: The system does not fall back to ERSC2 even when it is necessary.

The system is designed to fall back to ERSC 2 when the lane keeping function is no longer considered to be reliable due to environmental and/or roadway conditions. Failure to do so may be due to:

(F4.28.1) Software failure (S=10, O=2)

The effect of the failure is degradation of safety and the possibility of collision due to the degradation of the reliability of the lane keeping function.

The design requirements and recommendations are:

(F4.28.1) Reliable supervisory and diagnostics program shall be implemented.

Potential Failure Mode F4.28.2: Driver fails to assume roles for ERSC 2

The driver may fail to take over steering and operate as in ERSC 2 due to:

(F4.28.2.1) Warning delivery device failure (S=10, O=2)
(F4.28.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The effect of the above failures is degradation of safety and the possibility of collision due to the degradation of the reliability of the lane keeping function which could be the main reason for falling back to ERSC 2.

The design requirements and recommendations are:

(F4.28.2.1) The warning device shall be reliable. Redundant warning delivery methods shall be used.

(F4.28.2.2) The warnings shall be clear and distinguishable from each other. The warning shall be very effective in exercising driver's attention.

Potential Failure Mode F4.29.1: The system does not fall back to ERSC1 even when it is necessary.

The system may fail to revert to ERSC 1 when the RECA function is no longer reliable due to:

(F4.29.1) Software failure (S=10, O=2)

The effect of this failure is the possibility of rear-end collision due to the low reliability of the RECA function that was the main possible reason for reverting to ERSC 1.

The design requirements and recommendations are:

(F4.29.1) Reliable supervisory and diagnostics program shall be implemented.

Potential Failure Mode F4.29.2: The driver fails to assume roles for ERSC1.

When the system falls back to ERSC 1 the driver is warned to assume responsibility for rear-end collision avoidance. The driver may fail to do so due to:

(F4.29.2.1) Warning delivery device failure (S=10, O=2)
(F4.29.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The effect of the failure is the possibility of rear-end collision since the RECA function is no longer operating and the driver is not aware of it.

The design requirements and recommendations are:

(F4.29.2.1) The warning device shall be reliable. Redundant warning delivery methods shall be used.

(F4.29.2.2) The warnings shall be clear and distinguishable from each other. The warning shall be very effective in exercising driver's attention.

Potential Failure Mode F4.30.1: System does not fall back to manual even when it is necessary.

The system is designed to fall back to manual control when certain basic functions fail to operate. Failure to do so may be due to:

(F4.30.1) Software failure (S=10, O=2)

The effect of the failure could be catastrophic if the vehicle functions for lane keeping and/or RECA are no longer reliable and the system does not switch to manual mode.

The design requirements and recommendations are:

(F4.30.1) Reliable supervisory and diagnostics program shall be implemented.

Potential Failure Mode F4.30.2: Driver fails to assume roles for manual control.

The driver may fail to assume responsibilities for manual control due to:

(F4.30.2.1) Warning delivery device failure (S=10, O=2)
(F4.30.2.2) Driver ignores the warning unintentionally or becomes confused. (S=10, O=5)

The effects and design requirements and recommendations are the same as with failure mode F4.30.1.

The question whether a driver can switch from one mode of operation to another within a short time by following the warnings and instructions given by the system is a human factors issue that requires further research. Another issue is whether the driver can understand the different modes of operation and adjust to them fast enough.

Potential Failure Mode F4.31: Failure to notify driver of correct mode of operation.

The potential cause of the failure is:

(F4.31) Electronics or software failure. (S=9, O=2)

Failure of the system to notify the driver of its correct mode of operation may lead to confusion. As a result the driver may decide to initiate a check-out procedure and exit the lane. The driver may also panic under some situations where the wrong mode is displayed and cause an accident.

The design requirements and recommendations are:

(F4.31) The electronics and software must be very reliable. Redundancies and on board diagnostics may be used to improve reliability.

The amount of information given to the driver by the system is an issue that needs further research. The workload of the driver should be low and manageable. Any information given to the driver should be clear, brief and easy to process at all speeds and headways.[46]

Vehicle, Driver Diagnostics and Maintenance

Vehicle Diagnostics

The FMEA gives an extensive list of diagnostics for all automated functions of the vehicle. Every single function that affects the motion of the vehicle has to be protected with redundancies and/or extensive diagnostics. The complexity of the vehicle of ERSC4 in terms of hardware and software is very high.

The monitoring of redundancies is also essential since for safety reasons the failure of the most important redundant paths shall signal the initiation of check-out and eventual exit of the vehicle from AHS. This implies that the redundant paths may need to be activated continuously or occasionally for monitoring purposes. The roadway and all vehicles must assist each other in monitoring their functions and components such as lane reference aids, communications, software etc. This close interdependence

implies that common standards need to be established and vehicle functions and performance while on AHS must be as similar as possible.

As in the previous ERSCs the overall motion of the vehicle can be monitored by an executive controller using a validated vehicle model as shown in figure 8. This overall executive controller and diagnostics structure adds an additional layer of safety by detecting and accommodating failures that cannot be easily detected at the local component level. If vehicles have similar performance their models of motion are similar and therefore their behavior is predictable if their inputs and intentions are communicated among vehicles. Other vehicles models may be used for a second level of diagnostics and monitoring.

The design of diagnostics and the use of vehicle models for diagnostic purposes are all technical issues that depend on the specific system design and need to be researched.

Driver Diagnostics

Since driving is fully automated the driver may be sleeping, reading a paper etc. The system has to alert the driver for check-out and when it is time for transition to a lower ERSC or manual mode. Once the driver is alert the system has to determine whether the driver is fit to assume manual control of all or certain vehicle functions. The best method for alerting the driver and the best method for assessing his/her fitness are human factors issues that need to be addressed.

In our approach we concluded that a feasible method for assessing the fitness of the driver is to have him/her perform certain driving tasks under the supervision of the system and gradually increase the driver's authority over these driving tasks depending on his/her performance. Such a method calls for special hardware and software designs and driver's models and its practicality and effectiveness requires further research.

Maintenance

As in the previous ERSCs the trend of low maintenance will apply to vehicles for ERSC4 too. Reliable components and software with long mean time to failure and extensive diagnostics which can detect the need for maintenance are essential. These requirements will increase the initial cost of the vehicle considerably. The use of extensive electronic components and the replacement of mechanical and hydraulic components with electronic ones will keep maintenance needs very low.

The maintenance of the roadway such as lane reference aids, communications etc. which is the responsibility of the infrastructure is also essential and will be costly especially at places where environmental conditions are not favorable.

Retrofitting

Retrofitting vehicles for ERSC4 is going to be expensive and undesirable to the users and automobile manufacturers. The design and reliability requirements for ERSC4 are unique and upgrading vehicles build for lower ERSCs is also going to be costly.

The following table summarizes the results for retrofitting.

Table 6 Retrofitting for ERSC4

Category of Vehicles	Technically Feasible	Cost	User Acceptance
Vehicles with no ERSC 1, 2, 3 capabilities	Yes	Very High	Unlikely
Vehicles with ERSC 1, 2, 3 capabilities	Yes	High	Unlikely
Vehicles built for easy retrofit	Yes	High	Unlikely
Vehicles built independent of ERSC4 but with some capabilities	Yes	High	Unlikely

Deployment Scenarios

In ERSC4 the vehicle is fully automated and self guided and behaves as a fast moving robot. It does receive assistance from the roadway and other vehicles for performing certain maneuvers but it relies on its on-board sensors for any movement it makes.

The deployment of fully automated vehicles poses a lot of problems that need to be resolved. These problems are technical, legal, social and economic. In this study we have concentrated on the technical problems. Our analysis calls for extensive redundancies, diagnostics and sensors that can see and process much more information than a human can and much faster. It is unlikely to meet these strict requirements with today's technology or with the near future technology and still come up with vehicles and a roadway system where the trade-off between benefits and cost is reasonable. The sensor and processing requirements are enormous and unique. It is very difficult to emulate the senses of a good driver, especially his decision making in unpredictable situations. Whether ERSC4 will evolve from the previous ones is an issue that needs further study. There is no doubt that the deployment of any fully or partially automated function will help study and understand the technical, legal, social and economic issues involved and help the evolution process towards a fully automated vehicle and roadway system. The design and development of ERSC4, however, may not follow by upgrading the vehicles for ERSC3 due to the difference in performance and reliability requirements.

Key Results and Conclusions

1. The issues involved in ERSC4 from the point of view of reliability are enormous. All functions that affect the motion of the vehicle have to have multiple redundancies with appropriate diagnostics so that failures can be detected and accommodated without degradation of performance. In particular the longitudinal and lateral sensors, the throttle, brake and steering subsystems have to have double or triple if not more redundancies in order to meet the strict reliability requirements in ERSC4. The degree of redundancy depends on the design choices and the maturity of technology and needs to be studied.

2. Despite the use of communications and navigation capabilities of the vehicle, the vehicle has to rely on its on-board sensors for any movement it makes. The sensors emulate the driver's senses and are required to process information fast, accurately and reliably. These requirements are difficult to meet with today's technology under the constraint of affordability.

3. The calculation of the position and speed of the vehicle relative to other vehicles in other lanes is a crucial and risky issue that needs to be studied. The calculation of the safe headway involves the measurement of a variety of factors whose effect could be hard to measure with sufficient accuracy. Lane changing accuracy is another issue. The relative position and speed of the vehicle before, during and after the lane change is completed depends on a lot of factors that could be hard to predict or evaluate. A high level of conservatism may be necessary in order to overcome possible discrepancies and inaccuracies.

4. The calculation of the time to collision (TTC) for collision avoidance purposes is a very difficult problem. In a roadway with multiple lanes where vehicles are free to change lanes anywhere, anytime, every vehicle within certain range could be classified as threatening, leading to very short TTC and resulting in unnecessary activation of the collision avoidance function. One way to avoid these situations is to use vehicle to vehicle communications where vehicles continuously communicate their identification, position, speed, acceleration and intentions to all vehicles within a certain range. Such a communication system will require a large bandwidth which may be difficult to obtain. An alternative way that preserves bandwidth is to communicate only significant changes in, or intentions to change velocity and/or lane position.

5. In a multilane automated environment it is absolutely essential that vehicles coordinate their movement and most important their lane changes with each other. Such coordination implies the need for some form of communication between the vehicles and the existence of some protocols that defines unambiguously priorities and sequences of events. A protocol that is robust and allocates priorities in an unambiguous manner has to be developed. Furthermore, the communication medium is a problem that has to be solved in conjunction with the communication protocol, since the two together constitute essentially a wireless data network. Issues such as bandwidth allocation and utilization, capacity, range, immunity to interference and reliability are things that deserve further investigation. A large bandwidth may be required in order to meet the reliability and functionality requirements for ERSC 4.

6. The longitudinal ranging sensor that might satisfy the needs of ERSC1, 2 and 3 may not be sufficient for ERSC4. In ERSC4 it is absolutely essential to sense other vehicles with a high degree of accuracy and reliability. Existing sensor technology might not be sufficient for the requirements of ERSC4 in terms of target resolution, accuracy and reliability. Since sensor failure of any kind cannot be tolerated under any circumstance, multiple sensors employing different sensing methods will certainly be required.

7. The problem of sensing the position of the vehicle within the lane has not yet been solved satisfactorily. Several methods have been proposed based on different methods and operating principles such as magnetic paint, magnetic nails, electromagnetic signals from embedded wires, optical recognition and radar, but none of them has demonstrated either sufficient reliability and robustness in sensing or cost effectiveness. More research will definitely be needed in this area.

8. With the envisioned scenario of dense traffic moving at high speeds, despite the collision avoidance methods that may be available on the vehicle, a few collisions may be unavoidable. In today's freeways even a minor collision creates a major traffic disturbance that affects thousands of vehicles when the drivers stop to survey the damage and exchange insurance information. In an automated highway environment with vehicle to vehicle communication capability one can envision that in the event of a minor collision that does not affect the drivability of the vehicles involved, the exchange of vehicle and insurance information takes place through the vehicle to vehicle communication device. In the case of major collisions the roadway is expected to be responsible for managing the accident.

9. A critical issue associated with accident avoidance and coordination of traffic between vehicles is the choice of protocol that defines the right of way among vehicles and clearly defines the priorities of the

vehicle control algorithm. At ERSC4 each vehicle is a free agent that is allowed to select an optimal path according to its own criteria. A problem arises whenever the vehicle is facing a potentially threatening situation, or an imminent collision threat. The vehicle controller has the obligation to coordinate the path of the vehicle with every other vehicle within close range, but in the event of imminent collision there may not be enough time for such negotiation or the negotiation may result in dead-lock. Clearly the controller may choose a path that minimizes the collision risk to itself but creates an increased risk for several other vehicles in the neighborhood, while the optimal solution for the system as a whole might be to let that vehicle suffer more damage in the interest of minimizing the effect on a global level (for the region affected). The liability problems associated with this are really complicated.

10. Another important issue is how to deal with vehicles that are not equipped for ERSC4 once they manage to merge into the automated lanes of ERSC4 by bypassing the check-in procedures or vehicles whose hardware fails to perform after they have merged. This problem though is partially covered by the fallback function analysis.

11. An issue that needs further study is to identify what is the best method of alerting the driver to resume control of the vehicle for check-out and how far before the car reaches the check-out point. An associated problem is how to deal with a driver and vehicle that fails the check out procedure. Should the vehicle be taken to the next exit? Should the system guide the vehicle to the exit anyway and stop the vehicle? The best way might be to lead the vehicle to a stop at the end of the exit ramp, regardless of whether the driver passed or not the alertness and readiness test. The issue is that if the driver does not resume driving at that point, he will create a backup of traffic behind him, so methods have to be devised to circumvent that problem. With this method the check-out procedure may be unnecessary. The driver has to resume manual control by restarting the vehicle. The method, however, is expected to affect efficiency in urban areas with frequent exits. It may, however, be feasible and attractive in rural areas.

12. The assumption of fall-back modes where the driver will be alerted and instructed to assume responsibility of certain driving tasks raises many crucial human factors issues that need to be studied. In ERSC 4 a fail-soft failure of a particular driving function or redundant path may require driver's assistance to guide the vehicle to the next exit. Will driver's be able to understand the different modes of possible operations and act fast when need to?

13. In a fully automated vehicle environment drivers shall not be able to override any of the automated vehicle functions that affect the motion of the vehicle. Otherwise they may find themselves in a situation they cannot handle. The driver, however, should be able to request a return to manual control by first following a check-out procedure that puts the vehicle in a position where manual control is safe.

14. The vehicle for ERSC 4 will be highly instrumented with electronic components. Due to the low maintenance requirements of electronic components the current low trend of maintenance could continue with the AHS vehicles.

15. As with the previous ERSCs the retrofitting of vehicles not built for ERSC 4 is going to be expensive and unacceptable to users. The retrofitting of any component that affects the motion of the vehicle is expected to be very costly. The upgrading of vehicles built for ERSC 3 or 2 or 1 to those of ERSC 4 is also going to be costly due to the additional hardware and software tools and redundancies used for the vehicle of ERSC 4.

SECTION 6 ERSC 5 ANALYSIS

ERSC 5 is a small extension of ERSC 4 where the responsibility of vehicle navigation is given to the roadway. The roadway based vehicle navigation is not expected to affect the lateral and longitudinal functions of the vehicle. As a result there is a considerable overlap between ERSC 4 and 5. Our analysis will follow the same procedure as in ERSC 4 but it will concentrate on the issues related to roadway based vehicle navigation in order to avoid duplication.

Vehicle and Interface with Roadway and Driver Functions

ERSC 5 is similar to ERSC 4 as far as the basic vehicle functions are concerned. The number of functions of the roadway, however, increases to include optimization of traffic flow by controlling lane changes and coordinating vehicle maneuvers in general. The following operational scenario describes the functions of the vehicle associated with the new roadway functions.

Operational Scenario

The fitness of the vehicle to operate on AHS is displayed constantly through on-board diagnostics when the vehicle is operating either manually or automatically. When the vehicle approaches the AHS facility it establishes communication with the roadway in order to verify its communication capabilities. The intentions of the driver to enter the AHS facility are communicated to the roadway together with the vehicle's fitness status and identification. If the vehicle is fit the driver is notified and instructed to drive the vehicle to the entry point or area, enter his/her trip destination and switch on the automated mode. The automated mode includes all the functions presented in ERSC 4. The only difference is that the navigation function now receives direct routing commands from the roadway. In ERSC 5 the roadway determines the routes of the individual vehicles according to their destinations in an effort to minimize traffic disturbances and optimize the efficiency of the traffic network. The roadway computes the precise route of each vehicle on line and gives commands for lane changes, exiting and other relevant coordination maneuvers. The commands are communicated to the on-board navigation function, checked for consistency and passed on to the lateral/longitudinal automated functions for execution. As in ERSC 4 the vehicle responds to the navigation commands by relying on its own sensors for safety. The driver may change its trip destination while on the automated driving mode. These changes are communicated to the roadway to be taken into account in calculating the optimum route for the vehicle. The vehicle communicates to the roadway its position and speed continuously with time. This information is used by the roadway to compute optimum routes for vehicles and provide the appropriate navigation commands.

Apart from the roadway navigation commands all other functions that include lateral and longitudinal control check-out and exit are the same as in ERSC 4.

The functional block diagram shown in figure 25 indicates the interaction of the vehicle's automated functions with the roadway, driver and other vehicles.

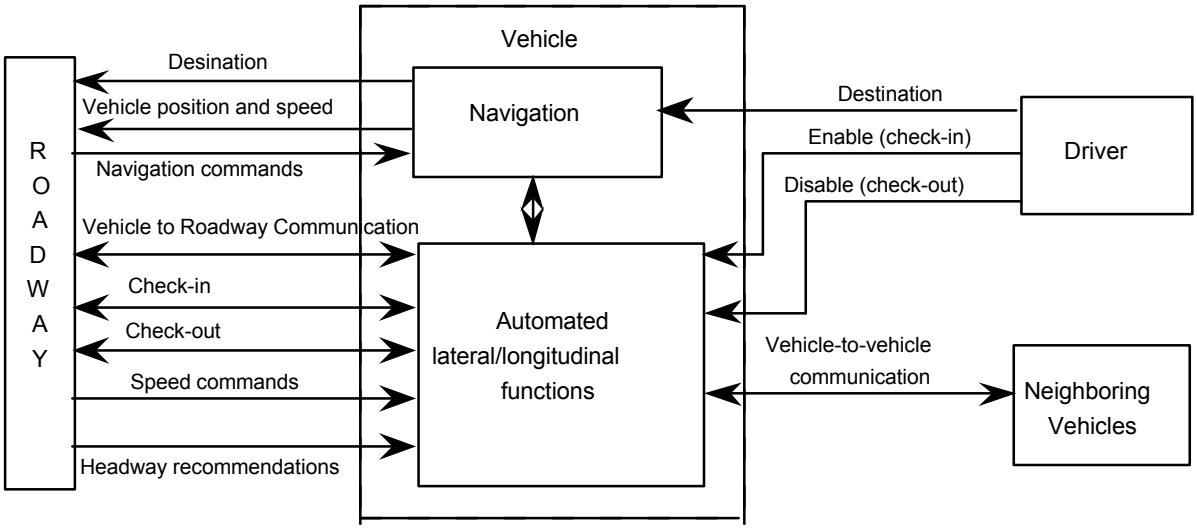

Figure 25: Functional block diagram of vehicle functions and interface with roadway, driver and neighboring vehicles.

The main high level functions associated with ERSC 5 are the same as in ERSC 4 with the addition of the roadway navigation function as listed below.

H5.1 Roadway Navigation Functions
H5.2 Vehicle Navigation Functions
H5.3 Automated Lateral/Longitudinal Control
H5.4 Driver Vehicle Roadway Interface

H5.1 Roadway Navigation Functions

Figure 26 shows the functional block diagram of the roadway navigation functions.

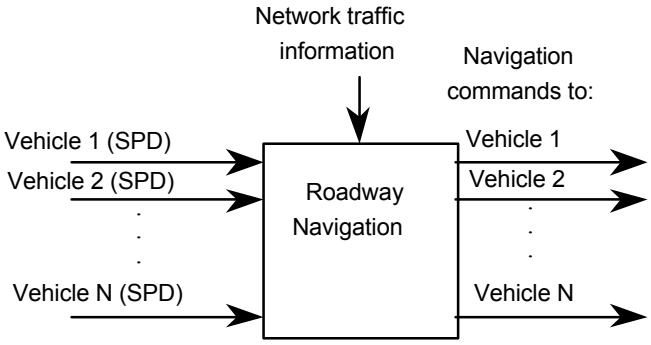

Figure 26: Roadway navigation function (SPD) = (speed, position and destination)

Inputs:

Identification, speed, position, and trip destination from each vehicle in each lane for a specified section of the automated highway consisting of an arbitrary number of vehicles N.
Traffic flow and traffic network information.

Outputs:

Lane change, check-out, exit commands to each vehicle

Functional Specification:

The roadway navigation system calculates the route of each vehicle and issues commands for lane change, check-out, exit to each individual vehicle in order to optimize the efficiency of the AHS. It receives the identification, position, speed and destination from each vehicle in a specified section of AHS as well as traffic flow network information from a central station. It performs the optimization and calculates the optimum route of each vehicle that results to an efficient operation of AHS.

The specific functions and functional and reliability requirements are:

F5.1 Receive position, speed and destination from a very large number of vehicles.
The roadway shall receive the identification, position, speed and trip destination from each vehicle continuously with time and shall identify where each vehicle is at each instant of time.

F5.2 Calculate navigation commands for each vehicle.
The roadway shall use network traffic flow information and the vehicle operational status at each time to calculate the navigation commands for each vehicle.

F5.3 Send navigation commands to each vehicle
The roadway shall send navigation commands to each vehicle. These commands include change lane, check-out, exit.

H5.2 Vehicle Navigation Functions

The functional block diagram of the vehicle navigation system is shown in Figure 27.

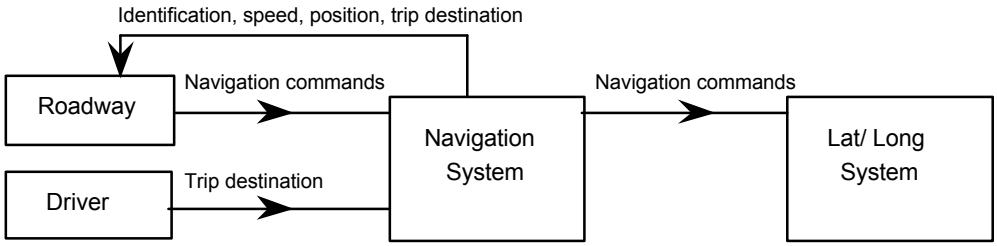

Figure 27: Functional block diagram of vehicle navigation system.

Inputs:
Roadway navigation commands: lane change, check-out, exit
Driver: trip destination

Outputs:
Navigation commands to lateral/longitudinal system.
Identification, speed, position, trip destination to roadway.

The vehicle navigation system communicates the identification, speed, position, and destination of the vehicle to the roadway and receives navigation commands from the roadway. It checks the roadway commands for consistency and passes them on to the lateral/longitudinal system for execution. The system acts as a backup to navigation system.

The specific functions and functional and reliability requirements of the vehicle navigation system are listed below:

F5.4 Send vehicle identification, position, speed and trip destination to roadway
The system shall send the identification, position, speed and trip destination of the vehicle to the roadway during specified intervals of time.

F5.5 Receive navigation commands from roadway
The system shall be able to receive navigation commands from the roadway.

F5.6 Check validity of navigation commands
The navigation system shall check the validity of the roadway navigation commands. If they are not consistent it shall send a message to the roadway.

F5.7 Transfer navigation commands to the lateral and longitudinal control function.
The system shall transfer the roadway navigation commands to the lateral/longitudinal control system.

F5.8 Enable Navigation
Upon driver's command the navigation functions shall switch on during check-in.

F5.9 Disable Navigation
Upon driver's command the navigation functions switches off.

H5.3 Automated Lateral/Longitudinal Control

The functional block diagram of the automated lateral/longitudinal functions is shown in figure 28.

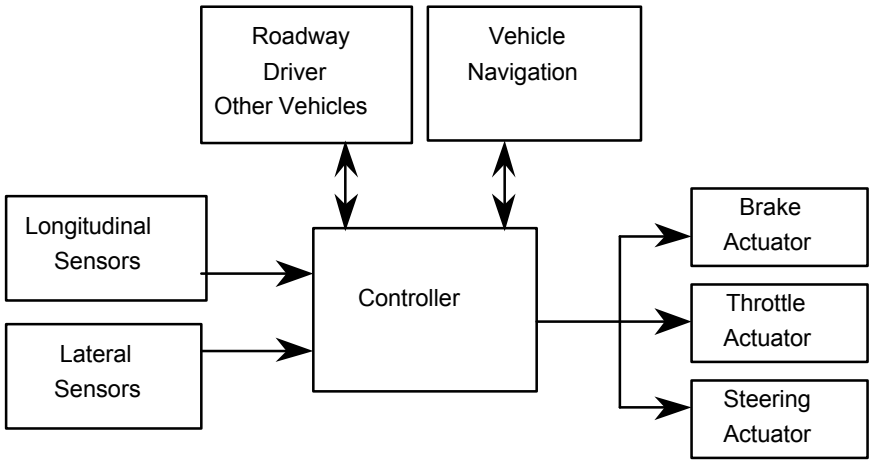

Figure 28: Functional block diagram of automated lateral/longitudinal control.

Inputs:

Longitudinal measurements: speed, relative speed and spacing, acceleration.
Lateral measurements: yaw rate, steering angle, preview, lateral position, closing rates and position of vehicles or objects in other lanes.
Roadway commands: target speed, headway recommendations, merging coordination.
Navigation commands: lane change, check-out, exit.
Other vehicles: braking capabilities and intentions, lane change, and merging intentions.
Driver commands: enable at check-in, disable at check-out.

Outputs:

Commands to brake, throttle and steering actuators.
Notify driver and roadway of mode of operation.
Braking capabilities and intentions, lane change and merging intentions to other vehicles.

Functional Specifications:

The automated lateral/longitudinal control system includes the SHM, LK, lane changing functions and the combined lateral and longitudinal collision avoidance function. The system is responsible for the lateral and longitudinal motion of the vehicle and for avoiding collision with all moving and stationary obstacles. It takes inputs from the vehicle navigation system for lane changing, check-out and exiting. It responds to target speed commands, roadway recommendations and merging coordination commands from the roadway. It communicates the braking capabilities and braking, lane changing and merging intentions of the vehicle to other neighboring vehicles and receives the corresponding information from the surrounding vehicles. It responds to driver's inputs for switching on during check-in and switching off during check-out.

The main functions and functional and reliability requirements of the lateral and longitudinal control system are:

F5.10 Calculate safe headway

The system uses information from on-board sensors that sense the vehicle's braking capabilities, the braking capabilities of the preceding vehicle obtained via communication and headway recommendations from the roadway to calculate a safe headway for vehicle following. The calculation of the safe headway shall take into account all factors and worst case stopping scenarios.

F5.11 Maintain speed

The vehicle shall track and maintain the roadway commanded speed as long as no valid target is present.

F5.12 Maintain headway

The vehicle shall maintain the headway selected by the vehicle under all environmental conditions, road geometry and freeway speeds.

F5.13 Switch from maintaining speed to maintaining headway

When the system senses a valid target in the same lane that is within certain range it shall switch to the following mode by maintaining a safe headway calculated by the vehicle.

F5.14 Switch from maintaining headway to maintaining cruise speed

When the target moves out of the sensing range or changes lane the system shall switch to maintaining roadway commanded speed.

F5.15 Keep vehicle in the center of lane

The system shall keep the vehicle in the center of the lane at all highway speeds, under all roadway and environmental conditions and during all modes of operation of the lateral and longitudinal controller.

F5.16 Coordinate lane change with other vehicles

The system shall coordinate a lane change maneuver with neighboring vehicles by communicating its identification, operational status and intentions to change lane. The system shall also accept similar lane change information from other vehicles and assist them during lane changing by obeying the traffic rules and the established "right of way."

F5.17 Synchronize speed and headway for lane change

The system shall synchronize its speed and headway to be ready for a lane change maneuver or to assist other vehicles during lane change.

F5.18 Change lane

The system shall use its on-board sensors and controllers to change lanes after functions F5.16, F5.17 are completed.

F5.19 Switch from lane changing to longitudinal control

The system shall position the vehicle in the center of the lane after a lane change maneuver is completed and switch to the speed or headway maintenance, and lane keeping mode.

F5.20 Combined lateral and longitudinal collision avoidance.

The system shall avoid colliding with any moving or stationary obstacle by monitoring the motion of the vehicle relative to the surroundings and providing the appropriate commands to the steering, throttle and brake actuators. The system uses on-board sensors and vehicle to vehicle communication to learn about the capabilities of the vehicles and their intentions for braking, lane changing. It calculates the TTC from all directions. If the TTC becomes less than a certain value then it sends the appropriate commands to the brake, throttle and steering actuators.

F5.21 Switch from collision avoidance function to normal operation

A collision avoidance maneuver may bring the vehicle to a full stop or place it in a different lane or make it deviate from its normal operation. The purpose of this function is to bring the vehicle back to the speed or headway maintenance and lane keeping function by using its on-board sensors and vehicle-to-vehicle communications.

F5.22 Enable the lateral/longitudinal functions

Upon driver's command during check-in the lateral/longitudinal functions shall switch on.

F5.23 Disable the lateral/longitudinal functions

The lateral/longitudinal functions shall switch off after the driver has passed the check-out test and assumed full manual control.

H5.4 Driver Vehicle Roadway Interface

The high level functional block diagram of the driver interface with vehicle and roadway is shown in figure 29.

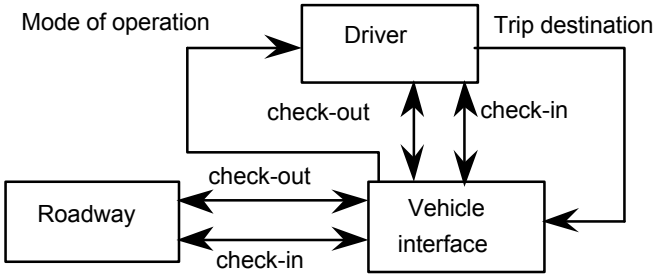

Figure 29: Functional block diagram of driver interface with vehicle and roadway.

The following functions are associated with the interface of the driver with the vehicle and roadway.

F5.24 Check-in

Driver shall use the on-board diagnostics to check the fitness of the vehicle to operate on the AHS facility. The vehicle shall establish communication with the roadway via vehicle-to-roadway communication and present its fitness status and identification to the roadway. If the vehicle is fit the roadway shall send an acknowledgment that the vehicle passed the check-in test and is ready to enter the AHS facility.

F5.25 Enter AHS

If the vehicle passes the check-in test the driver shall drive the vehicle to the entrance of the AHS facility, enter the trip destination and switch on the automated mode. The vehicle shall drive itself by using its on-board sensors and communications with the roadway and other vehicles.

F5.26 Merge into the automated lanes

The vehicle shall merge into the automated lane by communicating with other vehicles and the roadway in order to coordinate its maneuvers. Each maneuver shall be followed provided it is considered to be safe by the on-board sensors.

F5.27 Change of trip destination

The driver shall be able to change its trip destination while the vehicle is in the automated mode without interfering with the automated functions. The new trip input shall be fed into the navigation system that calculates the route of the vehicle based on the new destination.

F5.28 Alert driver for check-out

At the end of the trip the vehicle shall alert the driver to initiate a check-out procedure.

F5.29 Check-out

The driver shall initiate a check-out procedure after he/she has been alerted and warned by the system or after he/she has made a decision to abort the automated operation. The check-out procedure involves the gradual transition from the automated mode to the manual mode by transferring control to the driver depending on his/her driving performance. The check-out procedure starts by allowing the driver to provide small steering and throttle/brake inputs. These inputs are augmented by the system in order to maintain vehicle performance. If the driver performance is acceptable he/she is given additional authority over steering, throttle and brake until the system switches to manual mode. If the driver fails the check-out procedure by not performing well enough or by not responding the vehicle guides itself to a special ramp or shoulder of a lane, brings itself to a full stop and notifies the roadway. The roadway is also notified when the check-out procedure starts and ends. The vehicle can also initiate a check-out procedure if the driver cannot be alerted by the system. In this case the vehicle guides itself to a

special ramp or shoulder, stops and notifies the roadway. The check-out procedure may take place in a special transition lane or in a slow lane or special ramp.

F5.30 Exit lane

After passing the check-out test the driver assumes manual control of the vehicle and exits the AHS facility. The vehicle sends a notification to the roadway when the exit is completed.

F5.31 Fall back to ERSC 4

The vehicle functions shall switch to those of ERSC 4 when the roadway navigation system fails to provide navigation commands for the vehicle.

F5.32 Fall back to ERSC 3

The vehicle functions shall switch to those of ERSC 3 when the lane changing function and/or the overall collision avoidance function becomes inaccurate or their redundant paths fail. The transition involves an initial warning to the driver and monitoring of his/her actions. If the driver is fit to operate as required in ERSC 3 the system completes the transition. If not the system initiates a check-out procedure.

F5.33 Fall back to ERSC 2

The vehicle functions shall switch to those of ERSC 2 when the lane keeping function becomes inaccurate or when a redundant path fails. The transition involves an initial warning to the driver to assume the driving role required by ERSC 2 (i.e. steering). After the warning the system shall be monitoring the driver's performance. If the driver is alert, and his performance is acceptable then the transition is complete. If the driver cannot be alerted or he/she repeatedly fails the test the vehicle will be guided to a stop.

F5.34 Fall back to ERSC 1

The vehicle functions shall switch to those of ERSC 1 when the RECA function becomes inaccurate due to the inability of the system to assume responsibility for avoiding rear-end collisions. The transition involves an initial warning for the driver to assume the driving role required by ERSC1 (i.e. steering and collision avoidance). After the warning the system shall be monitoring the driver's performance. If the driver responds and his performance is acceptable, then the transition to ERSC 1 is complete. If the driver cannot be alerted or he/she repeatedly fails the test the system the vehicle will be guided to a stop.

F5.35 Fall back to manual control

When certain vehicle functions such as SHM are not functioning properly or the roadway and environmental conditions are inappropriate for automated operation the system shall switch to manual mode. The transition involves an initial warning for the driver to resume manual control of all vehicle functions. After the warning the system shall be monitoring the driver's performance. If the driver responds and his performance is acceptable, then the transition to manual mode is complete. If the driver cannot be alerted or he/she repeatedly fails the test the vehicle will be guided to a stop.

F5.36 Mode of Operation

The system shall continuously notify the driver of its mode of operation i.e. on, off, normal, emergency, malfunction, etc.

ERSC 5 is an extension of ERSC 4 and involves all the functions of ERSC 4 associated with the high level functions; automated lateral and longitudinal control and Driver Vehicle Roadway interface with the addition of the roadway navigation functions and the fall back to ERSC 4 function. The results of the FMEA for ERSC 5 presented in table 16 of Appendix B has therefore a considerable overlap with those of ERSC 4. Below we present and discuss the failure modes and results of the FMEA that are unique to ERSC 5 and do not overlap with those of ERSC 4 in order to avoid repetition.

Potential Failure Mode F5.1: The roadway navigation system does not receive position, speed and destination information from any vehicle.

The roadway may not be able to receive any information from the vehicles due to:

(F5.1) Roadway communication failure (S=7, O=3)

The potential effect of this failure is the loss of roadway navigation capability that may affect the efficiency of AHS. The vehicles have to rely on their own navigation systems for routing.

The design requirements and recommendations are:

(F5.1) The roadway must have redundant communication systems. The vehicle shall have their own navigation system as a backup to the roadway system. The roadway shall have independent means of measuring the position and speed and learning the identification of each vehicle.

Potential Failure Mode F5.2: Loss of ability to calculate correct navigation commands for each vehicle

The roadway may fail to calculate the correct navigation commands for each vehicle due to:

(F5.2.1) Software or electronics failure (S=7, O=4)
(F5.2.2) Lack of network traffic information (S=7, O=2)

The effect of the above failures is a possible loss of optimality in the operation of AHS.

The design requirements and recommendations are:

(F5.2.1) Supervisory elements (in hardware and software) are needed to monitor the navigation process. Each vehicle shall be notified when a malfunction in the roadway navigation system is detected. Vehicles shall notify the roadway if navigation commands are inconsistent with their destination.

(F5.2.2) Reliable network communication shall be implemented.

Potential Failure Mode F5.3.1: The roadway navigation system cannot send navigation commands to any vehicle.

The potential causes, effects and design requirements and recommendations are the same as with failure mode F5.1.

Potential Failure Mode F5.4: The vehicle can not send vehicle position, speed, and destination to roadway.

The potential causes of the above failure are:

(F5.4.1) Vehicle is unable to determine its position. (S=8, O=3)
(F5.4.2) On-board transmitter failure. (S=4, O=3)

The potential effect of failure (F5.4.1) is the possible loss of navigation capability for both the roadway and vehicle due to the inability of the vehicle to determine its absolute position. The effect of failure (F5.4.2) that is due to the transmitter on the vehicle is the potential loss of the roadway navigation function which may have a negative effect on efficiency and optimality of AHS. In this case the vehicle has to rely on its own navigation system.

The design requirements and recommendations are:

(F5.4.1) Redundant methods to determine absolute position are needed. The vehicle may send a position relative to another vehicle when it is unable to determine its absolute position.

(F5.4.2) Supervisory elements are needed to monitor the transmitter. The vehicle shall be asked to check out if transmitter fails.

Potential Failure Mode F5.5: The vehicle can not receive navigation commands from roadway.

The vehicle may fail to receive navigation commands from the roadway due to the following possible cause:

(F5.5) Vehicle receiver failure (S=7, O=4)

The potential effect of the failure is loss of the roadway navigation function that may have an adverse effect on the efficiency of AHS.

The design requirements and recommendations are:

(F5.5) Supervisory elements are needed to monitor communications. Redundant receivers may be required.

Potential Failure Mode F5.6: The vehicle navigation system can not check validity of roadway navigation commands.

The potential cause of this failure is due to:

(F5.6) Software failures or the lack of traffic information. (S=7, O=2)

Due to the failure the vehicle may follow the wrong route leading to an increased travel time.

The design requirements and recommendations are:

(F5.6) The navigation commands shall also be presented to the driver. When a new route is computed, driver shall be notified.

Potential Failure Mode F5.7: The vehicle navigation system can not transfer navigation commands to lateral and longitudinal controller.

The failure may be due to:

(F5.7) Coordination software failure (S=7, O=2)

The potential effect is loss of the navigation function of the vehicle. The driver may have to take over navigation.

The design requirements and recommendations are:

(F5.7) Supervisory programs are needed to monitor the navigation commands and lateral, longitudinal controller actions.

Potential Failure Mode F5.31: Roadway navigation not available but system does not fall back to ERSC 4

The potential causes of this failure are:

(F5.31.1) Software failure (S=7, O=2)
(F5.31.2) Vehicle navigation system failure (S=7, O=3)

The potential effects of these failures is the loss of vehicle navigation capability. The driver may have to take over navigation.

The design requirements and recommendations are:

(F5.31.1) Reliable supervisory and diagnostics program shall be implemented.

(F5.31.2) The vehicle navigation system shall use redundancies to improve reliability

The rest of the potential failure modes, their causes and effects are the same as in ERSC 4.

Vehicle, Driver Diagnostics and Maintenance

The vehicle and driver diagnostics and maintenance discussions presented in ERSC 4 hold for ERSC 5 too.

In ERSC 5 the roadway will be responsible for maintaining the operation and functionality of its navigation systems. Redundancies in the roadway equipment may be necessary in order to improve reliability but also for performing maintenance without disrupting the system operation.

Retrofitting

As with the previous ERSCs retrofitting is going to be expensive and unacceptable to users. The upgrading of vehicles built for ERSC 4 to operate for ERSC 5 may be feasible. The reason is that the roadway based vehicle navigation functions are not found to affect safety. Furthermore, the vehicle for ERSC 4 is already heavily equipped with electronics and therefore the addition of a few more will constitute a small percentage increase in the cost of the vehicle.

Deployment Scenarios

In ERSC5 the vehicle is fully automated and the roadway is fully instrumented and the roadway assumes the responsibility of calculating navigation commands for each vehicle. To assist the roadway in this task, each vehicle must frequently send information about its current status to the roadway. Therefore, the vehicle will periodically update its position, speed and destination information. The roadway must process the information it receives from all the vehicles within its range of authority and compute and update navigation commands for each vehicle with the goal of optimizing traffic density and efficiency for all the vehicles involved. The vehicle is also equipped with its own navigation instruments and sensors which enable it to execute the commands received from the roadway accurately and efficiently.

The deployment of ERSC 5 may be possible after a successful deployment of ERSC 4. The issues involved, however, are also enormous. Will the roadway be able to process a huge amount of information and optimize vehicle motion so that the overall system is efficient but not at the expense of increased travel time for a large number of vehicles? The development of optimization algorithms to deal with the dynamic environment of ERSC 5 will be a challenging problem. It will require bigger and faster computers and most likely a highly decentralized decision making process in order to manage the large amount of data.

The roadway in ERSC 5 may be highly instrumented in order to have an independent method of measuring the position, speed and identification of each vehicle. Otherwise the roadway may not be able to identify vehicles with lost communication capability. This requirement will increase the infrastructure cost and delay deployment of ERSC 5.

Key Results and Conclusions

The key results and conclusions developed for ERSC 4 are applicable to ERSC 5 with the addition of the following:

1. In ERSC 5 the roadway is required to process a large number of data that may require larger and faster computers than what is available today. The computational requirements for the roadway controller need to be researched.

2. The optimization of traffic by choosing the route and issuing navigation commands for each vehicle could be an intractable problem from the theoretical point of view. Some decentralized decision making may be necessary and sub optimal solutions may be more realistic.

3. The roadway may have to be heavily instrumented in order to have redundant means of measuring the position and speed of each vehicle. Such instrumentation will increase costs and needs for maintenance.

4. The retrofitting of vehicles for ERSC 5 is going to be expensive. The upgrade of vehicles built for ERSC 4 to be used for ERSC 5 may be feasible.

SECTION 7 CONCLUSIONS

In this report we study and analyze the vehicle operational issues associated with the development and deployment of vehicles for five evolutionary representative system configurations (ERSCs). In ERSC 1 the driver is responsible for all collision avoidance and steering functions. In ERSC 2 we introduce a full authority longitudinal control with the driver responsible for steering and lateral collision avoidance. In ERSC 3 the lane keeping function is automated and the driver is responsible for lane changing only. In ERSC 4 the vehicle is fully automated, self-guided with navigation capabilities and the driver is not required to perform any driving function during normal operation on AHS. In ERSC 5 the roadway is responsible for vehicle navigation by selecting the route of each vehicle based on its destination in a way that optimizes the efficiency of AHS. The issues addressed are associated with reliability and the need for redundancies, vehicle and driver diagnostics, retrofitting, maintenance and deployment scenarios. A system level failure mode and effects analysis (FMEA) is used to study reliability and the need for redundancies and diagnostics for each ERSC.

Below we list the overall key findings, issues and risks developed in this report according to the area of emphasis. The results and conclusions that are specific to each ERSC are presented before at the end of each section that is devoted to the analysis of the individual ERSC .

Reliability

1. The reliability requirements for the vehicle functions increase considerably as we go from ERSC 1 to ERSC 5. Figure 30 gives an indication of the number of potential failure modes with the highest severity rating generated by the FMEA for each ERSC. The biggest jump occurs when we go from ERSC1 to ERSC2. In ERSC1 the driver is a back-up for the speed and headway maintenance (SHM) function which is the main automated vehicle function in ERSC 1. The driver is responsible for collision avoidance and steering. As a result the number of potential vehicle failure modes with high severity is fairly small. By moving to ERSC2 where we introduce a full authority longitudinal controller that calculates on line the vehicle headway, a considerably larger number of high severity failure modes is possible. Table 7 gives a list of all the basic vehicle functions and subsystems that need redundancies in order to meet the required reliability levels and reduce the severity of the potential failure modes. The number of redundancies increases considerably as we automate additional driving functions by going from ERSC 1 to a higher one.

2. Redundancies alone will not achieve the high level of reliability that is essential for AHS. Appropriate diagnostics and control logic are essential in switching from a faulty redundant path to a healthy one without degrading performance and safety. Figures 15, 20 show simple block diagrams of redundant designs for a full authority longitudinal control and automatic lane keeping. The figures indicate the level of complexity that may be required for reliable operation.

3. A vehicle shall not be considered fit to operate on AHS if any one of the redundant paths is faulty. As a result all redundant paths shall have diagnostics that monitor their functionality. The monitoring is possible if all redundant paths are activated during vehicle operation. Special designs and control techniques need to be developed to make such operations possible. The control techniques may be also used for fast detection and accommodation of failures.

4. The vehicle functions shall be designed so that during normal operation and transitions the driver is never placed in a situation he/she cannot handle. For this reason the driver shall not have the capability of overriding automated driving functions such as the full authority longitudinal controller, the lane keeping and lateral controller. The driver, however, shall be able to request a transition to manual control. The system shall respond to this request if conditions are safe by following a check-out procedure during which the vehicle adjusts its speed and headway to comfortable for human driving levels and the driver takes over control gradually provided he/she is fit to operate the vehicle.

5. Our analysis indicates that all automated vehicle functions have to be protected from failures by using redundancies and on board diagnostics. Vehicles will not rely on the roadway to check their functionality and reliability. The redundancies and on board diagnostics will allow the monitoring of the vehicle components and subsystems even during manual driving. As a result no time consuming and elaborate on site check-in tests may be required. The driver may be notified before even reaching AHS whether his/her vehicle is fit to operate on AHS.

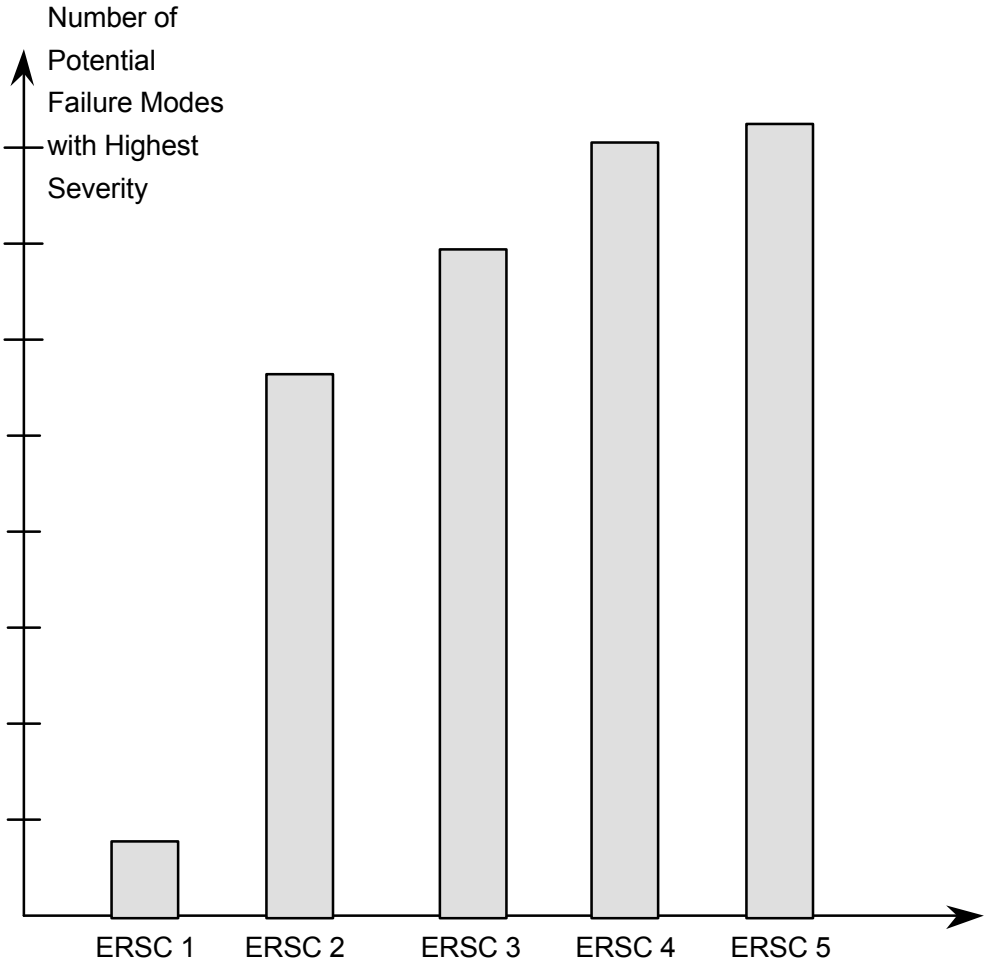

Figure 30: The number of potential failure modes with the highest severity rating generated by the FMEA.

Table 7: Required Redundancies

Vehicle functions and/or subsystems	ERSC 1	ERSC 2	ERSC 3	ERSC 4	ERSC 5
Longitudinal measurements (speed, range, relative speed)	X	XX	XX	XX	XX
Controller Electronics and Software	X	XX	XX	XX	XX
Disability of Automated Functions	X	X	X	X	X
Calculation of Headway		XX	XX	XX	XX
Vehicle to Vehicle Communication		X	X	XX	XX
Brake Subsystem		X	X	XX	XX
Roadway Lane Reference Aids		X	XX	XX	XX
Lateral Position Sensor		X	XX	XX	XX
Steering Subsystem			XX	XX	XX
Lateral Measurements for Lane Changing			X	XX	XX
Throttle Subsystems				X	X
Vehicle to Roadway Communication					X

6. The development of fully automated vehicles that can operate reliably at high speeds with today's technology within reasonable cost constraints is unrealistic. Despite several successful experiments in vehicle following and lane keeping the current sensor technology is not yet mature to meet the functional and reliability requirements of automated vehicles.

7. The choice of a safe headway to be used for vehicle following so that no rear-end collision takes place when the preceding vehicle brakes during collision avoidance maneuvers depends on a lot of factors that include the braking capabilities of the vehicles involved, sensor/actuator characteristics, the friction coefficient between tires and the road, the speed of the vehicles etc. The on line reliable measurement of these factors is an issue that needs to be resolved. A conservative choice may lead to a large headway that will affect capacity and efficiency whereas a short headway will have a negative impact on safety. For ERSC2 to ERSC5 we assume that the vehicle selects the headway by taking into account all relevant factors obtained through measurements and from vehicle to vehicle communication. This raises several liability issues that need to be resolved. The sensitivity of the minimum safe headway with respect to differences in velocity, braking capabilities, friction coefficient etc. makes it impossible to have very low headways (of the order of 0.3 sec or lower) and still guarantee a collision-free vehicle following.

8. In our approach we assume that the headway is chosen so that vehicle following is collision free under normal operation. We assume that no low DV collisions are acceptable. As a result the organization of vehicle into platoons of a specified size with very small inter vehicle space is not considered to be necessary.

9. The selection of the headway by the vehicle in ERSC2 to ERSC5 raises serious liability issues that need to be resolved. If the goal of AHS is to increase capacity the selection of the headway should not be left to the driver due to the randomness in human choices and the possibility of having considerably larger than necessary headways.

10. The evolution of vehicle functions from ERSC1 to ERSC5 does not imply that vehicle built for a lower ERSC can be upgraded to be used for higher ERSCs. The design and reliability requirements differ from one ERSC to another considerably. As a result each ERSC calls for new designs, vehicle functions, subsystems, and components.

11. Every vehicle function that affects the motion of the vehicle and/or has an impact on safety has to be designed so that it never puts the driver in a situation he/she cannot handle. Such situations were identified in ERSC2 and ERSC3 and modification of the vehicle and roadway functions were proposed to eliminate them.

12. The use of warnings in ERSC 1 to 3 together with automated driving functions raises several important human factors issues that need to be studied. For example when and how to give warnings; especially those warnings associated with lane departure and lane changing. How do warnings affect the driving tasks of the driver and his/her interface with the automated functions? What if two or more warnings are activated the same time causing confusion or panic to the driver?

13. The role of the driver during fall-back modes poses several human factors issues that need to be addressed. The fall-back from ERSC 5 to ERSC 4 doesn't pose any problem to safety. The fall-back from ERSC 4 to ERSC 3 or lower requires the driver to assume the responsibility of certain driving tasks. Whether the driver can understand the different modes of operation and is able to switch from one mode to another and perform his/her duties are human factors issues that need to be studied. These studies may conclude that the only possible mode that the driver can understand and adjust fast is the manual mode. This will imply that a malfunction in the automatic lane changing function of a vehicle in ERSC 4 will require the vehicle to return to manual mode and the driver to drive the vehicle to the exit by going through automated lanes. Such an approach will raise several human factors and safety issues that need to be addressed. The driver interface with the vehicle functions and roadway should be clear and simple. Human factors studies are required to understand the interface of the driver with the vehicle and roadway functions. Current human factors studies on intelligent cruise control systems may provide considerable knowledge in this direction.

14. A considerable number of technical issues need to be resolved before deploying a full authority longitudinal controller or an automated lane keeping controller or a full authority lateral controller.

15. Despite the availability of various sensors for intelligent cruise control, sensor technology is still not mature to meet the functional and reliability requirements involved in the implementation of a full authority longitudinal control.

16. Automated lane keeping shall keep the vehicle in the center of the lane under all highway speeds, environmental and traffic conditions and roadway configurations. This requirement cannot be met with today's "affordable" sensor technology despite the reported success of several lane keeping experiments.

17. Automated lane changing is one of the most difficult functions due to the tremendous sensor requirements involved. The sensors have to cover a wide field of view, process information fast and distinguish between threatening and non threatening situations. Emulating the human driver's senses in this case is a challenging technical problem that needs to be resolved. Vehicle to vehicle communications may be necessary in addition to all other sensor requirements in order to resolve the problem at least theoretically. The use of a large bandwidth communication system may be necessary in order to meet all the reliability requirements.

18. Collision avoidance is another important function that involves serious issues and risks. In ERSC 4, 5 where vehicles change lanes automatically while calculating the time to collision and distinguishing

between threatening and non threatening vehicles or obstacles is a difficult if not impossible task. In such an environment any vehicle in the vicinity could be classified as threatening. The use of vehicle to vehicle communications may help alleviate some of the problems but it is not clear whether all the reliability requirements can be met. Communications will not be helpful in the cases of obstacles other than a vehicle or vehicles that are still in motion but lost their communication capability.

19. The roadway based navigation of vehicle in ERSC 5 requires the acquisition and processing of a tremendous amount of data. It is unlikely that the computing requirements can be met with today's computer technology especially if the computations are performed by a central computer. Furthermore, the optimization of a dynamic system such as traffic flow on the vehicle level could be an intractable theoretical problem. More research is required in order to study the feasibility of optimizing traffic flow characteristics by controlling the motion of individual vehicles.

Vehicle diagnostics

20. Our analysis calls for a significant number of built-in tests and on-board diagnostics to monitor the functionality and health of all automated functions and of the components that affect them, as well as the health and their redundant paths. Every vehicle function that affects the motion and safety of the vehicle has to be protected from failures by using redundancies and extensive diagnostics. On-board diagnostics can be used to detect failures or malfunctions fast and help isolate them as early as possible.

21. The availability of fairly accurate vehicle models may be used to develop an executive controller with intelligent diagnostics that can monitor the overall motion of the vehicle, detect and isolate failures that may not be easily detectable on the component level. Figure 8 shows the block diagram of such a system.

22. The availability of relatively low cost electronics and computers makes the use of extensive diagnostics possible and desirable. The current trend in today's vehicle designs is the use of extensive diagnostics for components such as electronic fuel injection, electronic engine management, anti-lock brakes etc. This trend is expected to continue and dominate in the development of vehicles for ERSC 1 to 5.

Driver diagnostics

23. In ERSC 1, 2 the driver is responsible for steering and is expected to be alert. As a result there are no special demands for driver diagnostics that go beyond those that are researched for manual driving. For ERSC 3 and above driving is "feet off", " hands-off". The driver needs to be alerted and resume control of certain driving functions during malfunctions, check-out or during fall-back modes. The assessment of the fitness of the driver to assume manual control is therefore an issue. Our review of the driver diagnostics tools and devices researched and proposed in the literature suggest that an efficient method of assessing the fitness of the driver is to have him/her perform actual driving tasks. Our analysis indicates that the automated vehicle functions can be designed to allow the driver to interact with them during check-out by allowing him/her some authority over the control functions without affecting vehicle performance. The driver's behavior can then be monitored and his/her authority over the control of the vehicle increased or decreased accordingly depending on his/her performance. The design of such a system requires considerable research efforts in the area of design, controls, and human factors.

24. The availability of sensors on vehicles provides the flexibility of designing in-vehicle systems for monitoring driving behavior during manual driving as explained in Figure 9. This monitoring could be used for check-in purposes.

25. The AHS such as the one used for ERSC 3, 4, 5 could be designed so that the vehicle is guided to a special exit ramp, brought to a full stop and to warn the driver to take over the controls of the vehicle. Such a design will eliminate the need for assessing the fitness of the driver to resume manual control while the vehicle is in motion. The possibility of having frequent congested exit ramps as a result of this method, however, cannot be excluded.

Maintenance

26. The automotive industry has the goal of continuously improving product reliability, because it has been proven to be a strong customer desire and a fundamental product characterizing attribute. Therefore the manufacturers make efforts to design and build most vehicle components that are subjected to wear, so that their expected lifetime will match or exceed the expected lifetime of the entire vehicle.[14] This is not always possible though, because designing every component to meet this requirement would require over-designing certain components to the point of overburdening their cost. So it has become an accepted practice that certain components like brake friction materials, clutch friction material and engine and transmission lubricants will have to be replaced at certain periodic intervals.

The mean expected life or the Mean Time To Failure (MTTF) of electronic components is typically very high, because the wear-out mechanisms of electronic components are almost insignificant compared to that of mechanical components subjected to loads. Wear-out mechanisms for electronic components do exist, however. They affect mostly circuit areas that carry high current densities. Careful design of such susceptible areas can minimize the consequences and bring the reliability of those areas to the same level as the rest of the system. With the proper design, wear-out effects on electronic circuits and systems take very long to manifest.

The majority of the technologies required to equip a vehicle for AHS operation relies on electronic systems with inherently high MTTF. The mechanical components required for AHS are predominantly electromechanical or hydraulic actuators, which also have relatively high MTTF. Therefore, there is no identifiable component of the vehicle that will become the "weak link" of AHS operation, at least not because of its hardware failure rate. The outlook for the current and future vehicle seems to suggest that periodic maintenance of AHS components of the vehicle does not seem to be essential to guarantee the required reliability levels. Current vehicle electronics are designed to be free of maintenance for most of the life of the vehicle e.g. 10 years or 150,000 miles. This trend is expected to continue with vehicles for AHS where the number of electronic components will be considerably higher due to the higher number of automated functions and the replacement of many mechanical and hydraulic parts with electronic ones.

Retrofitting

27. Retrofitting today's vehicles with major components such as air conditioning units is expensive and not popular. The retrofitting of smaller components such as audio systems (radio) is more popular. Retrofitting major subsystems such as power steering and automatic transmission even though technically feasible is costly and very uncommon in today's vehicles. This current trend in today's vehicles suggests that the retrofitting of vehicles that were produced before the vehicles for an ERSC were developed even though technically feasible is going to be expensive. It is unlikely that it will be desirable to users and automobile manufactures. In general the retrofitting of any component that affects the motion and safety of the vehicle is going to be costly. The different reliability requirements for each ERSC also suggest that the retrofitting of a vehicle built for one ERSC to be used for a higher ERSC is

also going to be costly. The retrofitting of small electronic devices such as communication and navigation devices, displays may be feasible provided it is not costly and serves a purpose.

Deployment Scenarios

28. All the ERSCs call for an integration of the vehicle automated functions with the roadway functions in order to improve traffic flow efficiency. For such an integration to be possible the government has to work closely with the automobile manufacturers.

29. Due to the overwhelming technical issues involved in the development and deployment of fully automated vehicles, vehicle control will follow an evolutionary path. The vehicle for ERSC 1 is a natural evolution of the current vehicles and could be used in a first deployment stage of AHS. For such a deployment to be possible the government has to work closely with the automobile manufacturers in order to establish standards and resolve potential liability issues.

30. ERSC 2 and 3 pose several design deficiencies from the point of view of reliability and need to be modified in order to become possible candidates for deployment.

31. The deployment of ERSC 4 and 5 does not seem to be feasible in the near future due to the tremendous reliability requirements, the lack of mature and affordable sensor technology and the lack of clear understanding of the issues involved without the experience from the deployment of simpler AHS architectures. Even if the cost is not an issue the deployment of ERSC 4 or 5 from the technical point of view is a very challenging problem.

REFERENCES

(Selected set)

1. "Potential Failure Mode and Effects Analysis (FMEA)" Instruction Manual, Ford Motor Company.

2. Dimitri Kececioglou, "Reliability Engineering Handbook", Prentice Hall, 1991

3. "Lincoln Town Car, Crown Victoria, Grand Marquis Service Manual 1993", Ford Motor Company

4. "Ford Taurus, Mercury Sable Service Manual 1994", Ford Motor Company

5. Ribbens W., "Understanding Automotive Electronics", Fourth Edition, SAMS, 1992

6. Ioannou, P. and Xu, T., "Throttle and Brake Control for Automatic Vehicle Following," IVHS Journal, Volume 1, Issue 4, 345-377, 1994.

7. Ioannou, P. and Chien, C.C., "Autonomous Intelligent Cruise Control," IEEE Transactions on Vehicular Technology, Volume 42, Issue November, 657-672, 1993.

8. Sun, Y. and Ioannou, P., "A Handbook on Headway Calculation for Collision Free Vehicle Following," Southern California Center for Advanced Transportation, University of Southern California, Technical Report, 1994.

9. Triggs, T. and Harris, W.G., "Reaction time of drivers to road stimuli," Monash University, Melbourne, Australia, Human Factors Report, HFR-12, 1982.

10. Brouwer W., Waterink W., Wolffelaar P., Rothengatter T., "Divided attention in experienced young and older drivers: Lane tracking and visual analysis in a dynamic driving simulator", Univ. of Groningen, The Netherlands, from Human Factors, 33(5), 573-582, 1991

11. Steve Eckert,, "Failure Modes Effects Analysis (FMEA) for the Electronic Throttle Control System," Ford Motor Company, confidential.

12. Kady, M. and Shloss, P., "Electronic Messaging Using VRC (Vehicle to Roadside Communications)," in the Proc. of the IVHS America, Atlanta, 1994.

13. Greenberg, A., "AT&T Team, Amtech in Automatic Highway Toll Battle." Electronic News, July 20, 1992, 23, 1992.

14. Fukuhara, H. and Kurami, K., "Essential Issues Involved in Radar-based Collision Warning/Avoidance Systems," in the Proc. of the IVHS America, Atlanta, 1994.

15. Murphy, D.O. and Woll, J.D., "A Review of the VORAD Vehicle Detection and Driver Alert System," Society of Automotive Engineers, Report, SAE-922495, 1992.

16. Schwarzinger, M., "Vision-Based Car-Following: Detection, Tracking, and Identification," in the Proc. of the Intelligent Vehicles Symposium, 24-29, 1992.

17. Graham, R. and Hirst, S., "The Effect of a Collision Avoidance System on Driver's Braking Response," in the Proc. of the IVHS America, Atlanta, 1994.

18. Stove A.G., Chodyniecki W., "Radar Sensor for AICC", Wakeling, J. from Prometheus - Future Systems, proceedings Autotech '93.

19. Lerner, N.D., Kotwal, B.M., Lyons, R.D., and Gardner-Bonneau, D.J., "Preliminary Human Factors Guidelines for Crash Avoidance Warning Devices (Draft)," Office of Crash Avoidance Research, National Highway Traffic Safety Administration, Interim Report, DTNH22-91-C-07004, 1993.

20. Mackie R., Wylie C.D., "Countermeasures to loss of alertness in motor vehicle drivers: A taxonomy and evaluation", Proceedings Human Factors Society 35th Annual Meeting, 1991

21. Scholfield J., Wakeling R., Richardson J., Fairclough S., Fletcher W.S., "Progress Towards an Impaired Driver Attentiveness Detection System", Prometheus - Future Systems, proceedings Autotech '93.

22. Cointot B., Coblentz A., Mollard R., Siarry P., Boisvert E., Mevel Y., Bourhis S., Faidy J., "Detection of Driver's Low Vigilance Periods on Motorway", France. Proceedings of the 26th ISATA International Symposium on Automotive Technology and Automation p. 347, 1993

23. Sorsa T., Koivo H., "Application of Artificial Neural Networks in Process Fault Diagnosis", from Automatica, Vol. 29 No. 4, 1993

24. "Infiniti Q45", advertising brochure, Nissan Motors corp.

25. Private communication with Ford Motor Company engineers

26. Siewiorek D. and Swarz R., ``The Theory and Practice of Reliable System Design", Digital Press 1982

27. Syverud, K., "Liability and Insurance Implications of IVHS Technology," SAE, Technical Paper Series, 1990.

28. Stowers, J.R., "HOV Lessons from the Dulles Toll Road," TR News, Volume 170, Issue Jan-Feb, 5-9, 1994.

29. Gustafsson, F., "Slip-Based Estimation of Tire-Road Friction," Linkoping University, Sweden, Report, LiTH-ISY-R-1509, 1993.

30. Gustafsson, F. and Ekstrom, H., "Tire-Road Friction Estimation Results from Field Trials in Arvidsjaur," Linkoping University, Sweden, LiTH-ISY-R-1476, 1993.

31. Foreman, B., "Infrared Communication in PATH," in the Proc. of the PATH Short Course Notes, Berkeley, CA, 1994.

32. Park, Kyung S. "Human Reliability: analysis, prediction, and prevention of human errors", Elsevier, 1987

33. Kogure G., Katahara S., Aoki M., "Iris Motion and Blink Detection using video image sequence", Seikei University, Japan, Proceedings of the 26th ISATA International Symposium on Automotive Technology and Automation, p 375, 1993.

34. Wierwille W.W., Casali, J.G. and Repa, B.S., "Driver Steering Reaction Time to Abrupt-Onset Crosswinds, as Measured in a Moving-Base Driving Simulator," Human Factors, Volume 25, Issue 1, 103-116, 1983.

35. Shimizu, Y. and Kawai, T., "Development of Electric Power Steering," 1991.

36. Lee, A.Y., "Vehicle Stability Augmentation Systems Design using Parameter Optimization," General Motors Research Laboratories, Research Publication, GMR-6166, 1988.

37. Baron, S., "Pilot Control, " In Human Factors in Aviation, edited by Earl L. Wiener and David C. Nagel, 347-385, San Diego: Academic Press, Inc., 1988.

38. Begault, D.R., "Head-up Auditory Displays for Traffic Collision Avoidance System Advisories: A Preliminary Investigation," Human Factors, Volume 35, Issue 4, 707-717, 1993.

39. Limpert, R., Motor Vehicle Accident Reconstruction and Cause Analysis, Third Edition, Vol. Charlottesville, Va.: Michie Company, 1989.

40. Altan, O.D., Craig, D.B., Litkouhi, B.B., and Oberdier, L.M., "LANETRAK: A Vision-based Automatic Vehicle Steering System," General Motors Research, Research Publication, GMR-7835, 1992.

41. Heller, M. and Huie, M., "Vehicle Lateral Guidance using Vision, Passive Wire and Radar Sensors," in the Proc. of the IEEE-IEE Vehicle Navigation & Information Systems (VNIS'93) Conference, Ottawa, 505-508, 1993.

42. Peng, H., Zhang, W.-B., Shladover, S., Tomizuka, M., and Arai, A., "Magnetic Marker Based Lane Keeping: A Robustness Experimental Study," Society of Automotive Engineers, Issue Paper Number 930556, 127-132, 1993.

43. Tribe, R., Conlong, R. and Prynne, K., "Collision Warning," in the Proc. of the Autotech '93, Prometheus-Future Systems, 1993.

44. Kao, W.-W., "Integration of GPS and Dead-Reckoning Navigation Systems," in the Proc. of the Vehicle Navigation and Information Systems (VNIS'91), Dearborn, MI, SAE International, 635-643, 1991.

45. Tsuji, H., Maeda, H., Shibata, A., and Morisue, F., "Evaluation of Location System Combining a GPS Receiver with Inertial Sensor," in the Proc. of the Vehicle Navigation & Information Systems (VNIS '91), Dearborn, MI, SAE International, 645-649, 1991.

46. Woodson, W.E., Tillman, B. and Tillman, P., Human Factors Design Handbook, New York: McGraw-Hill, 1991.

APPENDIX A. RELIABILITY AND SAFETY ANALYSIS: THE FMEA APPROACH.

In this Appendix we present the notation and basic concepts of reliability and safety analysis that we employed in our study of reliability of the proposed five ERSCs.

A1. Definitions

Availability:

The availability of a system as a function of time, *A(t)*, is the probability that the system is operational at the instant of time, *t*. If the limit of this function exists as *t* goes to infinity, it expresses the expected fraction of time that the system is available to perform as intended.

Activities such as preventive maintenance and repair reduce the time that the system is available to the user. Availability is typically used as a figure of merit in systems in which service can be delayed or denied for short periods without serious consequences.

Reliability:

The reliability of a system as a function of time, *R(t)*, is the conditional probability that the system has survived the interval [0,*t*], given that it was operational at time *t*=0. Reliability is used to describe systems in which repair cannot take place (such as a satellite in orbit), or the system is serving a critical function and service cannot be delayed or lost even for the duration of a repair, or the repair is prohibitively expensive.

In general, it is more difficult to build a highly reliable system than a highly available one because of the more stringent requirements imposed by the reliability definition. An even more stringent definition than *R(t)*, sometimes used in aerospace applications, is the maximum number of failures, anywhere in the system, that the system can tolerate and still function correctly.

A2. Categories of faults and failures

Failure: Absence of expected action or performance. Also used to describe a physical change in the state of hardware.

Fault: Erroneous state of the system, either hardware or software, resulting from failure of components, physical interference from the environment, operator error or incorrect design.

Malfunction: Manifestation of a fault in the operation of the system. The malfunction may occur some distance from the fault site.

Permanent: Describes a failure, fault or malfunction that is continuous and stable. In mechanical systems and computer hardware, permanent failure reflects an irreversible physical change. The word *hard* may be used interchangeably with *permanent*.

Intermittent: Describes a fault or malfunction that is only occasionally present due to unstable hardware or software or due to varying conditions of a mechanical component. An intermittent problem may manifest itself randomly or as a function of load or activity.

Transient: Describes a fault or malfunction resulting from temporary environmental conditions. (Such as extreme environmental conditions.) The distinction from intermittent faults is sometimes difficult.

A permanent failure may lead to a permanent fault. Intermittent faults can be caused by unstable, marginally stable, or incorrect designs. Environmental conditions can lead to transient faults.

A3. Methods for Failure Analysis

The reliability and availability of a system is improved if the number of potential failures and their effects on the functionality of the system is reduced. Therefore, in order to improve reliability we first need to identify potential failures and understand their origin and effects on the performance of the system. Once the system is defined and its basic functions and components are identified one can start thinking about possible failure modes and their effects. Several systematic methods have been developed that aid this thought process. Below we give a summary of some of the most popular methods:

a. Failure Modes and Effects Analysis (FMEA)

FMEA is a systematic approach that employs a tabular method to aid the thought process for identifying potential failure modes and their effects.

b. Fault Tree Analysis (FTA)

FTA is a deductive analytical technique that uses a graphical "tree" to show cause-effect relationships between a single failure and the various contributing causes. The tree shows the logical branches from the single failure at the top of the tree, to the root cause(s) at the bottom of the tree.

c. Cause and Effect Diagrams

A Cause and Effect Diagram is a deductive analytical technique that uses a graphical "fishbone" to show the Cause-Effect relationships between a failure and the various contributing causes. The failure is shown on the right side of the fishbone chart and the major causes are listed to the left.

d. Failure Mode Analysis (FMA)

FMA is a discipline systematic approach to quantify the failure modes, failure rate, and root causes of known failures. It is based upon historical information including warranty data, field data, service data, and/or process data.

The above methods are used separately or to complement each other depending on the application. In our study we concentrate on the FMEA approach used by most engineers in the automotive industry. A detailed description of the FMEA approach is presented below.

A4. The FMEA Approach

A failure analysis can be done at the system level, design level or process level. The failure analysis done at the system level helps select the optimum system design alternatives.

The System Failure Mode Analysis is used to analyze Systems and subsystems in the early concept or design stages. Therefore it focuses on potential failure modes associated with the functions performed by a System, and includes any interaction of the system with any other systems or subsystems.

The Design Failure Mode Analysis is used to analyze products before they are ready for production. Therefore it focuses on potential failure modes of products or hardware designs, caused by design errors or design deficiencies.

The process Failure Mode Analysis is used to analyze manufacturing and assembly processes. Therefore it focuses on potential product failure modes caused by manufacturing or assembly process deficiencies.

In our approach the system FMEA is the appropriate one to use since we are in the early stage of design.

Benefits of an FMEA

By ranking the failure mode occurrence probabilities (even when the exact probabilities are not known or available) we can estimate whether the chosen system design alternative can achieve its reliability target. Another benefit is that the analysis identifies potential failure modes caused by system interaction with other systems and subsystems.

A key result of the FMEA analysis is that for every single failure mode we compute a risk priority index. The procedure of computing and associating a priority number to each failure mode provides one of the primary benefits of the process. The goal of the analysis is to identify the components or subsystems whose design needs to be changed or improved upon to increase their reliability and safety of operation. In a large and complex system it would not be possible to redesign every little part. There is not enough resources, time, engineers and money to do this. For that reason, the components that are most critical need to be scientifically singled out. A thorough FMEA done by experienced people can accomplish this task and find which components and which failure modes should be tackled first and improved upon. It can also help determine if hardware redundancy is required. Furthermore, the FMEA forms the basis for system failure diagnostic procedures and initiates the development of system fault management techniques.

The FMEA tables

There are several ways that the Failure Modes and Effects Analysis can be presented and that includes unformatted text. Typically though the analysis is presented in a table format that facilitates both the analysis phase and the usability of the results.

Each row in the FMEA table presents a single failure mode and attempts to associate a priority index to it. In doing that we have to consider the potential effects of that particular failure, weighted by the relative severity. We also must consider the potential causes of that failure, weighted by their relative probability of occurrence. Therefore the risk priority number (RPN) for a particular failure mode is the product of the Severity and Occurrence ratings. RPN numbers themselves have no value or meaning. RPNs are used only to rank the potential system design deficiencies. Table 8 shows the FMEA table that we use in this study.

Table 8: The FMEA table.

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN

The first column lists the system function, which is the design intent or purpose of the system. Functions may also include safety requirements or general system constraints.

The second column lists the potential failure mode. Typically a failure mode would be the loss of the corresponding system function. Sometimes it can also be expressed as the negative of the system function.

The third column lists the potential effects of the failure. A potential effect of a failure is the consequence of a system failure mode in terms of its impact on system operation and on other subsystems. For a system, the failure effect is generally the manner in which the system user observes or experiences the system failure mode.

The fourth column describes the severity of the effect. Severity is a rating of the seriousness of the effect of the potential system failure mode. Severity applies only to the effect of a failure mode. The severity ratings are explained in table 9.

Table 9: Severity rating for system level FMEA

Effect	Rating	Criteria
Negligible	1	Negligible Effect
Very Slight	2	Very slight effect on vehicle or System performance
Slight	3	Slight effect on vehicle or System performance
Minor	4	Minor effect on vehicle or System performance
Moderate	5	Moderate effect on vehicle or System performance
Significant	6	Vehicle performance degraded but operable and safe Partial loss of System function, but operable
Major	7	Vehicle performance severely affected but drivable and safe. System function impaired
Serious	8	Vehicle inoperable, but safe. System inoperable
Very Serious	9	Potential safety related vehicle failure Able to stop without mishap. Gradual failure.
Hazardous	10	Potentially hazardous failure. Safety related, sudden failure

The fifth column lists the potential causes of failure. The cause of a system failure mode is the system design deficiency that results in the failure mode. The system block diagram has to be referred to help identify causes of potential system failure modes. The block diagram shows the major functional elements and subsystems required to perform the system function. In analyzing each element of the block diagram we must include the inputs and outputs in addition to the element itself. An element failure mode will be identified as the inability of the element to perform its intended function. A system failure mode can be caused by one or more element failure modes or by the interaction between elements or the interaction between an element with other systems or the environment.

Analyzing the system interfaces and interactions is very important and helps identify potential system failure modes caused by these interactions. In addition to the block diagram elements, human factors are an important source of causes of potential failure modes at the system level and must be included in the analysis.

Typical causes of failure modes include the following:

- Premature operation

- Failure to start at the prescribed time

- Failure to stop at the prescribed time

- Intermittent operation

- Loss of output to function during operation

- Degradation of output or operational capability

- Strategic or logic software errors

- Unwanted interactions with other elements, systems or the environment

The sixth column describes the occurrence rating. The occurrence is a rating corresponding to the rate at which a cause and its resultant failure mode could occur over the lifetime of the system. Assuming single point failures and assuming that the causes of a failure mode are independent leads to that if a cause occurs a failure mode will occur. The occurrence rating is not affected by the ability to detect and correct a failure mode. The occurrence ratings are explained in table 10.

Table 10: Occurrence rating for system level FMEA

Occurrence	Rating	Criteria	Failure Rate
Almost impossible	1	Failure unlikely. History of similar designs shows no failures	< 1 in 1500000
Remote	2	Very few failures likely	1 in 150000
Very Slight	3	Few failures likely	1 in 2000
Slight	4	Infrequent failures likely	
Low	5	Some failures likely	1 in 400
Medium	6	Regular failures likely	1 in 80
Moderately High	7	Frequent failures likely	1 in 20
High	8	Many failures likely	1 in 7
Very High	9	Failures very likely	1 in 3
Almost Certain	10	Failures almost certain to occur. History of similar designs shows many failures.	> 1 in 3

The seventh column lists design requirements and recommendations. These are the system design approaches that need to be taken to reduce the Severity or the Occurrence rating or both. The intent is to eliminate system design deficiencies and eliminate potential system failure modes. The recommended

actions will generally seek to eliminate or reduce the causes of system failure modes, control or manage system failure modes and mitigate the effects of system failure modes. Design and Diagnostic requirements, and design actions can be listed. Typical system design actions may include the following:

- Add redundant subsystems that allow the system to continue operating at the same functional level if a subsystem fails.

- Provide other modes of system operation that allow system operation to continue at the same or at a degraded functional level.

- Add built-in devices to alert the operator to take action that will prevent or get past a system failure mode or mitigate its effect.

The eighth column has the computed Risk Priority Number (RPN). The RPN is the product of the Severity and Occurrence ratings. RPN numbers themselves have no value or meaning. RPNs are used only to rank the potential System design deficiencies. The criticality of a failure mode is evaluated by considering all factors such as severity, occurrence and RPN.

The mapping of the criticality ratings of the FMEA to the ratings developed during the Vehicle Operational Mini-Conference held in July 1994 at the University of Southern California are shown in table 11.

Table 11: Mapping of severity ratings.

FMEA Severity Rating	Equivalent Safety Criticality Rating From Mini-Conference
1	1 No Safety Impact
2	1 No Safety Impact
3	1 No Safety Impact
4	1 No Safety Impact
5	2 Negligible Collision
6	2 Negligible Collision
7	2 Negligible Collision
8	2 Negligible Collision
9	3 Minor Collision
10	4 Major Damage
10	5 Multiple deaths in multiple vehicles

Appendix B: FMEA Tables for each ERSC

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H1.1 Speed and Headway Maintenance (SHM)							
F1.1 Maintain cruise speed.	F1.1.1 Loss of speed maintenance function.	F1.1.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Driver may be annoyed. Traffic rules may be violated.	6	F1.1.1.1 Speed sensor gives erroneous or variable readings. (0% to 10% steady state error is typical of speed sensors. Sudden variation is rare)	2	F1.1.1.1 Diagnostics and built in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall return to manual control and provide warning to the driver.	12
		F1.1.1.2 As above.	6	F1.1.1.2 Controller electronics or software failure.	2	F1.1.1.2 The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall return to manual control and provide warning to the driver.	12
		F1.1.1.3 As above.	6	F1.1.1.3 Throttle actuator failure.	3	F1.1.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	18

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.1.1.4 Vehicle accelerates above desired speed or decelerates below desired speed. Driver may panic. Speed limit may be exceeded.	8	F1.1.1.4 Brake actuator failure (brake cannot be applied or brake is continuously applied)	3	F1.1.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	24
	F1.1.2 System switches to headway maintenance in the absence of valid target.	F1.1.2.1 Sudden change in speed. Unnecessary braking and rear-end collision warning is activated. Driver may panic and his steering performance may be affected.	8	F1.1.2.1 Ranging sensor detects an invalid target within the default headway	6	F1.1.2.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	48
F1.2 Maintain target speed.	F1.2.1 Vehicle cannot maintain target speed as commanded by the roadway.	F1.2.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Safety and efficiency are compromised.	6	F1.2.1.1 Speed sensor gives erroneous readings. (0% to 10% steady state error is typical of speed sensors. Sudden variation is rare)	2	F1.2.1.1 Diagnostics and built in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall return to manual control and provide warning to the driver.	12

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.2.1.2 Same as in F1.2.1.1	6	F1.2.1.2 Controller electronics or software failure.	2	F1.2.1.2 The system must have supervisory elements (in hardware or software) or adequate redundancies. When a controller malfunction is detected, system shall return to manual control and provide warning to the driver.	12
		F1.2.1.3 Same as in F1.2.1.1	6	F1.2.1.3 Throttle actuator failure.	3	F1.2.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	18
		F1.2.1.4 Same as in F1.2.1.1	8	F1.2.1.4 Brake actuator failure.	3	F1.2.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	24

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.2.1.5 Vehicle travels too fast which is unsafe or too slow which reduces capacity.	6	F1.2.1.5 Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication.	3	F1.2.1.5 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. I The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.) When a communication malfunction is detected the driver shall be notified.	18
		F1.2.1.6 As above	6	F1.2.1.6 Loss of target speed information due to receiver malfunction	3	F1.2.1.6 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.	18

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F1.2.2 System switches to headway maintenance in the absence of valid target.	F1.2.2 Sudden change in speed. Unnecessary braking and rear-end collision warning is activated. Driver may panic and his steering control may be affected.	8	F1.2.2 Ranging sensor detects an invalid target within the default headway	6	F1.2.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	48
F1.3 Maintain headway	F1.3 Cannot maintain headway	F1.3.1 SHM stops operating. Headway may become too large or too small, unexpectedly. Rear-end collision is possible.	10	F1.3.1 Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability.	6	F1.3.1 System must be able to detect and accommodate for an intermittent sensor failure. System software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and the driver shall be asked to resume control. Redundant ranging sensor, not subject to common mode failures, with appropriate logic may be required.	60

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.3.2 SHM switches to speed maintenance mode even if a valid target exists. Rear-end collision is possible if driver is not attentive.	10	F1.3.2 Sensor loses target due to road curvature or insufficient target reflectiveness.	7	F1.3.2 The sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Driver must be notified when target is ambiguous and cannot be followed reliably and possibly be given the option to resume manual control. Sensor redundancy might be needed	70
		F1.3.3 SHM accelerates or decelerates vehicle unexpectedly . The RECW may be activated. The driver may get annoyed, panic and his/her steering performance may be affected.	9	F1.3.3 Ranging sensor has locked on invalid target.	7	F1.3.3 The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. System must distinguish vehicles moving to adjacent lanes and around curves in the same lane. A redundant ranging sensor not subject to same failure with appropriate logic may be required.	63

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.3.4 System may fail to maintain selected headway, and headway may become too small. The RECW may be activated.	9	F1.3.4 Brake actuator failure. (Or intermittent failure to respond)	3	F1.3.4 System must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	27
		F1.3.5 System may fail to maintain selected headway, and headway may become too large or the system uses braking in an effort to maintain desired headway. In some cases the RECW may get activated. The driver may get annoyed, panic and his/her steering performance may be affected	6	F1.3.5 Throttle actuator failure.	3	F1.3.5 System must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	18
		F1.3.6 SHM disengages. System reverts to manual mode, unexpectedly. Driver may be annoyed. Potential rear-end collision.	9	F1.3.6 Controller electronics or software failure	2	F1.3.6 The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall return to manual control and provide warning to the driver.	18

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.3.7 SHM accelerates or decelerates vehicle unexpectedly. Headway becomes too small or too large. The RECW may have inappropriate response. If the driver is not attentive collision with the leading vehicle is possible.	10	F1.3.7 Ranging sensor gives erroneous readings.	6	F1.3.7 System must be able to discriminate against gross errors from the ranging sensor. The sensor and the controller must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. System shall provide warning and return control to the driver in case of a detected sensor failure. Sensor redundancy and appropriate logic may be needed to totally eliminate the possibility of undetected errors.	60
F1.4 Switch from maintaining speed to maintaining headway.	F1.4 Failure to switch mode. Stay at cruising (maintaining speed) mode even when a valid target exists.	F1.4.1 Headway may become too small. If the driver is not attentive collision with the leading vehicle 0r obstacle is possible.	10	F1.4.1 Ranging sensor fails to detect a valid target.	6	F1.4.1 System must be able to discriminate between valid and invalid targets. A Redundant ranging sensor not subject to common mode failures must be used with appropriate diagnostics.	60

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.4.2 The headway may become too small. The RECW may get activated and the driver may have to override the system.	9	F1.4.2 Hardware or software failure of the SHM.	2	F1.4.2 System must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware and software) or adequate redundancies. System shall provide warning and return control to the driver in case of failure.	18
F1.5 Switch from headway maintenance to speed maintenance.	F1.5 Failure to switch to speed maintenance mode when the target moves out of the lane and becomes unsuitable to follow.	F1.5.1 Vehicle speed varies instead of switching to speed maintenance mode in the absence of a valid target in the same lane. The RECW may get activated. Driver may get annoyed, panic and his/her steering performance may be affected.	8	F1.5.1 Target became unsuitable to follow by moving to adjacent lane or by following an exit ramp. There is no other valid target. Ranging sensor locks on the original target even after it becomes unsuitable to follow or locks on another target which is not a valid target.	6	F1.5.1 System must be able to discriminate between valid and invalid targets. A Redundant ranging sensor not subject to common mode failures must be used with appropriate diagnostics.	48

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.5.2 SHM switches to manual mode instead of switching to speed maintenance mode. Driver may get annoyed.	5	F1.5.2 Hardware or software failure of the SHM	2	F1.5.2 System must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. System shall provide warning and return control to the driver in case of a detected failure	10
F1.6 Switch from maintaining cruise speed to maintaining a target speed commanded by the roadway.	F1.6.1 Failure to respond to the roadway target speed command	F1.6.1.1 SHM fails to adjust speed as commanded by the roadway. Speed may be higher than the conditions permit or lower than optimal. Efficiency and safety are compromised.	6	F1.6.1.1 Loss of target speed information due to receiver malfunction.	4	F1.6.1.1 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.	24

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.6.1.2 SHM maintains current speed which may be higher than conditions permit or lower than optimal. Efficiency and safety are compromised.	6	F1.6.1.2 Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication.	3	F1.6.1.2 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.) When a communication malfunction is detected, system shall notify the driver and return to a default cruise speed.	18
	F1.6.2.1 System switches to headway maintenance in the absence of valid target.	F1.6.2.1 Sudden change in speed. Unnecessary braking and rear-end collision warning is activated. Driver may panic and his steering control may be affected.	6	F1.6.2.1 Ranging sensor detects an invalid target within the default headway.	6	F.1.6.2.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	36

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F1.6.2 Switching to headway maintenance instead.	F1.6.2 Brake may be unnecessarily applied. Vehicle may suddenly change speed. Rear-end collision warning may be activated. Driver may be panic and driver's steering capability may be affected.	8	F1.6.2 Ranging sensor detects an invalid target.	6	F1.6.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures may be required.	48
F1.7 Enable SHM	F1.7 SHM cannot be enabled	F1.7.1 SHM is not available to the driver. Vehicle can only be operated in manual mode.	6	F1.7.1 Electronic malfunction.	2	F1.7.1 The controller electronics must be sufficiently reliable. Diagnostics must be performed even when the SHM is in the standby mode. The driver shall be notified if there is any malfunction detected.	12
F1.8 Disable SHM	F1.8 SHM cannot be disabled.	F1.8.1 Driver cannot override the SHM controller. The vehicle accelerates or decelerates or maintains speed and the driver can only use braking to control the vehicle. Very annoying to the driver and under certain conditions driver may panic and cause a collision.	9	F1.8.1 Electronic or software malfunction.	2	F1.8.1 The controller electronics must be sufficiently reliable. There must be redundant means of disabling the SHM	18

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H1.2 Rear-end Collision Warning							
F1.9 Warn the driver.	F1.9.1 Failure to provide rear-end collision warning.	F1.9.1.1 Headway may become too short and unsafe. Rear-end collision is possible if the driver relies too much on the warning instead of his/her sight.	9	F1.9.1.1 Ranging sensor provides incorrect information.	6	F1.9.1.1 The ranging sensor and the controller must be very reliable. Redundant ranging sensor not subject to common failures together with the appropriate logic may be necessary.	54
		F1.9.1.2 Same as above	9	F1.9.2 Incorrect calculation of TTC (Time To Collision) due to wrong estimate of braking capabilities of vehicle and/or preceding one.	6	F1.9.2. System must perform tests of reasonableness of the estimated braking capabilities. System must be designed to tolerate some inaccuracies in the estimates of braking capabilities	54
		F1.9.3 Same as above.	9	F1.9.1.3 The threshold of warning is set too large.	5	F1.9.1.3 The driver shall be able to select a headway that he/she is comfortable with. The default threshold must be set to a low level.	45
		F1.9.1.4 Same as above.	9	F1.9.1.4 Warning device failure.	3	F1.9.1.4 Warning device must be reliable. Redundant warning delivery methods must be used.	27

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.9.1.5 Same as above	9	F1.9.1.5 Preceding vehicle's braking information is corrupted or lost during communication, due to noise, interference or blocking of communication.	3	F1.9.1.5 System must have diagnostic programs to test for reasonableness on received braking information data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.)	27
		F1.9.1.6 Vehicle cannot identify an emergency stop fast enough. Delayed rear-end collision warning. Collision is possible if driver relies too much on the warning and is not attentive.	9	F1.9.1.6 Vehicle cannot identify an emergency stop fast enough. Delayed rear-end collision warning. Collision is possible if driver relies too much on the warning and is not attentive.	3	F1.9.1.6 System should have diagnostic programs to monitor the operation of the communication devices. System should be able to accommodate temporary loss of communication. When a malfunction is detected, the transmitter and/or a backup transmitter should notify vehicles behind to increase headway by transmitting a special message.	27
	F1.9.2 False warnings	F1.9.2 Driver may be distracted and driver's confidence may be reduced.	5	F1.9.2.1 Ranging sensor provides incorrect information.	6	F1.9.2.1 The ranging sensor and must be very reliable. Redundant ranging sensor not subject to common failures together with the appropriate logic may be necessary.	30

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.9.2.2 Same as above.	5	F1.9.2.2 Incorrect calculation of TTC due to wrong estimate of braking capabilities of vehicle and/or preceding vehicle.	6	F1.9.2.2 System must perform tests of reasonableness of the estimated braking capabilities. System must be designed to tolerate some inaccuracies in the estimates of braking capabilities.	30
		F1.9.2.3 Same as above.	5	F1.9.2.3 The threshold of warning is set too low.	5	F1.9.2.3 The driver shall be able to select a headway that he/she is comfortable with. The default threshold shall be set to a low level.	25
		F1.9.2.4 Same as above.	5	F1.9.2.4 Preceding vehicle's braking information is corrupted or lost during communication, due to noise, interference or blocking of communication.	3	F1.9.2.4 System must have diagnostic programs to test for reasonableness on received braking information data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.)	15

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	a. Design Requirements b. Recommendations	RPN
F1.10 Enable Rear End Collision Warning (RECW)	F1.10 RECW cannot be enabled	F1.10.1 Driver does not receive warning when a Read End Collision is imminent.	6	F1.10.1 Electronics failure	2	F1.10.1 The controller electronics must be sufficiently reliable and must have supervisory elements in hardware. Driver shall be notified about the RECW operating mode.	12
F1.11 Disable RECW	F1.11 RECW cannot be disabled	F1.11.1 Driver cannot avoid receiving warnings and may get annoyed and distracted.	3	F1.11.1 Electronics failure	2	F1.11.1 The controller electronics must be sufficiently reliable and must have supervisory elements in hardware. The warning device shall be such that the driver can turn it off easily in case he/she cannot disable the RECW.	6
F1.12 Adjust Threshold	F1.12 Threshold cannot be adjusted.	F1.12.1 The RECW function may be lost if the threshold is set too high. Driver may be uncomfortable with the system selected headway threshold, and may be annoyed if the threshold is set too low and cannot be changed.	7	F1.12.1 Electronics failure	2	F1.12.1 The controller electronics must be sufficiently reliable. The threshold shall default to a low level when the RECW is enabled for the first time.	14

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	a. Design Requirements b. Recommendations	RPN
F1.13 Communicate braking capabilities and intentions to trailing vehicle.	F1.13 Failure to communicate correct braking capabilities and intentions to trailing vehicle.	F1.13.1 Trailing vehicle cannot identify an emergency stop fast enough. Delayed rear-end collision warning to the driver of trailing vehicle. Collision is possible if driver relies too much on the warning and he/she is not attentive.	9	F1.13.1 Sensor and/or diagnostics failure	6	F1.13.1 The vehicle must have reliable sensors and diagnostics for estimating braking capabilities and braking levels. The system must have diagnostics to monitor the performance of sensors and detect malfunctions. The trailing vehicle shall be notified of the inability of vehicle to accurately estimate braking capabilities and intentions. The driver shall be notified and possibly asked to exit lane.	54
		F1.13.2 Same as above.	9	F1.13.2 Transmitter failure.	3	F1.13.2 System must be able to detect transmitter failures, by employing supervisory elements in hardware, adjacent to the transmitter. The trailing vehicle shall be notified of the inability of vehicle to accurately estimate braking capabilities and intentions. The driver shall be notified and possibly asked to exit lane.	27

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H1.3 Blind-spot warning							
F1.14 Warn Driver.	F1.14.1 Unable to provide warning	F1.14.1.1 Safety is compromised during lane changing if driver relies on the warning too much.	7	F1.14.1.1 Blind spot sensor failure.	5	F1.14.1.1 Supervisory elements must monitor the output of the sensor for reasonableness and consistency. The driver shall be notified when a malfunction is detected.	35
		F1.14.1.2 Same as above.	7	F1.14.1.2 Electronics failure or software failure.	2	F1.14.1.2 Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.	14
		F1.14.1.3 Same as above.	7	F1.14.1.3 Threshold has been set too high.	4	F1.14.1.3 The default threshold must be set to a low level. The driver shall be aware of the lack of warnings due to the high threshold setting.	28
		F1.14.1.4 Same as above.	7	F1.14.1.4 Warning delivery device failure.	2	F1.14.1.4 Warning device must be reliable. Redundant warning delivery methods shall be used.	14

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F1.14.2 False warnings.	F1.14.2.1 There may be too many false alarms which distract the driver and reduce his/her confidence level.	5	F1.14.2.1 Blind spot sensor gives incorrect reading.	5	F1.14.2.1 Supervisory elements in hardware and software must be used to monitor the sensor. The driver shall be notified when a malfunction is detected.	25
		F1.14.2.2 Same as above.	5	F1.14.2.2 Electronics failure or software failure.	2	F1.14.2.2 Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.	10
		F1.14.2.3 Same as above.	5	F1.14.2.3 Threshold has been set too low.	4	F1.14.2.3 The driver shall be able to select a threshold level that he/she is comfortable with. The default threshold must be set to a level appropriate for typical conditions.	20

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F1.14.2.4 Same as above.	5	F1.14.2.4 System fails to sense correct intentions of driver to change lanes	7	F1.14.2.4 A reliable method must be used to sense correct intentions of driver to change lanes or the system must be redesigned to eliminate the necessity of sensing driver's intentions.	35
F1.15 Enable Blind Spot Warning (BSW)	F1.15 BSW cannot be enabled.	F1.15.1 Driver does not receive warning when a lateral collision is imminent. Safety is degraded.	6	F1.15.1 Electronics failure	2	F1.15.1 The controller electronics must be sufficiently reliable and must have supervisory elements in hardware and software. Driver shall be notified about changes in the BSW operating mode.	12
F1.16 Disable BSW	F1.16 BSW cannot be disabled	F1.16.1 Driver cannot avoid receiving warnings, may experience annoyance or discomfort.	3	F1.16.1 Electronics failure	2	F1.16.1 The controller electronics must be sufficiently reliable. There shall be redundant methods to disable the BSW.	6
F1.17 Adjust BSW Threshold.	F1.17 BSW Threshold cannot be adjusted.	F1.17.1 Driver may be uncomfortable with the currently selected threshold or the threshold may be inappropriate for the prevailing conditions.	6	F1.17.1 Electronics failure	2	F1.17.1 The controller electronics must be sufficiently reliable. The threshold setting shall default to a low level when the BSW is enabled for the first time. The driver shall be able to read and verify the selected threshold setting.	12

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H1.4 Driver Vehicle Roadway Interface							
F1.18 Check-in	F1.18 Failure of check-in function.	F1.18.1 Vehicle is operating in the dedicated lane even though it should not.	8	F1.18.1 On-board diagnostics failed to detect a fault in major functions of the vehicle.	3	F1.18.1 Diagnostics algorithms must be robust and highly reliable. Roadway shall be able to detect an unfit vehicle operating in the dedicated lane.	24
		F1.18.2 Same as above.	8	F1.18.2 Driver ignores the results of on-board diagnostics.	3	F1.18.2 Roadway must be able to identify an unfit vehicle operating in the dedicated lane. Traffic rules and regulations must be used to deter the driver from violating the rules.	24
		F1.18.3 Vehicle is not allowed to enter the lane, even though it is fit.	5	F1.18.3 On-board diagnostics made a wrong decision about a component or function that was not at fault.	2	F1.18.3 On board diagnostics must be highly reliable. Redundancies and supervisory elements must be considered for improving reliability.	10

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F1.19 Enter the lane	F1.19 Vehicle cannot enter the lane.	F1.19.1 Disturbance in the transition lane or entrance to the dedicated lane. Driver may get annoyed. Vehicle restricted from operating in the dedicated lane.	5	F1.19.1 Dedicated lane is congested or driver is not able to merge due to high speed and/or small headways in dedicated lane or driver does not have the required skills.	4	F1.18.1 Roadway must be able to enforce lower speeds and larger headway near the entry points. Driver skills for lane merging shall be tested as part of the licensing procedure.	20
F1.20 Respond to BSW and RECW.	F1.20 Driver fails to respond to BSW and RECW.	F1.20.1 Vehicle and system safety is degraded. Potentially dangerous situations and collisions may result.	9	F1.20.1 Driver ignores warning unintentionally or becomes confused.	6	F1.20.1 The warnings shall be very clear and unambiguous to the driver. Driver interface shall be as simple as possible.	54
		F1.20.2 Same as above.	8	F1.20.2 Driver ignores warning intentionally due to high false alarm rate.	6	F1.20.2 False alarm rate must be very low. Warning signals shall be easily distinguishable from each other. Warning threshold shall be adjustable by the driver. Driver interface shall appear simple to the driver.	48
F1.21 Respond to traffic information	F1.21 Driver fails to respond to traffic information.	F1.21.1 Roadway efficiency and vehicle safety is degraded.	4	F1.21.1 Driver capability is impaired or traffic information is unclear or confusing	5	F1.21.1 Roadway traffic information shall be clear and brief.	20

Table 12: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-1)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F1.22 Exit the lane	F1.22.1 Driver can not exit the dedicated lane.	F1.22.1 Vehicle has to remain in the dedicated lane. System performance is degraded.	4	F1.22.1 Congestion in manual lane or the transition lane.	5	F1.22.1 Dedicated transition lane or some form of regulation such as "yield to auto lane" must be implemented to ensure easy exit even when traffic congestion happens in the manual lane. Must warn the driver, of congestion ahead of time via traffic information communication.	20
	F1.22.2 Driver does not exit the dedicated lane and operates in manual mode.	F1.22.2 Vehicle remains in the dedicated lane. System performance is degraded. May violate traffic regulations and result in accidents.	4	F1.22.2 Driver fails to perform the necessary steering action.	5	F1.22.2 Law enforcement must be used when traffic rules are violated.	20
F1.23 Fall back to manual control	F1.23.1 System does not switch to manual mode.	F1.23.1 Vehicle may be under automatic control mode even after it should have switched to the manual mode. Safety may be compromised.	6	F1.23.1 Hardware or software failure.	4	F1.23.1 System shall have two independent ways to disable itself. The driver must be notified of the change of mode of operation. The driver shall have more than one way of disabling the system.	24
F1.24 Notify driver of mode of operation	F1.24 The system fails to notify driver of correct mode of operation	F1.24.1 Driver may get confused, become inattentive, get annoyed, panic. His/her steering performance may be affected.	9	F1.24.1 Electronic or software malfunction	2	F1.24.1 The electronics and software must be very reliable. Redundancies and diagnostics must be used to improve reliability.	18

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H2.1 Speed and Headway Maintenance and Rear-end Collision Avoidance.							
F2.1 Calculate safe headway	F2.1 Loss of ability to calculate correct value of safe headway	F2.1.1 Headway is set to the default value. Efficiency is affected.	6	F2.1.1 Detected malfunction or inability of the sensors to estimate the braking capabilities and intentions of the preceding vehicle and/or vehicle.	6	F2.1.1 The malfunction of sensors or gross inaccuracies in the estimation of the braking capabilities must be detected fast. The system must fall back to the default headway that takes into account the inaccuracies or malfunction of the sensors.	36
		F2.1.2 Headway is set to the default value. Efficiency is affected.	6	F2.1.2 Detected malfunction or loss of communication with preceding vehicle	6	F2.1.2 Diagnostics and built-in self tests must be used to guarantee a fast detection of the communication failures. When a malfunction occurs the headway must be automatically increased to the default safe level that takes into account the failure	36
		F2.1.3 Unsafe headway is used and rear-end collision is possible or a large headway is used and efficiency is affected	10	F2.1.3 Faulty or inaccurate measurements of braking capabilities of vehicle and/or preceding vehicle	6	F2.1.3 The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements must be monitored and taken into account in the calculation of the safe headway.	60

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.1.4 Unsafe headway is used and rear-end collision is possible or large headway is used and efficiency is affected.	10	F2.1.4 Incorrect braking capabilities and intentions is received through communication due to interference or noise corruption	6	F2.1.4 The measurements of braking capabilities of all vehicles must be accurate. The system must check the reasonableness of preceding vehicle's braking capability and take into account possible inaccuracies and inconsistencies in calculating the safe headway.	60
		F2.1.5 Headway is increased in order to maintain safety level. Efficiency is affected.	6	F2.1.5 Loss of communication with roadway and/or lack of headway recommendation	4	F2.1.5 System must be able to accommodate the lack of headway recommendation from roadway .	24
		F2.1.6 Headway is set to the default value if failure is detected . Efficiency is affected. If failure is not detected safety is affected due to possible use of an unsafe headway.	6	F2.1.6 Loss of braking data information from preceding vehicle due to receiver malfunction.	4	F2.1.6 System must have supervisory elements and diagnostics that monitor the functionality of the receiver and detect malfunctions. The malfunction of the receiver must be taken into account in calculating the safe headway.	24

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.2 Maintain cruise speed.	F2.2.1 Loss of speed maintenance function.	F2.2.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Driver may be annoyed. Traffic rules may be violated.	6	F2.2.1.1 Speed sensor gives erroneous or variable readings. (0% to 10% steady state error is typical of speed sensors. Sudden variation is rare)	2	F2.2.1.1 Diagnostics and built in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall return to manual control and provide warning to the driver.	12
		F2.2.1.2 As above.	6	F2.2.1.2 Controller electronics or software failure.	2	F2.2.1.2 The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall return to manual control and provide warning to the driver.	12
		F2.2.1.3 As above.	6	F2.2.1.3 Throttle actuator failure.	3	F2.2.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	18

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.2.1.4 Vehicle accelerates above desired speed or decelerates below desired speed. Driver may panic. Speed limit may be exceeded.	10	F2.2.1.4 Brake actuator failure (brake cannot be applied or brake is continuously applied)	3	F2.2.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	30
	F2.2.2 System switches to headway maintenance in the absence of valid target.	F2.2.2.1 Sudden change in speed. Unnecessary braking and rear-end collision warning is activated. Driver may panic and his steering performance may be affected.	8	F2.2.2.1 Ranging sensor detects an invalid target within the default headway	6	F2.2.2.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	48
F2.3 Maintain target speed.	F2.3.1 Vehicle cannot maintain target speed as commanded by the roadway.	F2.3.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Safety and efficiency are compromised.	6	F2.3.1.1 Speed sensor gives erroneous readings. (0% to 10% steady state error is typical of speed sensors. Sudden variation is rare)	2	F2.3.1.1 Diagnostics and built in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall return to manual control and provide warning to the driver.	12

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.3.1.2 Same as in F2.3.1.1	6	F2.3.1.2 Controller electronics or software failure.	2	F2.3.1.2 The system must have supervisory elements (in hardware or software) or adequate redundancies. When a controller malfunction is detected, system shall return to manual control and provide warning to the driver.	12
		F2.3.1.3 Same as in F2.3.1.1	6	F2.3.1.3 Throttle actuator failure.	3	F2.3.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	18
		F2.3.1.4 Same as in F2.3.1.1	10	F2.3.1.4 Brake actuator failure.	3	F2.3.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	30

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.3.1.5 Vehicle travels too fast which is unsafe or too slow which reduces capacity.	6	F2.3.1.5 Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication.	3	F2.3.1.5 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.) When a communication malfunction is detected the driver shall be notified.	18
		F2.3.1.6 Same as F2.2.1.5	6	F2.3.1.6 Loss of target speed information due to receiver malfunction	3	F2.3.1.6 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.	18

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F2.3.2 System switches to headway maintenance in the absence of valid target.	F2.3.2 Sudden change in speed. Unnecessary braking and RECA is activated. Driver may panic and his steering control may be affected.	8	F2.3.2 Ranging sensor detects an invalid target within the default headway	6	F2.3.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	48
F2.4 Maintain headway	F2.4 Cannot maintain headway	F2.4.1 SHM stops operating. Headway may become too large or too small, unexpectedly. Rear-end collision is possible.	10	F2.4.1 Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability.	6	F2.4.1 System must be able to detect and accommodate an intermittent sensor failure. System software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and the driver shall be given a warning to resume control. Redundant ranging sensors, not subject to common mode failures, with appropriate logic may be required.	60

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.4.2 SHM switches to speed maintenance mode even if a valid target exists. Rear-end collision is possible if driver is not attentive.	10	F2.4.2 Sensor loses target due to road curvature or insufficient target reflectiveness.	7	F2.4.2 The sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Vehicle shall slow down and the driver must be notified when target is ambiguous and cannot be followed reliably and possibly be given the option to resume manual control. Sensor redundancy may be needed to track targets around curves and minimize the possibility of interference.	70
		F2.4.3 SHM accelerates or decelerates vehicle unexpectedly . The RECA may be activated. The driver may get annoyed, panic and his/her steering performance may be affected if he/she gets confused with what the system is supposed to be doing.	9	F2.4.3 Ranging sensor has locked on an invalid target.	7	F2.4.3 The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. System must distinguish vehicles moving to adjacent lanes and around curves in the same lane. Redundant ranging sensors not subject to same failure mode with appropriate logic may be required.	63

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.4.4 System may fail to maintain selected headway. Rear-end collision is possible.	10	F2.4.4 Brake actuator failure. (Or intermittent failure to respond)	3	F2.4.4 System must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators that are not subject to common mode failures with appropriate logic are essential.	30
		F2.4.5 System may fail to maintain selected headway. Braking or the RECA function is used to avoid violating the minimum safe headway. Efficiency is compromised. The vehicle may have to exit the lane.	7	F2.4.5 Throttle actuator failure.	3	F2.4.5 The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs offer to monitor the throttle actuator. When an actuator malfunction is detected, system shall return to manual control and provide warning to the driver.	21

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.4.6 Headway may become too large or too small. The RECA may be activated. The driver may be required to resume control and drive the vehicle out of the lane. The driver's steering performance may be affected.	9	F2.4.6 Controller electronics or software failure.	2	F2.4.6. The system must have supervisory elements (in hardware and software) or adequate redundancies. System shall return control to the driver in case of failure by slowing down the vehicle and increasing headway.	18
		F2.4.7 SHM accelerates or decelerates vehicle unexpectedly. Headway becomes too small or too large. The RECA function may be turned on and off unexpectedly. Rear-end collision is possible.	10	F2.4.7 Ranging sensor gives erroneous readings.	4	F2.4.7 The system must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. The system must provide warning and return control to the driver in case of a detected sensor failure by reducing speed. Sensor redundancy may be needed to totally eliminate the possibility of undetected errors.	40

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.5 Switch from maintaining cruise speed to maintaining headway	F2.5 Failure to switch to maintaining headway even when a valid target exists.	F2.5.1 Headway may become too small without the RECA function been activated. Rear-end collision is possible.	10	F2.5.1 Ranging sensor fails to detect a valid target.	5	F2.5.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics. In case of sensor failure the system shall return control to the driver by slowing down the vehicle and providing warning.	50
		F2.5.2 Headway may become too large or too small. The RECA may be turned on and off in an effort to keep the headway within safe level. Driver may be annoyed and driver's steering performance may be affected.	7	F2.5.2 Hardware or software failure of the SHM.	2	F2.5.2 The system must have supervisory elements (in hardware or software) or adequate redundancies. System shall provide warning and return control to the driver in case of a detected failure by reducing speed and increasing headway to levels that are comfortable for the driver.	14

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.6 Switch from maintaining headway to maintaining cruise speed.	F2.6 Failure to switch to speed maintenance mode when the original target moves out of the lane and becomes unsuitable to follow, and no other valid target exists.	F2.6.1 Vehicle speed varies instead of being constant in the absence of a valid target. The RECA function may be activated unexpectedly. Driver may be annoyed and driver's steering performance may be affected.	7	F2.6.1 Ranging sensor locks on the original target or locks on another target which is invalid when the original target becomes unsuitable to follow.	6	F2.6.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	42
		F2.6.2 Vehicle speed varies instead of being constant in the absence of a valid target. The RECA function may be impaired or may be activated unexpectedly. The SHM may switch to manual mode instead of switching to speed maintenance mode. Driver may get annoyed.	6	F2.6.2 Hardware or software failure of the SHM	2	F2.6.2 System must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. System shall provide warning and return control to the driver in case of a detected failure	14

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.7 Switch from maintaining cruise speed to maintaining roadway commanded target speed.	F2.7.1 Failure to switch to maintaining roadway commanded target speed.	F2.7.1.1 System fails to adjust speed as commanded by the roadway. Speed may be higher than the conditions permit or lower than optimal. Efficiency and safety are compromised.	7	F2.7.1.1 Loss of target speed information input due to receiver malfunction.	3	F2.7.1.1 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to exit the lane.	21
		F2.7.1.2 Same as in F2.7.1.1	7	F2.7.1.2 Loss of roadway transmission capability or target speed is corrupted during communication	3	F2.7.1.2 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). The system must be able to accommodate momentary loss of roadway target speed command. When a communication malfunction is detected, system shall notify the driver and return to a default cruise speed.	21

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F2.7.2 Switching to headway maintenance instead.	F2.7.2 Brake may be unnecessarily applied. Vehicle may suddenly change speed. Rear-end collision avoidance may be activated. Driver may be panic and driver's steering capability may be affected.	7	F2.7.2 Ranging sensor detects an invalid target.	6	F2.7.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures may be required.	42
F2.8 Hard braking for rear-end collision avoidance.	F2.8.1 Failure to take action on time	F2.8.1.1 Rear-end collision	10	F2.8.1.1 Ranging sensor fails to provide signal or provides incorrect signal.	5	F2.8.1 The system must have redundant sensing inputs to reduce the probability of missing a target to essentially zero . If redundancy is lost, the system shall increase headway and reduce speed, warn the driver and revert to ERSC1 or to manual mode.	50
		F2.8.1.2 Originally calculated headway becomes unsafe. Rear-end collision is possible.	10	F2.8.1.2 Loss of communication of braking intentions of preceding vehicle	5	F2.8.1.2 A redundant method must be used to communicate the preceding vehicle's braking intention. The calculated safe headway must take into account momentary loss of vehicle to vehicle communication. If loss of communication is permanent, system shall take that into account in calculating the safe headway.	50

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.8.1.3 Rear-end collision	10	F2.8.1.3 Controller electronics or software failure	2	F2.8.1.3 The system must have supervisory elements in software and hardware and adequate redundancies. When a redundancy is lost, the system shall increase headway and reduce speed to comfortable levels and warn the driver to operate as in ERSC1 or manual mode.	20
		F2.8.1.4 Rear-end collision	10	F2.8.1.4 Brake actuator failure	3	F2.8.1.4 The system must have redundant braking actuators that are not subject to common mode failures and appropriate diagnostics that allow the fast detection and accommodation of failures without degrading the performance of the RECA function. When a redundant braking path fails the system shall return to ERSC1 or manual mode and warn the driver appropriately. The transition to ERSC1 or manual mode shall be done by first reducing speed and increasing headway to levels that are comfortable for the driver.	30

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.8.1.5 Rear end collision	10	F2.8.1.5 Calculated time to collision (TTC) is larger than actual TTC due to incorrect measurement of braking capabilities.	6	F2.8.1.5 TTC must be accurate and conservative in order to accommodate possible inaccuracies in measurements. Independent estimates of TTC based on independent measurements must be used.	60
		F2.8.1.6 The TTC is so short that a rear-end collision can not be avoided without steering.	10	F2.8.1.6 Ranging sensor switches from a valid target to another one with completely different operating status and braking capability e.g. preceding vehicle exits lane and next vehicle in lane is disabled.	3	F2.8.1.6 The system must be designed to account for such situations. Vehicle to vehicle communication may be used to notify trailing vehicle of condition ahead or the system is designed so that exiting from the lane is possible only at designated points where larger headways are imposed.	30
	F2.8.2 The RECA is activated unnecessarily.	F2.8.2 Driver may be annoyed and Driver's steering performance may be affected.	6	F2.8.2 Incorrect range is sensed or incorrect TTC is calculated.	4	F2.8.2.2 The system must minimize the number of faulty activations of the RECA function as much as possible. Independent ranging measurements and calculations of the TTC must be used.	24
F2.9 Enable the SHM and RECA	F2.9 SHM and RECA cannot be enabled	F2.9.1 SHM and RECA is not available to the driver. Vehicle can only be operated in manual mode.	7	F2.9.1 Electronic malfunction.	2	F2.9.1 The controller electronics must be sufficiently reliable. Diagnostics must be performed even when the SHM and RECA are in the standby mode. The driver shall be notified of any detected malfunctions.	14

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.10 Disable the SHM and RECA	F2.10.1 SHM and RECA cannot be disabled	F2.10.1 Driver cannot override the SHM controller and may panic, and driver's steering performance may be affected.	10	F2.10.1 Electronic malfunction.	2	F2.10.1 The controller electronics must be sufficiently reliable. The driver shall have redundant means of turning off the SHM and RECA. The switching off of the functions must follow the disabling procedure so that the driver is not put in a situation he/she cannot handle.	20
	F2.10.2 SHM and RECA are disabled without first reducing speed and increasing headway.	F2.10.2 Driver may be put in a situation of short headway and high speed that he/she cannot handle in case of emergencies. Collision is possible.	10	F2.10.2 Software failure or failure of the brake actuator	3	F2.10.2 The system must have redundancies in software and redundant braking actuator paths. The system must be designed to fall back to a default speed and headway in a reliable manner when a failure is detected before the SHM and RECA are disabled.	30
F2.11 Communicate braking capability and intention to trailing vehicle.	F2.11.1 Loss of communication with trailing vehicle	F2.11.1 If detected by trailing vehicle its headway may be increased in order to maintain safety level. Efficiency is affected. If undetected or detected too late the TTC of trailing vehicle may be too large leading to a possible collision	10	F2.11.1 Failure of transmitter	3	F2.11.1 The system must have supervisory elements to monitor the transmitter. Redundant transmitter may be necessary. If the transmitter fails permanently, the vehicle shall exit the lane.	30

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F2.11.2 Transmit incorrect braking capabilities or braking intention to trailing vehicle.	F2.11.2 Trailing vehicle may calculate and use unsafe headway, or may apply insufficient brake, leading to a possible rear-end collision.	10	F2.11.2 Faulty or inaccurate measurements of braking capabilities and/or braking intention	6	F2.11.2 The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements shall be monitored. Independent means for calculating braking capabilities must be employed.	60
F2.12 Speed control around curves	F2.12 Failure to adjust speed around curves.	F2.12.1 Vehicle goes out of control or driving comfort is seriously affected.	10	F2.12.1 Incorrect preview road data or incorrect steering angle information.	3	F2.12.1 There must be more than one source of preview data and steering angle information not subject to common mode failure.	30
		Same as F2.12.1	10	F2.12.2 Throttle and/or brake actuator failure.	3	F2.12.2 The system must use sensor and diagnostic programs to monitor the throttle and brake actuators. When a malfunction is detected the system shall slow down the vehicle and notify the driver.	30
		Same as F2.12.1	10	F2.12.3 Controller electronics and for software failure.	2	F2.2.1.2 The system must have supervisory elements or adequate redundancies. When a malfunction is detected system shall slow down the vehicle and notify the driver.	20

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H2.2 Blind-spot warning							
F2.13 Warn Driver.	F2.13.1 Unable to provide warning	F2.13.1.1 Safety is compromised during lane changing if driver relies on the warning too much.	7	F2.13.1.1 Blind spot sensor failure.	5	F2.13.1.1 Supervisory elements must monitor the output of the sensor for reasonableness and consistency. The driver shall be notified when a malfunction is detected.	35
		F2.13.1.2 Same as above.	7	F2.13.1.2 Electronics failure or software failure.	2	F2.13.1.2 Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.	14
		F2.13.1.3 Same as above.	7	F2.13.1.3 Threshold has been set too high.	4	F2.13.1.3 The default threshold must be set to a low level. The driver shall be given a warning when the threshold is set at a high level.	28
		F2.13.1.4 Same as above.	7	F2.13.1.4 Warning delivery device failure.	2	F2.13.1.4 Warning device must be reliable. Redundant warning delivery methods shall be used.	14

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F2.13.2 False warnings.	F2.13.2.1 There may be too many false alarms which distract the driver and reduce his/her confidence level.	5	F2.13.2.1 Blind spot sensor gives incorrect reading.	5	F2.13.2.1 Supervisory elements in hardware and software must be used to monitor the sensor. The driver shall be notified when a malfunction is detected.	25
		F2.13.2.2 Same as above.	5	F2.13.2.2 Electronics failure or software failure.	2	F2.13.2.2 Supervisory elements in hardware and software must be used to detect software or hardware failures. The driver shall be notified when a malfunction is detected.	10
		F2.13.2.3 Same as above.	5	F2.13.2.3 Threshold has been set too low.	4	F2.13.2.3 The driver shall be able to select a threshold level that he/she is comfortable with. The default threshold must be set to a level appropriate for typical conditions.	20
		F2.13.2.4 Same as above.	5	F2.13.2.4 System fails to sense correct intentions of driver to change lanes	7	F2.13.2.4 A reliable method must be used to sense correct intentions of driver to change lanes or the system must be redesigned to eliminate the necessity of sensing driver's intentions.	35
F2.14 Enable Blind Spot Warning (BSW)	F2.14 BSW cannot be enabled.	F2.14.1 Driver does not receive warning when a lateral collision is imminent. Safety is degraded.	6	F2.14.1 Electronics failure	2	F2.14.1 The system electronics must be sufficiently reliable and must have supervisory elements in hardware and software. Driver shall be notified about changes in the BSW operating mode.	12

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.15 Disable BSW	F2.15 BSW cannot be disabled	F2.15.1 Driver cannot avoid receiving warnings, may experience annoyance or discomfort.	3	F2.15.1 Electronics failure	2	F2.15.1 The system electronics must be sufficiently reliable. There shall be redundant methods to disable the BSW.	6
F2.16 Adjust BSW Threshold.	F2.16 BSW Threshold cannot be adjusted.	F2.16.1 Driver may be uncomfortable with the currently selected threshold or the threshold may be inappropriate for the prevailing conditions.	6	F2.16.1 Electronics failure	2	F2.16.1 The controller electronics must be sufficiently reliable. The threshold setting shall default to a low level when the BSW is enabled for the first time. The driver shall be able to read and verify the selected threshold setting.	12
H2.3 Lane Departure Warning							
F2.17 Warn Driver.	F2.17.1 Loss of lane departure warning function	F2.17.1 Vehicle may depart from lane and possibly have a collision if the driver is inattentive	9	F2.17.1.1 Loss of lane reference position due to damage or loss of roadway reference aids.	5	F2.17.1.1 Supervisory elements in lateral sensor processor (in software) must be able to detect the loss of reference. The driver shall be notified when roadway lane reference aids are lost. Redundant reference aids may be necessary.	45
		Same as in F2.17.1.1	9	F2.17.1.2 Lateral reference sensor fail or gives erroneous readings.	4	F2.17.1.2 Supervisory elements must be used to monitor the response of the lateral reference sensor. The driver must be notified if a malfunction is detected. A redundant lateral sensor with the appropriate logic may be essential.	36

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		Same as in F2.17.1.1	9	F2.17.1.3 Controller electronics or software failure	2	F2.17.1.3 The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall notify the driver.	18
		Same as in F2.17.1.1	9	F2.17.1.4 Warning delivery device failure	2	F2.17.1.4 Warning device must be reliable. Redundant warning delivery methods shall be used.	18
	F2.17.2 Give unnecessary warning.	F2.17.2 There may be too many false alarms. Driver may be distracted. Driver's confidence may be reduced.	5	F2.17.2.1 Lateral reference reading sensor gives erroneous readings.	5	F2.17.2.1 The system must check the reasonableness of sensor data by using an appropriate vehicle dynamics model. If a malfunction is detected, the driver shall be notified.	25
			5	F2.17.2.2 Controller electronics or software failure	2	F2.17.2.2 The system must have supervisory elements (in hardware and software). When a controller malfunction is detected, system shall notify the driver.	10

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.18 Enable LDW	F2.18 LDW cannot be enabled	F2.18 Driver has to assume full responsibility and exercise more caution.	6	F2.18 Electronics malfunction failure.	2	F2.18 The controller electronics must be sufficiently reliable. Driver shall be notified about the change in LDW operating mode.	12
F2.19 Disable LDW	F2.19 LDW cannot be disabled	F2.19 Driver may get annoyed by receiving unwanted warnings.	3	F2.19 Electronics malfunction.	2	F2.19 The system must be sufficiently reliable. The driver shall have a redundant way of turning the system off.	6
F2.20 Adjust threshold	F2.20 Threshold cannot be adjusted.	F2.20 Driver may be uncomfortable with the current selected threshold or the threshold may be inappropriate for current situation.	6	F2.20.1 Electronics malfunction in the controller or the driver interface	2	F2.20.1 The electronics must be sufficiently reliable. The default threshold must be at a low level when LDW is first enabled. Driver shall be able to read and verify the selected threshold setting.	12
H2.4 Steering assist							
F2.21 Assist driver in steering.	F2.21 Can not assist driver in steering.	F2.21 Ride quality may be degraded. Driver's workload may be increased.	5	F2.21.1 Lateral sensor failure	5	F2.21.1 System must employ supervisory elements to detect sensor failures. Driver shall be notified when a sensor malfunction is detected. Redundant lateral sensor and appropriate logic may be necessary.	30

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
			5	F2.21.2 Erratic steering actuator response or failure of steering actuator .	3	F2.21.2 System must employ supervisory elements and self diagnostics to monitor the steering actuator. The system must be designed to accommodate steering actuator failures without causing the vehicle to depart from the lane. When the failure is detected the system shall accommodate it or the steering assist system shall be disconnected and the driver shall be notified.	18
			5	F2.21.3 Controller electronics or software failure	2	F2.21.3 Controller must be sufficiently reliable. If a failure is detected, the steering actuator must be disconnected and the driver be notified. Controller and software redundancies may be necessary.	12
H2.5 Driver Vehicle Roadway Interface							
F2.22 Check-in	F2.22 Failure of check-in function.	F2.22.1 Vehicle is operating in the dedicated lane even though it should not.	9	F2.22.1 On-board diagnostics fail to detect a fault in major functions of the vehicle.	3	F2.22.1 Diagnostics algorithms must be robust and highly reliable. Roadway shall be able to detect an unfit vehicle operating in the dedicated lane. Law enforcement can be used to deal with the violators	

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F2.22.2 Vehicle is operating in the dedicated lane even though it should not.	9	F2.22.2 Driver ignores the results of the on-board diagnostics.	3	F2.22.2 Roadway shall be able to identify an unfit vehicle operating in the dedicated lane. Traffic rules and regulations must be used to deter the driver from violating the rules.	27
		F2.22.3 Vehicle is not allowed to enter the dedicated lane even though it is fit.	6	F2.22.3 On-board diagnostics make a wrong decision about a component or function that was not at fault.	2	F2.22.3 On board diagnostics must be highly reliable. Redundancies and supervisory elements must be considered for improving reliability	12
F2.23 Enter the lane	F2.23 Driver fails to enter the lane or enter the lane improperly	F2.23 Disturbance in the transition lane or entrance to the dedicated lane. Driver may get annoyed. Vehicle restricted from operating in the dedicated lane.	7	F2.23 Dedicated lane is congested or driver is not able to merge due to high speed and/or small headways in dedicated lane or driver does not have the required skills.	4	F2.23 Roadway must enforce lower speeds and larger headways near the entry points. Driver skills for merging into the dedicated lane shall be tested as part of the licensing procedure.	20
F2.24 Response to BSW and LDW	F2.24 Driver fails to respond to BSW and/or LDW	F2.24 System safety is degraded. Collision with a vehicle in an adjacent lane during a lane change maneuver is possible.	10	F2.24.1 Driver ignores warning unintentionally or becomes confused.	4	F2.24.1 The warnings shall be very clear and unambiguous to the driver. Driver interface shall be as simple as possible.	40
			10	F2.24.2 Driver ignores warning intentionally due to high false alarm rate.	4	F2.24.2 False alarm rate must be very low. Warning signals must be easily distinguishable from each other. Warning threshold shall be adjustable by the driver. Driver interface shall be as simple as possible	40

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.25 Respond to traffic information	F2.25 Driver fails to respond to traffic information	F2.25 Roadway efficiency and vehicle safety is degraded.	4	F2.25 Driver capability is impaired.	5	F2.25 Roadway traffic information must be clear and brief.	20
F2.26 Exit the lane	F2.26 The driver can not exit the lane.	F2.26 Vehicle has to remain in the dedicated lane. System performance is degraded.	6	F2.26 Congestion in manual lane or the transition lane	5	F2.26 Dedicated transition lane or some form of regulation such as "yield to auto lane" must be implemented to ensure easy exit even when traffic congestion happens in the manual lane. Must warn the driver, of congestion ahead of time via traffic information communication.	30
F2.27 Fall back to ERSC1.	F2.27.1 System does not fall back to ERSC1.	F2.27.1 Safety is compromised. Collision is possible.	10	F2.27.1 Software failure	2	F2.27.1 Reliable supervisory and diagnostics programs must be implemented. Redundant means for returning to the ERSC1 mode must be used.	20
	F2.27.2 Driver fails to assume role for ERSC 1.	F2.27.2 Safety is compromised. Collision is possible.	10	F2.27.2.1 Warning delivery device failure	2	F2.27.2.1 Warning device must be reliable. Redundant warning delivery methods must be used.	20
			10	F2.27.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F2.27.2.2 The warnings and instructions must be clear and understandable. Driver's workload must be manageable	50

Table 13: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-2)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F2.28 Fall back to manual control	F2.28.1 System does not fall back to manual control	F2.28.1.1 Vehicle may be under automatic control when it should be under manual control. Safety is compromised.	10	F2.28.1.1 Controller software failure	2	F2.28.1.1 Reliable supervisory and diagnostics programs must be used. Redundancies in hardware and software may be necessary.	20
	F2.28.2 Driver fails to assume full manual control.	F2.28.2 As in F2.28.1	10	F2.28.2.1 Warning delivery device failure	2	F2.28.2.1 Warning device must be reliable. Redundant warning delivery methods must be used.	20
			10	F2.28.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F2.28.2.2 Same as in F2.27.2.2.	50
F2.29 Notify driver of mode of operation	F2.29 Fail to notify driver of correct mode of operation.	F2.29.1 Driver may get confused and given the impression that the vehicle does not behave as expected. The driver may decide to initiate a check-out procedure and exit the lane. The driver may also panic and cause a collision under some situations.	8	F2.29.1 Electronics of software failure.	3	F2.29.1 The electronics and software must be very reliable. Redundancies and on board diagnostics must be used to improve reliability.	24

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H3.1 Speed and Headway Maintenance and Rear-end Collision Avoidance.							
F3.1 Calculate safe headway	F3.1 Loss of ability to calculate correct value of safe headway	F3.1.1 Headway is set to the default value. Efficiency is affected.	6	F3.1.1 Detected malfunction or inability of the sensors to estimate the braking capabilities and intentions of the preceding vehicle and/or vehicle.	6	F3.1.1 The malfunction of sensors or gross inaccuracies in the estimation of the braking capabilities must be detected fast. The system must fall back to the default headway that takes into account the inaccuracies or malfunction of the sensors.	36
		F3.1.2 Headway is set to the default value. Efficiency is affected.	6	F3.1.2 Detected malfunction or loss of communication with preceding vehicle	6	F3.1.2 Diagnostics and built-in self tests must be used to guarantee a fast detection of the communication failures. When a malfunction occurs the headway must be automatically increased to the default safe level that takes into account the failure	36
		F3.1.3 Unsafe headway is used and rear-end collision is possible or a large headway is used and efficiency is affected	10	F3.1.3 Faulty or inaccurate measurements of braking capabilities of vehicle and/or preceding vehicle	6	F3.1.3 The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements must be monitored and taken into account in the calculation of the safe headway.	60

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.1.4 Unsafe headway is used and rear-end collision is possible or large headway is used and efficiency is affected.	10	F3.1.4 Incorrect braking capabilities and intentions is received through communication due to interference or noise corruption	6	F3.1.4 The measurements of braking capabilities of all vehicles must be accurate. The system must check the reasonableness of preceding vehicle's braking capability and take into account possible inaccuracies and inconsistencies in calculating the safe headway.	60
		F3.1.5 Headway is increased in order to maintain safety level. Efficiency is affected.	6	F3.1.5 Loss of communication with roadway and/or lack of headway recommendation	4	F3.1.5 System must be able to accommodate the lack of headway recommendation from roadway .	24
		F3.1.6 Headway is set to the default value if failure is detected . Efficiency is affected. If failure is not detected safety is affected due to possible use of an unsafe headway.	9	F3.1.6 Loss of braking data information from preceding vehicle due to receiver malfunction.	4	F3.1.6 System must have supervisory elements and diagnostics that monitor the functionality of the receiver and detect malfunctions. The malfunction of the receiver must be taken into account in calculating the safe headway.	36

Table 14 Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.2 Maintain cruise speed.	F3.2.1 Loss of speed maintenance function.	F3.2.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Driver may be annoyed. Traffic rules may be violated. The lane keeping function may be affected especially around curves.	9	F3.2.1.1 Speed sensor gives erroneous or variable readings. (0% to 10% steady state error is typical of speed sensors. Sudden variation is rare)	2	F3.2.1.1 Diagnostics and built in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F3.2.1.2 As above.	9	F3.2.1.2 Controller electronics or software failure.	2	F3.2.1.2 The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F3.2.1.3 Braking may be used to control speed. Vehicle may be at low speed affecting capacity and efficiency.	8	F3.2.1.3 Throttle actuator failure.	3	F3.2.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	24

Table 14: Failure Modes and Effects Analysis (System FMEA) (ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.2.1.4 Vehicle accelerates above desired speed or decelerates below desired speed. Speed limit may be exceeded. The lane keeping function will be affected around curves. Vehicle may go out of control around curves.	10	F3.2.1.4 Brake actuator failure (brake cannot be applied or brake is continuously applied)	3	F3.2.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failures must be employed together with the appropriate logic and diagnostics that allow automatic switching from a failed actuator to a healthy one. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	30
	F3.2.2 System switches to headway maintenance in the absence of valid target.	F3.2.2.1 Sudden change in speed. Unnecessary braking .RECA may be activated. Driving comfort and efficiency are affected.	9	F3.2.2.1 Ranging sensor detects an invalid target within the default headway	6	F3.2.2.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	54

Table 14: Failure Modes and Effects Analysis (System FMEA) (ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.3 Maintain target speed as commanded by the roadway.	F3.3.1 Vehicle cannot maintain target speed as commanded by the roadway.	F3.3.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Safety and efficiency are compromised. The lane keeping function may be affected around curves.	9	F3.3.1.1 Speed sensor gives erroneous readings.	2	F3.3.1.1 Diagnostics and built-in tests must perform a test for reasonableness on sensor data. When sensor malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F3.3.1.2 Same as in F3.3.1.1	9	F3.3.1.2 Controller electronics or software failure.	2	F3.3.1.2 The system must have supervisory elements (in hardware or software) or adequate redundancies. When a controller malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F3.3.1.3 Same as in F3.2.1.3	8	F3.3.1.3 Throttle actuator failure.	3	F3.3.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	24

Table 14: Failure Modes and Effects Analysis (System FMEA) (ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.3.1.4 Same as in F3.2.1.4	10	F3.3.1.4 Brake actuator failure.	3	F3.3.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failures must be employed together with the appropriate logic and diagnostics that allow automatic switching from a failed actuator to a healthy one. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	30
		F3.3.1.5 Vehicle travels too fast which is unsafe or too slow which reduces capacity. Speed may be faster than what road conditions permit. It may affect the performance of the lane keeping function.	8	F3.3.1.5 Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication.	3	F3.3.1.5 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.) When a communication malfunction is detected the system shall fall back to a default lower speed if there is no valid target to follow. The driver shall be notified of the loss of communication.	24

Table 14: Failure Modes and Effects Analysis (System FMEA) (ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.3.1.6 Same as F3.3.1.5	8	F3.3.1.6 Loss of target speed information due to receiver malfunction	3	F3.3.1.6 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to initiate a check-out procedure and exit the lane.	24
	F3.3.2 System switches to headway maintenance in the absence of valid target.	F3.3.2 Sudden change in speed. Unnecessary braking and RECA may be activated. Riding comfort and efficiency are affected.	7	F3.3.2 Ranging sensor detects an invalid target within the default headway	6	F3.3.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	42

Table 14: Failure Modes and Effects Analysis (System FMEA) (ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.4 Maintain headway	F3.4 Cannot maintain headway	F3.4.1 SHM stops operating. Headway may become too large or too small, unexpectedly. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F3.4.1 Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability.	6	F3.4.1 System must be able to detect and accommodate an intermittent sensor failure. System software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and transition to manual control by following check-out procedure. Redundant ranging sensors, not subject to common mode failures, with appropriate logic must be used.	60
		F3.4.2 SHM switches to speed maintenance mode even if a valid target exists. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F3.4.2 Sensor loses target due to road curvature or insufficient target reflectiveness.	7	F3.4.2 The sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Vehicle shall slow down and transition to manual control when target is ambiguous and cannot be followed reliably. Sensor redundancies must be used to track targets around curves and minimize the possibility of interference.	70

Table 14: Failure Modes and Effects Analysis (System FMEA) (ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.4.3 SHM accelerates or decelerates vehicle unexpectedly . The RECA may be activated. Riding comfort and efficiency may be affected.	7	F3.4.3 Ranging sensor has locked on an invalid target.	7	F3.4.3 The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. System must distinguish vehicles moving to adjacent lanes and around curves in the same lane. Redundant ranging sensors not subject to same failure mode with appropriate logic may be required.	49
		F3.4.4 System may fail to maintain selected headway. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F3.4.4 Brake actuator failure. (Or intermittent failure to respond)	3	F3.4.4 System must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators that are not subject to common mode failures with appropriate logic must be used. When a redundant braking path fails the system shall initiate a check-out procedure.	30

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.4.5 System may fail to maintain selected headway. Braking or the RECA function is used to avoid violating the minimum safe headway.	8	F3.4.5 Throttle actuator failure.	3	F3.4.5 The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	24
		F3.4.6 System may fail to maintain selected headway. Braking or the RECA function is used to avoid violating the minimum safe headway. System may fail to adjust speed around curves leading to possible lane departure and collision.	9	F3.4.6 Controller electronics or software failure.	2	F3.4.6 The system must have supervisory elements (in hardware and software) or adequate redundancies. System shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.	18
		F3.4.7 SHM accelerates or decelerates vehicle unexpectedly. Headway becomes too small or too large. The RECA function may be turned on and off unexpectedly. Vehicle may depart lane, go out of control and cause multiple collisions.	10	F3.4.7 Ranging sensor gives erroneous readings.	4	F3.4.7 The system must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. System shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.	40

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.5 Switch from maintaining cruise speed to maintaining headway	F3.5 Failure to switch to maintaining headway even when a valid target exists.	F3.5.1 Headway may become too small without the RECA function been activated. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F3.5.1 Ranging sensor fails to detect a valid target.	5	F3.5.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics. In case of sensor failure the system shall switch to manual control by providing a warning to the driver slowing down and following the check-out procedure.	50
		F3.5.2 Headway may become too large or too small. The RECA function may be impaired or may be turned on and off in an effort to keep the headway within safe level. Riding comfort and efficiency are affected. The lane keeping function around curves may be affected.	9	F3.5.2 Hardware or software failure of the SHM.	2	F3.5.2 The system must have supervisory elements (in hardware or software) or adequate redundancies. System shall switch to manual control by warning driver and following a check-out procedure in case of a detected failure.	18

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.6 Switch from maintaining headway to maintaining cruise speed.	F3.6 Failure to switch to speed maintenance mode when the original target moves out of the lane and becomes unsuitable to follow, and no other valid target exists.	F3.6.1 Vehicle speed varies instead of being constant in the absence of a valid target. The RECA function may be activated unexpectedly. Riding comfort and efficiency may be affected.	8	F3.6.1 Ranging sensor locks on the original target or locks on another target which is invalid when the original target becomes unsuitable to follow.	6	F3.6.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	48
		F3.6.2 Vehicle speed varies instead of being constant in the absence of a valid target. The RECA function may be impaired or may be activated unexpectedly. Riding comfort and efficiency may be affected.	8	F2.6.2 Hardware or software failure of the SHM	2	F3.6.2 System must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. System shall switch to manual by warning the driver and following a check-out procedure in case of detected failures	16
F3.7 Switch from maintaining cruise speed to maintaining roadway commanded target speed.	F3.7.1 Failure to switch to maintaining roadway commanded target speed.	F3.7.1.1 System fails to adjust speed as commanded by the roadway. Speed may be higher than the conditions permit or lower than optimal. Efficiency and safety are compromised. It may affect the performance of lane keeping function.	8	F3.7.1.1 Loss of target speed information input due to receiver malfunction.	3	F3.7.1.1 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. Driver shall be notified that vehicle is not receiving roadway target speed commands. If the receiver has a malfunction the driver may be required to initiate a check-out procedure and exit the lane.	24

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.7.1.2 Same as in F3.7.1.1	8	F3.7.1.2 Loss of roadway transmission capability or target speed is corrupted during communication	3	F3.7.1.2 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme (parity, checksum etc.). The system must be able to accommodate momentary loss of roadway target speed command. When a communication malfunction is detected, system shall fall back to a default lower speed if there is no valid target to follow. The driver shall be notified of the loss of communication.	24
	F3.7.2 Switching to headway maintenance instead.	F3.7.2 Brake may be unnecessarily applied. Vehicle may suddenly change speed. Rear-end collision avoidance may be activated. Riding comfort and efficiency are affected. The lane keeping function may be affected.	8	F3.7.2 Ranging sensor detects an invalid target.	6	F3.7.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used.	48

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F4.8 Hard braking for rear-end collision avoidance.	F3.8.1 Failure to take action on time.	F3.8.1.1 Rear-end collision . Vehicle may depart lane, go out of control and cause multiple collisions.	10	F3.8.1.1 Ranging sensor fails to provide signal or provides incorrect signal.	5	F3.8.1.1 The system must have redundant sensing inputs to reduce the probability of missing a target to essentially zero . If redundancy is lost, the system shall increase headway and reduce speed and transition to manual control. The system and lane keeping function shall be designed so that vehicle does not depart lane during rear-end collisions.	50
		F3.8.1.2 Originally calculated headway becomes unsafe. Rear-end collision is possible.	10	F3.8.1.2 Loss of communication of braking intentions of preceding vehicle	5	F3.8.1.2 A redundant method must be used to communicate the preceding vehicle's braking intention. The calculated safe headway must take into account momentary loss of vehicle to vehicle communication. If loss of communication is permanent, system shall take that into account in calculating the safe headway.	50
		F3.8.1.3 Rear-end collision. Vehicle may depart lane, go out of control and cause multiple collisions.	10	F3.8.1.3 Controller electronics or software failure	2	F3.8.1.3 The system must have supervisory elements in software and hardware and adequate redundancies. When a redundancy is lost, the system shall increase headway and reduce speed to comfortable levels and warn the driver to operate at ERSC1 or the manual mode and exit the lane as soon as possible.	20

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.8.1.4 Rear-end collision. Vehicle may depart lane, go out of control and cause multiple collisions.	10	F3.8.1.4 Brake actuator failure	3	F3.8.1.4 The system must have redundant braking actuators that are not subject to common mode failures and appropriate diagnostics that allow the fast detection and accommodation of failures without degrading the performance of the RECA function. When a redundant braking path fails the system shall switch to ERSC1 or manual mode and warn the driver appropriately. The transition to ERSC1 or manual mode shall be done by first reducing speed and increasing headway to levels that are comfortable for the driver.	30
		F3.8.1.5 Rear end collision. Vehicle may depart lane, go out of control and cause multiple collisions.	10	F3.8.1.5 Calculated time to collision (TTC) is larger than actual TTC due to incorrect measurement of braking capabilities.	6	F3.8.1.5 TTC must be accurate and conservative in order to accommodate possible inaccuracies in measurements. Independent estimates of TTC based on independent measurements must be used. The system and lane keeping function shall be designed so that vehicle does not depart lane during rear-end collisions	60

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.8.1.6 The TTC is so short that a rear-end collision can not be avoided without steering. The vehicle may go out of control and cause multiple collisions.	10	F3.8.1.6 Ranging sensor switches from a valid target to another one with completely different operating status and braking capability e.g. preceding vehicle exits lane and next vehicle in lane is disabled.	3	F3.8.1.6 The system must be designed to account for such situations. Vehicle to vehicle communication may be used to notify trailing vehicle of condition ahead or the system is designed so that exiting from the lane is possible only at designated points where larger headways are imposed.	30
	F3.8.2 The RECA is activated unnecessarily.	F3.8.2 Riding comfort and efficiency may be affected.	7	F3.8.2 Incorrect range is sensed or incorrect TTC is calculated.	4	F3.8.2 The system must minimize the number of faulty activations of the RECA function as much as possible. Independent ranging measurements and calculations of the TTC must be used. Activation of the RECA shall not affect the performance of the lane keeping function and shall not cause the vehicle to depart the lane.	28
F3.9 Enable the SHM and RECA	F3.9 SHM and RECA cannot be enabled	F3.9 SHM and RECA is not available . Vehicle can only be operated in manual mode.	7	F3.9 Electronic malfunction.	2	F3.9 The controller electronics must be sufficiently reliable. Diagnostics must be per-formed even when the SHM and RECA are in the standby mode. The driver shall be notified of any detected malfunctions.	14

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.10 Disable the SHM and RECA	F3.10.1 SHM and RECA cannot be disabled	F3.10.1 Driver cannot take over the control of the throttle and brake. He/she may panic and his/her steering performance or transition from lane keeping to manual control may be affected.	10	F3.10.1 Electronic malfunction.	2	F3.10.1 The controller electronics must be sufficiently reliable. The driver shall have redundant means of turning off the SHM and RECA. The switching off of the functions must follow the disabling procedure so that the driver is not put in a situation he/she cannot handle.	20
	F3.10.2 SHM and RECA are disabled without first reducing speed and increasing headway.	F3.10.2 Driver may be put in a situation of short headway and high speed that he/she cannot handle in case of emergencies. Collision is possible.	10	F3.10.2 Software failure or failure of the brake actuator	3	F3.10.2 The system must have redundancies in software and redundant braking actuator paths. The system must be designed to fall back to a default speed and headway in a reliable manner when a failure is detected before the SHM and RECA are disabled.	30
F3.11 Communicate braking capability and intention to trailing vehicle.	F3.11.1 Loss of communication with trailing vehicle	F3.11.1 If detected by trailing vehicle its headway may be increased in order to maintain safety level. Efficiency is affected. If undetected or detected too late the TTC of trailing vehicle may be too large leading to a possible collision.	10	F3.11.1 Failure of transmitter	3	F3.11.1 The system must have supervisory elements to monitor the transmitter. Redundant transmitter may be necessary. If the transmitter fails permanently, the vehicle shall exit the lane. The lane keeping function and system must be designed so that vehicle does not go out of control due to rear end collisions.	30

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
	F3.11.2 Transmit incorrect braking capabilities or braking intention to trailing vehicle.	F3.11.2 Trailing vehicle may calculate and use unsafe headway, or may apply insufficient brake, leading to a possible rear-end collision.	10	F3.11.2 Faulty or inaccurate measurements of braking capabilities and/or braking intention	6	F3.11.2 The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements shall be monitored. Independent means for calculating braking capabilities must be employed. The lane keeping function and system must be designed so that vehicle does not go out of control due to rear end collisions.	60
F3.12 Coordinate with lane keeping and steering.	F3.12 Loss of coordination with lane keeping and steering	F3.12 Vehicle may skid out of lane, go out of control and collide with vehicles in adjacent lane around curves.	10	F3.12 Electronics or Software failure	3	F3.12 Redundancies in electronics and software must be used. When failure is detected vehicle shall slow down around curves and increase headway. driver shall be warned to initiate a check out procedure.	30
F3.13 Keep vehicle in the center of lane.	F3.13 Loss of lane keeping capability	F3.13.1 Vehicle departs lane, goes out of control and collides with other vehicles.	10	F3.13.1 Failure to detect vehicle's lateral position due to malfunction of sensor or roadway lane reference aid.	5	F3.13.1 The system must have redundant measurements of the lateral position of the vehicle. Redundant sensors and reference aids may be required with the appropriate diagnostics and logic. When a redundant component fails the system shall switch to manual control or lower ERSC and warn the driver	50

Table 1: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F3.13.2 Lane keeping performance is degraded. Vehicle may have to slow down or transition to lower ERSC.	8	F3.13.2 Lane preview information is not available.	3	F3.13.2 System must have redundant means of obtaining preview information. In the absence of preview information the system shall switch to a lower ERSC and warn the driver.	24
		F3.13.3 Vehicle may depart lane and go out of control causing multiple collisions.	10	F3.13.3 Control software or electronics failure	2	F3.13.3 All electronic components and software must have redundancies and appropriate diagnostics to detect failures. When a failure of a redundant component is detected the system shall switch to a lower ERSC and warn the driver. Detection and accommodation of failures shall be fast and shall not affect the performance of the lane keeping function.	20
		F3.13.4 same as F3.13.3	10	F3.13.4 Steering actuator failure	3	F3.13.4 Redundant steering actuators and components with the appropriate diagnostics and logic must be used. When a redundant component fails the system shall warn the driver to assume manual control of the steering function by following a check-out procedure.	30

Table 1: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F3.14 Enable lane keeping.	F3.14 Can not enable lane keeping.	F3.14.1 LK is not available to the driver. Vehicle can only be operated in manual mode or ERSC1, 2.	6	F3.14 Controller electronic circuitry or software failure	2	F3.14.1 The controller electronics and software must be sufficiently reliable. Diagnostics must be performed even when the LK is in the standby mode and the driver shall be notified of detected malfunctions.	12
F3.15 Disable the LK	F3.15.1 LK cannot be disabled	F3.15.1 System does not respond or follow the disabling procedure. Driver cannot override the LK controller and may panic.	8	F3.15.1 Electronic and/or software malfunction .	2	F3.15.1 The controller electronics must be sufficiently reliable. The driver shall have redundant means of disabling the LK. The disabling of the LK function shall follow the check-out procedure.	16
	F3.15.2 LK is disabled suddenly without following the check-out procedure.	F3.15.2 The driver may fail to take over steering. Vehicle may go out of control.	10	F3.15.2 Electronic and/or software failure	2	F3.15.2 All electronic components and software must have redundancies and appropriate diagnostics to detect failures. When a failure of a redundant component is detected the system shall switch to a lower ERSC and warn the driver. Detection and accommodation of failures shall be fast and shall not affect the performance of the lane keeping function.	20

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
H3.2 Lateral Collision Warning							
F3.16 Warn the driver	F3.16.1 Can not provide LCW.	F3.16.1.1 Safety is compromised during lane changing if driver relies on the system too much. Collision is possible.	9	F3.16.1.1 Sensor failure to detect lateral range and range rate of "threatening" vehicles.	5	F3.16.1.1 Supervisory elements and diagnostic programs must be used to monitor the reasonableness of the sensor measurements. Redundant sensors may be needed. The driver shall be notified of any malfunction.	45
		F3.16.1.1 Same as F3.16.1.1	9	F3.16.1.2 Control software or electronics failure	2	F3.16.12 Software and electronics must be reliable. Redundancies must be employed to improve reliability. The driver shall be notified of any malfunction.	18
		F3.16.1.3 Same as F3.16.1.1	9	F3.16.1.3 Threshold is set too high	4	F3.16.1.3 Supervisory element is needed to check threshold. The default level of threshold must be low. The level of the threshold and its consequences shall be transparent to the driver.	36
		F3.16.1.4 Same as F3.16.1.1	9	F3.16.1.4 Warning output device failure.	3	F3.16.1.4 Warning device must be reliable. Redundant warning methods must be used.	27

Table 1: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F3.16.1.5 Same as F3.16.1.1	9	F3.16.1.5 The calculated TTC is incorrect.	6	F3.16.1.5 There shall be independent methods of calculating the TTC. The most conservative estimate of TTC shall be used.	54
	F3.16.2 Give frequent false warnings	F3.16.2.1 May distract driver and affect his/her performance with the other driver functions.	6	F3.16.2.1 Threshold is too low.	5	F3.16.2.1 The driver shall be able to select a threshold level that he/she feels comfortable with. The default threshold must be set to a level appropriate for typical conditions.	30
		F3.16.2.2 May distract driver and affect his/her performance with the other driver functions.	6	F3.16.2.2 Control software malfunction or warning device failure	2	F3.16.2.2 The number of false alarms must be minimized by improving the reliability of hardware and software components. Redundant components and appropriate diagnostics may be used to improve reliability.	12
F3.17 Enable LCW.	F3.17 Can not enable LCW.	F3.17 Driver can not get help in lateral maneuver. Safety and efficiency are affected. Vehicle may not be allowed to operate in dedicated lane.	5	F3.17 Electronic circuitry or software failure	2	F3.17 System must have sufficiently reliable electronic circuitry and software. Redundancies shall be used to achieve a high level of reliability.	10

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F3.18 Disable LCW.	F3.18 LCW cannot be disabled.	F3.18 Driver cannot avoid receiving warnings and may get annoyed and distracted.	3	F3.18 Electronic circuitry failure	2	F3.18 System must have very reliable electronic circuitry. The driver shall have redundant means of turning off the LCW.	6
F3.19 Adjust Threshold	F3.19 LCW Threshold cannot be adjusted.	F3.19 Driver may be uncomfortable with the currently selected sensing region, or the sensing region may be inappropriate for the current conditions.	6	F3.19 Electronics or failure	2	F3.19 The controller electronics and software must be sufficiently reliable. The threshold setting shall default to a low level when the LCW is enabled for the first time or when a failure is detected. Driver shall be able to read and verify the selected threshold setting.	12
H3.3 Driver Vehicle Roadway Interface							
F3.20 Check-in	F3.20 Failure of check-in function.	F3.20.1 Some of the automated functions cannot be enabled. Safety and efficiency are affected. Driver may enter and exit the lane within a short period of time and disturb the traffic flow.	9	F3.20.1 On-board diagnostics fail to detect a fault in major functions of the vehicle.	3	F3.20.1 Diagnostics algorithms must be robust and highly reliable. Roadway must be able to detect an unfit vehicle operating in the dedicated lane.	27

Table 1: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F3.20.2 Vehicle is operating in the dedicated lane even though it should not. Driver may fail to keep vehicle in the lane if lane is narrow. Safety and efficiency are affected.	9	F3.20.2 Driver ignores the results of the on-board diagnostics.	3	F3.20.2 Roadway must be able to identify an unfit vehicle operating in the dedicated lane. Traffic rules and regulations must be used to deter the driver from violating the rules.	27
		F3.20.3 Vehicle is not allowed to enter the dedicated lane even though it is fit.	6	F3.20.3 On-board diagnostics make a wrong decision about a component or function that was not at fault.	2	F3.20.3 On board diagnostics must be highly reliable. Redundancies and supervisory elements must be considered for improving reliability.	12
F3.21 Enter the lane	F3.21 Driver fails to enter the lane	F3.21 Disturbance in the transition lane or entrance to the dedicated lane. Driver may get annoyed. Vehicle restricted from operating in the dedicated lane.	5	F3.21 Dedicated lane is congested or driver is not able to merge due to high speed and/or small headways in dedicated lane or driver does not have the required skills.	4	F3.21 Roadway must be able to enforce lower speeds and larger headway near the entry points. Driver skills for lane merging shall be tested as part of the licensing procedure.	20
F3.22 Respond to LCW	F3.22 Driver fails to respond to LCW.	F3.22.1 System safety is degraded. Collision with a vehicle in an adjacent lane is possible.	10	F3.22.1 Driver ignores warning unintentionally or becomes confused.	4	F3.22.1 The warnings must be very clear and unambiguous to the driver.	40

Table 14: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
			10	F3.22.2 Driver ignores warning intentionally due to high false alarm rate.	4	F3.22.2 False alarm rate must be very low. Warning signals must be easily distinguishable from each other. Warning threshold shall be adjustable by the driver. Driver interface shall appear simple to the driver.	40
F3.23 Respond to traffic information	F3.23 Driver fails to respond to traffic information	F3.23.1 Roadway capacity and traffic flow control.	5	F3.23.1 Driver capability is impaired.	5	F3.23.1 Roadway traffic information shall be clear and brief.	25
F3.24 Check out.	F3.24.1 Vehicle does not initiate or respond to a check-out request.	F3.24.1.1 Vehicle will keep on going in dedicated lane. Driver feels helpless.	9	F3.24.1.1 Controller failed to recognize check-out initiation input.	2	F3.24.1.1 The system must be sufficiently reliable. Some redundancy to initiate check-out is needed.	18
		F3.24.1.2 Same as F3.24.1.1	9	F3.24.1.2 Controller software failure.	2	F3.24.1.2 System must have supervisory elements in hardware and software. Once a failure is detected the system shall switch to a lower ERSC and warn the driver.	18
		F3.24.1.3 The driver is not warned to take over steering, throttle and brake control. Vehicle would keep on going in dedicated lane.	7	F3.24.1.3 Warning delivery device failure.	2	F3.24.1.3 Warning device must be reliable. Redundant warning delivery methods must be used.	14
	F3.24.2 Driver fails to pass check-out test.	F3.24.2 The vehicle is guided to an exit ramp or to a shoulder of the lane and then brought to a full stop.	7	F3.24.2 Driver's failure in handling throttle, brake, and steering properly during check-out.	4	F3.24.2 Handling throttle, brake, and steering during check-out must be no more difficult than in normal manual driving.	28

Table 1: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.25 Exit the lane	F3.25.The driver can not exit the lane.	F3.25 Vehicle remains in the dedicated lane. May violate traffic regulations. System performance is degraded.	6	F3.25 Congestion in manual lane or the transition lane	5	F3.25 Dedicated transition lane or some form of regulation such as "yield to auto lane" must be implemented to ensure easy exit even when traffic congestion happens in the manual lane. Must warn the driver, of congestion ahead of time via traffic information communication.	30
F3.26 Fall back to ERSC2.	F3.26.1 System does not fall back to ERSC2 even when it is necessary	F3.26.1 Safety is compromised. Collision is possible.	10	F3.26.1 Software failure	2	F3.26.1 Reliable supervisory and diagnostics program must be implemented.	20
	F3.26.2 Driver fails to assume role for ERSC 2	F3.26.2.1 Safety is compromised. Collision is possible.	10	F3.26.2.1 Warning delivery device failure	2	F3.26.2.1 Warning device must be reliable. Redundant warning delivery methods must be used.	20
			10	F3.26.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F3.26.2.2 The warnings must be clear and distinguishable from each other.	50

Table 1: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-3)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F3.27 Fall back to ERSC1.	F3.27.1 System does not fall back to ERSC1 when it should.	F3.27.1 Safety is compromised. Collision is possible.	10	F3.27.1 Software failure	2	F3.27.1 Reliable supervisory and diagnostics programs must be implemented.	20
	F3.27.2 Driver fails to assume roles for ERSC 1.	F3.27.2.1 Safety is compromised. Collision is possible.	10	F3.27.2.1 Warning delivery device failure	2	F3.27.2.1 Warning device must be reliable. Redundant warning delivery methods must be used.	20
		F3.27.2.2 same as F3.27.2.2	10	F3.27.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F3.27.2.2 The warnings must be clear and distinguishable from each other.	50
F3.28 Fall back to manual control.	F3.28.1 System does not fall back to manual control when it should.	F3.28.1 Safety is compromised. Collision is possible.	10	F3.28.1 Software failure	2	F3.28.1 Reliable supervisory and diagnostics program must be implemented.	20
	F3.28.2 Driver fails to assume full manual control.	F3.28.2.1 Vehicle remains under automatic control. Safety is compromised. Collision is possible.	10	F3.28.2.1 Warning delivery device failure	2	F3.28.2.1 Warning device must be reliable. Redundant warning delivery methods must be used.	20
		F3.28.2.2 same as in F3.28.2.1	10	F3.28.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F3.28.2.2 The warnings must be clear and distinguishable from each other.	50
F3.29 Notify driver of correct mode of operation.	F3.29 Fail to notify driver of correct mode of operation	F3.29 Driver may get confused by receiving or not receiving warnings when expected to.	7	F3.29 Electronics or software failure	3	F3.29 The electronics and software must be very reliable. Redundancies and on board diagnostics may be used to improve reliability.	21

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
H4.1 Navigation functions							
F4.1 Locate absolute position of vehicle.	F4.1 Can not locate correct absolute position of vehicle.	F4.1.1 Navigation capability is lost. Driver has to be responsible for navigation.	5	F4.1.1 Absolute position sensor failure (detected)	4	F4.1.1 Supervisory elements are needed to monitor the sensor. Redundant methods shall be used to calculate the position of the vehicle. The driver shall be warned to take over navigation tasks when the failure is detected. The driver shall be able to provide navigation commands without interfering with the automated functions.	20
		F4.1.2 Incorrect navigation command may be given. Travel time may be increased. Driver may be frustrated.	7	F4.1.2 Absolute position sensor gives erroneous readings. (undetected)	4	F4.1.2 Supervisory elements are needed to monitor the reasonableness of the sensor measurements. Roadway or vehicle to vehicle communication can help check the reasonableness of the sensor data by using other vehicles' positions.	28

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.2 Compute vehicle's route.	F4.2.1 Can not compute vehicle's route.	F4.2.1.1 Navigation capability is lost. Driver has to be responsible for navigation.	5	F4.2.1.1 Absolute position sensor failure (Detected)	4	F4.2.1.1 Supervisory elements are needed to monitor the sensors. Driver shall be able to choose the route manually without interfering with the operation of the other automated functions.	20
		F4.2.1.2 Non-optimum route may be computed. Travel time may increase.	5	F4.2.1.2 Traffic flow information is not available.	4	F4.2.1.2 Traffic flow information must be updated continuously. The vehicle shall be able to compute vehicle's route in the absence of traffic flow information.	20
		F4.2.1.3 Incorrect navigation command may be given. Travel time may be increased. Driver may be frustrated.	5	F4.2.1.3 Failure in software	2	F4.2.1.3 All the software units shall be carefully tested. Detection methods shall be used to detect failures and warn the driver to take over navigation.	10
	F4.2.2 Wrong route is computed.	F4.2.2.1 Driver travels longer time and may be frustrated.	5	F4.2.2.1 Wrong absolute position is sensed.	4	F4.2.2.1 The computed route shall be displayed to the driver .	20
		F4.2.2.2 Driver travels longer time and may be frustrated.	5	F4.2.2.2 Failure in communication with roadway.	3	F4.2.2.2 System shall be able to detect communication failures and warn the driver to take over navigation.	15

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.3 Generate commands for lateral and longitudinal control.	F4.3 Can not generate correct commands for lateral and longitudinal control.	F4.3.1 Navigation capability is lost. Vehicle may not be able to follow the planned route. Travel time may be increased. Driver may be annoyed.	5	F4.3.1 Absolute position sensor fails or gives erroneous readings	4	F4.3.1 Supervisory elements are needed to monitor the sensor. Redundant methods shall be used to calculate the position of the vehicle. The driver shall be warned of the failure and given the authority to take over navigation and generate the commands for lat./long. control.	20
		F4.3.2 Navigation capability is lost. Vehicle may not be able to follow the planned route. Travel time may be increased. Driver may be annoyed.	5	F4.3.2 Navigation software failure	2	F4.3.2 All the software units shall be carefully tested. Detection methods shall be used to detect failures and warn the driver to take over navigation and generate the commands for the lat./long. control.	10
F4.4 Enable navigation.	F4.4 Can not enable navigation.	F4.4 Vehicle depends on driver to give navigation commands. The vehicle may fail the check-in test.	5	F4.4 Electronic circuitry or software failure.	2	F4.4 Electronic circuitry and software shall be sufficiently reliable. The driver may have to ask for permission to operate on AHS without a navigation system.	10
F4.5 Disable navigation.	F4.5 Can not disable navigation.	F4.5 May distract driver.	1	F4.5 Electronic circuitry failure	2	F4.5 Electronic circuitry shall be sufficiently reliable.	2

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H4.2 Speed and Headway Maintenance and Rear-end Collision Avoidance.							
F4.6 Calculate safe headway	F4.6 Loss of ability to calculate correct value of safe headway	F4.6.1 Headway is set to the default value. Efficiency is affected.	6	F4.6.1 Detected malfunction or inability of the sensors to estimate the braking capabilities and intentions of the preceding vehicle and/or vehicle.	6	F4.6.1 The malfunction of sensors or gross inaccuracies in the estimation of the braking capabilities must be detected fast. The system must fall back to the default headway that takes into account the inaccuracies or malfunction of the sensors.	36
		F4.6.2 Headway is set to the default value. Efficiency is affected.	6	F4.6.2 Detected malfunction or loss of communication with preceding vehicle	6	F4.6.2 Diagnostics and built-in self tests must be used to guarantee a fast detection of the communication failures. When a malfunction occurs the headway must be automatically increased to the default safe level that takes into account the failure	36
		F4.6.3 Unsafe headway is used and rear-end collision is possible or a large headway is used and efficiency is affected	10	F4.6.3 Faulty or inaccurate measurements of braking capabilities of vehicle and/or preceding vehicle	6	F4.6.3 The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements must be monitored and taken into account in the calculation of the safe headway.	60

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F4.6.4 Unsafe headway is used and rear-end collision is possible or large headway is used and efficiency is affected.	10	F4.6.4 Incorrect braking capabilities and intentions is received through communication due to interference or noise corruption	6	F4.6.4 The measurements of braking capabilities of all vehicles must be accurate. The system must check the reasonableness of preceding vehicle's braking capability and take into account possible inaccuracies and inconsistencies in calculating the safe headway.	60
		F4.6.5 Headway is increased in order to maintain safety level. Efficiency is affected.	6	F4.6.5 Loss of communication with roadway and/or lack of headway recommendation	4	F4.6.5 System must be able to accommodate the lack of headway recommendation from roadway .	24
		F4.6.6 Headway is set to the default value if failure is detected . Efficiency is affected. If failure is not detected safety is affected due to possible use of an unsafe headway.	9	F4.6.6 Loss of braking data information from preceding vehicle due to receiver malfunction.	4	F4.6.6 System must have supervisory elements and diagnostics that monitor the functionality of the receiver and detect malfunctions. The malfunction of the receiver must be taken into account in calculating the safe headway.	36

Table 15 Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F4.7 Maintain speed.	F4.7.1 Loss of speed maintenance function.	F4.7.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Traffic rules may be violated. The steering functions may be affected especially around curves.	9	F4.7.1.1 Speed sensor gives erroneous or variable readings.	2	F4.7.1.1 Diagnostics and built in tests must perform a test for reasonableness on sensor data. Redundant speed sensors not subject to common mode failures must be used. When sensor malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F4.7.1.2 As above.	9	F4.7.1.2 Controller electronics or software failure.	2	F4.7.1.2 The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F4.7.1.3 Braking may be used to control speed. Vehicle may be at low speed affecting capacity and efficiency.	9	F4.7.1.3 Throttle actuator failure.	3	F4.7.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	27

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F4.7.1.4 Vehicle accelerates above desired speed or decelerates below desired speed. Speed limit may be exceeded. The steering function will be affected around curves. Vehicle may go out of control around curves.	10	F4.7.1.4 Brake actuator failure (brake cannot be applied or brake is continuously applied)	3	F4.7.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failures must be employed together with the appropriate logic and diagnostics that allow automatic switching from a failed actuator to a healthy one. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	30
		F4.7.1.5 Vehicle travels too fast which is unsafe or too slow which reduces capacity. Speed may be faster than what road conditions permit. It may affect the performance of the lane keeping function.	8	F4.7.1.5 Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication.	3	F4.7.1.5 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.) When a communication malfunction is detected the system shall fall back to a default lower speed if there is no valid target to follow.	24

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F4.7.1.6 Same as F3.3.1.5	8	F4.7.1.6 Loss of target speed information due to receiver malfunction	3	F4.7.1.6 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. If the receiver has a malfunction the driver may be required to initiate a check-out procedure and exit the lane.	24
	F4.7.2 System switches to headway maintenance in the absence of valid target.	F4.7.2 Sudden change in speed. Unnecessary braking. The collision avoidance function may be activated. Driving comfort and efficiency are affected.	9	F4.7.2 Ranging sensor detects an invalid target within the default headway	6	F4.7.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	54

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F4.8 Maintain headway	F4.8 Cannot maintain headway	F4.8.1 SHM stops operating. Headway may become too large or too small, unexpectedly. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F4.8.1 Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability.	6	F4.8.1 System must be able to detect and accommodate an intermittent sensor failure. System software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and transition to manual control by following check-out procedure. Redundant ranging sensors, not subject to common mode failures, with appropriate logic must be used.	60
		F4.8.2 SHM switches to speed maintenance mode even if a valid target exists. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F4.8.2 Sensor loses target due to road curvature or insufficient target reflectiveness.	7	F4.8.2 The sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Vehicle shall slow down and transition to manual control when target is ambiguous and cannot be followed reliably. Sensor redundancies must be used to track targets around curves and minimize the possibility of interference.	70

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F4.8.3 SHM accelerates or decelerates vehicle unexpectedly . The RECA may be activated. Riding comfort and efficiency may be affected.	7	F4.8.3 Ranging sensor has locked on an invalid target.	7	F4.8.3 The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. System must distinguish vehicles moving to adjacent lanes and around curves in the same lane. Redundant ranging sensors not subject to same failure mode with appropriate logic may be required.	49
		F4.8.4 System may fail to maintain selected headway. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F4.8.4 Brake actuator failure. (Or intermittent failure to respond)	3	F4.8.4 System must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators that are not subject to common mode failures with appropriate logic must be used. When a redundant braking path fails the system shall initiate a check-out procedure.	30

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F4.8.5 System may fail to maintain selected headway. The collision avoidance function may be affected.	10	F4.8.5 Throttle actuator failure.	3	F4.8.5 The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. Redundant throttle actuators must be used that are not subject to common mode failures. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	30
		F4.8.6 System may fail to maintain selected headway. The collision avoidance function may be activated. System may fail to adjust speed around curves leading to possible lane departure and collision.	10	F4.8.6 Controller electronics or software failure.	2	F4.8.6 The controller must have supervisory elements (in hardware and software) or adequate redundancies. System shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.	20
		F4.8.7 SHM accelerates or decelerates vehicle unexpectedly. Headway becomes too small or too large. The collision avoidance function may be turned on and off unexpectedly. Vehicle may depart lane, go out of control and cause multiple collisions.	10	F4.8.7 Ranging sensor gives erroneous readings.	4	F4.8.7 The system must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. Redundant ranging sensors not subject to common mode failures must be used. System shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.	40

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F4.9 Switch from maintaining cruise speed to maintaining headway	F4.9 Failure to switch to maintaining headway even when a valid target exists.	F4.9.1 Headway may become too small without the collision avoidance function been activated. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F4.9.1 Ranging sensor fails to detect a valid target.	5	F4.9.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics. In case of sensor failure the system shall switch to manual control by providing a warning to the driver slowing down and following the check-out procedure.	50
		F4.9.2 Headway may become too large or too small. The collision avoidance function may be impaired or may be turned on and off in an effort to keep the headway within safe level. Riding comfort and efficiency are affected. The lane keeping function around curves may be affected.	9	F4.9.2 Hardware or software failure of the SHM.	2	F4.9.2 The system must have supervisory elements (in hardware or software) or adequate redundancies. System shall switch to manual control by warning driver and following a check-out procedure in case of a detected failure.	18

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F4.10 Switch from maintaining headway to maintaining cruise speed.	F4.10 Failure to switch to speed maintenance mode when the original target moves out of the lane and becomes unsuitable to follow, and no other valid target exists.	F4.10.1 Vehicle speed varies instead of being constant in the absence of a valid target. The collision avoidance function may be activated unexpectedly. Riding comfort and efficiency may be affected.	8	F4.10.1 Ranging sensor locks on the original target or locks on another target which is invalid when the original target becomes unsuitable to follow.	6	F4.10.1 System must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics.	48
		F4.10.2 Vehicle speed varies instead of being constant in the absence of a valid target. The collision avoidance function may be activated unexpectedly. Riding comfort and efficiency may be affected.	8	F4.10.2 Hardware or software failure of the SHM	2	F4.10.2 System must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. System shall switch to manual by warning the driver and following a check-out procedure in case of detected failures	16

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F4.11 Keep vehicle in the center of lane.	F4.11 Loss of lane keeping capability	F4.11.1 Vehicle departs lane, goes out of control and collides with other vehicles.	10	F4.11.1 Failure to detect vehicle's lateral position due to malfunction of sensor or roadway lane reference aid.	5	F4.11.1 The system must have redundant measurements of the lateral position of the vehicle. Redundant sensors and reference aids may be required with the appropriate diagnostics and logic. When a redundant component fails the system shall switch to manual control or lower ERSC and warn the driver.	50
		F4.11.2 Lane keeping performance is degraded. Vehicle may have to slow down or transition to lower ERSC.	8	F4.11.2 Lane preview information is not available.	3	F4.11.2 System must have redundant means of obtaining preview information. In the absence of preview information the system shall switch to a lower ERSC and warn the driver.	24
		F4.11.3 Vehicle may depart lane and go out of control causing multiple collisions.	10	F4.11.3 Control software or electronics failure	2	F4.11.3 All electronic components and software must have redundancies and appropriate diagnostics to detect failures. When a failure of a redundant component is detected the system shall switch to a lower ERSC and warn the driver. Detection and accommodation of failures shall be fast and shall not affect the performance of the lane keeping function.	20

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F4.11.4 same as F4.11.3	10	F4.11.4 Steering actuator failure	3	F4.11.4 Redundant steering actuators and components with the appropriate diagnostics and logic must be used. When a redundant component fails the system shall warn the driver to assume manual control of the steering function by following a check-out procedure.	30
F4.12 Coordinate lane change with other vehicles.	F4.12 Loss of coordination of lane changing with other vehicles.	F4.12 Traffic may be disturbed. Collision avoidance function may be activated unnecessarily. Collision is possible.	9	F4.12.1 Loss of vehicle to vehicle communication	3	F4.12.1 Vehicles shall have supervisory program to check communications. If any failure takes place either in transmitting or receiving signals, the vehicle shall be advised to check out. Roadway may be used as backup for the coordination	27
		Same as above	9	F4.12.2 Coordination software failure	2	The system software must be tested thoroughly for all possible situations before implemented. Some redundancies in software may be necessary i.e., similar algorithms are implemented using different software tools.	18

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.13 Synchronize speed and headway for lane change.	F4.13 Can not synchronize speed and headway during lane change.	F4.13 Lane change may not be completed or may be not be smooth Collision avoidance function may be activated. Collision with other vehicles is possible	10	F4.13.1 Failure in getting position and/or velocity of vehicles in adjacent lane.	4	F4.13.1 Vehicle shall have the capability to sense the position and velocity of multi-vehicles both in front and in adjacent lanes; supervisory elements and adequate redundancies are needed. Fall back to ERSC 3 when malfunction is detected.	40
		Same as above	10	F4.13.2 Control software or electronics failure	2	F4.13.2 The system shall have supervisory elements and adequate redundancies. Warn driver to check out when malfunction is detected.	20
		Same as above	10	F4.13.3 Throttle actuator or brake actuator failure	3	F4.13.3 Sensors and diagnostic programs are needed to monitor throttle and brake actuator actions. Redundant actuators must be used. Driver shall be warned to check out when failure is detected.	30
F4.14 Change lane.	F4.14 Loss of lane change function	F4.14 If failure is detected early the lane change will not take place. In such case the driver may have to take over. If failure is undetected and lane change is attempted collision may take place.	10	F4.14.1 Lateral sensor failure	4	F4.14.1 Redundant lateral sensors must be used. Diagnostics shall be used to detect failures before the initiation of a lane change.	40

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F4.14.2 Same as for F4.14.1	10	F4.14.2 Control software or electronics failure	2	F4.14.2 System shall have supervisory programs (in hardware and software) and adequate redundancies. Diagnostics shall be used to detect failures before the initiation of a lane change.	20
		F4.14.3 Vehicle may go out of control and cause multiple collisions.	10	F4.14.3 Steering actuator failure	3	F4.14.3 Redundant steering actuators are required. Sensors and diagnostic program are needed to monitor steering actuator actions. Switching from one redundant path to another shall not affect steering performance. If a redundant path fails a check out procedure shall be initiated.	30

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.15 Switch from lane changing to longitudinal control.	F4.15 Vehicle fails to resume lane keeping and longitudinal control in the new lane	F4.15.1 Traffic may be disturbed. Collision avoidance function may be activated, bringing the vehicle to a complete stop. Collision is possible.	10	F4.15.1 The lateral position sensor gives erroneous readings (the vehicle does not know it has reached the desired lane).	3	F4.15.1 Supervisory elements and adequate redundancies are needed. When failure is detected the vehicle shall stop and warn the driver to check-out.	30
		F4.15.2 Same as in F4.15.1	10	F4.15.2 Control software failure	2	F4.15.2 Supervisory programs shall be used. All software units must be tested for full range of inputs before implemented. When failure is detected the vehicle shall stop and warn the driver to check out.	20
		F4.15.3 Same as in F4.15.1	10	F4.15.3 The SHM function fails.	5	F4.15.1 The system shall have supervisory and redundant elements that detect and accommodate SHM function failures. In case of failure the vehicle shall stop, warn the driver to take over and check-out.	50

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.16 Combined lateral and longitudinal collision avoidance	F4.16 Loss of combined lateral and longitudinal collision avoidance	F4.16.1 Multiple collisions may take place.	10	F4.16.1 Loss of communication with surrounding vehicles	3	F4.16.1 Supervisory elements are needed to monitor communication. Driver shall be warned to check out when communication capability is lost.	30
		F4.16.2 Same as in F4.16.1	10	F4.16.2 On-board sensors fail to detect surrounding vehicles' positions speeds and intentions.	4	F4.16.2 Redundant sensors are needed; the system shall continuously monitor the reasonableness of sensor data. The driver shall be warned to check out when a redundant path fails.	40
		F4.16.3 Same as in F4.16.1	10	F4.16.3 Control software or electronics failure	2	F4.16.3 System supervisory elements both in software and hardware must be used. All software shall be tested for full range of inputs.	20
		F4.16.4 Same as in F4.16.1	10	F4.16.4 Brake or throttle or steering actuator failure	4	F4.16.4 Sensors and diagnostic program are needed to monitor actuator response. Redundant brake, throttle steering actuators are needed.	40
		F4.16.5 Same as in F4.16.1	10	F4.16.5 The incorrect TTC is calculated	7	F4.16.5 All factors affecting the calculation of TTC as well as the discrepancies involved in evaluating these factors shall be taken into account. Redundant methods shall be used to calculate TTC.	70

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.17 Switch to normal operation after the activation of the collision avoidance function.	F4.17 Can not switch from collision avoidance back to normal operation.	F4.17 Vehicle may come to full stop unnecessarily. Traffic may be disturbed. Driver may need to intervene.	8	F4.17 Control software failure in switching logic	2	F4.17 The control software must be reliable. It shall be tested under all possible conditions before implemented. Redundant software tools may be essential.	16
F4.18 Enable lat./long. functions	F4.18 Can not enable the automatic control system.	F4.18 Vehicle has to be controlled manually. Vehicle fails the check-in test.	6	F4.18 Electronic circuitry failure	2	F4.18 The electronic circuitry must be sufficiently reliable. Driver shall be notified about the vehicle operating mode.	12
F4.19 Disable (check out)	F4.19 Can not disable the automatic control system.	F4.19.1 Vehicle may not be able to get out of the auto lane. The check-out procedure cannot be carried out.	8	F4.19.1 Electronic circuitry failure	2	F4.19.1 The electronic circuitry must be sufficiently reliable. Some redundancy is needed.	16
			6	F4.19.2 Driver does not handle throttle, brake, and steering properly and fails to pass the check-out test.	4	F4.19.2 Handling the throttle, brake, and steering during check-out shall be no more difficult than in normal driving. Supervisory elements are needed to monitor driver operation.	24

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
H4.3 Driver Vehicle Roadway Interface							
F4.20 Check in.	F4.20 Failure of check-in function.	F4.20.1 Vehicle is operating in the auto lane even though it should not.	9	F4.20.1 On-board diagnostics fail to detect a fault in major functions of the vehicle.	3	F4.20.1 Diagnostics algorithms shall be robust and highly reliable. Roadway shall be able to detect an unfit vehicle operating in the auto-lane.	27
		F4.20.2 Vehicle is operating in the auto lane even though it should not.	9	F4.20.2 Roadway failed to detect that vehicle is not fit for AHS.	3	F4.20.2 Roadway shall be able to identify unfit vehicles at check-in.	27
		F4.20.3 Vehicle is not allowed to enter the auto lane even though it is fit.	6	F4.20.3 On-board diagnostics make a wrong decision about a component or function that was not at fault.	2	F4.20.3 Diagnostic algorithms shall be highly reliable. The system shall repeat the diagnostics if the vehicle is rejected.	12
F4.21 Enter AHS.	F4.21 Can not enter AHS.	F4.21 Driver has to drive the vehicle on manual lane and try to enter AHS in another time	4	F4.21 There is not enough gap in entry point or entry area.	2	F4.21 Entry area shall have enough space to accommodate vehicles. Vehicles have to be notified in advance of the availability of space.	8
F4.22 Merge into the auto lanes.	F4.22 Can not merge into the auto lane.	F4.22.1 The vehicle has to wait in the entry point or area.	4	F4.22.1 Roadway fails to coordinate a gap.	4	F4.22.1 The roadway shall have redundant algorithms and back-up modes for coordination of vehicle speeds and headway.	16
		F4.22.2 The vehicle has to wait in the entry point or area.	4	F4.22.2 On board sensors give incorrect measurements.	6	F4.22.2 Check-in tests shall be able to test correctness and functionality of on-board sensors.	24

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.23 Change of trip destination	F4.23.1 Give wrong destination.	F4.23.1 Driver may not get to the desired destination through navigation. Travel time may be increased.	5	F4.23.1 Driver error	4	F4.23.1 The destination and the computed route shall be displayed to the driver. Call for driver's attention when a new route is calculated each time.	20
	F4.23.2 Can not change the trip destination.	F4.23.2 The navigation system can not be used. Vehicle has to check out. Driver may be frustrated or may be required to take over navigation.	5	F4.23.2 Input device failure	1	F4.23.2 The input device shall be sufficiently reliable.	5
F4.24 Alert driver to check out.	F4.24.1 System does not alert driver to check out when necessary.	F4.24.1 Vehicle may stay under automatic mode even if it should not. Collisions may take place.	10	F4.24.1 Software failure	2	F4.24.1 System shall have reliable diagnostic algorithms.	20
		F4.24.2 Vehicle may stay under automatic mode even if it should not. Collisions may take place.	10	F4.24.2 Alert device failure	3	F4.24.2 Adequate redundant alert devices are needed.	30
F4.25 Check out.	F4.25.1 Can not check out.	F4.25.1.1 The vehicle will keep going on. Driver may feel out of control, panic, get frustrated.	7	F4.25.1.1 Controller failed to recognize check-out initiation input.	2	F4.25.1.1 The system shall be sufficiently reliable. Some redundancy to initiate check-out is needed.	14

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F4.25.1.2 Failure to reduce speed or increase headway or to notify the roadway.	7	F4.25.1.2 Controller software failure.	2	F4.25.1.2 System shall have supervisory elements in software. Once a failure is detected vehicle shall automatically slow down and stop, and warn the driver to take over.	14
		F4.25.1.3 The driver is not warned to take over steering, throttle and brake control. Vehicle keeps on going in auto lane.	7	F4.25.1.3 Warning delivery device failure.	2	F4.25.1.3 Warning device shall be reliable. Redundant warning delivery methods shall be used.	14
	F4.25.2 Driver fails to pass check-out test.	F4.25.2 The vehicle is guided to an exit ramp or to a shoulder of the lane and then brought to a full stop.	7	F4.25.2 Driver's failure in handling throttle, brake, and steering properly during check-out.	4	F4.25.2 System shall employ driver status diagnostics. Supervisory program is needed to monitor driver's reaction. Roadway shall be able to access on-board computer database for the diagnostics results. Handling throttle, brake, and steering during check-out shall be no more difficult than in normal manual driving.	28

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.26 Exit auto lane.	F4.26 Driver can not drive the vehicle to the exit of the auto lane.	F4.26 Vehicle remains in the auto lane. Traffic regulations may be violated. System performance may be degraded.	7	F4.26 There is not enough gap in manual lane.	6	F4.26 Dedicated transition lane or some form of regulation such as "yield to auto lane" shall be implemented to ensure easy exit even when traffic congestion happens in the manual lane. The driver shall be warned of congestion ahead of time via traffic information communication.	42
F4.27 Fall back to ERSC 3	F4.27.1 System does not fall back to ERSC3 even when it is necessary.	F4.27.1 The system may continue operating as in ERSC4 even though it should not. Unreliable operation may lead to collisions.	10	F4.27.1 Software failure	2	F4.27.1 Reliable supervisory and diagnostics programs shall be implemented.	20
	F4.27.2 Driver fails to assume responsibility for lane changing and navigation when lane change function or overall collision avoidance function become inaccurate or their redundant paths fail.	F4.27.2.1 Same as in F4.27.1	10	F4.27.2.1 Warning delivery device failure.	2	F4.27.2.1 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F4.27.2.2 Same as in F4.27.1	10	F4.27.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F4.27.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50
F4.28 Fall back to ERSC2.	F4.28.1 System does not fall back to ERSC2 even when it is necessary (reduce speed, increase headway).	F4.28.1 Safety is compromised. Collision is possible.	10	F4.28.1 Software failure	2	F4.28.1 Reliable supervisory and diagnostics program shall be implemented.	20
	F4.28.2 Driver fails to assume roles for ERSC2.	F4.28.2.1 Safety is compromised. Collision is possible.	10	F4.28.2.1 Warning delivery device failure	2	F4.28.2.1 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20
		F4.28.2.2 Same as in F4.28.2.1	10	F4.28.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F4.28.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.29 Fall back to ERSC1.	F4.29.1 System does not fall back to ERSC1 even when it is necessary (reduce speed, increase headway).	F4.29.1 Safety is compromised. Collision is possible.	10	F4.29.1 Software failure	2	F4.29.1 Reliable supervisory and diagnostics program shall be implemented.	20
	F4.29.2 Driver fails to assume roles for ERSC1.	F4.29.2.1 Safety is compromised. Collision is possible.	10	F4.29.2.1 Warning delivery device failure	2	F4.29.2.1 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20
		F4.29.2.2 Same as in F4.29.2.1	10	F4.29.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F4.29.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50

Table 15: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-4)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F4.30 Fall back to manual control.	F4.30.1 System does not fall back to manual even when it is necessary.	F4.30.1 Safety is compromised. Collision is possible.	10	F4.30.1 Software failure	2	F4.30.1 Reliable supervisory and diagnostics program shall be implemented.	20
	F4.30.2 Driver fails to assume roles for manual control.	F4.30.2.1 Safety is compromised. Collision is possible.	10	F4.30.2.1 Warning delivery device failure	2	F4.30.2.1 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20
		F4.30.2.2 Safety is compromised. Collision is possible.	10	F4.30.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F4.30.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50
F4.31 Notify driver of correct mode of operation.	F4.31 Fail to notify driver of correct mode of operation.	F4.31 Driver may get confused by receiving or not receiving warnings when expected to.	8	F4.31 Electronics or software failure.	3	F4.31 The electronics and software must be very reliable. Redundancies and on board diagnostics may be used to improve reliability.	24

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
H5.1 Roadway navigation Functions							
F5.1 Receive i.d., position, speed and destination from all vehicles in a designated section.	F5.1. Does not receive position, speed and destination information from any vehicle.	F5.1 Roadway can not provide navigation to vehicles and can not optimize traffic flow. Efficiency may be reduced.	7	F5.1 Roadway communication failure	3	F5.1 Roadway must have redundant communication systems. Vehicle shall have their own navigation system as a backup to the roadway system.	21
F5.2 Calculate navigation commands for each vehicle.	F5.2 Loss of ability to calculate correct navigation commands for each vehicle	F5.2 Roadway can not provide navigation to vehicles and can not optimize traffic flow. Efficiency may be reduced.	7	F5.2.1 Software or electronics failure	4	F5.2.1 Supervisory elements (in hardware and software) are needed to monitor the navigation process. Notify each vehicle when malfunction in roadway navigation system is detected. Vehicles shall notify the roadway if navigation commands are inconsistent with destination.	28
		F5.2 Roadway can not provide navigation to vehicles and can not optimize traffic flow. Efficiency may be reduced.	7	F5.2.2 Lack of network traffic information	2	F5.2.2 Reliable network communication shall be implemented.	14
F5.3 Send navigation commands to each vehicle.	F5.3.1 Can not send navigation command to any vehicle.	F5.3.1 Loss of roadway navigation capability	7	F5.3.1 Roadway communication failure	3	F5.3.1 Roadway shall have redundant communication system. Vehicle shall have their own navigation system as a backup to the roadway system.	21

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
H5.2 Vehicle Navigation Functions							
F5.4 Send vehicle i.d., position, speed, and destination to roadway.	F5.4 Can not send vehicle position, speed, and destination to roadway.	F5.4.1 Roadway can not compute navigation command for the vehicle and loses the ability to optimize traffic flow. Vehicle is not able to navigate itself either.	8	F5.4.1 Vehicle is unable to determine its position.	3	F5.4.1 Redundant method to determine absolute position are needed. Vehicle may send a position relative to another vehicle when it is unable to determine its absolute position.	24
		F5.4.2 Roadway can not compute navigation command for the vehicle and loses the ability to optimize traffic flow.	7	F5.4.2 On-board transmitter failure.	3	F5.4.2 Supervisory elements are needed to monitor the transmitter. The vehicle shall be asked to check out if transmitter fails.	21
F5.5 Receive navigation commands from roadway.	F5.5Can not receive navigation commands from roadway.	F5.5 Loss of roadway navigation capability	7	F5.5 Vehicle receiver failure	4	F5.5 Supervisory elements are needed to monitor communication. Redundant receivers may be required.	28
F5.6 Check validity of navigation commands.	F5.6 Can not check validity of navigation commands.	F5.6 Vehicle may follow the wrong route. Travel time may be increased.	7	F5.6. Software fails or traffic information is not available.	2	F5.6 Navigation commands shall be presented to the driver. When a new route is computed, driver shall be notified.	14

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.7 Transfer navigation commands to lateral and longitudinal controller.	F5.7 Can not transfer navigation commands to lateral and longitudinal controller.	F5.6 Loss of navigation function	8	F5.7 Coordination software failure	2	F5.7 Supervisory programs are needed to monitor the navigation commands and lateral, longitudinal controller action.	16
F5.8 Enable navigation.	F5.8 Can not enable navigation.	F5.8 Vehicle depends on driver to give navigation commands.	3	F5.8 Electronic circuitry failure.	2	F5.8 Electronic circuitry shall be sufficiently reliable. The vehicle shall be rejected during check-in if navigation can not be enabled.	6
F5.9 Disable navigation.	F5.9 Can not disable navigation.	F5.9 Driver may be distracted.	3	F5.9 Electronic circuitry failure	2	F5.9 Electronic circuitry should be sufficiently reliable. There should be redundant methods to turn off navigation system.	6

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
H5.3 Automated Lateral / Longitudinal Control							
F5.10 Calculate safe headway	F5.10 Loss of ability to calculate correct value of safe headway	F5.10.1 Headway is set to the default value. Efficiency is affected.	6	F5.10.1 Detected malfunction or inability of the sensors to estimate the braking capabilities and intentions of the preceding vehicle and/or vehicle.	6	F5.10.1 The malfunction of sensors or gross inaccuracies in the estimation of the braking capabilities must be detected fast. The system must fall back to the default headway that takes into account the inaccuracies or malfunction of the sensors.	36
		F5.10.2 Headway is set to the default value. Efficiency is affected.	6	F5.10.2 Detected malfunction or loss of communication with preceding vehicle	6	F5.10.2 Diagnostics and built-in self tests must be used to guarantee a fast detection of the communication failures. When a malfunction occurs the headway must be automatically increased to the default safe level that takes into account the failure	36
		F5.10.3 Unsafe headway is used and rear-end collision is possible or a large headway is used and efficiency is affected	10	F5.10.3 Faulty or inaccurate measurements of braking capabilities of vehicle and/or preceding vehicle	6	F5.10.3 The measurement of braking capabilities must be accurate and reliable. The consistency and accuracy of these measurements must be monitored and taken into account in the calculation of the safe headway.	60

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F5.10.4 Unsafe headway is used and rear-end collision is possible or large headway is used and efficiency is affected.	10	F5.10.4 Incorrect braking capabilities and intentions is received through communication due to interference or noise corruption	6	F5.10.4 The measurements of braking capabilities of all vehicles must be accurate. The system must check the reasonableness of preceding vehicle's braking capability and take into account possible inaccuracies and inconsistencies in calculating the safe headway.	60
		F5.10.5 Headway is increased in order to maintain safety level. Efficiency is affected.	6	F5.10.5 Loss of communication with roadway and/or lack of headway recommendation	4	F5.10.5 System must be able to accommodate the lack of headway recommendation from roadway .	24
		F5.10.6 Headway is set to the default value if failure is detected . Efficiency is affected. If failure is not detected safety is affected due to possible use of an unsafe headway.	9	F5.10.6 Loss of braking data information from preceding vehicle due to receiver malfunction.	4	F5.10.6 System must have supervisory elements and diagnostics that monitor the functionality of the receiver and detect malfunctions. The malfunction of the receiver must be taken into account in calculating the safe headway.	36

Table 16 Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F5.11 Maintain speed.	F5.11.1 Loss of speed maintenance function.	F5.11.1.1 Vehicle accelerates above or decelerates below desired speed instead of maintaining constant speed or maintains incorrect level of constant speed. Traffic rules may be violated. The steering functions may be affected especially around curves.	9	F5.11.1.1 Speed sensor gives erroneous or variable readings.	2	F5.11.1.1 Diagnostics and built in tests must perform a test for reasonableness on sensor data. Redundant speed sensors not subject to common mode failures must be used. When sensor malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F5.11.1.2 Same as above.	9	F5.11.1.2 Controller electronics or software failure.	2	F5.11.1.2 The system must have supervisory elements (in hardware and software) or adequate redundancies. When a controller malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	18
		F5.11.1.3 Braking may be used to control speed. Vehicle may be at low speed affecting capacity and efficiency.	9	F5.11.1.3 Throttle actuator failure.	3	F5.11.1.3 The system must use sensors and diagnostic programs to monitor the throttle actuator. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	27

Table 16: Failure Modes and Effects Analysis (System FMEA) (ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F5.11.1.4 Vehicle accelerates above desired speed or decelerates below desired speed. Speed limit may be exceeded. The steering function will be affected around curves. Vehicle may go out of control around curves.	10	F5.11.1.4 Brake actuator failure (brake cannot be applied or brake is continuously applied)	3	F5.11.1.4 The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators not subject to common mode failures must be employed together with the appropriate logic and diagnostics that allow automatic switching from a failed actuator to a healthy one. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	30
		F5.11.1.5 Vehicle travels too fast which is unsafe or too slow which reduces capacity. Speed may be faster than what road conditions permit. It may affect the performance of the lane keeping function.	8	F5.11.1.5 Loss of target speed information due to receiver malfunction	3	F5.11.1.5 System must have supervisory elements in controller software and receiver that detect any receiver malfunction. The roadway must assist in testing receiver functionality. If the receiver has a malfunction the driver may be required to initiate a check-out procedure and exit the lane.	24

Table 16: Failure Modes and Effects Analysis (System FMEA) (ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F5.11.1.6 Same as F3.3.1.5	8	F5.11.1.6 Vehicle does not receive target speed due to loss of communication or target speed is corrupted during communication.	3	F5.11.1.6 System must have diagnostic programs to test for reasonableness on received target speed data and monitor the operation of communication devices. System must be able to accommodate temporary loss of communication. The system must ensure data integrity by some error detection and correction scheme. (parity, checksum etc.) When a communication malfunction is detected the system shall fall back to a default lower speed if there is no valid target to follow.	24
	F5.11.2 System switches to headway maintenance in the absence of valid target.	F5.11.2 Sudden change in speed. Unnecessary braking. The collision avoidance function may be activated. Driving comfort and efficiency are affected.	9	F5.11.2 Ranging sensor detects an invalid target within the default headway	6	F5.11.2 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics.	54

Table 16: Failure Modes and Effects Analysis (System FMEA) (ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F5.12 Maintain headway	F5.12 Cannot maintain headway	F5.12.1 SHM stops operating. Headway may become too large or too small, unexpectedly. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F5.12.1 Ranging sensor fails to provide signal. Intermittent or sudden loss of ranging capability.	6	F5.12.1 System must be able to detect and accommodate an intermittent sensor failure. System software must compensate for momentary loss of ranging capability. If the loss of ranging capability cannot be masked or compensated for, the vehicle shall slow down and transition to manual control by following check-out procedure. Redundant ranging sensors, not subject to common mode failures, with appropriate logic must be used.	60
		F5.12.2 SHM switches to speed maintenance mode even if a valid target exists. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F5.12.2 Sensor loses target due to road curvature or insufficient target reflectiveness.	7	F5.12.2 The sensor must have an adequately wide field of view and employ suitable algorithms to reduce the likelihood of missing or losing a valid target. Vehicle shall slow down and transition to manual control when target is ambiguous and cannot be followed reliably. Sensor redundancies must be used to track targets around curves and minimize the possibility of interference.	70

Table 4: Failure Modes and Effects Analysis (System FMEA) (ERSC-4)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F5.12.3 SHM accelerates or decelerates vehicle unexpectedly . The collision avoidance function may be activated. Riding comfort and efficiency may be affected.	7	F5.12.3 Ranging sensor has locked on an invalid target.	7	F5.12.3 The system must incorporate supervisory elements in software to perform range gating, target discrimination and tests for reasonableness. System must distinguish vehicles moving to adjacent lanes and around curves in the same lane. Redundant ranging sensors not subject to same failure mode with appropriate logic may be required.	49
		F5.12.4 System may fail to maintain selected headway. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F5.12.4 Brake actuator failure. (Or intermittent failure to respond)	3	F5.12.4 System must be able to detect brake actuator failures. The system must use sensors and diagnostic programs to monitor the brake actuator. Redundant brake actuators that are not subject to common mode failures with appropriate logic must be used. When a redundant braking path fails the system shall initiate a check-out procedure.	30

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
		F5.12.5 System may fail to maintain selected headway. The collision avoidance function may be affected.	10	F5.12.5 Throttle actuator failure.	3	F5.12.5 The system must be able to detect throttle actuator failures. The system must use sensors and diagnostic programs to monitor the throttle actuator. Redundant throttle actuators must be used that are not subject to common mode failures. When an actuator malfunction is detected, system shall switch to manual control by warning the driver and following the check-out procedure.	30
		F5.12.6 System may fail to maintain selected headway. The collision avoidance function may be activated. System may fail to adjust speed around curves leading to possible lane departure and collision.	10	F5.12.6 Controller electronics or software failure.	2	F5.12.6 The system must have supervisory elements (in hardware and software) or adequate redundancies. System shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.	20
		F5.12.7 SHM accelerates or decelerates vehicle unexpectedly. Headway becomes too small or too large. The collision avoidance function may be turned on and off unexpectedly. Vehicle may depart lane, go out of control and cause multiple collisions.	10	F5.12.7 Ranging sensor gives erroneous readings.	4	F5.12.7 The system must incorporate supervisory elements (in software) to perform tests for reasonableness on sensor data. Redundant ranging sensors not subject to common mode failures must be used. System shall switch to manual control by warning the driver and following the check-out procedure when failure is detected.	40

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F5.13 Switch from maintaining cruise speed to maintaining headway	F5.13 Failure to switch to maintaining headway even when a valid target exists.	F5.13.1 Headway may become too small without the collision avoidance function been activated. Rear-end collision is possible. Vehicle may depart the lane, go out of control and cause multiple collisions.	10	F5.13.1 Ranging sensor fails to detect a valid target.	5	F5.13.1 System must be able to discriminate between valid and invalid targets. Redundant ranging sensors not subject to common mode failures must be used with appropriate diagnostics. In case of sensor failure the system shall switch to manual control by providing a warning to the driver slowing down and following the check-out procedure.	50
		F5.13.2 Headway may become too large or too small. The collision avoidance function may be impaired or may be turned on and off in an effort to keep the headway within safe level. Riding comfort and efficiency are affected. The lane keeping function around curves may be affected.	9	F5.13.2 Hardware or software failure of the SHM.	2	F5.13.2 The system must have supervisory elements (in hardware or software) or adequate redundancies. System shall switch to manual control by warning driver and following a check-out procedure in case of a detected failure.	18

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F5.14 Switch from maintaining headway to maintaining cruise speed.	F5.14 Failure to switch to speed maintenance mode when the original target moves out of the lane and becomes unsuitable to follow, and no other valid target exists.	F5.14.1 Vehicle speed varies instead of being constant in the absence of a valid target. The collision avoidance function may be activated unexpectedly. Riding comfort and efficiency may be affected.	8	F5.14.1 Ranging sensor locks on the original target or locks on another target which is invalid when the original target becomes unsuitable to follow.	6	F5.14.1 System must be able to discriminate between valid and invalid targets. Redundant sensors not subject to common mode failures must be used with appropriate diagnostics.	48
		F5.14.2 Vehicle speed varies instead of being constant in the absence of a valid target. The collision avoidance function may be activated unexpectedly. Riding comfort and efficiency may be affected.	8	F5.14.2 Hardware or software failure of the SHM	2	F5.14.2 System must be able to detect controller electronics failures. The controller must have supervisory elements (in hardware) or adequate redundancies. System shall switch to manual by warning the driver and following a check-out procedure in case of detected failures	16

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function or subfunction	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Requirements Recommendations	RPN
F5.15 Keep vehicle in the center of lane.	F5.15 Loss of lane keeping capability	F5.15.1 Vehicle departs lane, goes out of control and collides with other vehicles.	10	F5.15.1 Failure to detect vehicle's lateral position due to malfunction of sensor or roadway lane reference aid.	5	F5.15.1 The system must have redundant measurements of the lateral position of the vehicle. Redundant sensors and reference aids may be required with the appropriate diagnostics and logic. When a redundant component fails the system shall switch to manual control or lower ERSC and warn the driver.	50
		F5.15.2 Lane keeping performance is degraded. Vehicle may have to slow down or transition to lower ERSC.	8	F5.15.2 Lane preview information is not available.	3	F5.15.2 System must have redundant means of obtaining preview information. In the absence of preview information the system shall switch to a lower ERSC and warn the driver.	24
		F5.15.3 Vehicle may depart lane and go out of control causing multiple collisions.	10	F5.15.3 Control software or electronics failure	2	F5.15.3 All electronic components and software must have redundancies and appropriate diagnostics to detect failures. When a failure of a redundant component is detected the system shall switch to a lower ERSC and warn the driver. Detection and accommodation of failures shall be fast and shall not affect the performance of the lane keeping function.	20

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F5.15.4 same as F5.15.3	10	F5.15.4 Steering actuator failure	3	F5.15.4 Redundant steering actuators and components with the appropriate diagnostics and logic must be used. When a redundant component fails the system shall warn the driver to assume manual control of the steering function by following a check-out procedure.	30
F5.16 Coordinate lane change with other vehicles.	F5.16 Loss of the coordination capability	F5.16 Traffic may be disturbed. Collision avoidance function may be activated unnecessarily. Collision is possible.	9	F5.16.1 Loss of vehicle to vehicle communication	3	F5.16.1 Vehicles shall have supervisory program to check communications. If any failure takes place either in transmitting or receiving signals, the vehicle shall be advised to check out. Roadway may be used as backup for the coordination	27
			9	F5.16.2 Coordination software failure	2	F5.16.2 The system software must be tested thoroughly for all possible situations before implemented. Some redundancies in software may be necessary i.e., similar algorithms are implemented using different software tools.	18

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.17 Synchronize speed and headway for lane change.	F5.17 Can not synchronize speed and headway during lane change.	F5.17 Lane change may not be completed or may be not be smooth Collision avoidance function may be activated. Collision with other vehicles is possible	10	F5.17.1 Failure in getting position and/or velocity of vehicles in adjacent lane.	4	F5.17.1 Vehicle shall have the capability to sense the position and velocity of multi-vehicles both in front and in adjacent lanes; supervisory elements and adequate redundancies are needed. Fall back to ERSC 3 when malfunction is detected.	40
			10	F5.17.2 Control software or electronics failure	2	F5.17.2 The system shall have supervisory elements and adequate redundancies. Warn driver to check out when malfunction is detected.	20
			10	F5.17.3 Throttle actuator or brake actuator failure	3	F5.17.3 Sensors and diagnostic programs are needed to monitor throttle and brake actuator actions. Redundant actuators must be used. Driver shall be warned to check out when failure is detected.	30
F5.18 Change lane.	F5.18 Loss of lane change function	F5.18 If failure is detected early the lane change will not take place. In such case the driver may have to take over. If failure is undetected and lane change is attempted collision may take place.	10	F5.18.1 Lateral sensor failure	4	F5.18.1 Redundant lateral sensors must be used. Diagnostics shall be used to detect failures before the initiation of a lane change.	40

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F5.18.2 Same as for F5.18.1	10	F5.18.2 Control software or electronics failure	2	F5.18.2 System shall have supervisory programs (in hardware and software) and adequate redundancies. Diagnostics shall be used to detect failures before the initiation of a lane change.	20
		F5.18.3 Vehicle may go out of control and cause multiple collisions.	10	F5.18.3 Steering actuator failure	3	F5.18.3 Redundant steering actuators are required. Sensors and diagnostic program are needed to monitor steering actuator actions. Switching from one redundant path to another shall not affect steering performance. If a redundant path fails a check out procedure shall be initiated.	30

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.19 Switch from lane changing to longitudinal control.	F5.19 Vehicle fails to resume lane keeping and longitudinal control in the new lane	F5.19.1 Traffic may be disturbed. Collision avoidance function may be activated, bringing the vehicle to a complete stop. Collision is possible.	10	F5.19.1 lateral position sensor gives erroneous readings (the vehicle does not know it has reached the desired lane).	3	F5.19.1 Supervisory elements and adequate redundancies are needed. When failure is detected the vehicle shall stop and warn the driver to check-out.	30
		F5.19.2 Same as in F5.19.1	10	F5.19.2 Control software failure	2	F5.19.2 Supervisory programs shall be used. All software units must be tested for full range of inputs before implemented. When failure is detected the vehicle shall stop and warn the driver to check out.	20
		F5.19.3 Same as in F5.19.1	10	F5.19.3 The SHM function fails.	5	F5.19.1 The system shall have supervisory and redundant elements that detect and accommodate SHM function failures. In case of failure the vehicle shall stop, warn the driver to take over and check-out.	50

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.20 Combined lateral and longitudinal collision avoidance	F5.20 Loss of combined lateral and longitudinal collision avoidance	F5.20.1 Multiple collisions may take place.	10	F5.20.1 Loss of communication with surrounding vehicles	3	F5.20.1 Supervisory elements are needed to monitor communication. Driver shall be warned to check out when communication capability is lost.	30
		F5.20.2 Same as in F5.20.1	10	F5.20.2 On-board sensors fail to detect surrounding vehicles' positions speeds and intentions.	4	F5.20.2 Redundant sensors are needed; the system shall continuously monitor the reasonableness of sensor data. The driver be warned to check out when a redundant path fails.	40
		F5.20.3 Same as in F5.20.1	10	F5.20.3 Control software or electronics failure	2	F5.20.3 System supervisory elements both in software and hardware must be used. All software shall be tested for full range of inputs.	20
		F5.20.4 Same as in F5.20.1	10	F5.20.4 Brake or throttle or steering actuator failure	4	F5.20.4 Sensors and diagnostic program are needed to monitor actuator actions. Redundant brake, throttle steering actuators are needed.	40
		F5.20.5 Same as in F5.20.1	10	F5.20.5	7	F5.20.5 All factors affecting the calculation of TTC as well as the discrepancies involved in evaluating these factors shall be taken into account. Redundant methods shall be used to calculate TTC.	70

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.21 Switch from collision avoidance function to normal operation.	F5.21 Can not switch from collision avoidance back to normal operation.	F5.21 Vehicle may come to full stop unnecessarily. Traffic may be disturbed. Driver may need to intervene.	7	F5.21 Control software failure in switching logic	2	F5.21 Redundant sensors are needed; the system shall continuously monitor the reasonableness of sensor data. The driver be warned to check out when a redundant path fails.	14
F5.22 Enable lat./long. functions	F5.22 Can not enable the automatic control system.	F5.22 Vehicle has to be controlled manually. Vehicle fails the check-in test.	6	F5.22 Electronic circuitry failure	2	F5.22 The electronic circuitry must be sufficiently reliable. Driver shall be notified about the vehicle operating mode.	12
F5.23 Disable (check out)	F5.23 Can not disable the automatic control system.	F5.23.1 Vehicle may not be able to get out of the auto lane. The check-out procedure cannot be carried out.	8	F5.23.1 Electronic circuitry failure	2	F5.23.1 The electronic circuitry must be sufficiently reliable. Some redundancy is needed.	16
			6	F5.23.2 Driver does not handle throttle, brake, and steering properly and fails to pass the check-out test.	4	F5.23.2 Handling the throttle, brake, and steering during check-out shall be no more difficult than in normal driving. Supervisory elements are needed to monitor driver operation.	24

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req.. Recommend.	RPN
H5.4 Driver Vehicle Roadway Interface							
F5.24 Check in.	F5.24 Failure of check-in function.	F5.24.1 Vehicle is operating in the auto lane even though it should not.	9	F5.24.1 On-board diagnostics fail to detect a fault in major functions of the vehicle.	3	F5.24.1 Diagnostics algorithms shall be robust and highly reliable. Roadway shall be able to detect an unfit vehicle operating in the auto-lane.	27
		F5.24.2 Vehicle is operating in the auto lane even though it should not.	9	F5.24.2 Roadway failed to detect that vehicle is not fit for AHS.	3	F5.24.2 Roadway shall be able to identify unfit vehicles at check-in.	27
		F5.24.3 Vehicle is not allowed to enter the auto lane even though it is fit.	6	F5.24.3 On-board diagnostics make a wrong decision about a component or function that was not at fault.	2	F5.24.3 Diagnostics algorithms shall be highly reliable. The system shall repeat the diagnostics if the vehicle is rejected.	12
F5.25 Enter AHS.	F5.25 Can not enter AHS.	F5.25 Driver has to drive the vehicle on manual lane and try to enter AHS in another time	4	F5.25 There is no enough gap in entry point or entry area.	2	F5.25 Entry area shall have enough space	8
F5.26 Merge into the auto lanes.	F5.26 Can not merge into the auto lane.	F5.26.1 The vehicle has to wait in the entry point or area.	4	F5.26.1 Roadway fails to coordinate a gap.	4	F5.26.1 The roadway shall have redundant algorithms and back-up modes for coordination of vehicle speeds and headway.	16
		F5.26.2 The vehicle has to wait in the entry point or area.	4	F5.26.2 On board sensors give incorrect measurements.	6	F5.26.2 Check-in tests shall be able to test correctness and functionality of on-board sensors.	24

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.27 Change of trip destination	F5.27.1 Give wrong destination.	F5.27.1 Driver may not get to the desired destination through navigation. Travel time may be increased.	5	F5.27.1 Driver operation failure	4	F5.27.1 The destination and the computed route shall be displayed to the driver. Call for driver's attention when a new route is calculated each time.	20
	F5.27.2 Can not change the trip destination.	F5.27.2 The navigation system can not be used. Vehicle has to check out. Driver may be frustrated.	5	F5.27.2 Input device failure	1	F5.27.2 The input device shall be sufficiently reliable.	5
F5.28 Alert driver to check out.	F5.28.1 System does not alert driver to check out when necessary.	F5.28.1 Vehicle may stay under automatic mode even if it should not. Collisions may take place.	10	F5.28.1 Software failure	2	F5.28.1 System shall have reliable diagnostic algorithms.	20
	F5.28.2 Can not alert driver.	F5.28.2 The vehicle will stay in the auto lane. Travel time may increase.	10	F5.28.2 Alert device failure	3	F5.28.2 Adequate redundant alert devices are needed.	30
F5.29 Check out.	F5.29.1 Can not check out.	F5.29.1.1 The vehicle will keep going on. Driver may feel out of control, panic, get frustrated.	7	F5.29.1.1 Controller failed to recognize check-out initiation input.	2	F5.29.1.1 The system shall be sufficiently reliable. Some redundancy to initiate check-out is needed.	14

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
		F5.29.1.2 Failure to reduce speed or increase headway or to notify the roadway.	7	F5.29.1.2 Controller software failure.	2	F5.29.1.2 System shall have supervisory elements in software. Once a failure is detected vehicle shall automatically slow down and stop, and warn the driver to take over.	14
		F5.29.1.3 The driver is not warned to take over steering, throttle and brake control. Vehicle keeps on going in auto lane.	7	F5.29.1.3 Warning delivery device failure.	2	F5.29.1.3 Warning device shall be reliable. Redundant warning delivery methods shall be used.	14
	F5.29.2 Driver fails to pass check-out test.	F5.29.2 The vehicle is guided to an exit ramp or to a shoulder of the lane and then brought to a full stop.	7	F5.29.2 Driver's failure in handling throttle, brake, and steering properly during check-out.	4	F5.29.2 System shall employ driver status diagnostics. Supervisory program is needed to monitor driver's reaction. Roadway shall be able to access on-board computer database for the diagnostics results. Handling throttle, brake, and steering during check-out shall be no more difficult than in normal manual driving.	28

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.30 Exit auto lane.	F5.30 Driver can not drive the vehicle to the exit of auto lane.	F5.30 Vehicle remains in the auto lane. Traffic regulations may be violated. System performance may be degraded.	7	F5.30 There is not enough gap in manual lane.	6	F5.30 Dedicated transition lane or some form of regulation such as "yield to auto lane" shall be implemented to ensure easy exit even when traffic congestion happens in the manual lane. The driver shall be warned of congestion ahead of time via traffic information communication.	42
F5.31 Fall back to ERSC 4	F5.31 Roadway navigation not available but vehicle does not fall back to ERSC 4	F5.31 Vehicle navigation capability is lost. Driver may have to take over navigation	7	F5.31.1 Software failure	2	F5.31.1 Reliable supervisory and diagnostics program shall be implemented.	14
			7	F5.31.2 Vehicle navigation system failure	3	F5.31.2 The vehicle navigation system shall use redundancies to improve reliability	21
F5.32 Fall back to ERSC 3	F5.32.1 System does not fall back to ERSC3 even when it is necessary.	F5.32.1 Vehicle can not change lane automatically and may not follow the right route. Travel time may be increased. Safety is compromised.	10	F5.32.1 Software failure	2	F5.32.1 Reliable supervisory and diagnostics program shall be implemented.	20
	F5.32.2 Driver fails to assume responsibility for lane changing and navigation when lane change function or overall collision avoidance function become inaccurate or their redundant paths fail.	F5.32.2 Vehicle can not change lane automatically and may not follow the right route. Travel time may be increased. Safety is compromised.	10	F5.32.2 Warning delivery device failure.	2	F5.32.2 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
			10	F5.32.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F5.32.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50
F5.33 Fall back to ERSC2.	F5.33.1 System does not fall back to ERSC2 even when it is necessary (reduce speed, increase headway).	F5.33.1 Safety is compromised. Collision is possible.	10	F5.33.1 Software failure	2	F5.33.1 Reliable supervisory and diagnostics program shall be implemented.	20
	F5.33.2 Driver fails to assume roles for ERSC 2	F5.33.2.1 Safety is compromised. Collision is possible.	10	F5.33.2.1 Warning delivery device failure	2	F5.33.2.1 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20
			10	F5.33.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F5.33.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.34 Fall back to ERSC1.	F5.34.1 System does not fall back to ERSC1 even when it is necessary (reduce speed, increase headway).	F5.34.1 Safety is compromised. Collision is possible.	10	F5.34.1 Software failure	2	F5.34.1 Reliable supervisory and diagnostics program shall be implemented.	20
	F5.34.2 Driver fails to assume roles for ERSC1.	F5.34.2.1 Safety is compromised. Collision is possible.	10	F5.34.2.1 Warning delivery device failure	2	F5.34.2.1 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20
			10	F5.34.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F5.34.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50

Table 16: Failure Modes and Effects Analysis (System FMEA) (VOA: ERSC-5)

System Function	Potential Failure Mode	Potential Effects	S	Potential Causes	O	Design Req. Recommend.	RPN
F5.35 Fall back to manual control.	F5.35.1 Vehicle does not fall back to manual even when it is necessary.	F5.35.1 Safety is compromised. Collision is possible.	10	F5.35.1 Software failure	2	F5.35.1 Reliable supervisory and diagnostics program shall be implemented.	20
	F5.35.2 Driver fails to assume roles for manual control.	F5.35.2.1 Safety is compromised. Collision is possible.	10	F5.35.2.1 Warning delivery device failure	2	F5.35.2.1 Warning device shall be reliable. Redundant warning delivery methods shall be used.	20
			10	F5.35.2.2 Driver ignores the warning unintentionally or becomes confused.	5	F5.35.2.2 The warnings shall be clear and distinguishable from each other. The system shall attempt to exercise driver's attention ("wake him up") from time to time.	50
F5.36 Notify driver of correct mode of operation.	F5.36 Fail to notify driver of correct mode of operation.	F5.36 Driver may get confused by receiving or not receiving warnings when expected to.	8	F5.36 Electronics or software failure.	3	F5.36 The electronics and software must be very reliable. Redundancies and on board diagnostics may be used to improve reliability.	24