Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Malfunction Management Activity Area Report for AHS Health Management

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-95-047
November 1995

FOREWORD

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

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

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

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

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

NOTICE

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

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

1. Report No.
FHWA-

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
MALFUNCTION MANAGEMENT ACTIVITY AREA REPORT FOR AHS HEALTH MANAGEMENT PRECURSOR SYSTEM ANALYSIS

5. Report Date
11/30/94

6. Performing Organization Code

7. Author(s)
DeMers, R.E., Meisner, J.W., Frazzini, R., Funk, H.B., Plocher, T., Krueze, F., Johnson, D., Case, A., Barrett, M., Zhang, W.B., Kittelson, D., Williston, R.B.

8. Performing Organization Report No.

10. Work Unit No. (TRAIS)

9. Performing Organization Name and Address
Honeywell Technology Center
3660 Technology Drive
Minneapolis, Minnesota 55418

11. Contract or Grant No.
DTFH61-93-C-00197

13. Type of Report and Period Covered
Final Report

12. Sponsoring Agency Name and Address
Office of Safety and Traffic Operations R&D
Federal Highway Administration
6300 Georgetown Pike
McLean, Virginia 22101-2296

14. Sponsoring Agency Code

15. Supplementary Notes
Contracting Officer's Technical Representative (COTR)—Richard Bishop, HSR-??

16. Abstract

This report is the final (draft) in a series describing an effort to determine a viable approach to ensuring that the elements of such an Automated Highway System (AHS) are ensured operational, or healthy. The system which performs this assessment, and intervenes if an element is found wanting, we will term a Health Management System. Assessing the health of the vehicle, its operator and the associated infrastructure prior to entry into instrumented mode (check-in), again prior to entry into manual mode (check-out), and the actions to take when either of those assessments are found wanting (malfunction management) are the primary elements of a total health management system (HMS). Previous papers have presented the scenarios and functions, function criticality assessment, allocation, and preliminary mechanization analysis. This paper will present a brief overview of the process used to perform the Health Management study, followed by a discussion of the results produced in this period of performance, including detailed mechanizations of vehicle and roadside functions, reliability and safety analyses, vehicle simulations, and a driver check-out analysis.

17. Key Words
Automated highway system, safety, health management, diagnostics, fault tolerance

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

19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 214	**22. Price**

Table of Contents

List of Figures

List of Tables

INTRODUCTION

DESCRIPTION OF ACTIVITY AREA

Assessing the health of the vehicle, its operator and the associated infrastructure prior to entry into instrumented mode (check-in), again prior to entry into manual mode (check-out), and the actions to take when either of those assessments are found wanting (malfunction management) are critical elements of a total health management system (HMS). Check-in and check-out are thought to be operations that are distributed over time, with some checks or tests occurring as periodic inspections, and others performed "continuously" while the vehicle is in operation, and still others performed at a single phase of operation (power-on, or AHS entry). Of course, they are distributed geographically as well, as on-board tests, tests requiring roadside equipment, or specialized inspection station equipment. The system's capability to adapt to results of these tests forms the final block in the system structure as malfunction management, and the technical study approach addresses these critical factors in a step by step procedure.

The study integrates the three areas of check-in, check-out and malfunction management, and consequently all of the tasks are common to the three areas and cannot be separated. In order to satisfy the requirement for a separate report for each activity area, these reports will be generated such that each will incorporate most, if not all, of the results from the other two areas.

PURPOSE

The purpose of this effort is to identify and analyze the requirements associated with the check-in, check-out and malfunction management aspects of the automated highway system.

ISSUES ADDRESSED

The following issues have been addressed:

- Test of vehicle functions.
- Test of operator characteristics.
- Current and projected state-of-the-art in vehicle critical subsystem design and manufacturing.
- Infrastructure requirements.
- Failure mode analysis.
- Major alternative ways to ensure safe and efficient operation.
- Component check upon start-up.
- Component check on non-AHS roads.
- "On the fly" check-in.
- Built-in vs. dynamic tests.
- System reaction under fault conditions.
- False alarm effects.

THE ANALYSIS AND PROBLEM-SOLVING APPROACH

Our experience in safety critical avionics systems has shown that a comprehensive, effective approach to health management requires that several characteristics be defined early, and maintained throughout the system definition process. Definition of these characteristics is a process of asking a series of related questions, each tier of which depends on the answer to the previous tier. The questions are:

- What operational procedures are involved?
- What functions are involved?
- What systems are required to satisfy the functions?
- For each system, what are the elements or components?
- For each system component, how can it fail?
- For each way it can fail (mode),
  - How bad is that failure?
  - How long do you have to detect and respond?
- For each failure, how can you detect (test for) it?
- For that test,
  - What is the cost?
  - Is any specialized equipment and/or personnel required?
  - When would you perform it?
  - Where would you perform it?
  - How long does the test take to run?
  - How good are the results?
- If that test reports a failure,
  - How long do you have to act?
  - What should your action be?

Processing the above series of questions is captured in a methodology which is standard for performing systems analyses in safety critical design domains such as aircraft flight control. This methodology is depicted in figure 1.

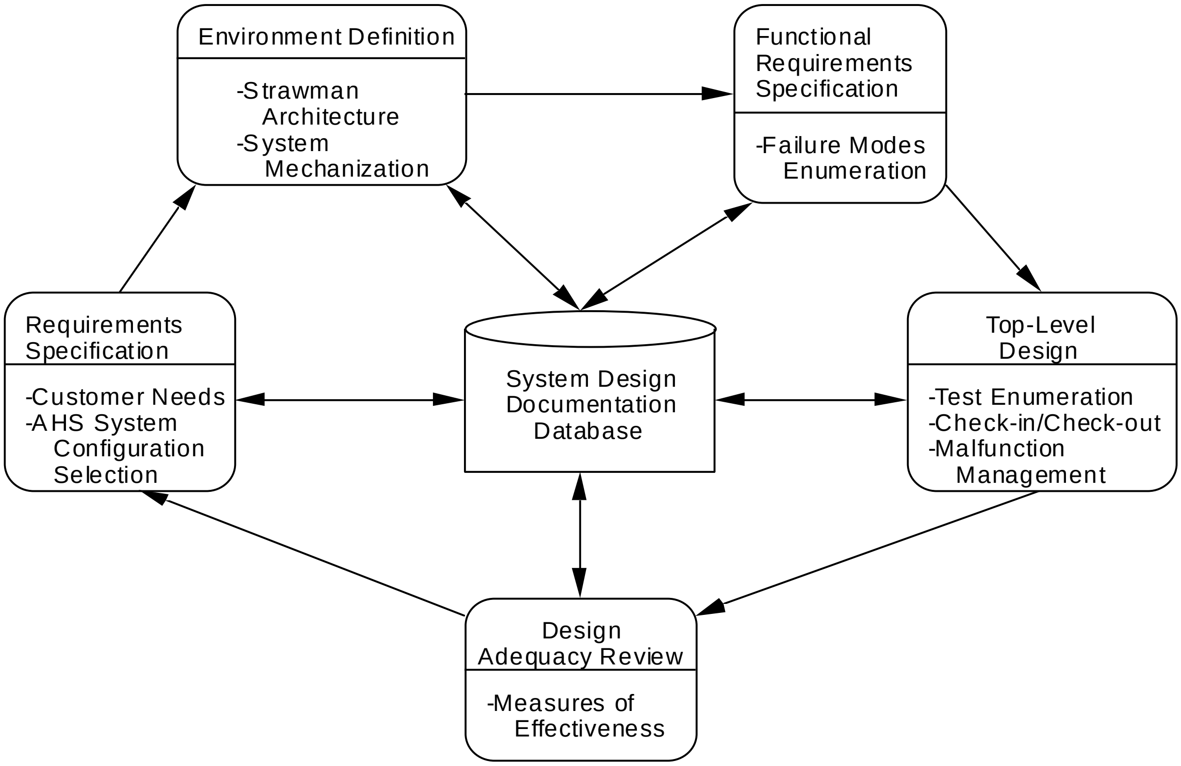

Environment Definition
-Strawman Architecture
-System Mechanization
Functional Requirements Specification
-Failure Modes Enumeration
Requirements Specification
-Customer Needs
-AHS System Configuration Selection
System Design Documentation Database
Top-Level Design
-Test Enumeration
-Check-in/Check-out
-Malfunction Management
Design Adequacy Review
-Measures of Effectiveness

Figure 1. System Engineering Process

Requirements Specification

Customer Needs

When Honeywell builds a system for the aircraft industry, not only is the airframer (Boeing, Douglas, et. al.) the customer, but also the FAA, airlines, and to a certain extent, the airline passengers. Analogously for the AHS, the customers are the car manufacturers, FHWA, individual car owners, and perhaps even the passengers. Since the first step in any system definition is to establish requirements, the object is to consider as many of these "customers" as possible. Consequently, Honeywell has drafted requirements jointly with UCB, the UofM, and the FHWA technical monitor to draw from the broadest possible spectrum.

AHS System Configuration Selection

The AHS configurations were defined to satisfy the following criteria:

- Configurations are sufficiently *specific* to allow for a detailed study of the issues arising for the proposed activities, without being unnecessarily over constrained.
- The two configurations selected are sufficiently *broad* to cover the widest possible range of issues pertinent to our study.
- The Configurations are *realistic* and highly probable implementations for the actual AHS system.

An overall view of the general system configuration is shown in figure 2. This is condensed from two detailed scenarios developed during the study which provide the baseline for the study requirements. It provides a view of the highway, vehicles, control stations and the general overlapping control configuration of the links.

Safety and Performance

A goal or baseline requirement for system safety, that is the probability of an incident resulting in property damage, injury or death, is necessary to begin defining architectures. Based on literature data, the goal was established at 1E-6 failures per hour of operation.

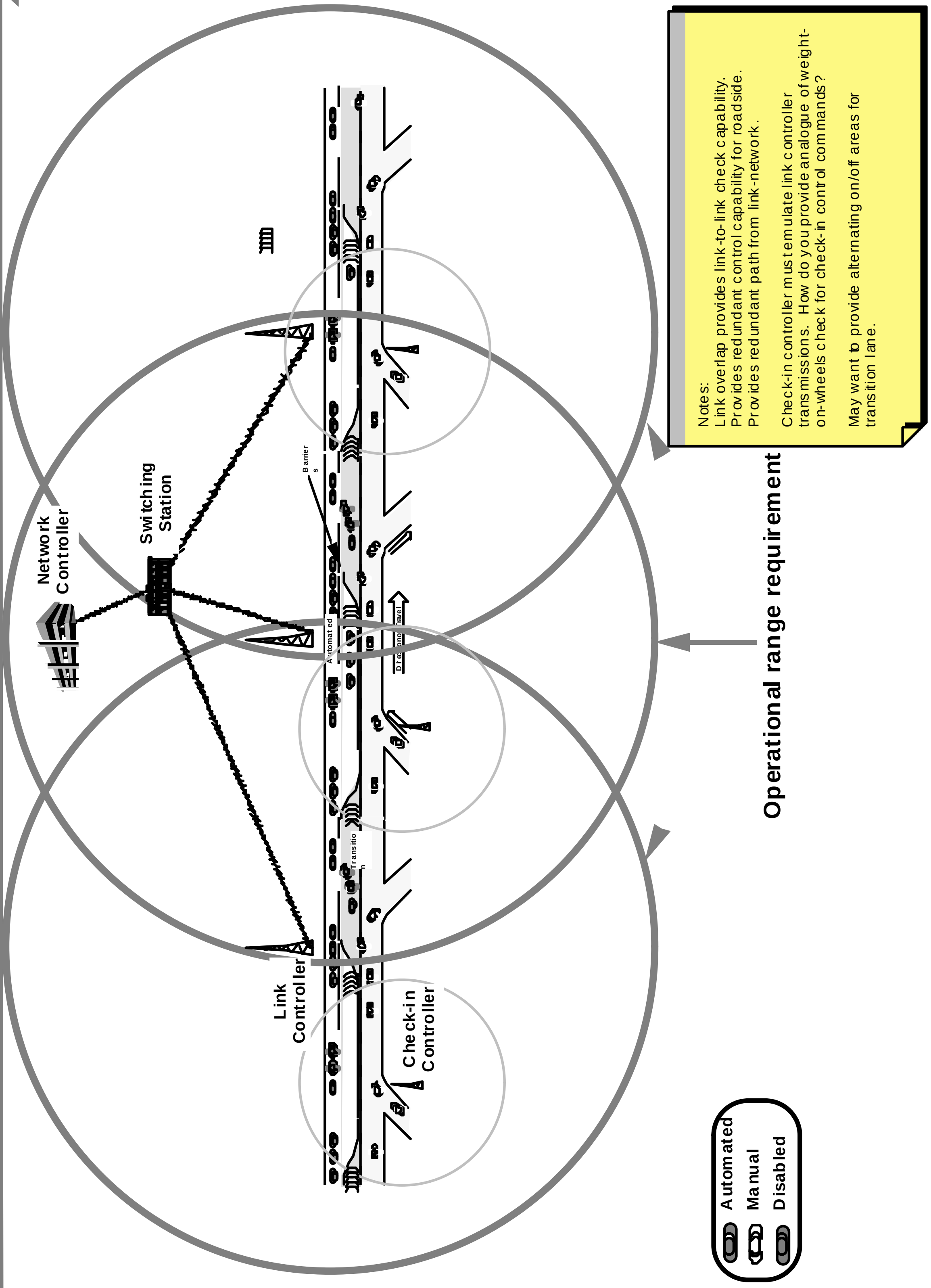
A performance requirement is more difficult, however baseline vehicle velocities of 60 to 90 miles per hour and some isolated cases to 120 mph were established. Dynamic performance for critical subsystems was derived from known vehicle assemblies.

Environment Definition

Strawman Architecture

The objective of this task is to define the representative system configurations in sufficient detail to facilitate the study of check-in procedures. Methods used in designing and analyzing control systems for space and aviation guided the study of architecture and mechanization issues, and in the analysis of failures, check-in/check-out and malfunction management.

The top level architecture is based on the PATH formulation shown in figure 3a, and shows the generalized layers of functionality for the entire system.



Notes:
Link overlap provides link-to-link check capability.
Provides redundant control capability for roadside.
Provides redundant path from link-network.

Check-in controller must emulate link controller transmissions. How do you provide analogue of weight-on-wheels check for check-in control commands?

May want to provide alternating on/off areas for transition lane.

Figure 2. Roadside Overview

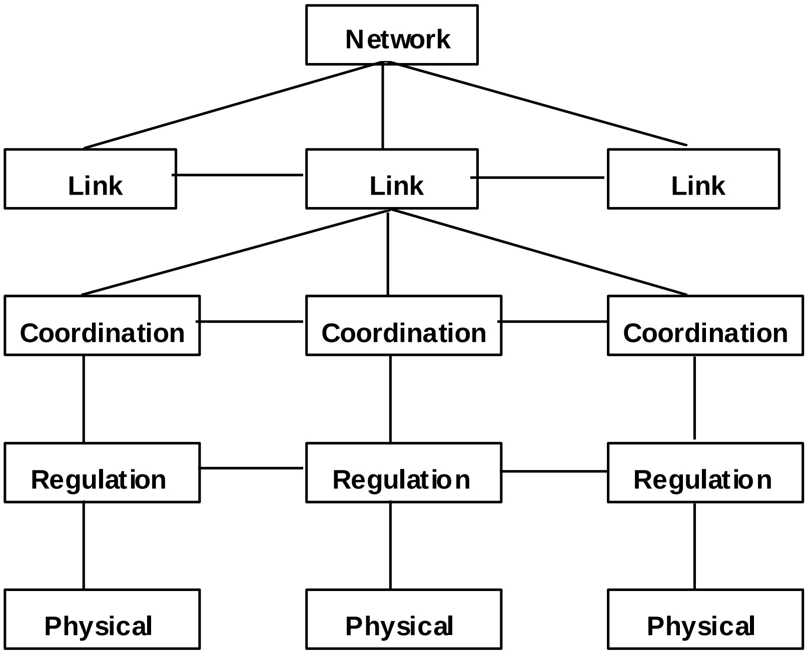


Figure 3a. Top Level System Architecture

The functions must then be mapped to the areas in which they are to be mechanized, such as roadside or vehicle. This mapping is shown in figure 3b. Once this allocation is completed, the subsystem architectures can be designed. Along with the allocation is the determination of criticality for the functions involved.

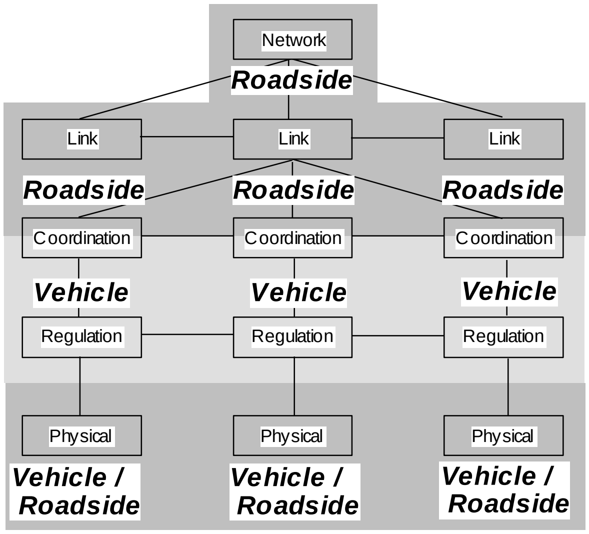


Figure 3b. Functional to Physical Mapping

System Mechanization

Following the functional decomposition of the above areas, realistic and detailed mechanizations were created which allowed a detailed study of the failure modes of the AHS, and the issues and risks involved in an AHS Health Management System. Where criticality was particularly sensitive, failure identification matrices, and failure simulations were completed.

A study at the functional level is not sufficient since one can then only consider the implications of “missing functionality.” For example, what are the consequences of losing the ability to control a vehicle's speed? Although it is possible to analyze the monitoring and diagnosis issues at this level, it is important to realize that a significant portion of the failure modes that must be examined consists of unanticipated interactions between system components. For example, a failure in the system responsible for “speed control” results not only in the loss of ability to maintain speed, but possibly, and more importantly, in an unexpected, uncontrolled, rapid acceleration. For such an analysis and for a thorough malfunction management investigation , a system definition at the mechanization level is required.

Functional Requirements Specification

Failure Modes Enumeration

For a given system element, failure enumeration is the process of identifying all the ways a system element can fail. For most hardware that would be considered feasible within the present state of the art (hydraulics, EMAs, processors, busses, connector technology), these failure mode definitions exist. For each of the potential mechanizations we collected existing failure mode enumerations, determined the relevant groupings or classes of failure from a functional perspective, and documented them in tabular format presented elsewhere in this report. Starting from existing detailed data has provided a high confidence that all failure mode classes are identified.

Where such data did not already exist, we met with cognizant engineers to develop a list of failure classes and the associated mode class characteristics. We used the resources of the University of Minnesota when appropriate to verify the completeness and accuracy of our results. With failure information and a newly compiled set of reliability numbers, configuration failure rates and overall system safety figures were computed. For example, a detailed block diagram was constructed from the following steering configuration shown in figure 3c.

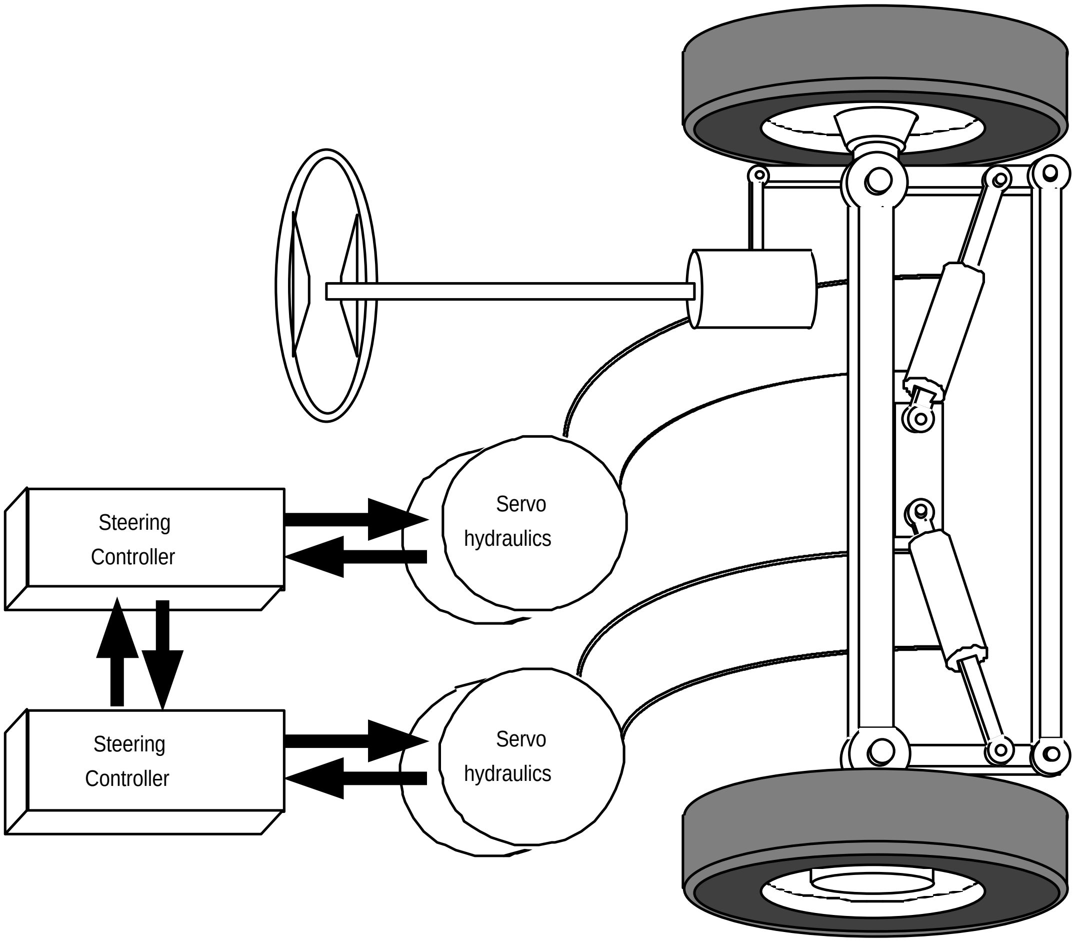
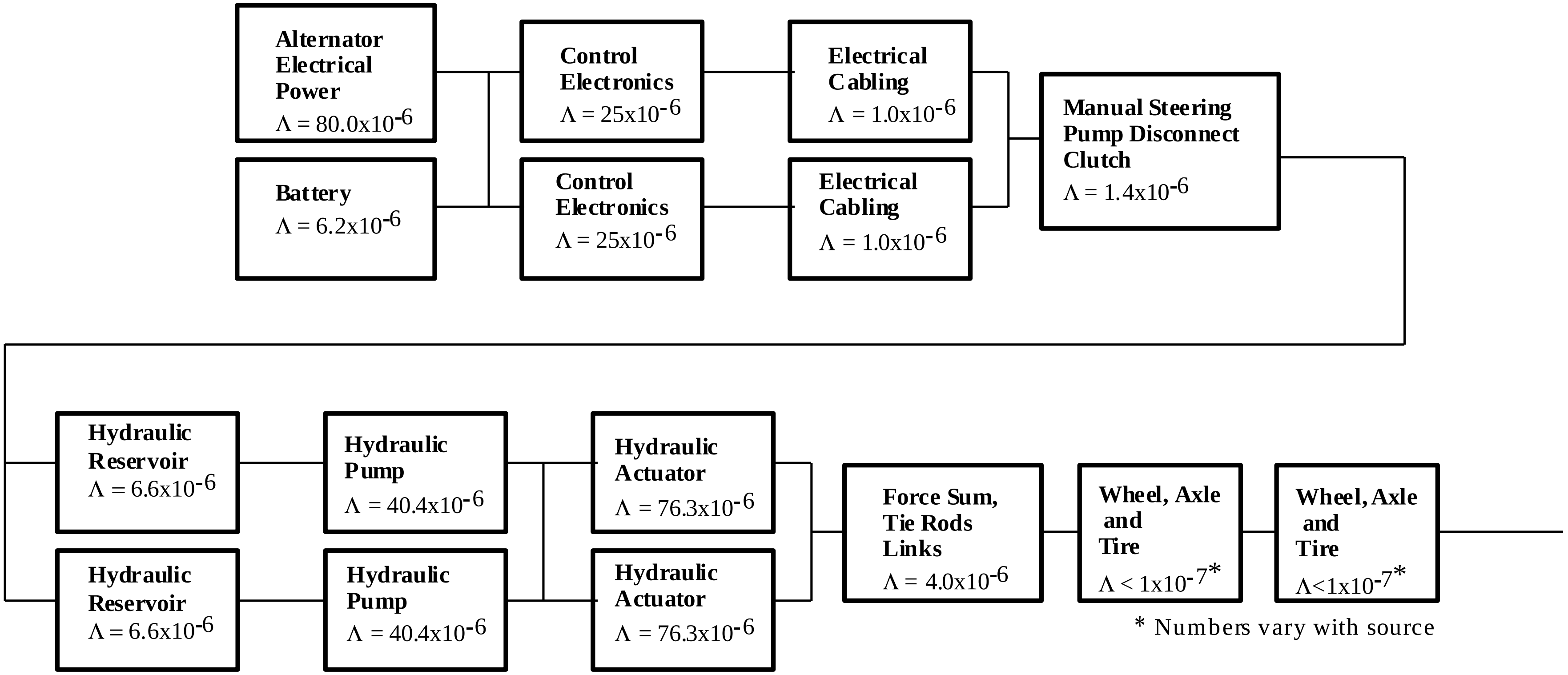


Figure 3c. Steering Configuration

A safety flow diagram was created from this which allowed probability of failure projections, and is shown in figure 3d.



* Numbers vary with source

Figure 3d. System Steering Safety Diagram

Top Level Design

Previously, the AHS was analyzed to identify the potential failure modes and the severity of those modes. Given that these failure modes exist, methods are included to either detect the failure quickly enough to allow the failure to be managed, or the design was modified to increase the reliability of the underlying system (to reduce the possibility of failure.)

Test Enumeration

This task concentrates on identifying and characterizing the techniques that can be used to detect failure. For each failure mode previously described, tests are hypothesized which detect that failure. For these tests to be useful in the analyses which follow, they must be realizable. Each failure mode has at least one test, and a single test may test more than one failure mode. Each test has a top-level description of the implementation as well as other characteristics such as test description, effectiveness, test externals, test phase and duration.

CHECK-IN

Our approach has established the system requirements, the failure modes, and the set of tests that can identify those failure modes. We also identified the testing requirements necessary to successfully perform check-in. This includes the roadway, the vehicle operator, and the vehicle itself.

The check-in process must not only verify that the vehicle is fit to enter the automated highway, but must also test to verify that the vehicle is capable of operating correctly in the automated lane, and that the vehicle will be capable of check-out at the end of the trip. In the cases where tests do not exist to verify the proper operation of necessary functions in a timely fashion, the system reliability must be improved either by redesigning the system using more reliable and costly parts, or by adding redundant functionality so a single path can fail, but the overall functionality will remain.

CHECK-OUT

An approach to identifying the system requirements has established the failure modes and the set of tests that can identify those failure modes. The testing requirements necessary to successfully perform check-out have also been identified. This includes the roadway, the vehicle operator, and the vehicle itself. Most of these equipment tests are similar or identical to the check-in process.

The testing requirements for a vehicle to leave the automated portion of the highway may be less strict than for entry. Because the vehicle has been operating on the highway, most of the automated portion of the system as well as many of the manual control elements have passed the continuous functional tests. Once control is restored to the driver, the automated functions are no longer required. A second possible reason for check-out may be better classified as expulsion. If a vehicle suffers the failure of a critical function, the vehicle must be expeditiously and safely removed from the roadway.

Across the entire range of AHS concepts, including those that involve only partial automation, driver alertness will be a significant concern. To create a set of limitations and inputs for the health management design, various test approaches and driver acceptance criteria has been compared and applied to the appropriate tests.

MALFUNCTION MANAGEMENT

The known failure mode classes have been identified and characterized, and an approach to detecting these failure modes has been determined. Malfunction management is the process which acts to prevent, mask or mitigate the effects of a failure mode. Figure 4 illustrates a very top level view of the malfunction management hierarchy.

Tools available to a malfunction management approach to perform its function include:

- Annunciation or recording of faults and the failure modes which result.
- Physical redundancy.
- Analytical redundancy.

Within each of these tools are a number of options for approach. For example, with annunciation and recording, the detected fault can be reported to the driver, the control system, a roadside system, or merely stored on-board for later debrief and interpretation by maintenance personnel. The option selected is driven by the required intervention time.

The study approach has considered the elements available to the malfunction management scheme, and selected the configuration most suitable to the system element. Prevention of the malfunction occurrence is clearly the desirable approach. If detection is only possible after the fault occurs, then masking of the fault to prevent disturbance to the system is desired. Finally, if some disturbance occurs as a result of the detection and correction process, then the design must reduce or mitigate the negative impact of the disturbance on system performance. The timelines associated with these options are illustrated in figure 4. An example of this is the simulated steering fault shown in figure 79. This represents a dual system which has sustained a failure, and corrected for it, resulting in a small lateral disturbance for the vehicle.

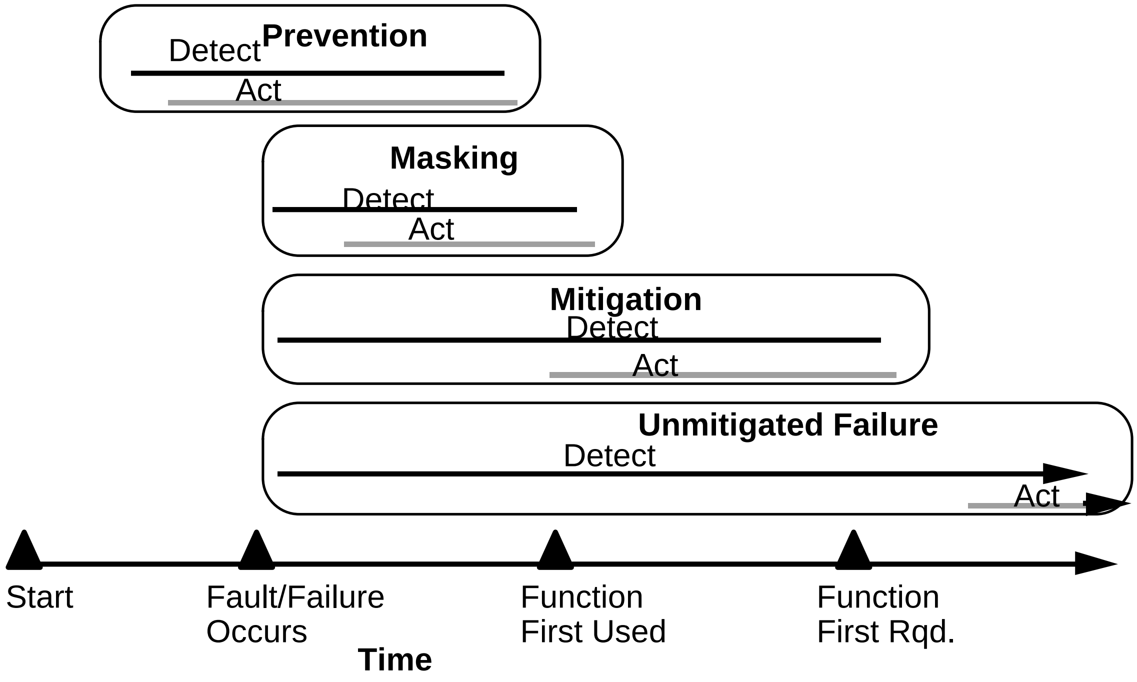


Figure 4. Malfunction Management Scheme

Design Adequacy Review

The combination of configurations, testing concepts, vehicle to roadside partitioning and the methods of handling faults are all part of the total health management approach when treated as a systems problem. As such, the measures of effectiveness must consider the overall performance of the health management concept in terms of total cost, minimum impact on the correct operation of the system, incident avoidance, and operator involvement. The final measurement of effectiveness (MOE) is directly related to the achievement of the system safety goal.

Step Outline

1. Determine the Representative Systems Configurations
2. Identify/Allocate Functions
3. Characterize Functions
4. Analyze Reliability of the AHS
5. Mechanize Critical Functions
6. Simulate Malfunctions to Verify Mechanization
7. Driver Check-Out

A SUMMARY OF CONCLUSIONS

Driver checkout: We will be trying to detect small differences amid high random variability in people who are highly motivated to fool us. No driver readiness test will work perfectly. Tests which only address motor behaviors (such as steering) do not address necessary cognitive skills such as situation awareness.

A set of requirements for system safety and necessary performance are required almost immediately if realistic designs are to be completed.

A car cannot remain within an 8 foot lane when a (standby dual-redundant) steering failure occurs, given reasonable assumptions about detection and response time.

Vehicles cannot perform road surface condition monitoring alone - it would result in the lead vehicle sensing the hazardous condition when it is too late to respond.

Collision avoidance is a basic critical function - if it works correctly, many other functions become "essential", not "critical".

Reasonable test coverage assumptions (95%) cause single or dual systems to rise above Pf budget almost immediately.

Consortium will need realistic, industry-wide database of component reliabilities that does not currently exist.

TECHNICAL DISCUSSION OF EACH STEP

REPRESENTATIVE SYSTEMS CONFIGURATIONS

Base Configuration

The procedures were identified by examining the previous work , “Human Factors Design of AHS" performed by Honeywell for the FHWA, in which viable AHS operational scenarios were defined. The scenarios are differentiated based on 1) degree of separation between automated and conventional, manual traffic, 2) type of vehicle control rules used on the AHS (grouped versus individual versus autonomous or free agent vehicles), and 3) degree to which decisions related to lane selection, speed, and spacing are automated. Seven AHS scenarios have been developed that vary systematically along these dimensions and include operational events that depict key human factors issues. The seven scenarios are:

1. Free agency/self-contained.
2. No barriers on shared highway with individual vehicles.
3. No barriers on shared highway with grouped vehicles.
4. Barriers on shared highway with individual vehicles.
5. Barriers on shared highway with grouped vehicles.
6. Segregated highway with individual vehicles.
7. Segregated highway with grouped vehicles.

From this set of seven, primary and secondary scenarios or configurations were selected from which the operational procedures could be extracted. We based this selection on the desire to select two scenarios that would have high levels of automated functionality, high susceptibility to external (AHS) errors, and high levels of critical functionality. In our assessment, the relevant factors in this selection proved to be the three addressed by the Human Factors effort above, while the values of those factors or parameters that resulted in high levels of automation, error susceptibility and critical functionality were:

- Shared lanes (mixed traffic).
- Grouped vehicles (communications and coordination requirements).
- Barriers (synchronous maneuver requirements).

To arrive at the primary scenario, we combined these three dimension variables. This combination corresponds to scenario 5. The following descriptions of the scenarios and their associated procedures are derived from the literature.[18]

The base configuration selected is "Barriers on the Shared Highway with Grouped Vehicles." In this scenario, automated and manual traffic will share the same highway structure, and vehicles will move as groups. Control of traffic flow will be fully automated as well. Normal automated driving will require only limited driver involvement (e.g., informing the roadside system of the desired destination). As illustrated in figure 5, there will be three types of lanes: automated, transition, and manual. Automated lanes will always be to the left of the highway and manual lanes will always be to the right, with a transition lane in between. Only automated vehicles will be able to use automated lanes. A vehicle equipped for automated driving and moving in a manual lane will be able to use a transition lane to gain entry to an automated lane.

Alternatively, on some roadways, if so equipped, it may be able to enter an automated lane through an automated on-ramp at some locations. Unequipped vehicles will be prevented by law from driving in a transition lane or an automated lane. Barriers will separate transition lanes from automated lanes and automated lanes from other automated lanes. The primary intent of the barriers will be to prevent debris caused by incidents in manual or other automated lanes (if any) from intruding into an automated lane uninvolved in the incident.

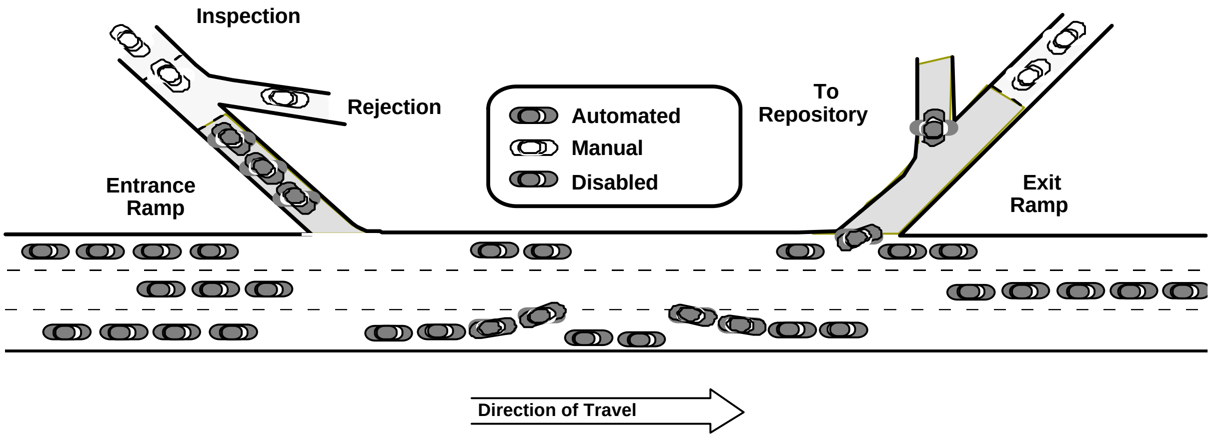


Figure 5. Segregated Highways with Grouped Vehicles

Features

The following features of the AHS are assumed under this scenario:

- Vehicles will enter and leave an automated lane from a transition lane. Vehicles may also have access to automated access ramps at selected locations.
- Maneuvers will be performed by vehicles in groups (as opposed to individual vehicles). Vehicles will be formed into groups in the transition lane. Entry onto the automated lanes and all subsequent maneuvers, including lane changing, will be conducted automatically by groups of vehicles (Note that a single vehicle is a permissible, though presumably rare, group size).
- There will be openings in the barriers between the transition and automated lanes and between different automated lanes to allow vehicle groups to change lanes. The total length of these openings will be only a fraction of the total length of the lanes. Because a lane change will be able to occur only when a vehicle (or vehicle group), a barrier opening, and a gap between vehicles in the neighboring lane are aligned, the roadside system will need to be more sophisticated in scheduling and controlling lane changes than in scenarios without barriers.
- The roadside system will provide limits for maximum speed, the spacing between groups, and the spacing between vehicles within groups.
- The roadside system will be responsible for ensuring smooth traffic flow. Included in the latter will be the ability to meter entry to an automated lane both from automated

entrances and from transition lanes. Also, the system will be responsible for automatically selecting lanes of travel.

Normal Operational Events

ENTER THE AHS

There will be two ways to enter the system:

- Through a transition lane. The driver will enter the system via a normal entrance ramp and join a manual lane of traffic. Then, the driver will inform the roadside system of the desired destination. If the destination does not meet certain criteria (e.g., if it’s too close to the vehicle’s current location), the roadside system will reject the vehicle from the system. Otherwise, the driver will be directed to manually enter the transition lane. While in the transition lane, the system will perform an inspection of the vehicle. If the vehicle fails the inspection, it will be rejected for AHS use and the driver will be directed to leave the transition lane. A vehicle that passes the inspection will be switched to the Automated mode. Vehicles with compatible destinations will be grouped together by the system. This does not imply shuffling cars, simply that cars will be grouped so that the set of groups taken as a whole will hold together for a maximum travel time. The roadside system then will make a request to move the group into an automated lane. Before they are assigned to a group, vehicles will move as individuals. Therefore, traffic on the transition and automated lanes will include groups of vehicles, as well as individuals who have yet to be assigned to a group, or who have not yet closed with another vehicle or vehicles to form a group.
- Through an automated on-ramp. With this method of entry, vehicle inspection will be done at a particular site rather than at an arbitrary position in the transition lane. The driver will inform the roadside system of the destination and the roadside system will inspect the vehicle. Subject to the constraints noted in the paragraph immediately above, a vehicle that passes the inspection will be switched to the Automated mode. The vehicle will be placed in a group with other vehicles and metered into an automated lane.

ENTER AN AUTOMATED LANE

Again, there will be two ways to do this, corresponding to the two ways to enter the AHS:

- From a transition lane. Groups of vehicles will enter through an opening in the barrier. The group may join with an existing group in the automated lane or may remain a separate group.
- From an automated on-ramp. Groups of vehicles will enter directly into an automated lane from the on-ramp. The vehicles will not have to use a transition lane to accomplish this.

MOVE WITHIN AUTOMATED LANES

All movement of vehicles within automated lanes will be fully controlled by the vehicle automation under instruction from the roadside system. Included will be control of speed, lateral position, spacing between groups, and spacing of individual vehicles within groups. In addition, a driver will be allowed to change destinations if the change does not violate certain parameters (e.g., the new destination is too close to allow safe exit under existing traffic conditions). If the change of destination requires a lane change, the system will plan and execute the necessary maneuvers.

CHANGE LANES WITHIN AUTOMATED LANES

All lane changes will be scheduled by and executed under instruction from the roadside system, with collision avoidance responsibility remaining at the vehicle. Included will be traffic movements required when two lanes merge or a single lane splits. Changes to existing groups that occur in conjunction with lane changes (e.g., splitting to allow exit of one or more vehicles, or slowing down or speeding up to accommodate an arriving group from another lane) will be part of moving within automated lanes (see paragraph immediately above). Note that lane changes may be made by single vehicles or by groups of vehicles, depending upon the immediate need. In the former case, the group may separate around the vehicle requiring a lane change to allow sufficient spacing for that maneuver to take place. Having changed lanes, this vehicle may be incorporated by the system into a new group, rather than allowed to operate individually. To accomplish this, the system will identify an appropriate group to accept the vehicle and negotiate a space for it. The vehicle then will be maneuvered under system instruction to join up with its new group.

EXIT AN AUTOMATED LANE

As with entering an automated lane, there will be two methods of exit:

- <u>To a transition lane</u>. Groups will exit through an opening in the barrier. The group will pass into a stream of vehicles on the transition lane, some of which will be under manual control and others of which will be under automated control. Among the automated vehicles in this transition lane will be individual vehicles, some awaiting formation into groups, and others having been just released from their groups. Other automated vehicles in the transition lane will be still moving in groups, either about to enter the automated lanes or having just exited the automated lanes.
- <u>To an automated off-ramp</u>. Groups will exit directly onto an automated off-ramp.

EXIT THE AHS

There will be two ways to do this, corresponding to the two methods of exiting an automated lane:

- <u>From a transition lane</u>. On the transition lane, groups will separate and perhaps also reduce their speeds to allow sufficient space for the drivers to resume manual control of their vehicles.   The system will have to verify that the driver is ready to resume manual control of the vehicle. After the criteria for readiness have been met, the vehicle will be switched from Automated to Manual mode. At that point, the driver will resume manual control of the vehicle and, when appropriate, move from the transition lane to a manual lane. If the readiness criteria are not met, the vehicle will remain in Automated mode and the roadside system will drive it to some safe repository and stop the vehicle.
- <u>From an automated off-ramp</u>. This method differs from the one above only in that a vehicle will not have to go through a transition lane and subsequent on-highway manual lane when exiting the system, but will go directly from an automated lane to an automated off-ramp. Prior to transferring control of the vehicle to the driver, the system will have to verify that the driver is attentive and ready. The nature of this interrogation, and what the driver's response might be has significant human factors implications as well as system implications. After the criteria for readiness have been met, the vehicle will be switched from Automated to Manual mode. At that point, the driver will resume manual control of the vehicle. If the readiness criteria are not met, the vehicle will remain in Automated mode and the roadside system will drive it to some safe repository and stop the vehicle.

Emergency Events

Loss of automatic control in a grouped-vehicle scenario will present a special set of challenges, particularly when combined with the presence of barriers between lanes of automated traffic. Traveling in the midst of a group, following at a close gap, it is unlikely that the driver will be able to manually maintain speed and steering control as precisely as the automated controller. Empirical investigation will be required to better define the conditions under which the driver can perform this emergency control recovery task successfully. However, as an aid to the driver, the system could isolate the impaired vehicle immediately upon being informed of the failure. This could be done by instructing the other vehicles in the group to speed up or slow down and thus increase their separation with the impaired vehicle. The driver will then have a larger longitudinal envelope in which to maneuver manually. The presence of barriers complicates the complete loss of automatic control. In a system without barriers between the automated lanes, the system could isolate the impaired vehicle by removing traffic from a neighboring lane. This will serve to increase the driver's envelope for lateral maneuvering. However, the barriers will prevent the system from doing this. In the absence of the enlarged lateral envelope, the driver will have to recover steering control and steer with sufficient accuracy to avoid hitting the barriers.

Alternate Configuration

Our selection of a secondary scenario was based on our desire to reveal all functions which might occur in viable AHS scenarios which will not have surfaced in the primary scenario. Thus, the selected scenario inverts the parameters chosen for the primary scenario, resulting in scenario 6, Segregated Highway with Individual Vehicles.

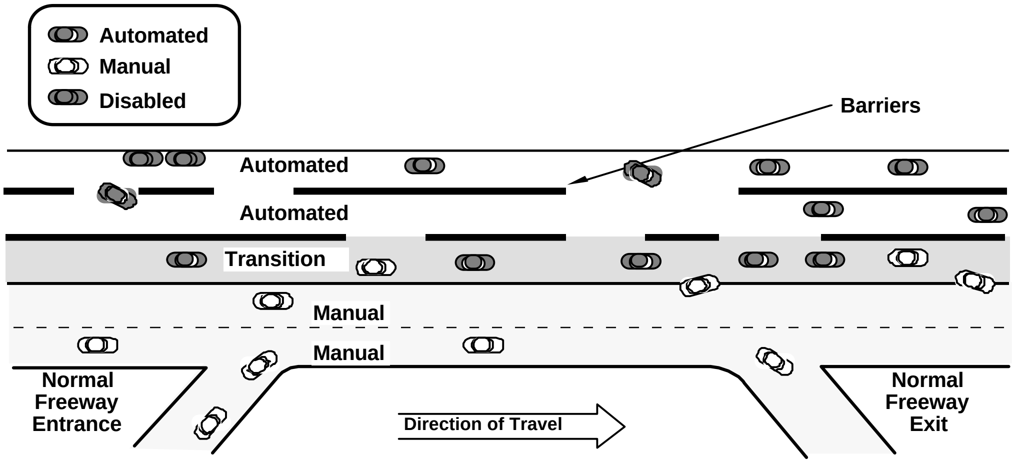


Figure 6. Shared Highways with Non-Grouped Vehicles

In this scenario, illustrated in figure 6, automated traffic will be physically segregated from other traffic, and vehicles will move as individuals. Control of traffic flow is fully automated via metering, control of speed and gap, and automated lane selection. Segregation may be accomplished in a number of ways, including an elevated structure for the automated traffic above the current highways. Normal automated driving will require only limited driver involvement (e.g., informing the roadside system of a destination). There will not be barriers between lanes of traffic moving in the same direction.

Features

The following features of the AHS are assumed under this scenario:

- Individual vehicles will enter and exit the automated lanes by means of automated entry and exit ramps.
- Lane changes will be automated.
- Maneuvers will be performed by individual vehicles.
- The roadside system will regulate spacing between vehicles and maximum speed.
- The roadside system will be responsible for ensuring smooth traffic flow through metering vehicle entry to the AHS and selecting lanes of travel.

Normal Operational Events

ENTER THE AHS

The roadside system will inspect each vehicle at some point of access. If the vehicle passes, it will be allowed entry to the AHS. If it fails, it will be rejected. A vehicle that passes will be switched to the Automated mode while on the on-ramp, and the roadside system will then invoke those features noted above in the previous section. While still on the on-ramp, the vehicle group will pass through a metering process to provide the most efficient entry onto the AHS. Also, the driver will input the desired destination and the roadside system will select a lane and schedule the trip to accommodate the request.

ENTER AN AUTOMATED LANE

The vehicle will enter an automated lane under instruction of the roadside system, which shall maintain control of all maneuvering.

MOVE WITHIN AUTOMATED LANES

Movement of vehicles within automated lanes will be fully automated, carried out by the vehicle automation under instructions from the roadside system. Included will be control of speed, lateral position, and spacing between vehicles. A driver will be allowed to change destinations if the change does not violate certain parameters (e.g., the new destination is too close to allow safe exit under existing traffic conditions). The system will respond to the request with a lane change as necessary to attain the new destination.

CHANGE LANES WITHIN AUTOMATED LANES

All lane changes will be scheduled by the roadside system and carried out by the vehicle automation according to instructions from the roadside system. This will include the lane changing maneuvers required when two lanes merge or a single lane splits. The system will automatically negotiate spaces in the traffic to accommodate vehicles changing lanes. This will be accomplished by speeding up or slowing down vehicles.

EXIT AN AUTOMATED LANE

Vehicles will exit the automated lanes automatically, under the instructions of the roadside system.

EXIT THE AHS

Issues regarding transfer of control to the driver are the same as for the preceding scenario. The readiness of the driver to resume control must be ascertained, and the vehicle directed to a safe repository if the driver is not capable (or cannot be determined to be capable) of resuming control.

Emergency Events

The loss of the lateral tracking function in an automated vehicle will present more or less difficulty for a malfunction management approach (including use of the driver as a backup system) depending upon the width of the automated lanes. An automatic lateral control system that can operate *error free* with a maximum steering error of 8 cm (3.1 in) can indeed utilize extremely narrow lanes, perhaps as narrow as 2.5 m (8 ft). It is unlikely that a human driver can steer that accurately, particularly if steering control must resume after little or no warning. Experimental studies could establish more precise expectations for driver performance under these conditions. Again, the system could aid the driver in this emergency situation by isolating the affected vehicle, and effectively giving it more room for lateral error. Even if the system has a redundant steering capability, with a hard-over fault at an assumed rate limit of 40 deg/s, the lateral deviation from track is already approximately 0.5m (1.6 ft). By 1 second after fault, the lateral deviation is approximately 4 m (13 ft). Thus, reconfiguration time requirements for narrower lane widths are on the order of those required for critical avionics systems.

System Performance Definition

The following paragraphs will define the top level performance requirements that are of importance in establishing the system architecture and mechanization. These requirements are, in many cases, based on experience of the organizations involved in the contract work.

Allowable Vehicle Class

The primary vehicle for this study is a full sized passenger vehicle or light truck. Most of the results, with the exception of fault simulations, are also applicable to high performance and CVO vehicles as well.

System Probability of Failure for Critical Equipment Items

The following data were obtained from a literature search:

No. of Trips:	2,201,258 per day on the network
AHS Usage:	Based on projected 45 percent penetration, 990,566 trips per day

For a 52 week, 5 day per week usage, the total number of AHS trips for the Southern California freeway network system area is about 52x10^6 trips per year during a two hour morning period.[23] It seems unlikely that greater than 10 incidents per year on the Southern California AHS system for the morning traffic would be acceptable. These incidents are assumed to be totally due to equipment malfunctions which presently represent about 12 percent of all accidents.[6] If we use the above data and determine a very rough requirement for probability of failure, the result is:

(10 incidents per year)/(52x10^{6} trips per year)(.12) = 1.6x10^{-6}.
(1a)

If λ represents the system failure rate, and t the operational time of two hours, then for an exponential distribution assumption:

λt = Probability of System Failure = 1.6x10^{-6}, and;
λ = 1.6x10^{-6}/2hours, or λ = 8x10^{-7} failures per hour.

This is roughly 1.0 x 10^{-6} failures per hour for critical equipment items, which we used as a goal.

As a means of assessing the credibility of this goal, one can compare this figure to the current injury accident rate on the Interim National Highway System, which is 89.6 per 100 million miles traveled[29]. Assuming an average rate of travel of 50 mph, this becomes:

(89.6 injury accidents/10^{8} miles) * (50 miles/hour) * (0.12 mechanical)
= 5.38 x 10^{-6} injury accidents/hour.
(1b)

This figure is somewhat higher than the critical equipment probability of failure rate. In order to relate the two, one must make decisions or assumptions about: 1) the probability that a failure of a critical equipment item will cause an injury accident, and 2) the desired reduction in the rate of occurrence of injury accidents from current day rates.

Safety

The primary areas of concern for this set of study requirements are the vehicle and the roadside control and test equipment. Only the items pertaining to critical vehicle or roadside equipment are assigned a numerical value either by published data where known, or by expert opinion.

Another important assumption is that any software has been thoroughly tested and verified, and that errors and failures due to improper algorithm programming are negligible (that is, have a contribution to the system failure rate which is one to two orders of magnitude smaller than that attributable to hardware failures). This is reasonable following a thorough, and well controlled software development effort which **must** be a part of any safety critical system application. Standards for performing this sort of development are found in documents such as DO-178 in the commercial domain, and MIL-STD-2167 procedures and tests in the military domain.

P_F ALLOCATION FOR EQUIPMENT

ROADSIDE

At an estimated 30 percent of the system complexity, the roadside operational and test equipment is allotted a Pf_{rdside} = 4.8x10^{-7}, or about 5x10^{-7}.

ROADWAY (SURFACE)

Estimating the roadway at 10 percent of the complexity, Pf_{rdway} = 1.6x10^{-7}.

VEHICLE

The vehicle is estimated to have the greater complexity of the system element based on the chosen system scenarios. At 60 percent, Pf_{veh} = 9.6x10^{-7}, or about 1x10^{-6}.

EXTERNALS

Externals are things not a part of the AHS system per se, which have the ability to negatively impact performance of the system. Examples are things such as debris, intruders, and sabotage events. These items are not assumed to contribute to the failures due to equipment. While it is arguable that failures in the system would cause an incident due to these items, it is assumed that the control and protection systems have been designed to account for these events, and if an incident occurs, it is because of equipment failure which is covered above.

Throughput (Efficiency)

DENSITY

The speeds and headway times assumed are within those presently being considered for the AHS implementation. As such, it is assumed that these conditions are optimum for desired pollution reduction, and energy efficiency.

HEADWAY

This is provided by the assumed gap distances and the range of speeds assumed for the study: At 0.91m (3 ft) and 97 kph (60 mph), headway time = 0.034 s. At 9.1m (30 feet) and 97kph, headway time = 0.34 s.

SPEED

The range of speeds selected is within the ranges presently being considered for the AHS implementation. Maximum speed is assumed to be 153 kph (95 mph) , and the minimum speed 97 kph (60 mph). These figures may be revised as the Human Factors Design for AHS effort determines through experimentation the capability of various driver populations to handle the required vehicle control tasks at these speeds.

ACCELERATION

The following values are strawman figures existing in the AHS BAA material, and are considered sufficient to use as initial study assumptions.[24] Maximum acceleration capability will be taken as 3.0 m/s^2 (10 ft/s^2), and minimum as 1.5 m/s^2 (5.0 ft/s^2).

DECELERATION

Based on recent data for AVCS research and test vehicle specifications, a preliminary value for required deceleration is -7.6 m/s^2 (-25 ft/s^2). This results in a stopping distance of 64m (210 ft) from 112 kph (70 mph).[14]

Comfort

At this point, the above requirements for acceleration and braking will be assumed to be in the comfort zone of a driver/passenger. Further development of these parameters from a human perspective will come from human factors work presently in progress. Some of the major items affecting comfort would be: acceleration and jerk in three axes (lateral, longitudinal, and vertical), and perceived safety.

Cost

The cost of the combined control and built-in-test (BIT) systems on the vehicle will of course be greater than present electronic system elements primarily because of the operation critical nature of the system. Where driver safety is involved, redundant systems may be employed in addition to a standard mechanical backup system. We have assumed a cost factor of about 10 percent of the cost of the vehicle as a preliminary goal. As the factors evolve defining the complexity required for safety, a better figure can be derived.

Roadside cost per mile will be discussed in connection with the mechanization definition. These costs do not represent a minor modification to an existing infrastructure, and are thus harder to estimate.

Range of Gaps

Since greater problems with test accuracy and timeliness occur with smaller gaps, and the time required for malfunction management is significantly reduced, the shorter gaps are chosen for the top requirement.

APPORTIONMENT OF GAP FOR SENSOR TOLERANCES

A portion of the gap distance must be reserved for the tolerance stackup due to sensors and control system. With an assumption of 10 percent of the gap distance allowed for sensor tolerances, and another 10 percent allowed for control tolerance including overshoot, and general static tolerances, table 1 applies.

Table 1. Sensor Tolerance Values for Various Gap Distances

Gap, m	**h = 0.914**	**h = 3.05**	**h = 6.10**	**h = 9.14**
Position Tolerance, fm	0.0914	0.305	0.610	0.914
Control Time Constant, s	0.1 to 1.0	0.1 to 1.0	0.1 to 1.0	0.1 to 1.0
Velocity tolerance, m/s	0.5 to 0.06	1.5 to 0.15	3 to 0.3	4.5 to 0.45
Acceleration tolerance, m/s^2	9 to 0.09	30 to 0.3	61 to 0.6	91 to 0.91

The significance of these tolerances is in the capability of the vehicle to accurately track its longitudinal position while following. The lateral tolerances are addressed in the lateral motion simulation section of this report.

Note - Velocity and acceleration tolerances are commensurate with the spread in control time constants.

At this point, we will consider the lateral and longitudinal control time constants to be in the same ranges.

Range and Rate of Steering Control

These values have direct impact on the severity of any steering failures, and ultimately must be part of a tradeoff between capability of the built-in-test (BIT) and control system, and the width and configuration of the highway. The value ranges assumed for the initial part of the study are as follows:

RATE

Minimum:	± 20 deg/s
Maximum:	± 30 deg/s

RANGE

	± 40 degrees

ROADWAY WIDTHS

Roadway widths directly affect the time available to the vehicle or roadside control for correction of malfunctions which would cause rapid steering deviations. For this study, roadway widths will be assumed to be the standard of 3.7 m (12 ft). Reasonable recovery times for hard-over steering faults will reflect this requirement. 2.4 m (8 ft) lanes have also been proposed. At this time, these appear to be too narrow to allow system fault corrections.

On-the-fly Check-In

ALLOWABLE CHECK-IN TIMES

Two locations are being considered for the performance of check-in tests, either on-ramps or selected portions of the transition lane. Since the velocities experienced in the transition lane will be higher, this will form the tighter requirement. At 97 kph, assuming the following events must happen in the time interval between driver entering the transition lane and vehicle entering automated lane:

J1: Driver merges with traffic in transition lane.
J2: Vehicle systems tested.
J3: Roadside determines acceptance/rejection, assigns ID.
J4: Driver asked to relinquish control.
J5: Driver acknowledges control transfer request.
J6: Vehicle takes/driver relinquishes control.
J7: Vehicle announces control transition complete.
J8: Driver acknowledges control transition complete.
J9: Vehicle joins group (including wait time for adjacent vehicles to finish
above process).
J10: Roadside creates gap in automated lane.
J11: Group enters automated lane.

The following are time allotments:

J1: 2s.
J2: 2s (1s to read on-board info., 200ms each brakes, steering, accel, tracking,
and comm/transmission of results).
J3: 1s.
J4: 100ms.
J5: 3s.
J6: 1s.
J7: 100ms.
J8: 3s.
J9: 8s.
J10: 8s.
J11: 2s (assuming barrier gap correctly located).

There is a total of ~30 seconds, which at 105 kph (65mph, 95 fps) is about 875 m (2850 ft), or a little over 1/2 mile. These are not worst case times, they are intended to reflect nominal values. This assumes that there are no maneuvers resulting from the exit of vehicles from the automated lanes, and that the destination of the driver has already been specified. Testing which requires supplemental equipment that is to be performed within the allotted 2 second window would have to be place within a 58 m (190 ft) space, or the time allotted extended.

IDENTIFICATION REQUIRED

Each AHS equipped vehicle will need an identifier which is used to address messages. This could be a temporary or permanently assigned identifier (ethernet addresses or internet address allocation schemes are analogues.)

STATUS OF INSPECTION ON VEHICLE

If the inspection status of a vehicle is not carried on board, but resides in an infrastructure database, then the vehicle identifier would need to be permanent to allow association of the vehicle to its inspection data. In either case, vehicle health data obtained at regular inspections is obtained by the roadside and used as part of the assessment criteria.

POINT OF RELEASE FROM HUMAN CONTROL

Research conducted under the "Human Factors Design of Automated Highway Systems" contract indicates that automation should take control of the vehicle on either the on-ramp or in a transition lane, not after the vehicle has entered the automated lane. Vehicles should only be brought into the automated lane under AHS control. The risks associated with a manual vehicle in the automated lanes are extreme, especially with the speeds and lane widths being proposed.

ACTION REQUIRED BY DRIVER ON GO OR NO-GO.

Once the driver has requested admittance to the AHS and the vehicle has passed inspection, automated systems will take control of the vehicle and inform the driver that manual control is no longer necessary. The driver then releases the controls. If for some reason the vehicle is denied access to the AHS, the driver will be directed to return to the manual lanes of traffic. The driver continues to control the vehicle manually.

COMMUNICATION REQUIRED BY ROADSIDE

These requirements are dependent on the functional allocation, which in turn is driven by the ability to satisfy the failure rate requirements given different levels of vehicle and infrastructure redundancy. These requirements are addressed in the Function Identification/Allocation section of this report.

On-the-fly Check-Out

These requirements are being developed by the "Human Factors Design of AHS" project.[25] The requirements are sensitive to the definition of the driver check-out event sequence, which can be quite varied. This is an area requiring a significant amount of research, and is described in a later section of the report. It is assumed that there will be a testing procedure carried out in the automated lane, while under full AHS control. This test may require upwards of 10 minutes to complete.

Identification of Minimum Driver Capabilities

These requirements are critical to the development of a driver check-out procedure. Determining a minimum capabilities set represents a major human factors research effort. Discussion of some aspects of this research is found in the Driver Checkout section of this report. For the purposes of this paper, it is assumed that there is some minimum set of capabilities that will be tested for.

Minimum Data Set for Driver Information

This data was obtained from the human factors research.[25]

Acceptable Failure Maneuvers

These items are necessary to the consideration of the malfunction management strategies. It is likely that all considered strategies will be desirable under some conditions, and the action will have to be determined by the vehicle or roadway at the time of failure. The initial set of maneuvers for failures not masked by internal redundancy includes:

- Run-off-road for failed vehicle.
- Maximum individual braking.
- Maximum group braking.
- Maximum individual acceleration.
- Maximum group acceleration.
- Steering avoidance.

It is assumed that a larger set of failure maneuvers will be defined as the set of considered failure modes develops.

Classification of Tests

These are the test groupings for all operation of the vehicle and roadway.

STARTUP

The set of startup tests consists of tests run after powering on the system (engine start, in the case of a vehicle), and tests completed following start, but prior to system operation.

PRE-ENTRY

Pre entry tests are those performed while in some operational mode, prior to entry into some other, typically more demanding operational mode. For the vehicle, this set of tests would be run en-route to an AHS-equipped roadway. For the roadside, such a set of tests would be run if the AHS roadside equipment had more than one operational mode. These tests are likely to be similar to the continuous tests described below.

CHECK-IN

Check-in tests are distinguished from pre-entry tests either due to their time-critical nature (the system wants to know the results of the test immediately prior to acceptance) or the requirement for off-vehicle equipment to perform the test. This could include debriefing on-vehicle records of inspections, and external verification of sensor/actuator performance. There is no equivalent to a vehicle check-in for the roadside equipment.

CONTINUOUS

Continuous tests are regular checks of equipment performance by either redundant "channels" (replicated operational equipment) or built-in-test equipment (BITE). They are typically non-intrusive, meaning that they do not change the functional characteristics of the equipment. Due to this restriction, they may have less visibility into system health than tests performed when the system is not operational.

CHECK-OUT

Check-out tests are those performed on the driver and vehicle prior to resuming manual control of the vehicle. Analogous to check-in tests, these tests are time sensitive, since the driver's ability to resume control will change over time. There may be no need for vehicle check-out tests.

FUNCTION IDENTIFICATION/ALLOCATION

The abstract architecture (figure 7) includes five layers: the network layer (responsible for route and flow control), the link layer (responsible for path and congestion control), the coordination layer (responsible for vehicle maneuver coordination), the regulation layer (responsible for vehicle maneuver control command), and the physical layer (responsible for vehicle actuation).

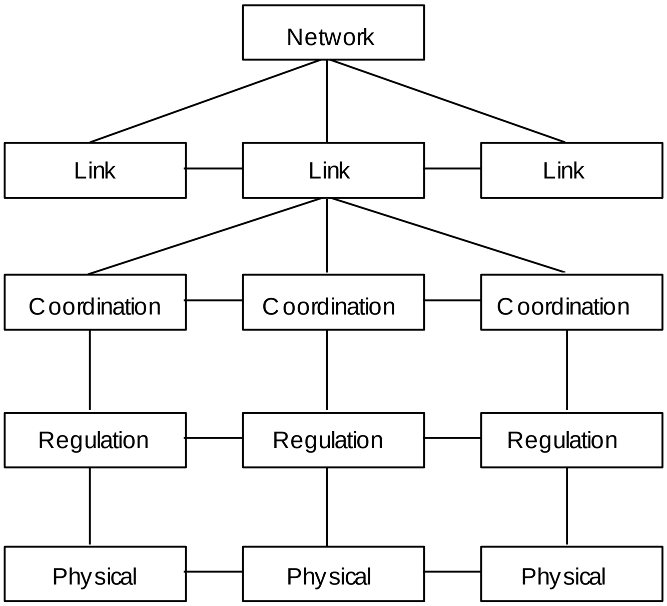


Figure 7. Abstract Architecture Model

The layered architecture is defined in such a way that each control layer is built on top of the lower functional layer and accomplishes a unique traffic management or vehicle control task with minimal support from other layers. Corresponding to the layered architecture, the elemental functions are grouped into five hierarchical layers, each of which possesses a set of elemental functions dealing with sensing, monitoring, decision making, and actuation.

Network layer

The network layer is responsible for route and flow control within a network. Based on the nature of an inquiry, the network layer can provide either information reflecting the traffic conditions on a specific route or route recommendations designed to achieve a desired traffic flow. The vehicle operator finalizes the route selection and informs the network of his/her selected route.

N1 Monitor traffic condition and predict congestion

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

N2 Recommend route

Upon receiving the location and the destination of a vehicle, the network layer may recommend the shortest/fastest route. Route recommendation may be provided at the beginning of a trip or anytime during the trip.

N3 Receive information from link layer

The network layer receives information regarding regional traffic condition and route selection request from the link layer.

N4 Provide information to/via link layer

The route recommendation, traffic prediction information, and vehicle ID assignment will be sent to the requester via link layer.

Link Layer

Each route in the automated highway network can be subdivided into sections, defined as links. The link layer is responsible for path and congestion control within individual links on the assigned route. The link layer may select a lane for each vehicle, set target speeds for vehicles or groups for each section of the route, and manipulate group size (when relevant) depending on the flow. It may also prioritize the vehicle's operation during cooperative maneuvers and manage incident responses.

L1 Assign lane

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

L2 Assign target speed

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

L3 Set maximum group size

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

L4 Set minimal separations

The required minimal headway is provided in accordance with the weather and roadway conditions. In a system with groups the required minimum spacing between groups is provided.

L5 Prioritize vehicle operations

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

L6 Monitor regional traffic condition and manage incidents

Traffic conditions are monitored. Under incident conditions, the link layer selects paths for vehicles, adjusts target speed, or instructs vehicles to changes lane for diversion around incidents.

L7 Monitor road surface conditions and weather

The link layer determines weather and road surface conditions, based in part on vehicle traction reports.

L8 Receive information from the coordination layer

The link layer receives information regarding traffic condition of the subsections within the link and vehicle's destination from the coordination layer. The link layer also receives information addressing the network layer from the coordination layer.

L9 Receive information from the network layer

The link layer receives information regarding the traffic condition predictions and route recommendations from the network layer. The link layer may also receive information addressing the vehicle from the network layer.

L10 Receive information from neighboring link

Receive handoff information as vehicle passes from one link to the next.

L11 Provide information to the network layer

The link layer provides information regarding regional traffic condition to the network layer. The link layer also transfers the information intended for the network layer from the coordination layer.

L12 Provide information to the coordination layer

The link layer provides information regarding vehicle operation parameters such as target speed and minimal separation to the coordination layer. The link layer also transfers the information intended for the coordination layer from the network layer.

L13 Provide information to neighboring link

Provide handoff information as vehicle passes from one link to the next.

Coordination Layer

The coordination layer is responsible for microscopic management of a subsection within a link. The coordination layer inspects and monitors vehicle and traffic flows, issues permission/rejection, and coordinates complicated maneuvers under both normal and incident conditions. The coordination layer also provides information regarding the road surface conditions and weather, and sets minimal separations. In a system with groups, the coordination layer is also responsible for joining and splitting groups.

C1 Perform off-vehicle inspection and monitoring

Vehicle inspection requiring supplemental off-vehicle equipment could be performed before the vehicle enters the AHS, or while the vehicle is on the AHS. These inspection and monitoring functions, which may work together with on-vehicle detection/diagnosis devices, provide vehicle health or condition reports

C2 Issue permission/rejection

Based on the inspection/monitoring outcome, traffic flow and destination parameters, the coordination layer issues permission for entering or remaining on the AHS. Should a fault(s) be detected, a rejection command will be issued.

C3 Plan maneuver coordination

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

C3.1 PLAN MANEUVER COORDINATION FOR NORMAL CONDITIONS

Normal maneuvers that require coordination between vehicles, such as lane-changing, merging, entering or exiting an AHS, or joining or splitting a group, are handled by the coordination layer. The coordination layer sets up coordination protocols among the involved vehicles and determines commanded speed, location, and condition for maneuvering action.

C3.2 PLAN MANEUVER COORDINATION FOR HAZARDOUS CONDITIONS

Under hazardous conditions, the coordination layer provides information regarding specific hazards to vehicles which are potentially affected, and provides instructions for avoiding collisions.

C4 Supervise the sequences of coordinated maneuvers

The coordination maneuvers will be monitored by the coordination layer.

C5 Obtain vehicle ID

Obtain identification address used to communicate with a particular vehicle.

C6 Receive information from the link layer

The coordination layer receives information regarding the vehicle operation parameters such as target speed and minimal separation from the link layer. The coordination layer also receives information intended for the regulation layer from the link layer.

C7 Receive information from the regulation layer

Two types of information will be acquired by the coordination layer, including the requests for a maneuver that will require coordination, such as lane-changing, and status information about vehicles.

C8 Receive information from neighboring coord. element

Receive information on coordination maneuvers planned for neighboring coordination element's span of control.

C9 Provide information to the link layer

The coordination layer provides information regarding traffic condition of the subsections within the link and vehicle's destination. The coordination layer also transfers the information intended for the link layer or the network layer from the regulation layer.

C10 Provide information to the regulation layer

The coordination layer provides operation commands defining the sequences of coordination maneuvers and information such as road surface condition and weather to the regulation layer.

C11 Provide information to neighboring coord. element

Provide information on coordination maneuvers planned for this coordination element's span of control.

C12 Determine roadway operational limits

Determine the maximum safe speed and minimum safe gap for this segment of roadway based on road surface conditions, known curvature, anticipated weather including wind, temperature and rain/snow.

Regulation Layer

The regulation layer carries out the directions of the coordination layer. It tracks target speeds, maintains separations between vehicles and between groups, and provides commands to perform steering and speed control for maintaining the lateral position of the vehicle and the longitudinal separation between vehicles. It also provides commands to implement lane-changing, merging, and splitting/joining a group. The regulation layer is also responsible for monitoring vehicle conditions and for on-board failure detection/diagnosis.

R1 Provide steering control command

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

R2 Provide speed regulation command

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

R2.1 PROVIDE HEADWAY KEEPING COMMAND

Headway keeping (for groups only) forms an "inner loop" of the speed regulation command, overriding target speed considerations

R2.2 PROVIDE TARGET SPEED TRACKING COMMAND

Maintain speed commanded by coordination layer. Overridden by headway keeping and collision avoidance.

R3 Provide braking command

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

R4 Manage vehicle health

Vehicle conditions are monitored using the sensory information provided by the physical layer. Failure detection and diagnosis are performed when a system fault is discovered. Failure response actions are determined. On-board actions are performed. Failure response actions requiring roadside involvement are communicated.

R4.1 MONITOR PROPULSION SYSTEM

Several parameters such as temperature, pressure (for an internal combustion system), or current (for an electrical system) are selected to represent the health of the propulsion system.

R4.2 MONITOR BRAKING SYSTEM

Several parameters such as temperature of brake discs or shoes and pressure of brake hydraulic system are selected to characterize the health of the braking system.

R4.3 MONITOR STEERING SYSTEM

Several parameters such as hydraulic pressure (for a hydraulic steering actuator) or current (for an electrical steering actuator) and temperature will be used to characterize the health of the steering system.

R4.4 MONITOR ELECTRICAL SYSTEM

Several parameters such as voltage, current, and temperature will be used to characterize the electrical system.

R4.5 MONITOR ENERGY SUPPLY

Determine remaining energy, e.g., fuel level, battery voltage, ...

R4.6 MONITOR DISPLAYS

Determine correct function of displays.

R4.7 MONITOR CONTROLS

Determine correct function of controls.

R4.8 MONITOR COMM

Determine correct function of the communications subsystem.

R5 Monitor driver health/readiness

Ensure driver is prepared to undertake manual operation

R6 Monitor roadside health

Roadside function is monitored using sensory information from monitored functions and (potentially) vehicle cross-checks.

R6.1 MONITOR ROADSIDE COMM

Determine correct function of the communications subsystem.

R6.2 MONITOR ROADSIDE COMPUTING EQUIPMENT

Determine correct function of the computers & associated peripheral equipment.

R6.3 MONITOR ROADSIDE SENSORS

Determine correct function of the roadside sensing equipment.

R7 Monitor trip progress

The trip progress is monitored by reporting to the operator the information regarding vehicle location and traffic condition and estimated arrival time.

R8 Receive information from the coordination layer

The regulation layer receives information regarding operation commands which defines the sequences of coordination maneuvers and information such as road surface condition and weather from the coordination layer.

R9 Receive information from physical layer

The regulation layer receives information regarding sensory measurements and user's requests from the physical layer.

R10 Provide information to the coordination layer

The regulation layer provides information about maneuvers requiring coordination, such as lane-changes, and the status of vehicles.

R11 Provide information to the physical layer

The regulation layer provides control commands to the physical layer.

R12 Detect obstacle

Determine whether information from physical layer concerning front/rear/side detections constitutes obstacle. Includes loss of road.

R13 Determine dynamic response of propulsion system

The dynamic response of the propulsion system is characterized by the time interval required for accelerating the vehicle to a target speed from a specified initial speed.

R14 Determine dynamic response of braking system

The dynamic response of the braking system is characterized by the time interval required for decelerating a vehicle from certain speed to a stop.

R15 Determine dynamic response of steering system

The dynamic response of the steering system is characterized by the frequency response of the steering system and the deadband.

R16 Determine traction

The parameters which affect the vehicle's slip or traction will be monitored.

R17 Determine visibility

The visibility (e.g., of the collision avoidance sensor) will be monitored and graded.

R18 Convey information to driver

Format information for display.

R18.1 CONVEY VEHICLE SPEED

Convey speed information

R18.2 CONVEY HEADWAY

Convey distance to leading vehicle

R18.3 CONVEY ENERGY LEVEL

Convey remaining energy (fuel, voltage)

R18.4 CONVEY DIAGNOSIS INFORMATION AND WARNING SIGNALS

Alert driver to problems with vehicle that reduce capability or reserve.

R18.5 CONVEY MODE STATUS

Effectively tell driver what mode the vehicle is in, e.g., auto, manual, emergency.

R18.6 CONVEY ROUTE RECOMMENDATION INFORMATION

Effectively tell driver what route is optimal in the estimation of network layer.

R18.7 CONVEY YELLOW PAGE INFORMATION

Effectively tell driver relevant local (business?)information

R18.8 CONVEY TRIP PROGRESS REPORT

Effectively tell driver progress of vehicle

R18.9 CONVEY LOCATION

Effectively tell driver current location.

R18.10 CONVEY LANE RECOGNITION

Effectively tell driver current lane.

R19 Request information

The driver or other system elements may request various kinds of information from the system.

R19.1 REQUEST VEHICLE STATUS

Driver or other system element may request vehicle status.

R19.2 REQUEST SYSTEM STATUS

Driver asks for roadside health info.

R19.3 REQUEST TRIP PROGRESS

Driver asks for progress of vehicle.

R19.4 REQUEST TRAFFIC CONDITION

Driver requests network level view of system status.

R19.5 REQUEST PERFORMANCE ADJUSTMENT

Driver may request that vehicle perform within certain constraints on acceleration, headway, etc.

R20 Receive information

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

R21 Provide information/acknowledgments

The driver will be required to provide information to the system. This includes the following:

R21.1 PROVIDE REQUESTS TO ENTER THE AHS

The vehicle operator requests permission to enter the AHS

R21.2 PROVIDE DESTINATION

The driver will be required to designate a destination for his/her trip. This function also will allow the driver to change that destination during the trip.

R21.3 PROVIDE REQUESTS TO IMMEDIATELY EXIT AHS

The driver may request to leave the system at the closest possible exit or to leave the transition lane prior to entering the automated lane.

R21.4 GRANT AUTHORIZATION FOR CHANGE FROM MANUAL TO AUTOMATED MODE

The driver must provide a final authorization in order for the manual to automated control transition to proceed.

R21.5 PROVIDE RESPONSES TO MANUAL CONTROL READINESS TESTS

The driver will have to make some input when cued by the system to indicate his/her readiness to resume manual control.

R22 Perform mode selection

Determine and initiate the appropriate mode of operation for the vehicle, including automatic, manual, and crisis operational status.

R23 Configure for manual operation

Ensure that the vehicle has all functions necessary for manual operation enabled (e.g., wipers, lights, defroster...)

Physical Layer

The physical layer includes the actuation and sensing devices that actually carry out the control commands of the regulation layer and feed information back to it. The physical layer is also responsible for human-machine interaction.

P1 Sensing

Four groups of sensory information are needed. The sensory information can be obtained through direct sensing or combined sensing and signal processing. The following information may be entirely or partially needed for any specific AHS design.

P1.1 SENSE LATERAL DISPLACEMENT

The distance from a point along the longitudinal center line of the vehicle to a reference line or marker. The reference can be a roadway reference which delineates the center or the edge of a traffic lane or a roadside reference which retains a constant

P1.2 SENSE BEARING

Determine bearing of vehicle.

P1.3 SENSE LONGITUDINAL POSITION

The vehicle acquires its longitudinal position of the vehicle relative to a milepost.

P1.4 RECOGNIZE LANE

The vehicle recognizes the number of the lane on which the vehicle is traveling.

P1.5 SENSE VELOCITY

The vehicle measures its velocity as the distance traveled in a specified time interval.

P1.6 SENSE LATERAL ACCELERATION

The lateral acceleration is measured as the variation in velocity in the lateral direction during a specified time interval at the mass center.

P1.7 SENSE LONGITUDINAL ACCELERATION

The longitudinal acceleration is measured as the variation in velocity in the longitudinal direction during a specified time interval at the mass center.

P1.8 SENSE YAW RATE

Yaw rate is measured as the angular change in a specified time interval along the axis perpendicular to the road surface.

P1.9 SENSE ROLL RATE

Roll rate is measured as the angular change in a specified time interval along the longitudinal axis through the center of gravity of the vehicle

P1.10 SENSE PITCH RATE

Pitch rate is measured as the angular change in a specified time interval along the lateral axis through the center of gravity of the vehicle.

P1.11 SENSE RANGE TO A FRONTAL OBJECT/VEHICLE

The distance to a frontal vehicle is measured as the separation between the controlled vehicle and the frontal vehicle.

P1.12 DETERMINE CLOSING RATE TO A FRONT OBJECT/VEHICLE

The closing rate to a frontal vehicle is measured as the variation in distance between the controlled vehicle and the frontal vehicle in a specified time interval.

P1.13 SENSE RANGE TO A NEIGHBORING (SIDE) OBJECT/VEHICLE

The distance to a neighboring vehicle is measured as the separation between the controlled vehicle and the neighboring vehicle.

P1.14 DETERMINE CLOSING RATE TO A NEIGHBORING OBJECT/VEHICLE.

The closing rate to a neighboring vehicle is measured as the variation in distance between the controlled vehicle and the neighboring vehicle in a specified time interval.

P1.15 SENSE RANGE TO A REAR OBJECT/VEHICLE

The distance to a rear vehicle is measured as the separation between the controlled vehicle and the rear vehicle.

P1.16 DETERMINE CLOSING RATE TO A REAR OBJECT/VEHICLE

The closing rate to a read vehicle/obstacle is measured as the variation in distance between the controlled vehicle and the rear vehicle/obstacle in a specified time interval.

P1.17 DETERMINE TIRE PRESSURE

Tire pressure can be physical measurements or estimation based on dynamic performance.

P1.18 SENSE ENERGY LEVEL

Energy level can be fuel level (for an internal combustion propulsion system) or voltage (for an electrical propulsion system) or both (for an hybrid vehicle).

P1.19 SENSE OR READ CURVATURE

A horizontal curve is characterized by several parameters, i.e. radius and length of the curvature, and the distance to the curvature.

P1.20 SENSE OR READ GRADE

A vertical curvature is characterized by gradient and the length of the curvature and the distance to the curvature.

P1.21 SENSE OR READ BANK

A bank is characterized by length of the bank, bank angle, and distance to bank.

P1.22 SENSE OR READ CONFIGURATION AND LOCATION OF ENTRANCE/EXIT GATES

When entrance/exit gates are present, the distance to a gate, the direction of the gate, and the size of the gate will be given.

P1.23 SENSE ROAD SURFACE CONDITION

The condition of the road, particularly the parameters which will affect the vehicle cornering force, will be monitored.

P1.24 SENSE VISIBILITY

The visibility will be monitored and graded.

P1.25 CHARACTERIZE WIND

The direction and magnitude of the wind will be measured.

P1.26 OBTAIN TRAFFIC SIGNAL INFORMATION

Traffic signals for speed control will be transmitted to or recognized by the vehicle.

P1.27 OBTAIN TRAFFIC SIGN INFORMATION

Traffic signs will be transmitted or recognized by the vehicle.

P2 Actuation

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

P2.1 PERFORM STEERING ACTUATION

The steering actuation causes the wheels to turn forcing the vehicle to change its direction of motion.

P2.2 PERFORM PROPULSION ACTUATION

The propulsion actuation causes a vehicle accelerate or decelerate (using engine brake).

P2.3 PERFORM BRAKE ACTUATION

The brake actuation causes a vehicle to decelerate.

P2.4 SHUTDOWN PROPULSION SYSTEM

In the event of an overspeed condition, the propulsion system must be capable of being deactivated

P3 Human-machine interface

The human-machine interface enables the human operator to monitor the performance of the vehicle, to adjust performance parameters within a reasonable working range, to be aware of hazardous conditions, and to take over control tasks if necessary. It may

P3.1 PROVIDE OPERATOR DISPLAYS

The operator requires some set of devices which will be used to convey information to him/her. Audio, lights, flat panel displays are all possible examples.

P3.2 PROVIDE SWITCH. MECH. FOR ALTERNATING BTW AUTO AND MANUAL CONTROL

Engagement/disengagement of automated commands.

P3.3 PROVIDE EMERGENCY SWITCHING MECHANISM FOR HUMAN BACKUP OPERATION

Disengagement of auto functions for emergency conditions.

P3.4 PROVIDE MANUAL STEERING CAPABILITY

Standard functions. Criticality implications for AHS in mixed traffic.

P3.5 PROVIDE MANUAL PROPULSION CONTROL CAPABILITY

Standard functions. Criticality implications for AHS in mixed traffic.

P3.6 PROVIDE MANUAL BRAKE CONTROL CAPABILITY

Standard functions. Criticality implications for AHS in mixed traffic.

P3.7 PROVIDE OPERATOR AHS INPUT CAPABILITY

Provide means for operator to convey information to AHS. Keypad, voice recognition, etc., are all examples.

P4 Store/provide maintenance history

Maintain record of when maintenance and or inspection was last performed on given system elements.

P5 Provide receiver channel from the roadside

The physical layer receives control commands from the regulation layer.

P6 Provide transmitter channel to the roadside

The physical layer provides sensory information and user's request to the regulation layer.

P7 Provide receiver channel from adjacent vehicle

Obtain information on neighboring vehicles, such as location and potential actions.

P8 Provide transmitter channel to adjacent vehicle

Information on existence, upcoming commands and actions are conveyed.

P9 Perform secondary functions

The secondary functions that exist on the existing vehicles such as windshield wipers, defroster and lights will be incorporated in the AHS.

P10 Provide electrical power

Provide power for electronics, any electrically powered actuators, lights, displays, etc.

P11 Obtain ID

Provide means for roadside to obtain ID of vehicle. Presence of this function implies that the ID is not transmitted via the standard comm link.

P12 Provide ID

Provide a unique vehicle identifier to the roadside. This identifier is used to key inspection records and past performance history.

FUNCTION CHARACTERIZATION

Criticality

For the purposes of this discussion, we have take our definition of criticality from the aerospace industry, in particular the Federal Aviation Regulations (FAR), Part 25.1309: Equipment, Systems, and Installation. Following this model, a function’s criticality can have three values: critical, essential, or non-essential. A function is critical if the loss of that function results in injury or property damages. A function is essential, if the loss of that function significantly degrades the operation of an AHS. All other function are non-essential.

An example of a critical function is *sense lateral displacement*. If a vehicle is unable to maintain its position in a lane, the vehicle could impact a barrier, impact another vehicle, or leave the road entirely. An example of an essential function is *assign target speed*. If a vehicle is assigned a target speed that is lower than the optimum speed in current traffic, other vehicles will slow to avoid collision and the overall throughput of the AHS will decrease. Note that for this function to be essential, the a collision avoidance system that can override the *assign target speed* function must be critical. An example of a non-essential function is *effectively tell driver relevant local business information*. Due to the process by which the function list was derived, very few non-essential functions are listed in this paper. The non-essential functions have negligible impact on the check-in, check-out, and malfunction management tasks.

In our analysis of function criticality, great pains were taken to ensure that no functions were labeled as critical that could not be accomplished or safeguarded by some other (critical) function to prevent accidents, as in the example of *assign target speed* above. When this can be done, the equipment necessary to satisfy the essential function does not need to be accounted for in the safety reliability estimate. The safety reliability goal only applies to equipment that performs critical functions.

Partitioning

Partitioning the functions examined each function and identified the actor that performed that function. Functions are performed by the vehicle, the roadside, the operator, or by some other entity. An example of an other entity is a local facility that is authorized to inspect the vehicle’s brake wear. In partitioning the function, our goal was to hypothesize an implementation which, in our combined judgment, was implementable with respect to cost, safety and technology state of the art considerations.

An example of this allocation is for the function *plan maneuver coordination* . In this case, we considered it impractical to implement the function using solely roadside equipment. Though technically feasible (perhaps by means of IR or EO spectrum camera equipment), it would be quite expensive to provide the roadside equipment full knowledge of each car's (AHS-equipped and intruders alike) position to sub-meter accuracy to allow maneuver planning. On the other hand, we could easily postulate scenarios in which the performance of the vehicle operating on its local knowledge would be suboptimal. Thus, we proposed an allocation in which the vehicle performed the precise maneuver planning, and the roadside provided a benign environment in which to maneuver, by commanding gap sizes and speed. See the function definition table located in the appendix for the complete allocation listing.

RELIABILITY OF THE AUTOMATED HIGHWAY SYSTEM

The following definitions are proposed to form a baseline for discussing requirements, and preparing system and subsystem specifications. Many basic design functions are dependent on the requirements stemming from these definitions as well as the overall performance requirements.

Definitions

Many of these definitions are derived from the aircraft industry where safety of flight has been an ongoing design consideration for many years. As we proceed with the preliminary systems analysis, refinements of these definitions as well as the creation of those specifically oriented to the automated highway problem will occur.

Safety

The central concept is safety. A system's safety is provided by a (subset) of functions whose performance is [safety] critical. A function is safety critical when its randomly occurring loss would cause death, injury, or property damage. A system is [increasingly] safe when it can deliver the safety critical functions reliably. A function is said to be [increasingly] reliable when the probability that the function performs correctly at time T is high, given that the function was performing correctly at time t(0). This reliability is often measured in terms of the Mean Time Between Failures (MTBF).

Mean Time Between Failures

This is the familiar reliability requirement (MTBF) applied to any vehicle component or subsystem. Each component has a failure rate assigned to it, and is measured in terms of failures per hour. A typical number for an actuator for example, is on the order of $10x10^{-6}$ to $80x10^{-6}$ fail/hr, and represents the sum of all component failure rates within the actuator mechanism. The actuator is then a component in the control subsystem.

The inverse of the sum of all the component failure rates in the system is the MTBF measured in hours between failures.

Mean Time to First Failure

Closely related to MTBF is MTTFF which is time to the failure of <u>any</u> device in the system, so it is the inverse of the sum of <u>all</u> components within the system. This may or may not cause a mission failure, since it may be a non essential part such as torn braid on a cable, or the bulb in the fuel level gage. In a system properly designed for safety criticality, the probability of any first fault causing a catastrophic failure is extremely low due to redundancy.

Probability of Mission Success

This is defined as the probability of sustaining any failure that would cause loss of the automated highway function, but not necessarily result in a catastrophic fault. An example might be loss of route recommendation. This would curtail one of the useful functions of the AHS design, but not cause a crash. Another might be the loss of the capability to monitor trip progress, which might result in a missed exit, but not a catastrophic event. The rules applied to the amount of equipment required to maintain operational status at any time also affect the mission success probability.

If for example you have a dual path system that requires both paths to fail for a catastrophic fault, then; P{success(not having catastrophic fault)}=P{success of each path}^{2}+2P{success of one & failure of the other}. If our rule for completing the mission says both paths must be operative, and that if one fails, you must abort (leave the roadway as soon as possible), then P{success(completing the mission)}=P{success of each path}^{2}. If a display (route plan, etc.) is necessary to complete the mission, but does not "crash" the vehicle if lost, then P{success}=[P{success of each path}^{2}][P{success of display}]. This process would continue for all mission critical elements.

Probability of Catastrophic Loss

This is the probability of having a fault affecting safety, or, a fault which will result in the loss of control of the vehicle For the AHS health management study, we have established a preliminary requirement for the system (includes elements of the vehicle and roadside) of $1x10^{-6}$. Included within this are only the portions of the system relating to safe operation which would include the system operation functions, and any diagnostic of test equipment needed to maintain operation.

Mean Time Between Unscheduled Maintenance Actions

The mean time between events which would cause an unscheduled maintenance action (MTBUMA) would be a relatively new standard to the industry. Maintenance standards for new cars exist, with specified times (or miles) between "required" maintenance actions. Most maintenance on older vehicles, and even some new, is only completed as needed by the owner.

This standard would represent the probability of breakdown between the recommended service times. The breakdowns which contribute to the MTBUMA are not only those which could cause a catastrophic event, but also less critical failures. If a part can be diagnosed with on-board equipment to have an impending failure possibility, a replacement recommendation could be made for the next scheduled maintenance visit. In general, however, even with the better maintenance management available, owners may tend to ignore such a recommendation, and drive it till it breaks unless a vehicle with a predicted failure would not be allowed on the highway.

The MTBUMA is computed by the inverse of the sum of the failure rates for all parts which, if they fail, would cause an immediate repair action. One failure of this type would be a second path in a dual redundant subsystem. The vehicle is still in operational condition (no safety critical fault, and it could still accomplish its destination) but rules for access to the highway would probably require replacement of the failed channel. A fault of this type could also require removal from the highway at the next exit, or breakdown lane area

False Alarm Rate

False alarms are the result of indications or alarms by fault detection monitors that are built in to the system that a fault has occurred under operating conditions where no actual fault existed. These have important effects on the throughput of the highway and general traffic flow, and occur because of the following:

1. Design tolerance growth of an otherwise operational part beyond that allowed by the monitor design. This is caused by greater than the normally used root mean square combinations of tolerance, environmental effects, and aging.

2. Noise causing a monitor to exceed detection limits.

3. Dynamic conditions in the system operation beyond the design limits of the specification.

4. Incomplete dynamic analysis and testing during the monitor development.

5. Mechanical aberrations that disappear when device is pulled for maintenance. This could include cracked circuit board, damaged connector pin, poor connections within individual integrated circuits etc. There are procedures which will find these over a period of time including on board recording of all events that cause excursion beyond monitor detect tolerances, and tracking at the service location (records kept within the device) to locate repeating, similar faults.

6. Greater than design specification limits for EMI and power surges. Intermittents are defined as faults which exist for a period shorter than the time set for the monitor between detection and alarm or "trip." These occurrences may be recorded for further maintenance work, but do not cause a permanent fault monitor latch.

False alarm rates are typically required to be in the 2 to 5 percent of the system or device failure rate.

Dynamic System Performance Under Failure Conditions

This category deals with failures at the moment of occurrence, through the detection and transition to a reconfigured system or device. This is an extremely important specification and will be dealt with in some detail in the section on malfunction management.

A typical specification for this system characteristic is shown in figure 8. There are a family of curves which in effect represent the sensitivity of the system to ever increasing lengths of time at fault.

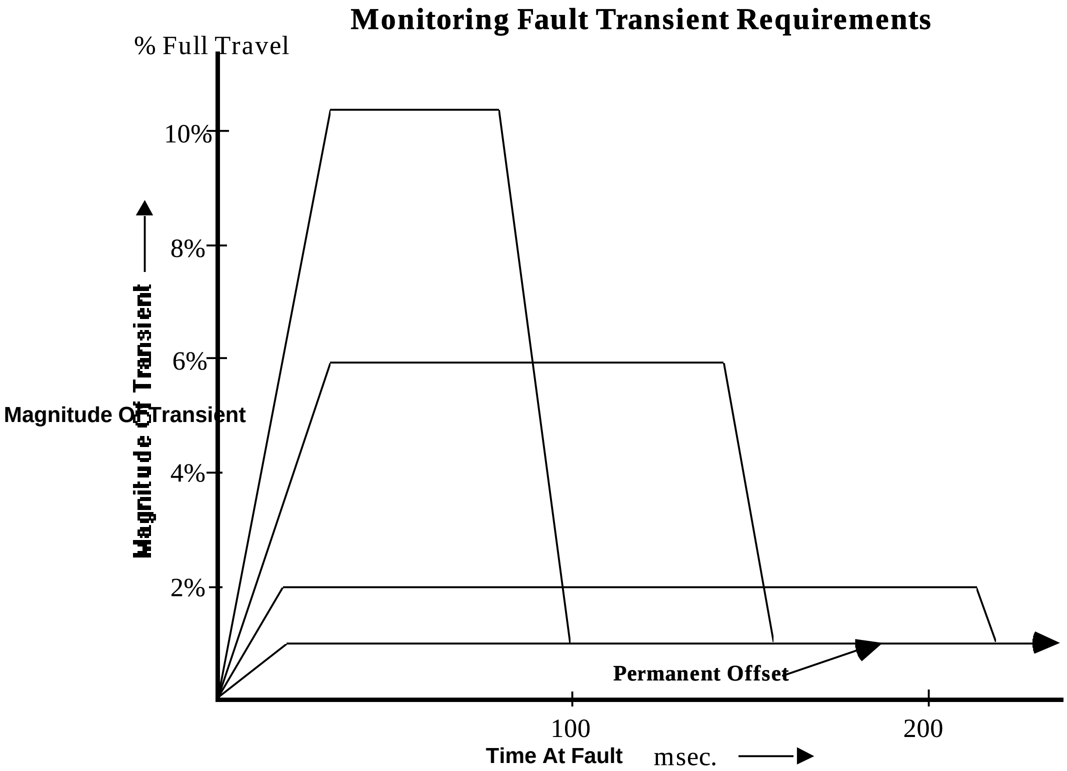
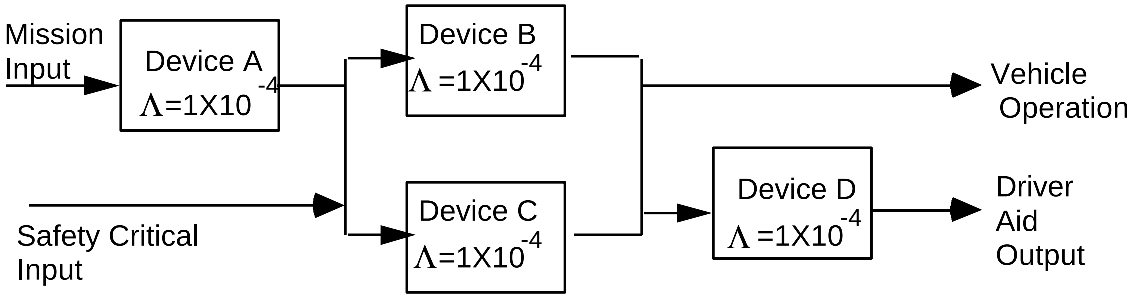


Figure 8. System Sensitivity to Time

Typical numbers are shown based on past experience with systems with similar dynamic performance requirements. These requirements indicate that large faults must be removed quickly, while smaller faults may be given more time and possibly be better identified as a real fault. Therefore, the monitoring concept can utilize this in an adaptive manner, or simply design for the worst case and detect and exclude faults assuming they are all large. The other area of interest is the bottom curve which in effect indicates the limit of the permanent offset introduced by the reconfiguration mechanization.

Basis of Estimates for System Health Management

The following paragraphs define the computational method for the various safety and reliability terms. The example in figure 9 will be used to show computation techniques where applicable.



Sample Vehicle System

Figure 9. Sample Vehicle System

This is a system representing two serial devices, A and D in series with a dual element composed of B and C. For each device, A through D, the failure rate (i.e. probability that the device will fail in any given hour of operation) is $1\text{x}10^{-4}$.

Mean Time Between Failures

The MTBF for this system would be the inverse of the sum of the failure rates or;

$$\text{MTBF} = 1/\Lambda_{sys} = 1/(\Lambda_a+\Lambda_b+\Lambda_c+\Lambda_d)= 1/5\text{x}10^{-4} = 2500 \text{ hours} \qquad (2)$$

Where:

Λ_x = Failure rate of device x

Probability of Mission Success

This probability is dependent upon the individual subsystem MTBFs, the architecture in which the subsystems are interconnected and the mission time. The devices which can sustain failures, but still allow the mission to proceed must be accounted for. For the above example, it is assumed that when one of the dual devices fails, the vehicle must leave the highway as soon as practicable, therefore not completing the mission. When device D fails, the mission can still be completed. So, the probability of mission success requires that devices A, B and C all continue to function, and with perfect test coverage and a one hour mission;

$$P_{sm}= P_{sa}\{P_{sb}P_{sc}\} \qquad (3)$$

$$= (1-P_{fa})\{(1-P_{fb})(1-P_{fc})\}$$
$$= (1-\Lambda_a t)\{(1-\Lambda_b t)(1-\Lambda_c t)\}$$
$$= 0.9997$$

$$P_{fm} = 1-P_{sm}= 3\text{x}10^{-4} \qquad (4)$$

Where:

P_{sx}= Probability of success of device x.

Psm= Probability of mission success

Pfx= Probability of failure of device x (= 1-Psx)
Λ_x= Failure rate of device x
t= Time, hours

If we change our assumtion and allow mission completion upon failure of one of the dual paths (this might be half of a dual redundant steering system), the above probability is improved as follows:

$P_{sm} = P_{sa}\{P_{sb}P_{sc}+(1-P_{sb})P_{sc}+(1-P_{sc})P_{sb}\}$
(5)

$= (1-P_{fa})\{(1-P_{fb})(1-P_{fc})+(P_{fb})(1-P_{fc})+(P_{fc})(1-P_{fb})\}$
$= (1-\Lambda_{a}t)\{(1-\Lambda_{b}t)(1-\Lambda_{c}t)+(\Lambda_{b}t)(1-\Lambda_{c}t)+(\Lambda_{c}t)(1-\Lambda_{b}t)\}$
$= .999899980$

$P_{fm} = 1-P_{ms}$ Å$1.001x10^{-4}$
(6)

This mission success equation can be interpreted as the probability that device A works correctly and either both B and C work, or B fails in a detected manner and C works, or C fails in a detected manner and B works."

If the above example is recomputed with imperfect test coverage, the results are again altered. Test coverage is the ability for any one device to monitor itself, that is, 95 percent coverage means that 5 percent of the device is not tested (on the series of tests being considered). This means that the capability of distinguishing which of the dual devices has failed is reduced to a probability of 0.95, and although conservative, we assume that this lack of capability represents a failure of the mission.

$P_{sm} = P_{sa}\{P_{sb}P_{sc}+(1-P_{sb})C_{b}P_{sc}+(1-P_{sc})C_{c}P_{sb}\}$
(7)
$= (1-P_{fa})\{(1-P_{fb})(1-P_{fc})+(P_{fb})C_{b}(1-P_{fc})+(P_{fc})C_{c}(1-P_{fb})\}$

$P_{fm} = 1-P_{sm}$ (8)

Where:
C_x= Coverage of device x

The results of the above equations with the same values for failure rates, and range of coverages is shown in figure 10.

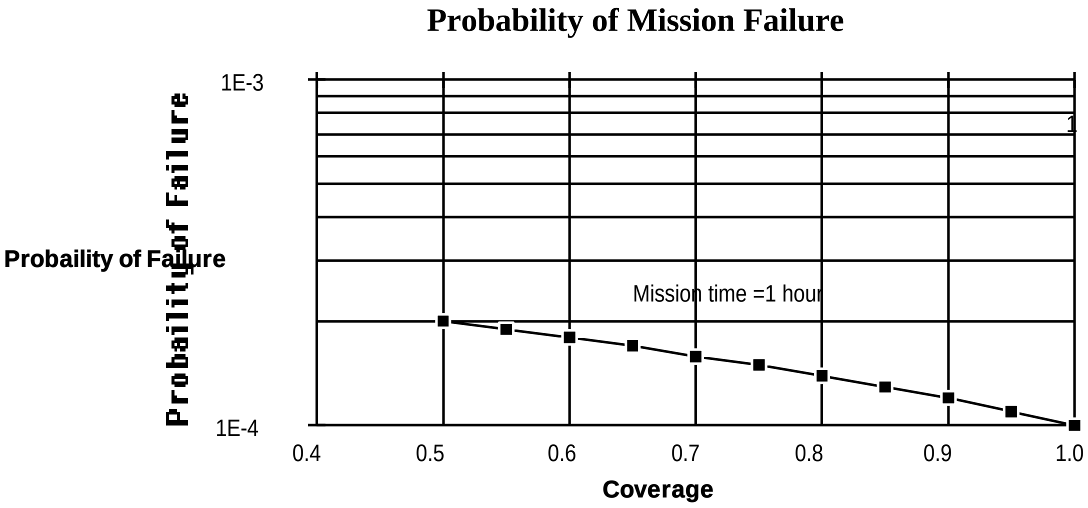


Figure 10. Probability of Mission Failure

In this case, the effect of coverage is not extremely sensitive.

Probability of Catastrophic Loss

For the example system, the portion relating only to safety would be the dual redundant pair of devices, B and C. Device A is critical to the mission success, but D and E are non safety or mission critical. Consequently, including the imperfect coverage once again, the probability may be determined as follows:

$$\begin{aligned} P_{ssys} &= P_{sb}P_{sc}+(1-P_{sb})C_bP_{sc}+(1-P_{sc})C_cP_{sb} \\ &= (1-P_{fb})(1-P_{fc})+(P_{fb})C_b(1-P_{fc})+(P_{fc})C_c(1-P_{fb}) \qquad (9) \end{aligned}$$

The results of these equations with the same system values we have been using are presented in figure 11.

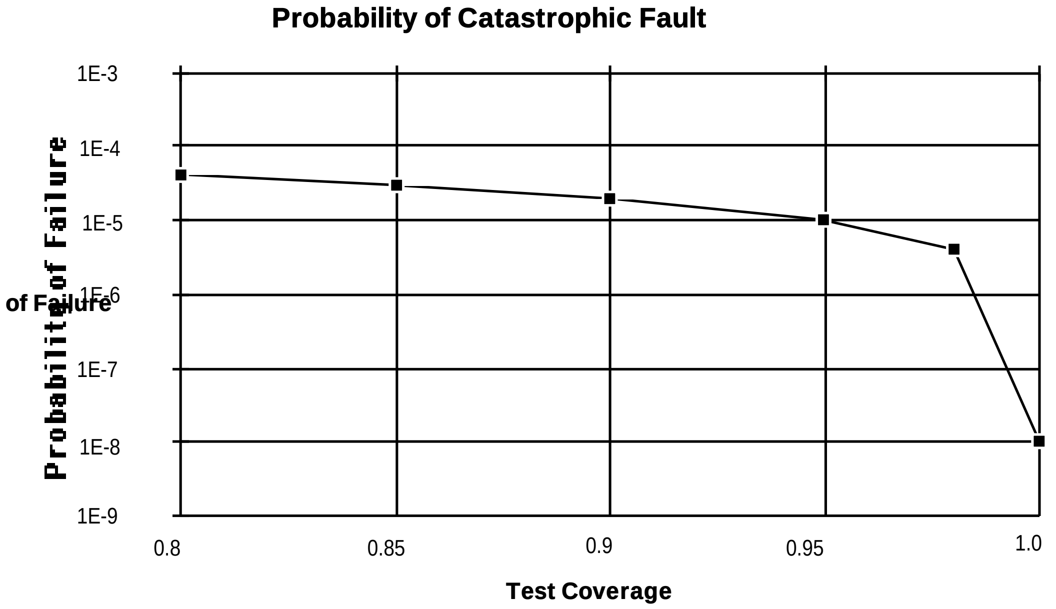


Figure 11. Probability of Catastrophic Fault

As shown, the effect of coverage on the safety critical performance is significant, changing three orders of magnitude for a 5 percent change in test coverage, and two orders of magnitude for a 3 percent change.

Mean Time Between Unscheduled Maintenance Actions

MTBUMA is computed from the failure rates of all parts which would cause a repair action. If device D fails, but the repair can wait until a normal service time then the MTBUMA would be:

$$\text{MTBUMA} = 1/(\Lambda_a+\Lambda_b+\Lambda_c) = 1/3\text{x}10^{-4} \text{ Å } 3300 \text{ hours} \qquad (10)$$

False Alarm Rate

At 2 percent of the system failure rate, the false alarm limit would be:

$$(.02)\Lambda_{sys} = (.02)(\Lambda_a+\Lambda_b+\Lambda_c+\Lambda_d)= (.02)(5\text{x}10^{-4}) \qquad (11)$$

$$= 1\text{x}10^{-5} \text{ false alarms/hour of operation}$$

Predicting this value requires careful analysis and simulation of the dynamic system conditions with all monitors and their tolerances in place. Estimates of the items found in the definition section can be done based on past experience with similar system mechanizations.

Summary

This section attempted to identify and quantify the primary elements of the system reliability and safety. Each of these has design implications on the quality of parts, and the level of redundancy necessary to meet an overall system requirement. The design of health management for the AHS will require each of these to be thoroughly evaluated and specified as requirements, then analyzed and simulated where applicable during the design phase. The failure rate data and its derivation is given in the Appendix.

CRITICAL FUNCTION MECHANIZATION

The mechanization diagrams provide a representational form that permits discussion and analysis of an AHS implementation. The mechanizations take the form of block diagrams. These diagrams show physical components and the interconnections between them.

Vehicle

The critical functions allocated to the vehicle in an AHS have been divided according to subsystems to simplify the task of deriving mechanizations: steering, braking, sensors, engine, processing, communication, and displays and controls. Table 2 shows a mapping of function to subsystem. In order to analyze check-in, monitoring, and malfunction management, a block diagram is provided for each subsystem, showing mechanical components, inputs for control commands, and sensing elements.

Table 2. Function to Subsystem Allocation

	Steering	Braking	Sensors Mechanization	Obstacle detection	Lateral sensing	Acceleration and rate sensing	Processing	Communications	Displays and Controls	Engine	Function Coverage
P11. Provide ID								X			X
P10. Provide electrical power										X	X
P9. Perform secondary functions (lights, etc?)							X		X		X
P8 Provide transmitter channel to an adjacent vehicle								X			X
P7. Provide receiver channel from an adjacent vehicle								X			X
P6. Provide transmitter channel to the roadside							X				X
P5 Provide receiver channel from the roadside							X				X
P3.7 Provide operator AHS input capability							X		X		X
P3.5 Provide manual brake control capability		X							X		X
P3.5 Provide manual propulsion control capability										X	X
P3.4 Provide manual steering capability	X								X		X
P3.3 Provide mechanism for human backup operation	X	X								X	X
P3.2 Provide switch mech for auto-manual control	X	X					X		X	X	X
P3.1 Provide operator displays							X		X		X
P2.4 Shutdown propulsion system							X			X	X
P2.3 Perform brake actuation		X					X				X
P2.1 Perform steering actuation	X						X				X
P1.25 Sense visibility				X							X
P1.24 Characterize wind							X				X
P1.23 Sense road surface condition		X					X				X
P1.22 Sense or read configuration of entrance / exit gates					X						X
P1.21 Sense or read bank					X						X
P1.20 Sense or read grade					X						X
P1.19 Sense or read road curvature					X						X
P1.16 Determine closing rate to rear object/vehicle				X							X
P1.15 Sense range to a rear object/vehicle				X							X
P1.14 Determine closing rate to a neighboring object/vehicle				X							X
P1.13 Sense range to a neighboring object/vehicle				X							X
P1.12 Determine closing rate to a front object/vehicle				X							X
P1.11 Sense range to a frontal object/vehicle				X							X
P1.10 Sense pitch rate						X					X
P1.9 Sense roll rate						X					X
P1.8 Sense yaw rate						X					X
P1.7 Sense longitudinal acceleration						X					X
P1.6 Sense lateral acceleration						X					X
P1.5 Sense velocity					X					X	X
P1.2 Sense bearing			X								X
P1.1 Sense lateral displacement					X						X

Steering

The steering mechanization used in this paper is based upon a design used by Daimler-Benz in a guided bus system and in their channel tunnel service vehicle. It incorporates dual redundant steering actuators that operate independently of the manual steering components. Figure 12 depicts this system.

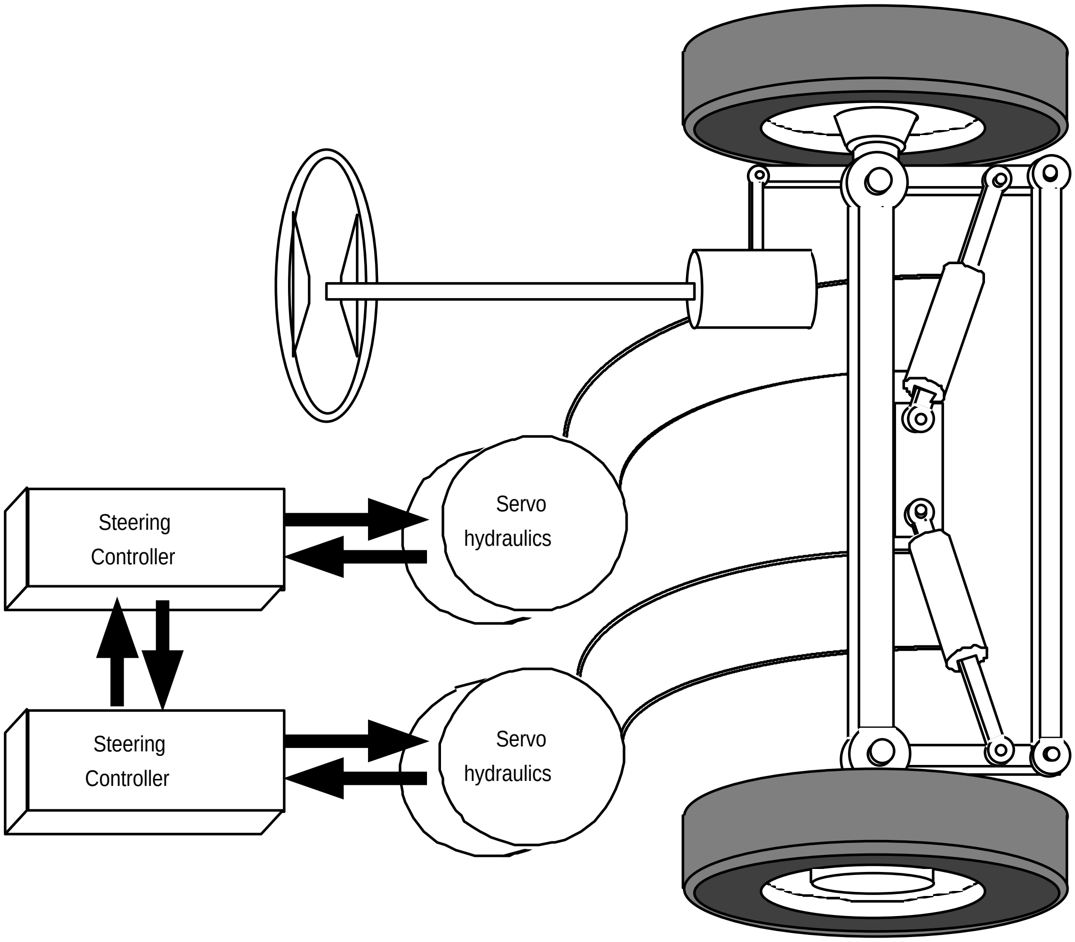


Figure 12. Conceptual Automatic Steering

STEERING MECHANIZATION I

Some modification of the Daimler-Benz concept is necessary in order to meet the requirements of an AHS. The mechanization diagram of Figure 13 depicts the steering subsystem showing elements for computer control and elements for switching out the manual components.

The manual system has been modified by the addition of sensing elements and a clutch for disengaging the hydraulic assist. The sensing elements allow for monitoring manual steering capability. In case of a failure, it may be desirable to have the vehicle driven to a safe repository under automatic control, rather than return faulty control to the driver. The steering wheel clutch serves to isolate the steering system from undesired human inputs during automated steering.

Each of the redundant automated steering assemblies contains independent hydraulic actuators and position sensors. Each actuator has a control valve, a bypass valve, a pump and a fluid reservoir. The control valve allows the actuation of the steering to be controlled by computer (not shown in this diagram.) The bypass valve allows the system to shut off automatic steering control, and allows the driver to resume control. A position sensor allows for a simple feedback loop around the steering command.

The existing axles, wheels, and tires have been used, with the modification of using run-flat tires. Since they are currently available for some vehicles, this seems a reasonable assumption.

FMEA FOR DUAL STEERING

The FMEA appearing in Table 2a was completed for the dual standby steering configuration. This process needs to be accomplished on all critical subsystems in order to assure a proper design and analysis has been completed. An example of the importance is the effects of various failures in the manual steering. While no safety effect is realized, the driver cannot take control, and an automated assignment of a repository is necessary.

Control valve A	**Steering system response to failure of the listed component.**	**Vehicle response to subsystem failure**
Notes: Nomenclature is based on figure 13, Dual Redundant Steering Mechanism.	Notes: After detection of the fault, in all cases system A is shut off and B is engaged.	Notes: Vehicle divergence following a fault will vary with the type of fault and monitor settings.
freeze (stuck on)	Actuator A moves towards a position limit at a constant rate until the failure monitor trips.	Vehicle diverges from the desired path. Correction takes place after system B is engaged.
hard open (full flow)	Actuator A moves towards a position limit at maximum rate until the failure monitor trips.	Vehicle diverges from the desired path. Correction takes place after system B is engaged.
stuck in no flow condition	Actuator A is held in current position until command to wheel position monitor detects fault.	Vehicle slowly diverges from desired path.
sticky (slow rate)	Actuator A moves slower than normal. Command to wheel position monitor will detect at set rate or lower.	Vehicle response sluggish, with greater than normal lateral errors
oscillatory	Actuator A oscillates about a bias point. Command to position monitor will detect above a set amplitude.	Vehicle will drift side to side with an error dependent upon the frequency and amplitude of the oscillation.
control bypass A		
freeze (stuck at)	Actuator A will move at a rate dependent on the bypass opening. Actuator will not disengage if a second failure occurs.	Vehicle response sluggish, with greater than normal lateral errors
hard open	Actuator will not disengage if a second failure occurs.	No effect
hard close	Actuator will not operate	Vehicle slowly diverges from desired path.
sticky (slow rate)	Fault amplitude will exceed normal value due to slow actuator shutoff.	Vehicle divergence will be greater than specified value.

oscillatory	Actuator will slow and speed up depending on amlitude and frequency of oscillation.	Vehicle tracking error will increase.
hydraulic actuator A		
stuck	wheels will be fixed until command to wheel position monitor detects fault.	Vehicle slowly diverges from desired path.
increased friction level	Wheels will move slowly. command to wheel position monitor will detect when rate falls below set value.	Vehicle response sluggish, with greater than normal lateral errors
hydraulic pump A		
high pressure	Increased wear, higher than normal actuator rates.	Vehicle lateral error will be greater than specified value.
low pressure	lower than normal actuator rates.	Vehicle divergence will be greater than specified value.
no pressure (belt lifetime)	no actuator movement. command to wheel position monitor will detect.	Vehicle slowly diverges from desired path.
oscillating pressure	Variable actuator rates	Vehicle lateral error will be greater than specified value.
hydraulic reservoir A		
insufficient fluid	actuator loses load holding capability, and/or stops. detected by command to position monitor, and lateral error monitor	Vehicle lateral error will increase.
contaminated fluid	auses valve failure in any of the ways specified under control valve A.	See control valve failures.
hydraulic pressure sensor A		
reads no pressure	system A will shut down due to pressure monitor.	no effect, assuming system B is functioning
drop out / dead zone	causes pressure reading to be outside acceptable range for a time greater than monitor will allow. system A will shut down.	no effect, assuming system B is functioning
bias	Will shut down system A if bias exceeds value allowed by monitor.	no effect, assuming system B is functioning
actuator A position sensor		
lost signal	actuator will extend or retract. Fault will be detected by command to wheel position monitor.	Vehicle diverges from the desired path. Correction takes place after system B is engaged.
max position	Actuator will attempt to extend fully. command to wheel position monitor will detect.	Vehicle diverges from the desired path. Correction takes place after system B is engaged.
min position	Actuator will attempt to retract fully. command to wheel position monitor will detect.	Vehicle diverges from the desired path. Correction takes place after system B is engaged.
bias	command will be issued with ofsetting bias. command to position monitor will detect when bias reches detection level.	no effect.
Hydraulic level sensor A		

stuck	stuck full or at acceptable level has no effect until fluid loss failure. stuck below acceptable level will shut down system A.	no effect.
no signal	System is shut down.	no effect.
electronics A		
no current	actuator does not respond to command. detected with command to position monitor.	Vehicle diverges from the desired path. Correction takes place after system B is engaged.
full current	actuator extends or retracts at full rate. detected with command to position monitor.	Vehicle diverges from the desired path. Correction takes place after system B is engaged.
bias	command will be issued with ofsetting bias. command to position monitor will detect when bias reches detection level.	no effect.
oscillate	Actuator A oscillates about a bias point. Command to position monitor will detect above a set amplitude.	Vehicle will drift side to side with an error dependent upon the frequency and amplitude of the oscillation.
steering clutch A		
slip	Manual steering will be ineffective	no effect in automatic mode.
frozen in	clutch B will decouple steering wheel	no effect.
frozen out	Manual steering impossible.	no effect in automatic mode. will not be able to give control to the driver upon leaving highway.
tie rod and other linkages		
physical break	total loss of control	vehicle diverges to barrier
wheel		
seize	Actuators sized to take this force level, steering remains effective.	vehicle brought to emergency stop
fall off	total loss of control	vehicle diverges to barrier
pressure sensor, assist pump		
reads no pressure	manual control warning. turnover to driver control impossible.	vehicle guided to depository at exit.
drop out / dead zone	manual control warning. turnover to driver control impossible.	vehicle guided to depository at exit.
bias	manual control warning if bias exceeds set level. turnover to driver control impossible.	vehicle guided to depository at exit.
hydraulic reservoir, manual		
insufficient fluid	Manual control ineffective. turn over to driver impossible.	vehicle guided to depository at exit.
contaminated fluid	no effect until secondary failure occurs.	no effect
hydraulic level sensor, manual		
stuck	no effect if stuck at acceptable level. manual control warning if not.	no effect unless manual warning given. vehicle guided to depository at exit.
no signal	manual control warning	no effect unless manual warning given. vehicle guided to depository at exit.
hydraulic pump, manual		
high pressure	detection monitor will trip if outside range. manual control warning will be issued.	vehicle guided to depository at exit.

low pressure	detection monitor will trip if outside range. manual control warning will be issued.	vehicle guided to depository at exit.
no pressure (belt lifetime)	detection monitor will trip if outside range. manual control warning will be issued.	vehicle guided to depository at exit.
oscillating pressure	detection monitor will trip if outside range. manual control warning will be issued.	vehicle guided to depository at exit.
hydraulic assist		
loss of fluid	Pressure sensor will detect. Manual control warning will be issued.	vehicle guided to depository at exit.
freeze in current position	Driver test prior to exiting highway will detect, and warning will be issued.	vehicle guided to depository at exit.
slow rate	Driver test prior to exiting highway will detect, and warning will be issued.	vehicle guided to depository at exit.
bias	driver test prior to exit will detect. unless bias is too big to compensate by driver, there is no effect on performance. otherwise, warning will be issued.	vehicle guided to depository at exit if warning issued. otherwise there is no effect.
power assist position sensor		
lost signal	manual warning issued	vehicle guided to depository at exit.
max position	manual warning issued	vehicle guided to depository at exit.
min position	manual warning issued	vehicle guided to depository at exit.
bias	manual warning issued	vehicle guided to depository at exit.

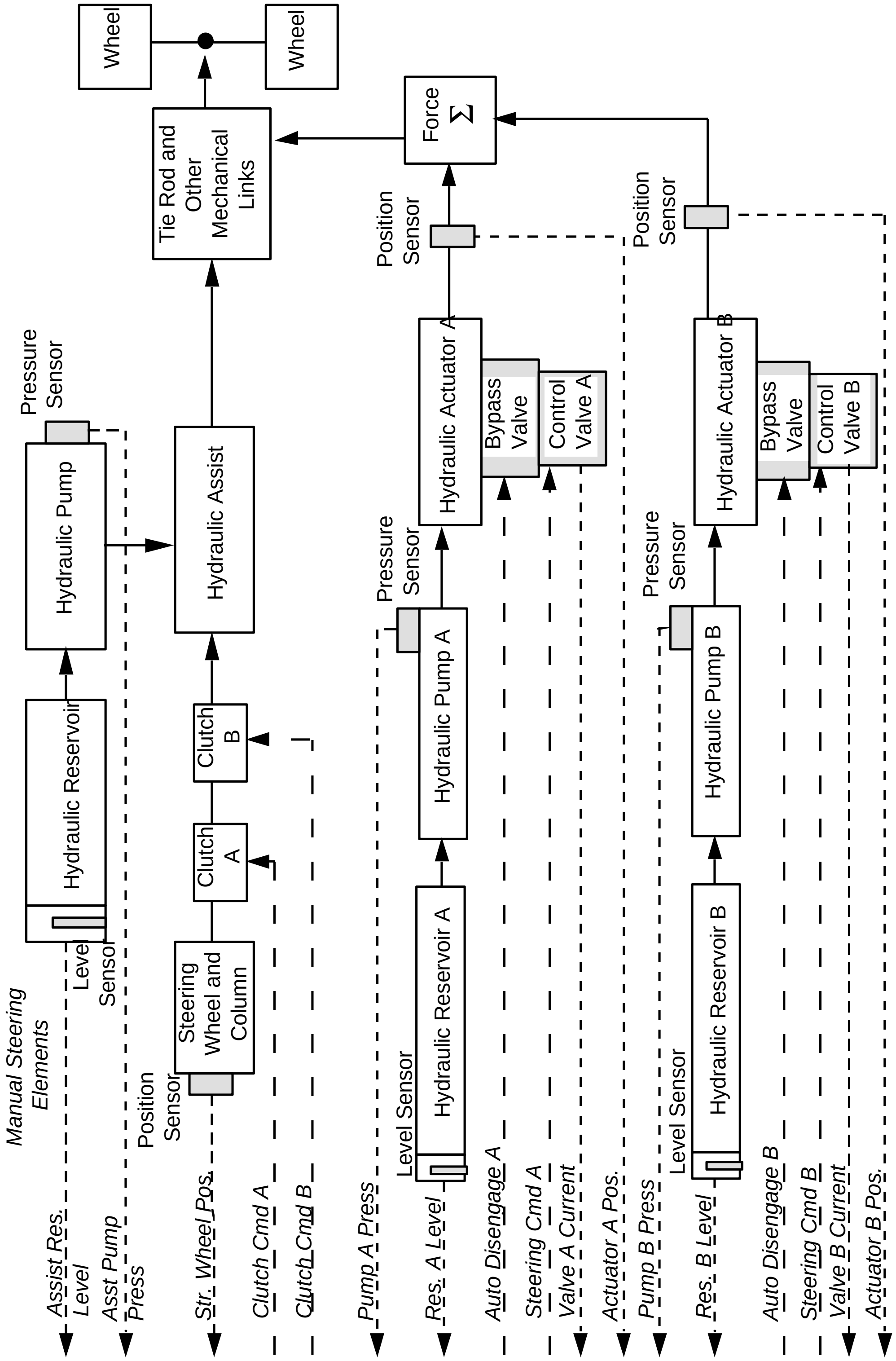


Figure 13 Dual Redundant Steering Mechanization

DUAL REDUNDANT STEERING PROBABILITY OF FAILURE CALCULATION

Each of the physical elements in the mechanization diagram has a probability of failure associated with it. For example, the probability of failure for the steering subsystem's hydraulic pump is designated by $\lambda_{\mathrm{strHPump}}$. The failure of any of the elements in the mechanization could result in the loss of a critical function. The steering subsystem probability of failure can by calculated by the following formula:

$$_{steer} = \sum_{i=1}^{n} {}_{i} \qquad (12)$$

The vehicle probability of failure is the sum of failure probabilities of the vehicles critical subsystems. The system probability of failure is the sum of the vehicle system's probability of failure and the roadside system's probability of failure. The overall AHS probability of failure must be less than the goal of 1 x 10^{-6}.

For the steering subsystem, reliability has been increased by adding redundancy. Note that some elements were not made redundant. For example, there are only two wheels for steering. If either one fails, then the steering function will be seriously impaired, if not lost altogether. However, it is unlikely that redundant axles/wheels will be added to most vehicles. For the elements that were duplicated, the failure rate for the pair is the square of the single failure rate because both independent devices must fail before the system will fail. This assumes 100% test coverage, meaning that the failure can always be detected. Figure 14 is a safety diagram showing how the failure probabilities of the standalone and redundant components are summed.

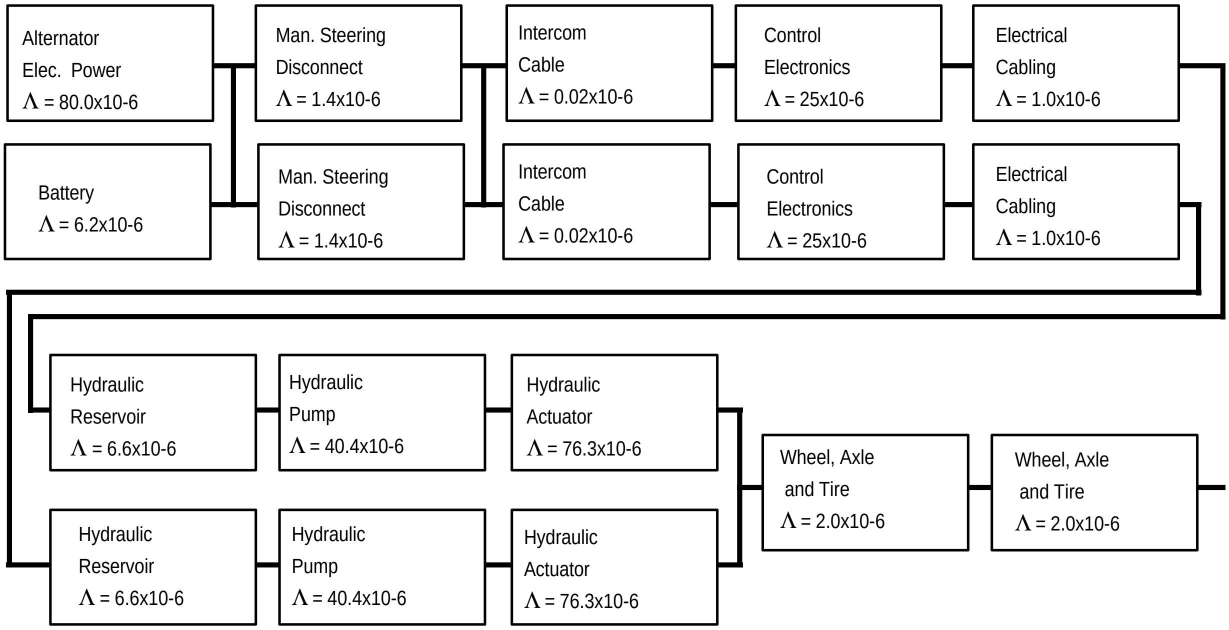


Figure 14. Dual Redundant Steering Safety Diagram

Before adding any other components, it was apparent that the probability of failure for a single wheel, axle, and tire combination would exceed the budget for the entire AHS. A major contributor to this is the tire. The reliability data that was obtained included vehicles with bald tires, improper inflation, or regular maintenance of the axles and wheels. The failure rate used for the wheel, axle, and tire does not reflect the use of run-flat tires, or improved wheels and axles. Improvements like these will be necessary in order to meet our system reliability. This will, of course, increase the cost of the system.

For this analysis, the wheel, axle, and tire failure rate is not included. It is assumed that the reliability will be high enough to allow for this omission. Run-flat tires support this assumption since they act as a dual redundant system with perfect coverage.

The Probability of failure for the steering system was calculated for both 100% and 95% test coverage. The 95% coverage number was selected as representative of multiple string systems currently in use. Figure 15 shows the plots of probability of failure versus time in hours for the two cases.

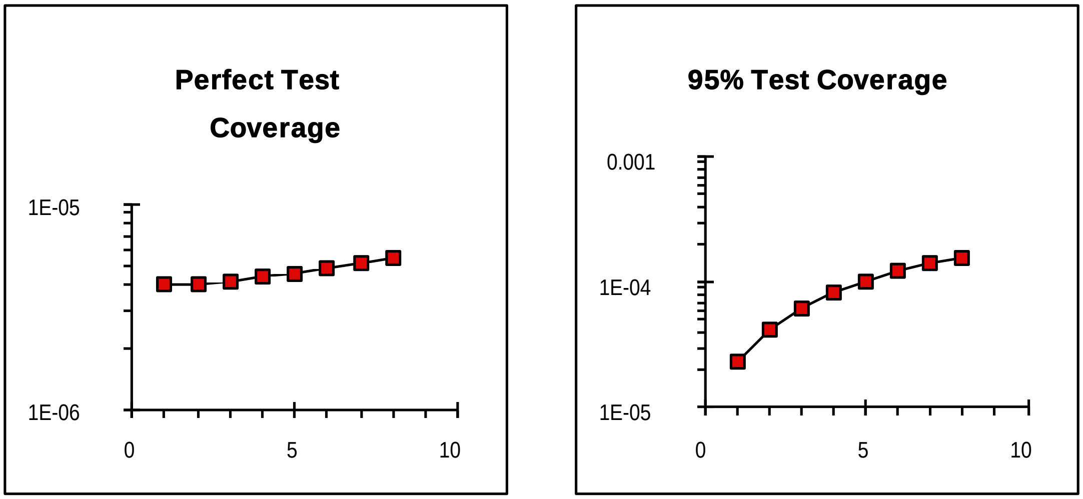


Figure 15. Dual Redundant Steering: Probability of Failure vs. Time (hrs)

Even allowing for perfect test coverage, the failure probability of the dual-redundant steering system is way too high.

STEERING MECHANIZATION II

Adding redundancy greatly reduces the probability of failure since it has a multiplicative effect on reliability rather than an additive one. Figure 16 shows the steering system with triply redundant actuation. The power supply and steering wheel clutch remain dual redundant.

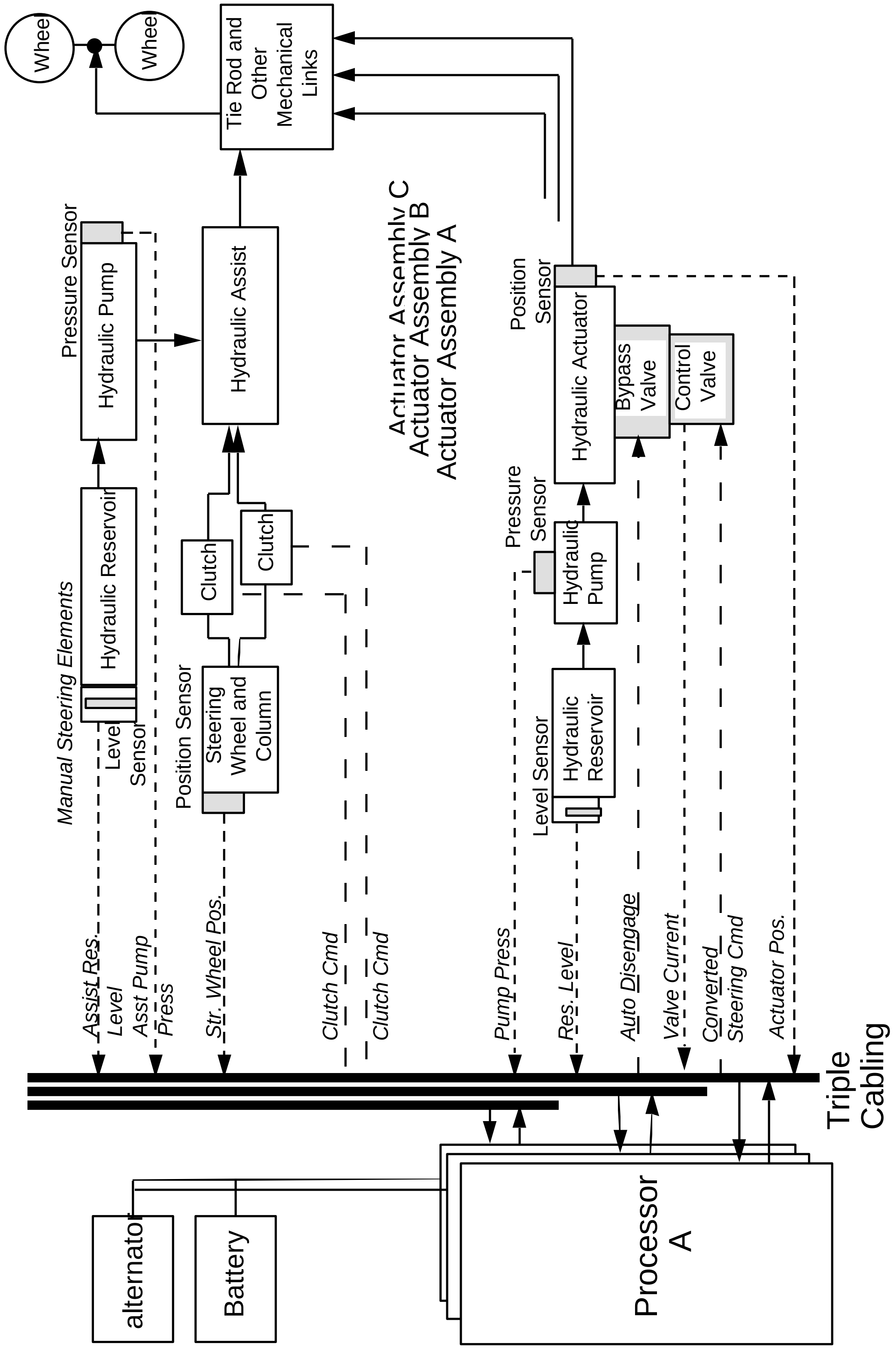


Figure 16. Partial Triple Redundant Mechanization

PROBABILITY OF FAILURE CALCULATION

Figure 17 shows the safety diagram for the partial triple redundant steering system. As before, the wheels are shown in the diagram, but these failure rates will not be incorporated.

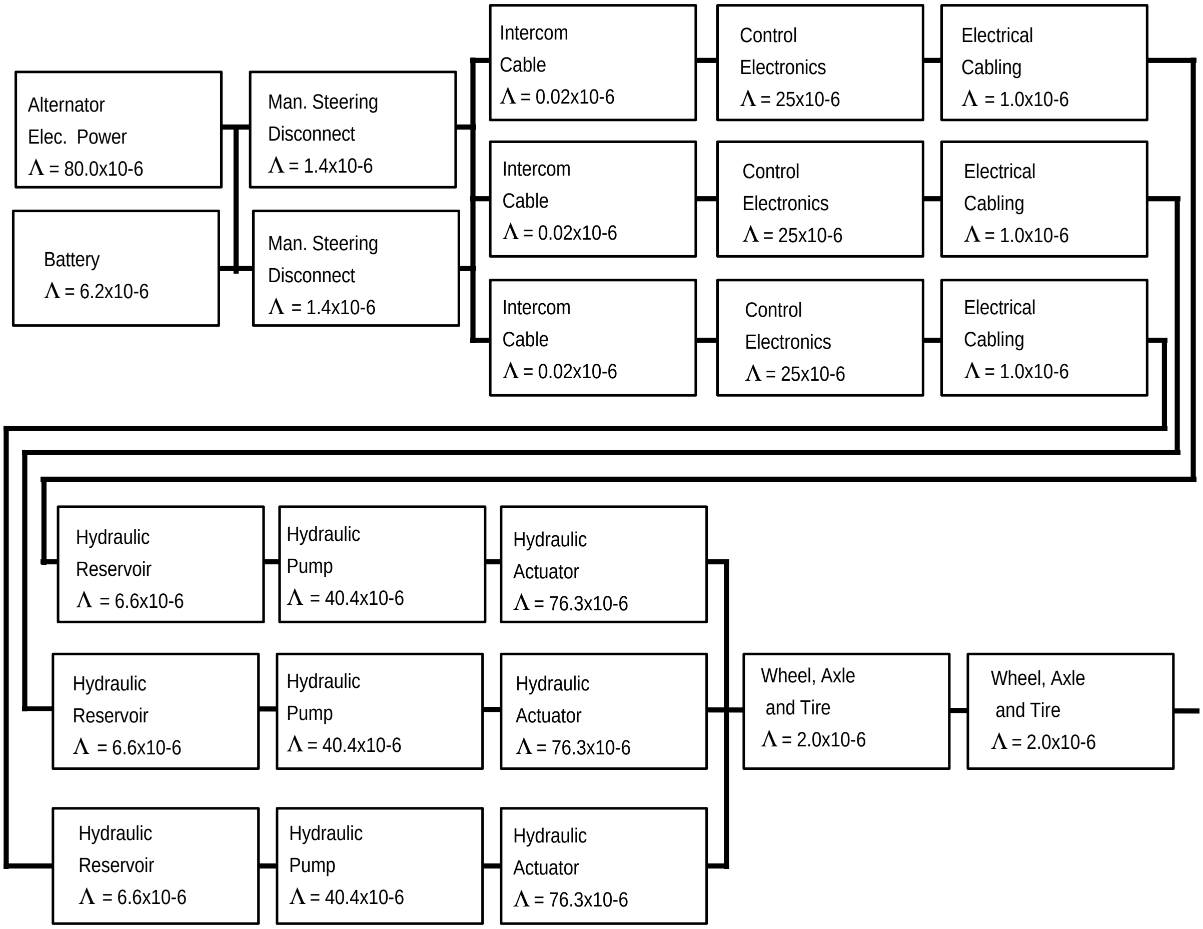


Figure 17. Partial Triple Redundant Steering Safety Diagram

When considering only the 100% test coverage case (figure 18), this system now seems to be acceptable. However, The importance of looking at coverage is revealed when the 95% case is studied. Steering system probability of failure is still high.

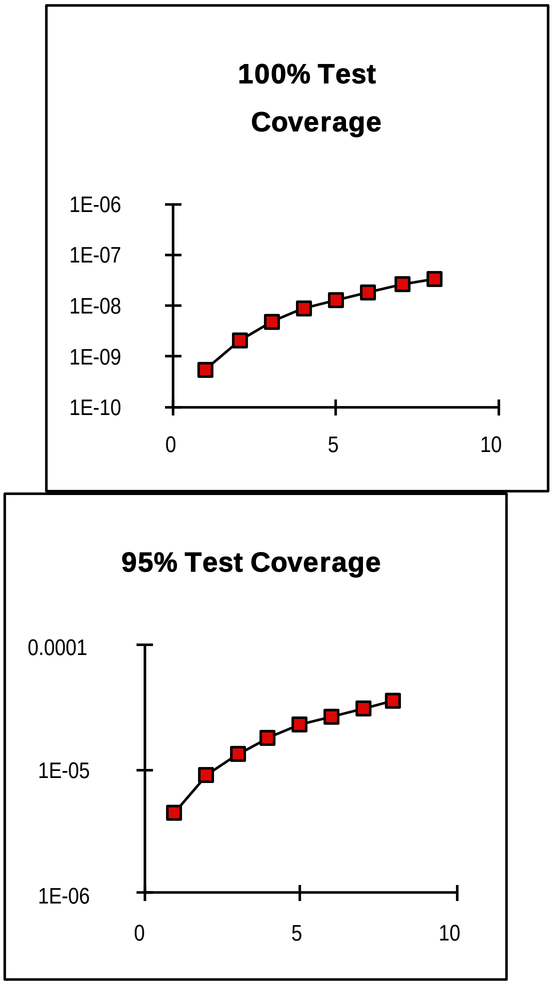


Figure 18. Partial Triple Redundant Steering: Probability of Failure vs. Time (hrs)

MECHANIZATION III

In order to improve reliability, full triple redundancy is investigated, now including the power supply and the steering wheel clutches, as shown in figure 19.

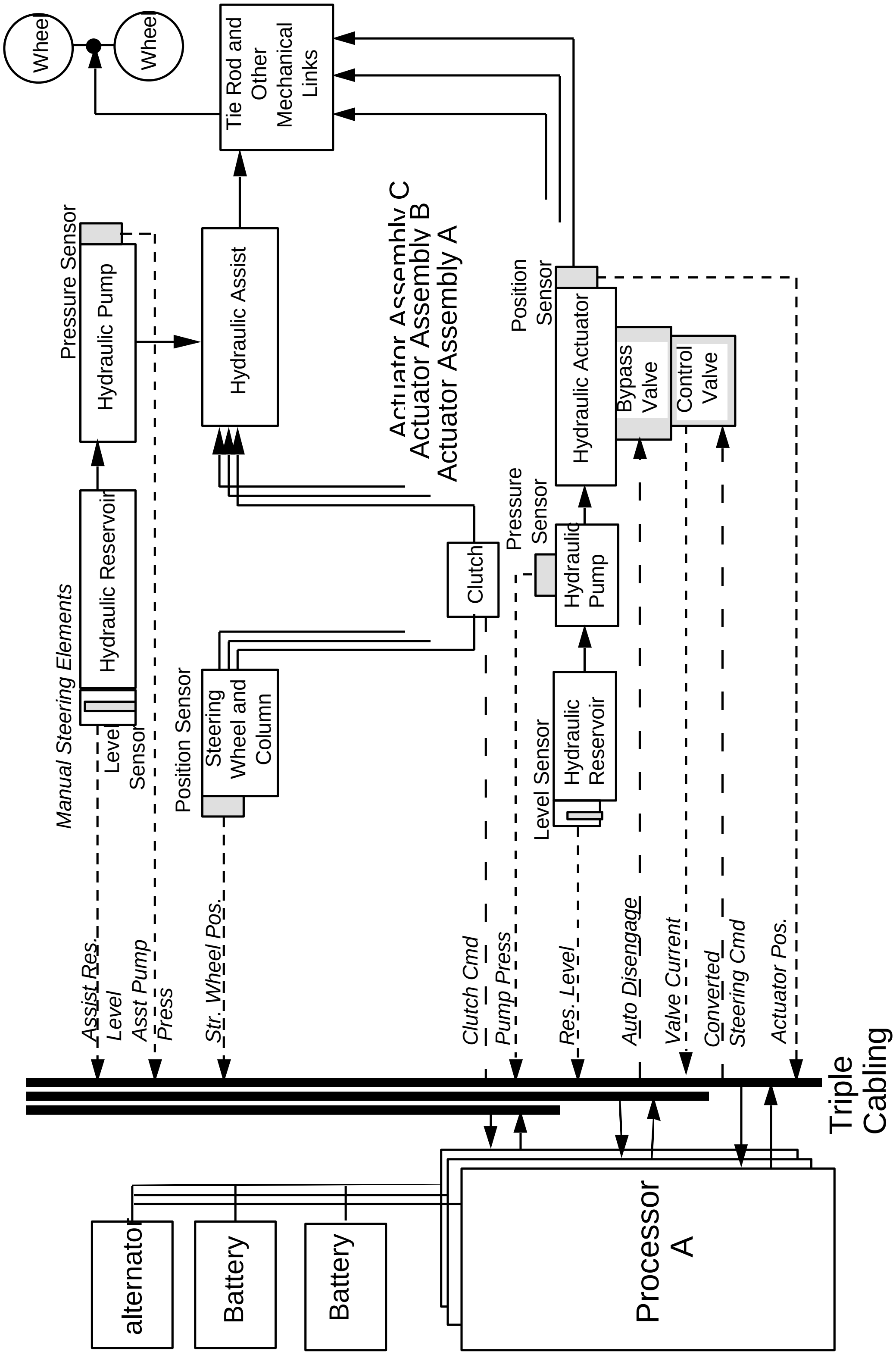


Figure 19. Triple Redundant Steering

PROBABILITY OF FAILURE CALCULATION

Figure 20 shows the safety diagram for the full triply redundant steering system. The failure probability for wheels, axles, and tires are omitted, as in the previous examples.

The manual steering disconnect is only critical due to the fact that it allows for the possibility of the driver introducing random, interfering forces to the steering control system. A failure in the disconnect will not cause a steering failure in and of itself.

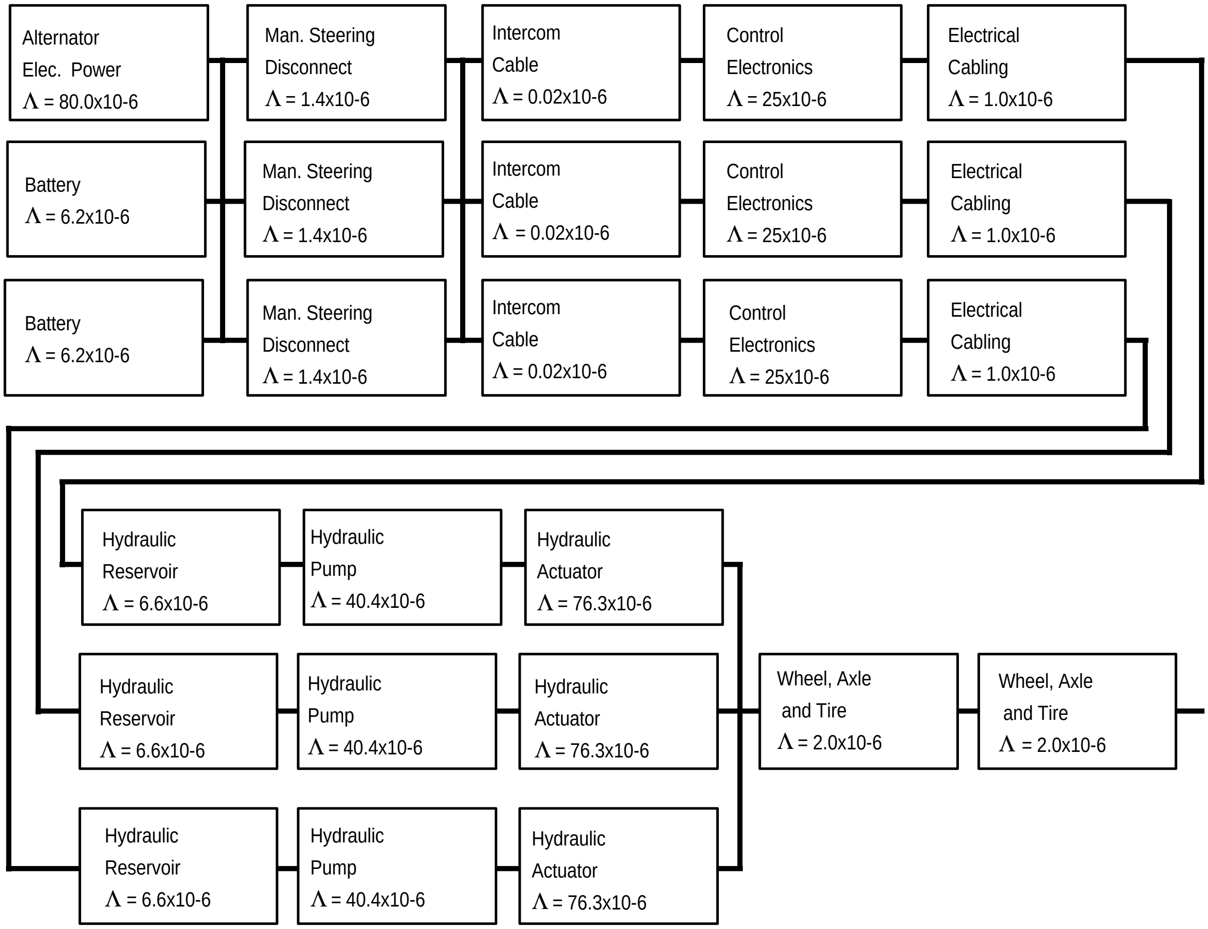
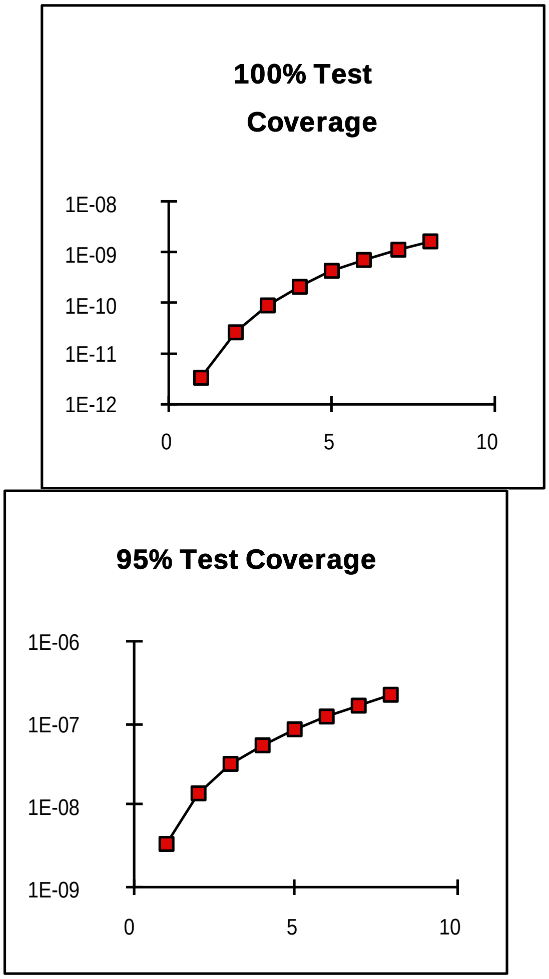


Figure 20. Full Triple Redundant Steering Safety Diagram



100% Test Coverage

95% Test Coverage

Figure 21. Full Triple Redundant Steering: Probability of Failure vs. Time (hrs)

Figure 21 shows the increasing probability of failure with time, for the steering system. For the time period shown, it falls below the limits set by our reliability budget. If additional improvements are found to be necessary, it may be easier and cheaper to improve the reliability of individual components or improve test coverage rather than adding additional redundancy.

MONITORING AND TESTING

Adding extra visibility into the system allows testing of the system in operation. For example, if the hydraulic reservoir (λ = 6.6 x 10^{-6}) is examined 100 times per hour, the exposure of that component to latent or simultaneous faults is actually 6.6 x 10^{-6} / 100 = 6.6 x 10^{-8}.

Extra monitor points also allow better fault detection, isolation and recovery. The steering mechanization includes monitors to test the level of hydraulic fluid in the hydraulic reservoirs, the pressure that is generated by the hydraulic pumps, the position of the actuators, and the electric current used to position the control valves.

In order to determine which tests to carry out, each component is analyzed to determine failure modes. This is then compared to what is known about the system, both from the control system (i.e. what is commanded) and from the output of sensors. If a failure mode cannot be detected by analyzing the sensor data, it may indicate a need for additional sensors. Table 3 lists the failure modes for the components of the steering subsystem.

Table 3. Failure Modes Table

control valve A, B, C freeze (stuck) hard open hard close sticky (slow rate) oscillatory	hydraulic pump, manual high pressure low pressure no pressure (belt lifetime) oscillating pressure
control bypass A, B, C freeze (stuck) hard open hard close sticky (slow rate) oscillatory	hydraulic assist actuator loss of fluid freeze in current position slow rate bias
hydraulic actuator A, B, C stuck increased friction level	steering wheel and column frozen broken link
hydraulic pump A, B, C high pressure low pressure no pressure (belt lifetime) oscillating pressure	hydraulic assist position sensor lost signal max position min position bias
hydraulic reservoir A, B, C insufficient fluid contaminated fluid	wheel seize fall off
hydraulic pressure sensor A, B, C reads no pressure drop out, dead zone bias	manual steering pump clutch slip frozen engaged frozen disengaged
actuator position sensor A, B, C lost signal max position min position bias	assist pump pressure sensor read no pressure drop out, dead zone bias
hydraulic level sensor A, B, C stuck no signal	hydraulic level sensor, manual stuck no signal
electronics A, B, C no current full current (short?) bias oscillate	hydraulic reservoir, manual insufficient fluid contaminated fluid
manual disconnect A, B, C hard open hard close	tie rod and other linkages physical break

The following commands and sensor outputs are monitored:

Table 4. Steering System Monitoring

disengage manual steering command	wheel/actuator position A, B, C
auto control disengage	valve current signal A, B, C
pump pressure A, B, C	pump pressure, manual
reservoir level A, B, C	reservoir level, manual
steering command A, B, C	hydraulic assist position

Relationships may exist between different signals. Figure 22 shows a technique of combining the steering command, the sensed wheel position and the sensed control valve current. In normal operation the resulting value should fall within a tolerance band. Periodically, the resulting value is inspected to see if it is within tolerance. If it is out of tolerance, a defect counter is incremented. If the defect counter is 1, a failure has been detected, and the steering command is by-passed. If the result was within tolerance, the defect counter is decremented, and the by-pass is disabled. False alarms can be reduced by increasing the tolerance band or by changing the strike count logic to allow, e.g., three bad values before by-passing the control.

The monitor of figure 22 effectively tests the hydraulic pump, the tie rod, the position sensor, the control valve and the by-pass valve, as well as the inner feedback loop. Depending on the frequency of this monitor, the effective subsystem probability of failure can be reduced.

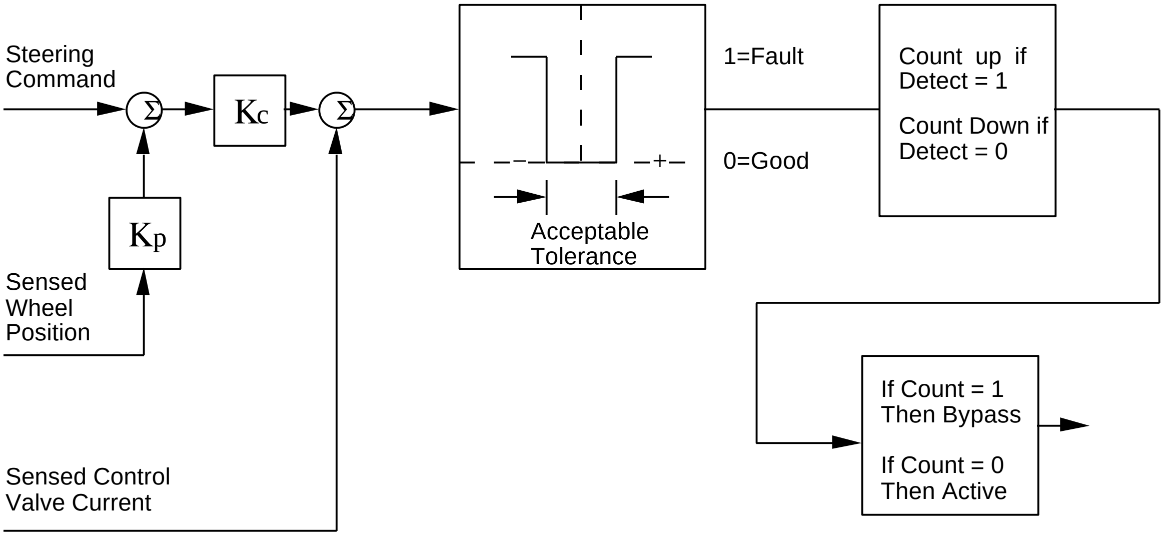


Figure 22. A Steering Channel Monitor

Braking

MECHANIZATION I

The braking mechanization was developed by modifying a commercially available anti-lock braking system (ABS) to allow computer activation. The ABS already incorporates control valves at each wheel cylinder and a hydraulic pump. It also follows the standard practice of dividing the hydraulic circuit into two independent sections so that a brake line failure could only remove braking power from two of the wheels. Some control valves were added to allow for fully automatic control. The mechanization diagram of figure 23 depicts the braking subsystem showing elements for computer control and elements for switching out the manual components.

During manual operation, the brakes act as a standard ABS, with the vacuum boosted pedal as the source of fluid pressure. The wheel cylinder solenoids regulate the pressure in the wheel cylinder to prevent the brakes from locking up. Lock-up is determined by the wheel speed sensor.

Under automatic control, master cylinder motion is prevented by a locking mechanism. This prevents the driver from interfering with the automation. Fluid pressure is obtained from the dual accumulators by opening solenoid valves. Pressure is maintained in the accumulators by two independent hydraulic pumps. The accumulators also serve as an emergency reserve of hydraulic power for the brakes, in the event the pumps lose power. Each of the two independent brake circuits has its own fluid reservoir, to insure that a failure in one line won't drain the entire system. As with the steering subsystem, the existing axles, wheels, and tires have been used, with the modification of using run-flat tires.

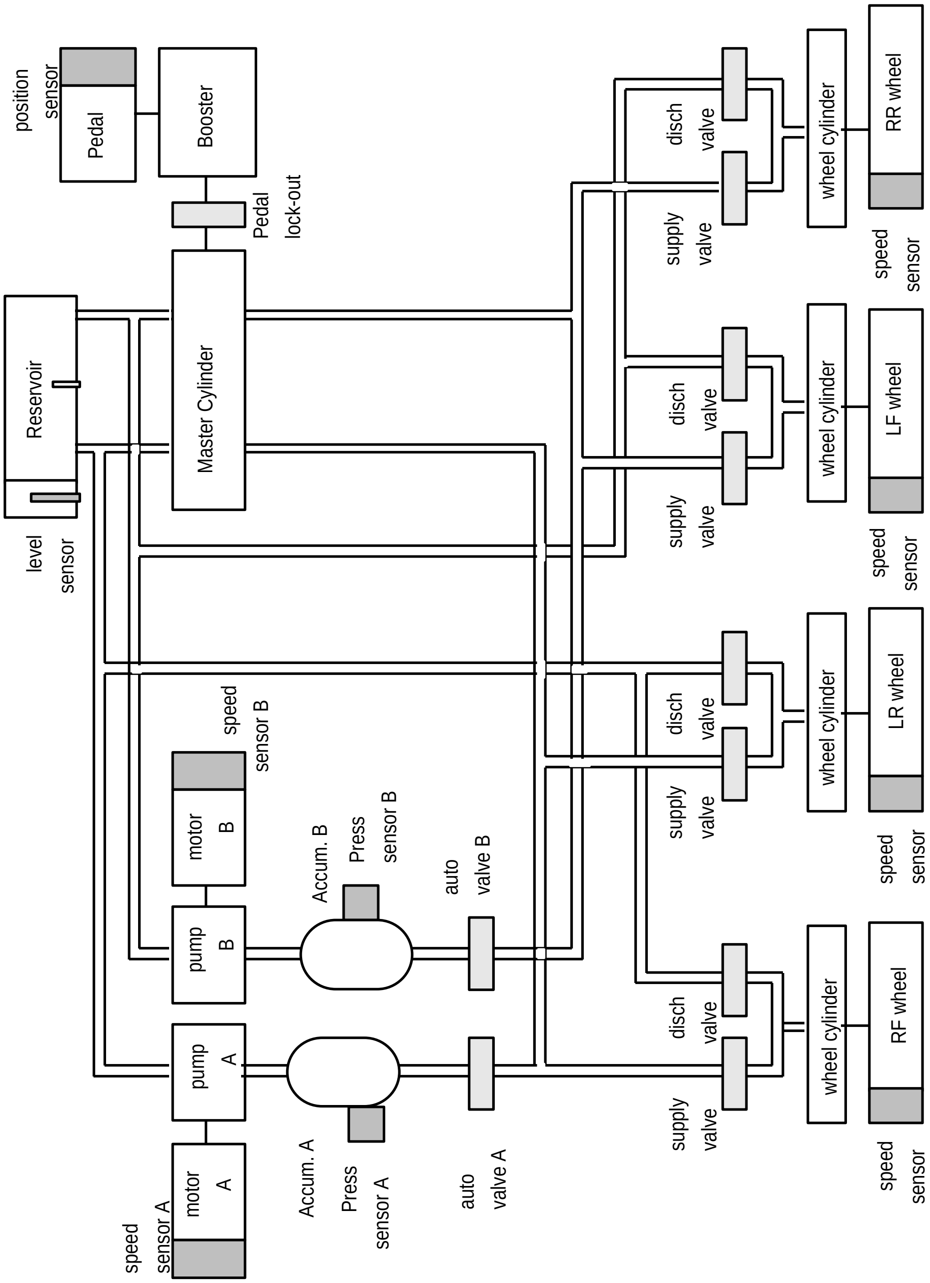


Figure 23 Dual Redundant Brake Mechanization

PROBABILITY OF FAILURE CALCULATION

Figure 24 shows the safety diagram for the dual redundant braking system. With regards to the wheels, it is assumed that some braking ability will remain even in the event of losing one of the wheels in a braking circuit. That is why the wheels are shown as redundant. This may be overly optimistic for a real world situation.

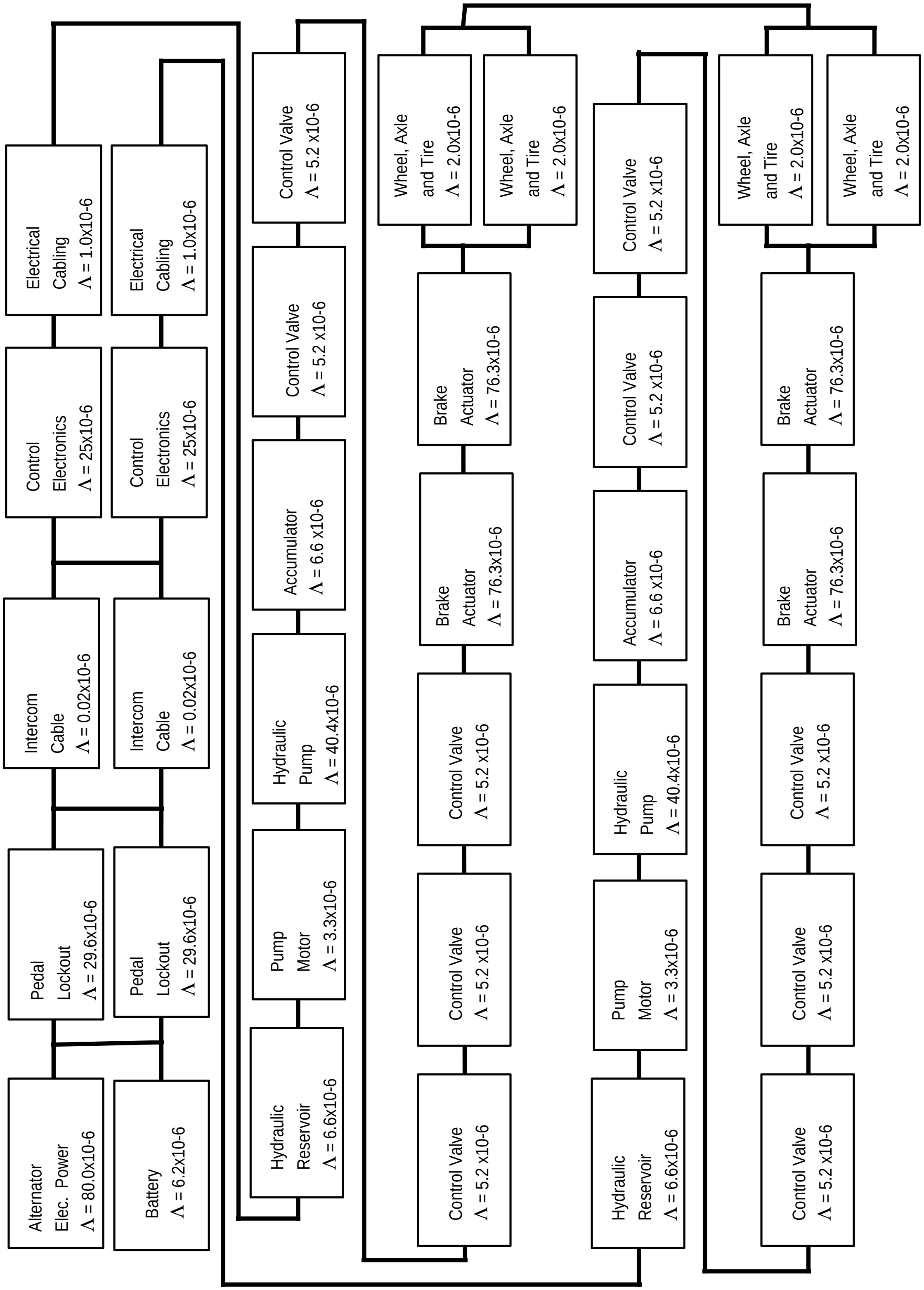


Figure 24. Dual Redundant Braking Safety Diagram

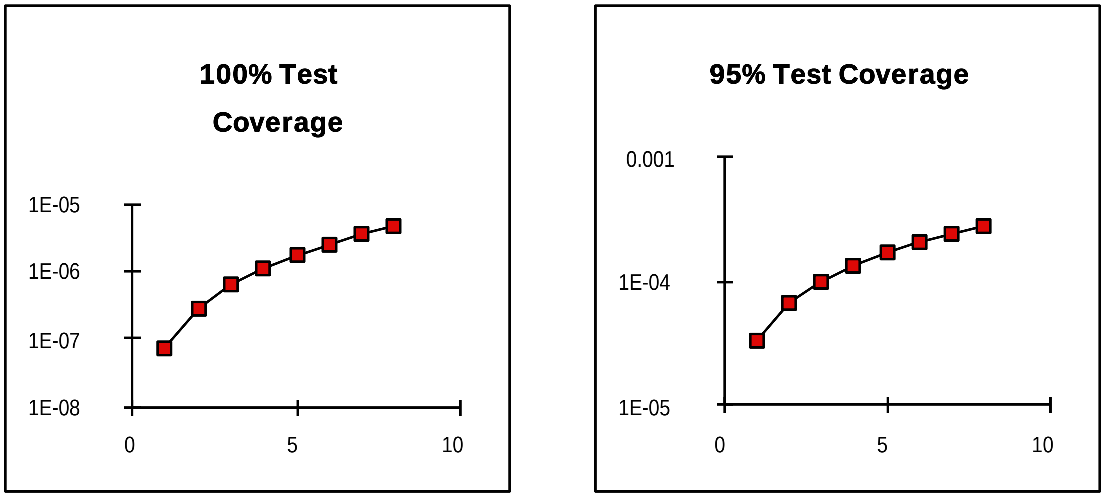


Figure 25. Dual Redundant Brake Probability of Failure vs. Time (hrs)

Figure 25 shows the effects of time and coverage on the probability of failure for the braking system. As with the steering subsystem, dual-redundancy is not sufficient to meet our goals.

MECHANIZATION II

Figure 26 shows a triple redundant braking system, with individual actuators for each wheel.

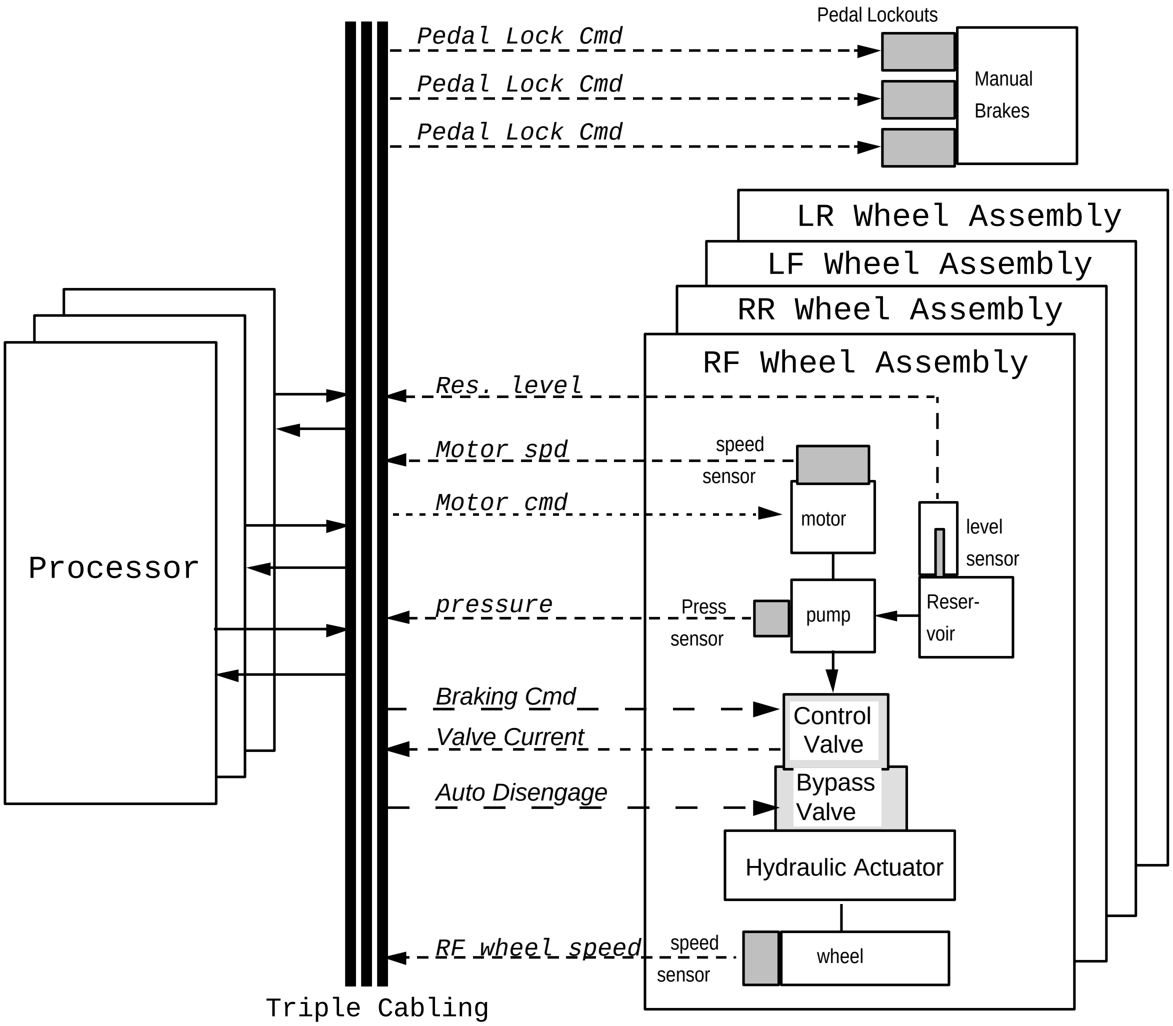


Figure 26. Multi-string Brake Mechanization

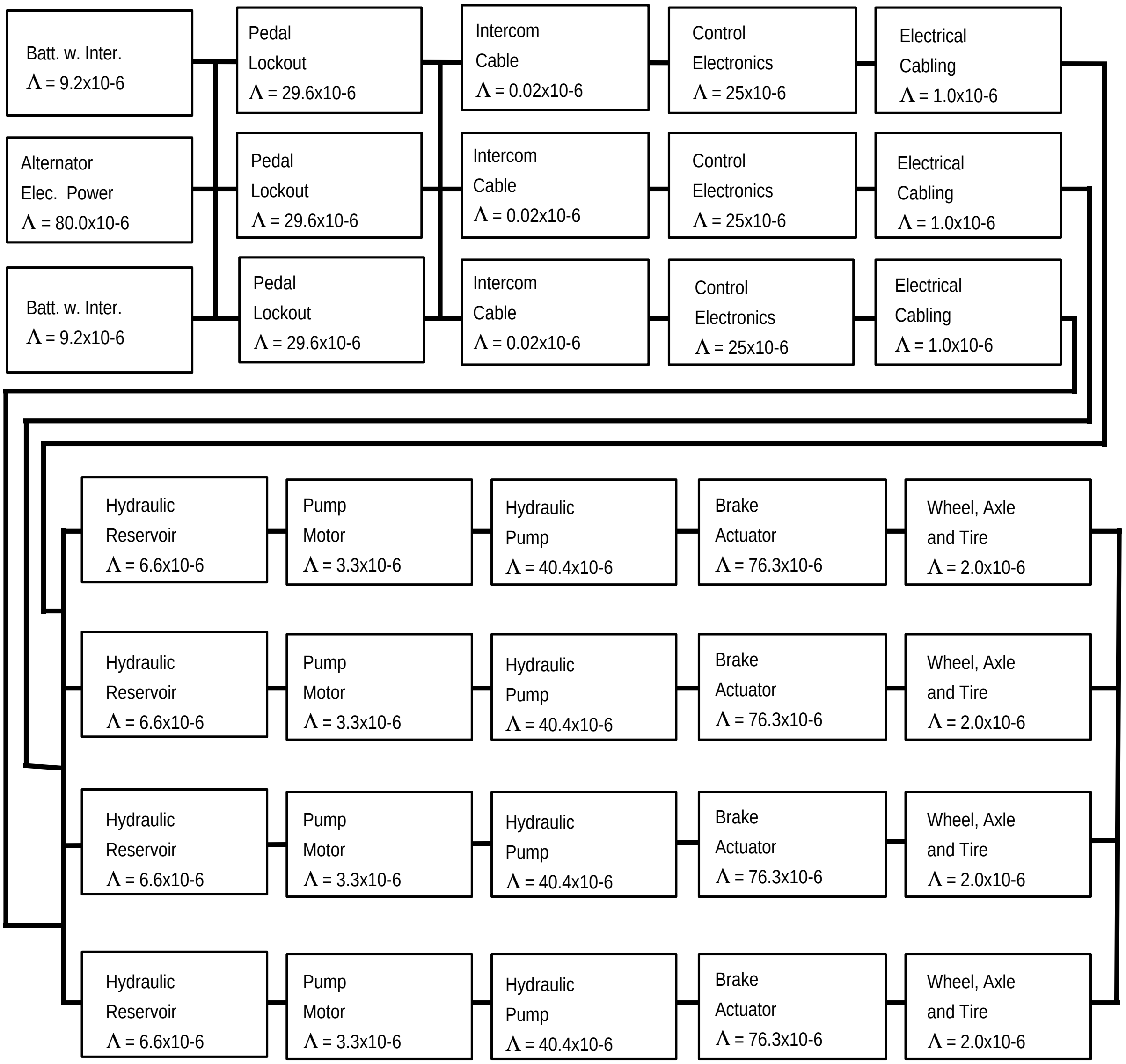


Figure 27. Multi-string Brake Safety Diagram

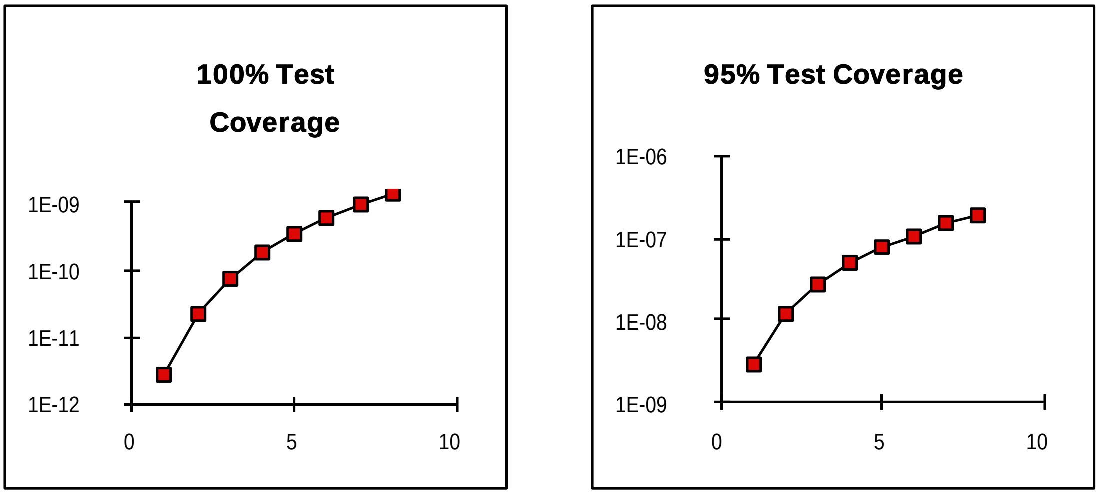


Figure 28. Multi-string Brake Probability of Failure vs. Time (hrs)

MONITORING AND TESTING

The standard ABS incorporates wheel speed sensors for control, and a pedal position sensor for maintaining pedal height. This mechanization adds a pressure sensor to each fluid circuit, speed sensors to the pump motors, and reservoir level sensors. In addition to the sensor data, the computer generated commands are known for each solenoid valve in the system.

Table 5 shows the failure modes associated with each component in the braking system.

Table 5. Braking System Component Failure Modes

pedal position sensor lost signal max position min position bias	wheel speed sensor A, B, C, D loss of signal	reservoir A, B, C, D insufficient fluid contaminated fluid
pump A, B, C, D high pressure low pressure no pressure (belt lifetime) oscillating pressure	pressure sensor A, B, C, D reads no pressure drop out / dead zone bias	motor A, B, C, D short bearing failure
pedal lock-out A, B, C stuck on stuck off	pedal frozen broken link	booster vacuum leak
master cylinder fluid leak air in lines Fading (bad piston seal)	wheel cylinder A, B, C, D stuck increased friction level	level sensor A, B, C, D stuck no signal
control valve A, B, C, D freeze (stuck at) hard open hard close sticky (slow rate) oscillatory	bypass valve A, B, C, D freeze (stuck at) hard open hard close sticky (slow rate) oscillatory	wheel A, B, C, D seize fall off
motor A, B, C, D speed sensor loss of signal		

The following commands and sensor outputs are monitored:

Table 6. Brake System Monitoring Table

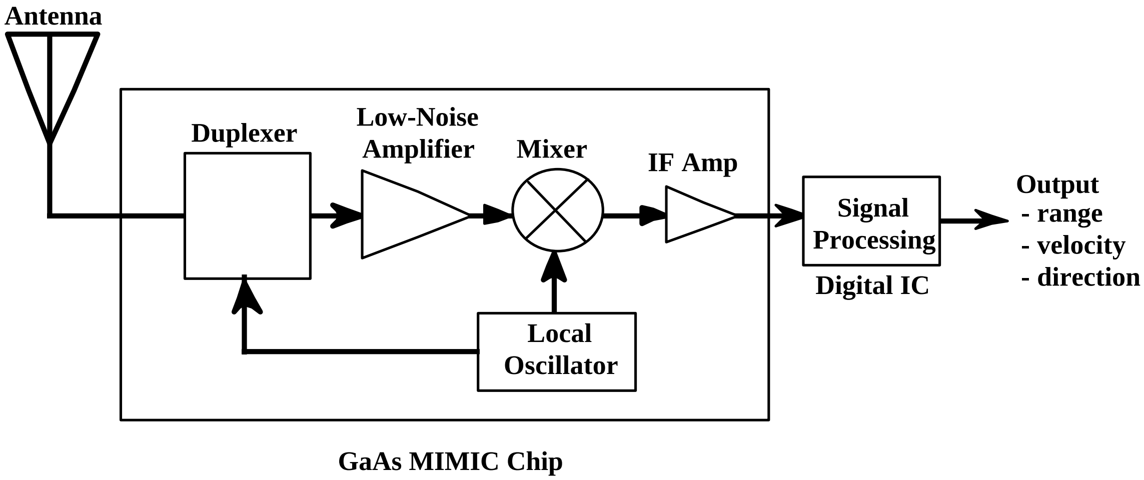
pedal position	wheel speed A, B, C, D
pedal lock-out command	pressure A, B, C, D
reservoir level A, B, C, D	control valve A, B, C, D command
motor speed A, B, C, D	bypass valve A, B, C, D command
motor command A, B, C, D	

Sensors: Object Detection, Lateral Position/Roadway Data, Gyros and Accelerometers

MECHANIZATION

OBJECT DETECTION

The object detection system serves two purposes, determining the gap to the next vehicle and sensing obstacles either in the path of the vehicle or on an intersecting course. Radar has been chosen as a representative workable system. This may be an expensive option, but the technology exists. Mass production will ameliorate this problem to some extent. Figure 29 shows the components in a gallium arsenide based radar. This technology allows for a very small package size.



MIMIC: Microwave & Millimeter Monolithic Integrated Circuit
Antenna: Planar Microstrip Switched Array

Figure 29. Object Detection Mechanization

Multiple beams will be necessary for both headway maintenance and obstacle detection. This can be accomplished by either having multiple, individual radars, or by having multiple antennas feeding a central box. It has not yet been determined which is the better option, in terms of both reliability and cost. Figure 30 shows a possible beam configuration. Three forward looking beams are used for gap determination so that a leading vehicle will not be lost as the road curves. Sideways looking beams insure that the vehicle will not maneuver into an obstacle during a lane change. The diagonal rear-facing beams provide coverage against closing vehicles during a lane change. In effect, they watch the blind spot. The rearward facing beam provides warning of vehicles closing from the rear.

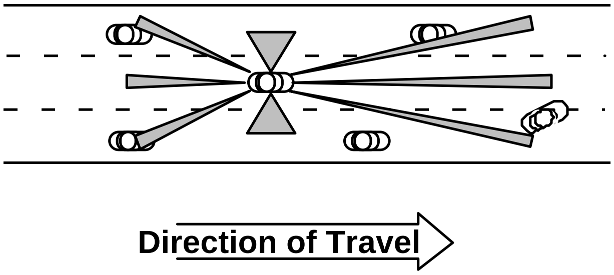
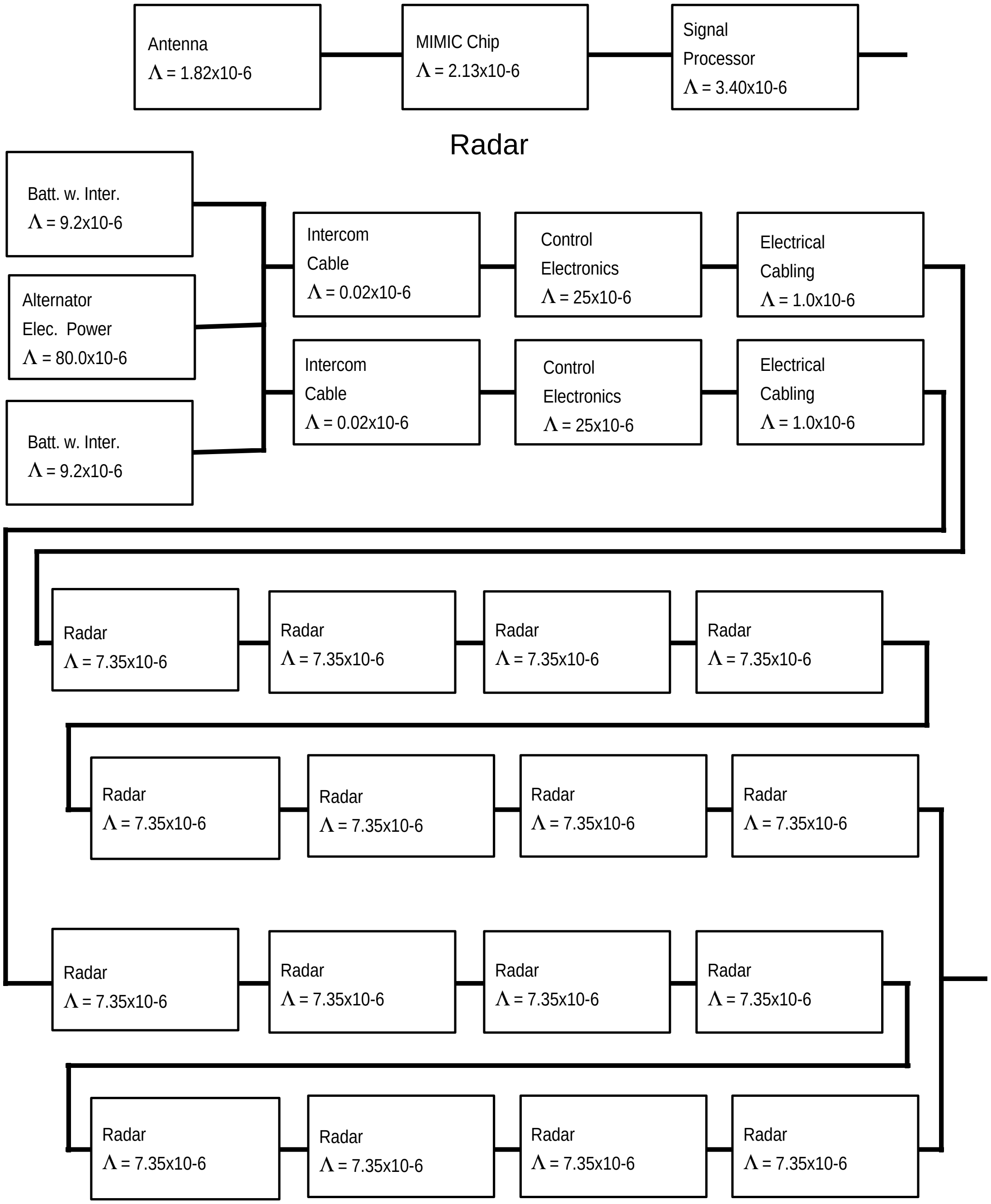


Figure 30. Object Detection Coverage

PROBABILITY OF FAILURE CALCULATION

In an effort to keep costs down, a dual redundant object detection system was proposed. Figures 31 and 32 show the safety diagram and failure probability with time for this system. Not unexpectedly, failures probabilities are too high. Figures 33 and 34 show the safety diagram and failure plots for a triple redundant system. This appears to have acceptable performance. As mentioned before, some cost reduction may be possible by attaching multiple antennas to each processing chip.



Radar

Radar Assembly

Figure 31. Dual Object Detection Safety Diagram

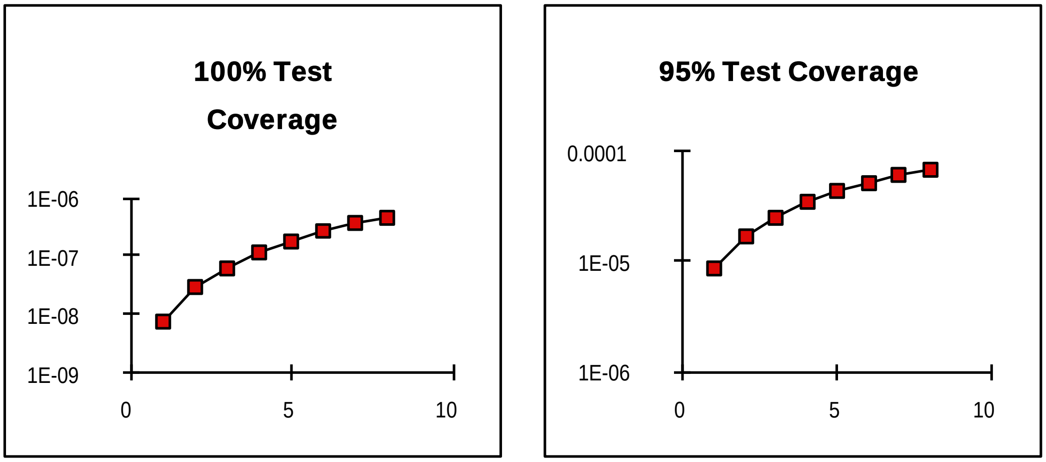


Figure 32. Dual Object Detection Probability of Failure vs. Time (hrs)

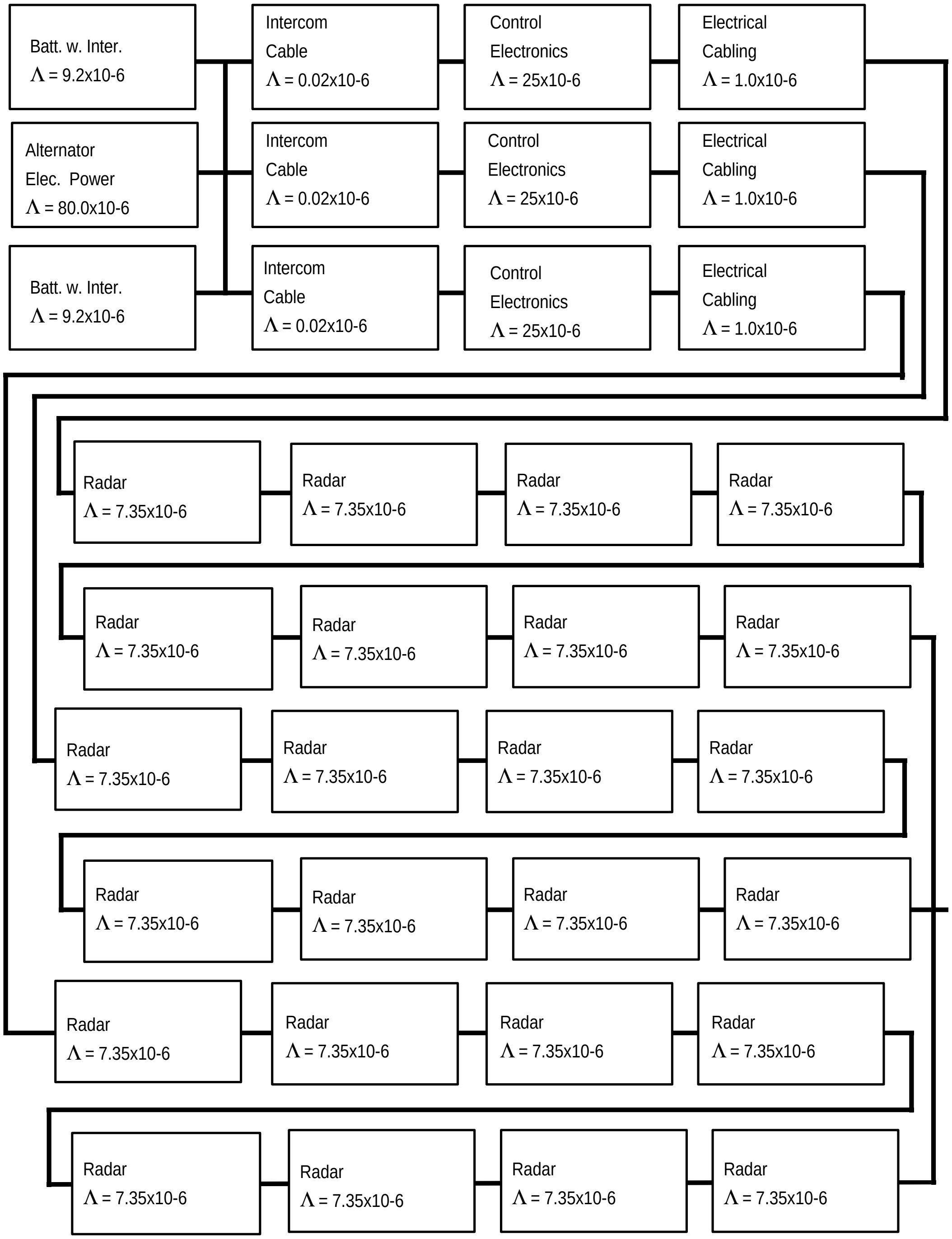


Figure 33. Triple Object Detection Safety Diagram

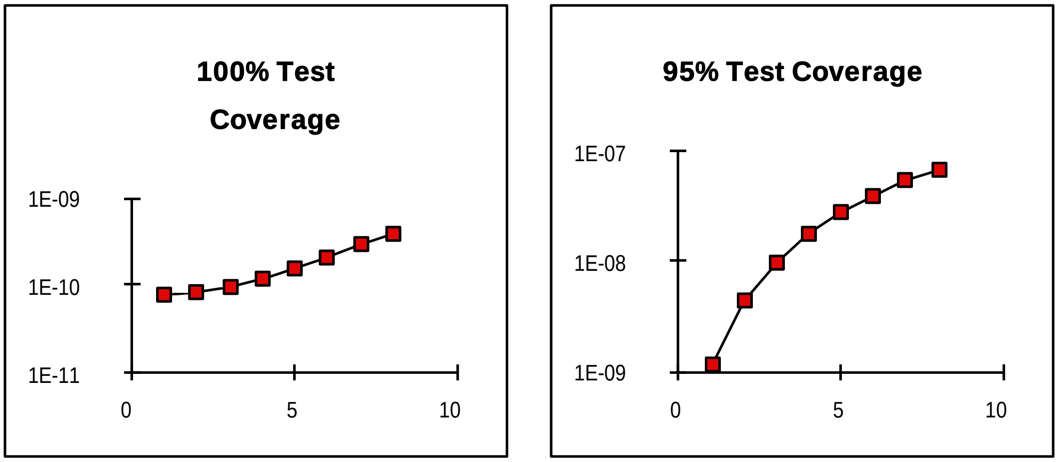


Figure 34. Triple Object Detection Probability of Failure vs. Time (hrs)

LATERAL POSITION

Magnetic path following was selected for lateral position/lane following mechanization. It has been demonstrated in the Berkeley PATH program and other ongoing research projects. Figure 35 shows two sensors for reading position. Depending on the range of the sensors and the design of the roadway markers, the sensors may be mounted along the front bumper or in line on the axis of the vehicle.

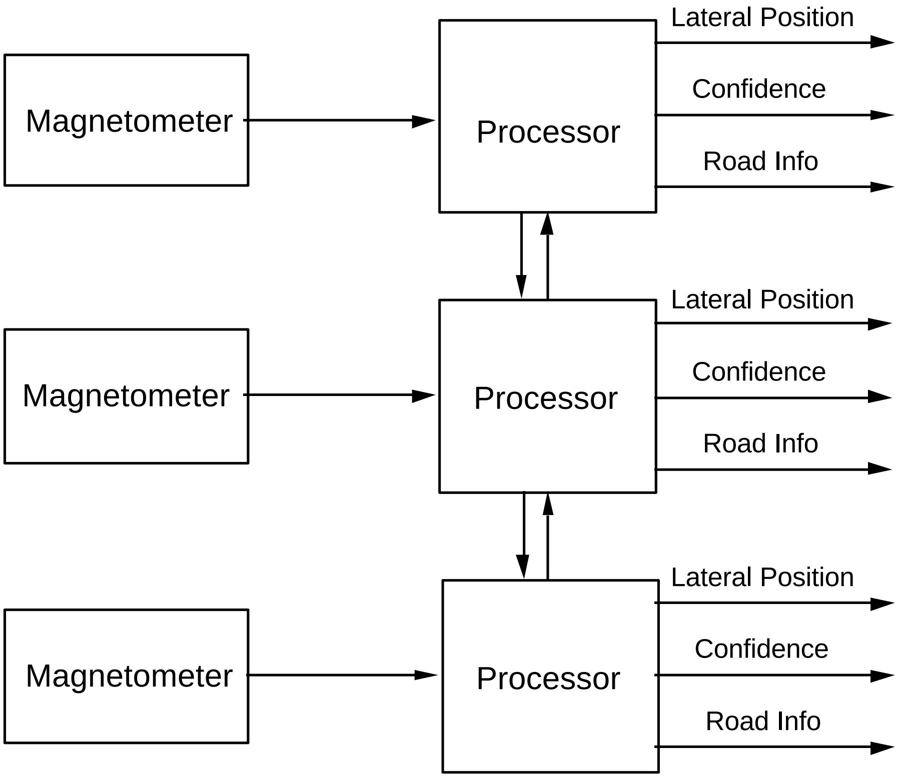


Figure 35. Lateral Position Mechanization

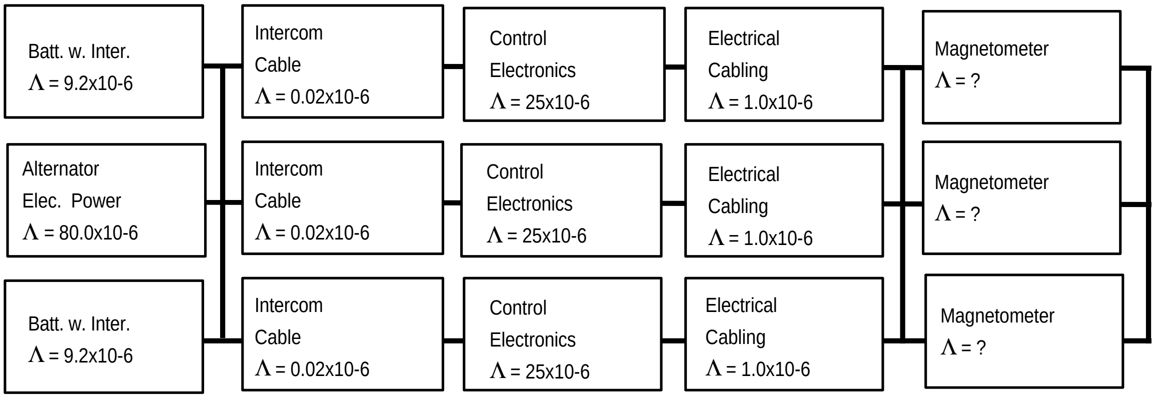


Figure 36. Lateral Position Safety Diagram

As can be seen in figure 36, reliability data for the magnetometers could not be found. Triple redundancy was assumed sufficient for our purposes, having worked for other subsystems. A triple power supply and triple processing were shown since they are already required to support other subsystems.

GYROS AND ACCELEROMETERS

Gyros for angular rate information and accelerometers for a vehicle accelerations are important for precise steering control and to monitor vehicle performance for insuring ride quality. They are also useful for monitoring the health of other systems. Early tests of steering failures indicate that acceleration data may be necessary for timely detections. Loss of these sensors will not result in an immediate crash. However, they will force the vehicle to move in a degraded manner to insure that steering failures can be detected in time to manage the malfunction. Allocation of criticality for these sensors is very dependent upon the control design for the vehicle. A simple mechanization is included here, but a full safety analysis was not carried out.

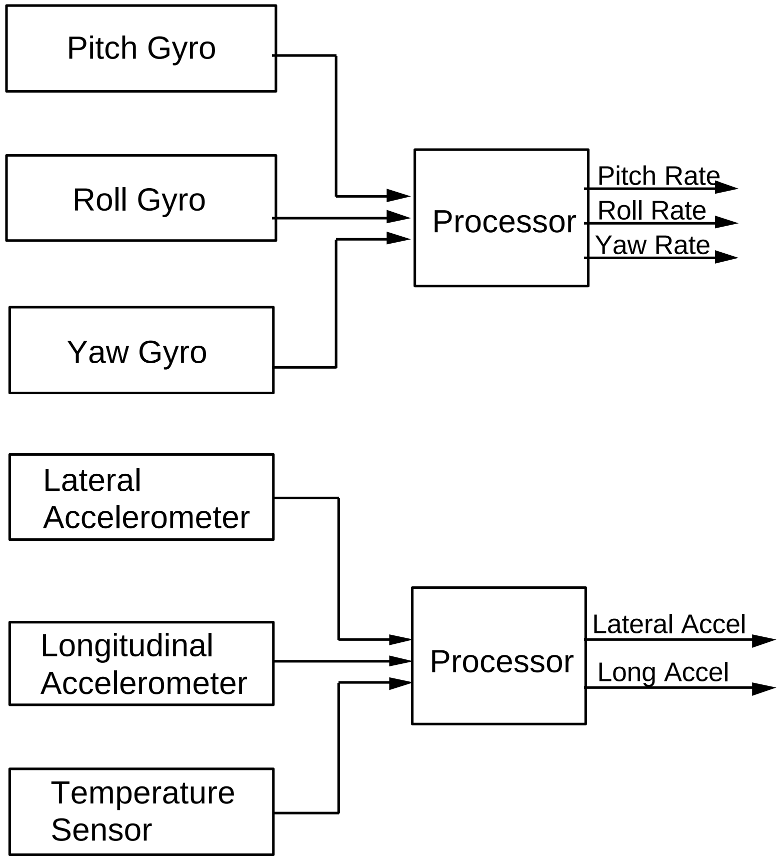


Figure 37. Gyros and Accelerometers Mechanization

Processing

MECHANIZATION

Figure 38 shows a standard processor architecture for use in determining reliability. Due to the number of critical functions that it will perform, it will be necessary to provide redundant processors. A likely candidate for the CPU is the PPC601. This is an embedded form of the Power PC processor now appearing in high-end Macintoshes. It is currently being looked at by auto manufacturers for on-board control. Provision is made for interconnection between the processors. Specialized hardware and software is required to identify which processor has failed in the event that they don't agree.

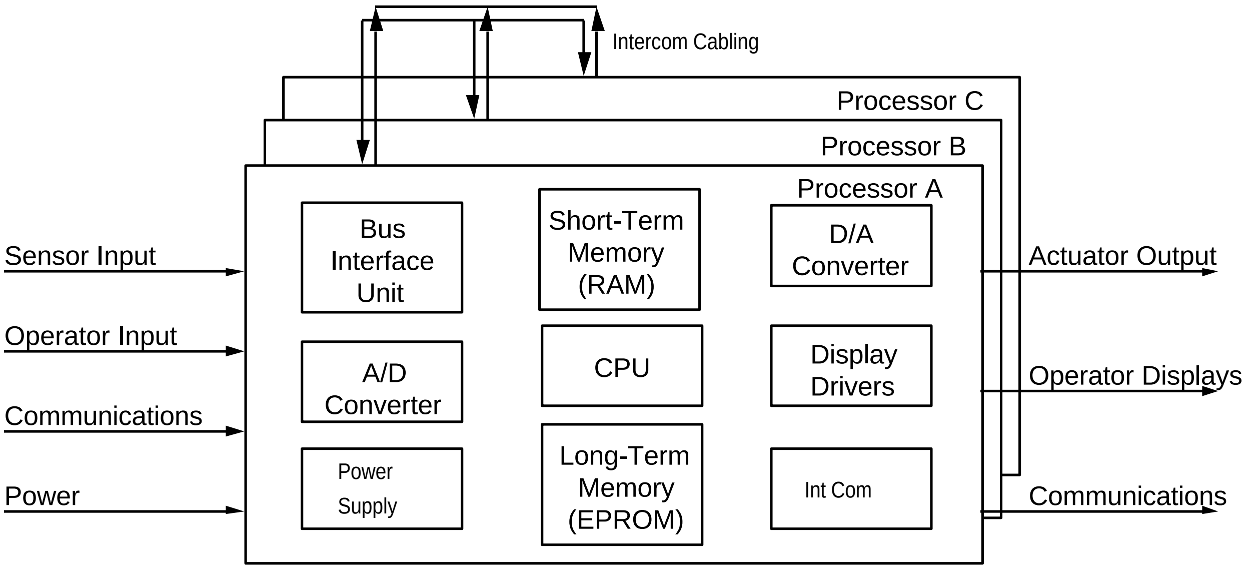


Figure 38. Triple Processor Mechanization

PROBABILITY OF FAILURE CALCULATION

The failure probability of the processors has been shown before, as part of the subsystems. It is repeated here to show the contribution of on-board processing to the overall system reliability.

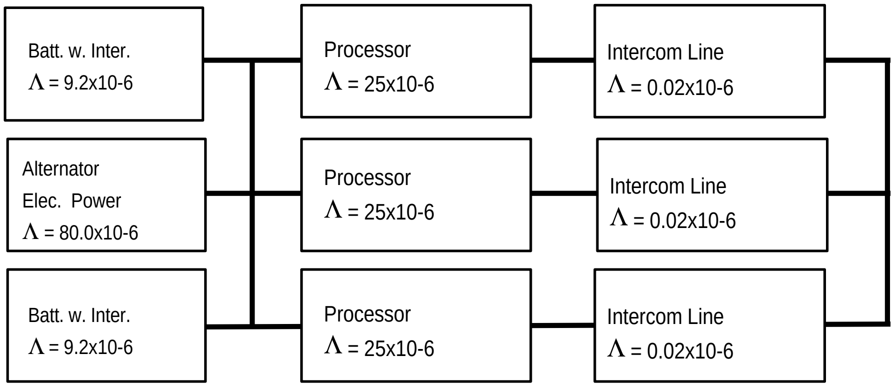


Figure 39. Triple Processor Safety Diagram

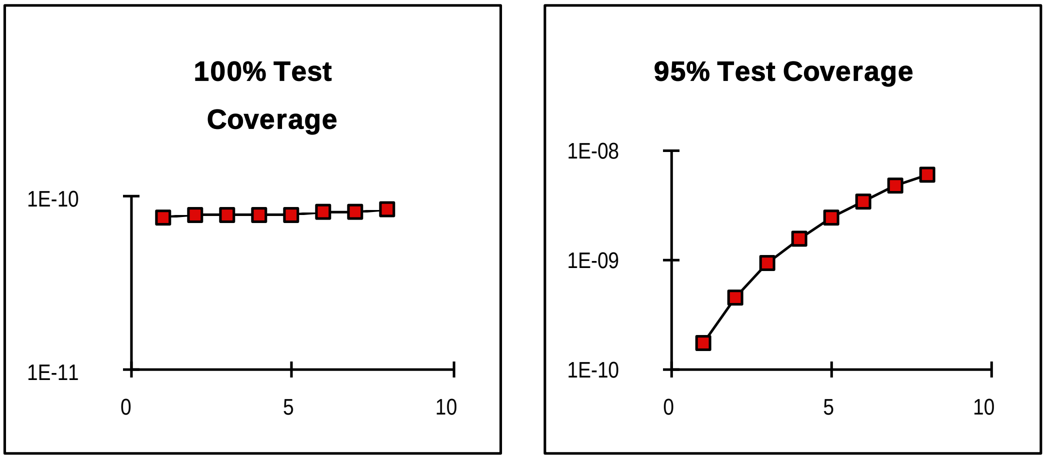


Figure 40. Triple Processor Probability of Failure vs. Time (hrs)

Communications

MECHANIZATION

A major goal of this system design has been to eliminate critical communications functions. They are particularly difficult to make reliable. However, a few functions remain. Vehicle identification must be acquired by the roadside. A passive transponder, either radio or radar triggered, looks promising (figure 41). These transponders derive their power from the interrogation beam transmitted by the roadside. They then emit an identification code in response. More elaborate communications with the roadside will probably be via radio. It may be possible to share some components with the radar system, reducing the cost. Communications with adjacent vehicles poses the problem of limiting the target. It may be possible to avoid specific targeting by specifying a lane position and time slot that is desired. The receiving vehicles would then avoid being in that position at the requested time by adjusting their headway. Figure 42 shows a compact radio design.

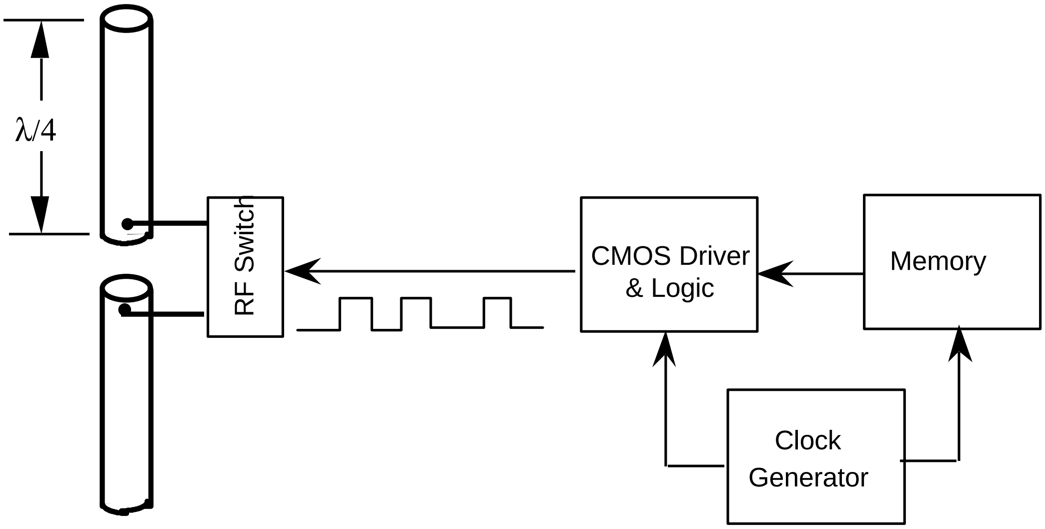


Figure 41. Vehicle ID (RF Tag) Mechanization

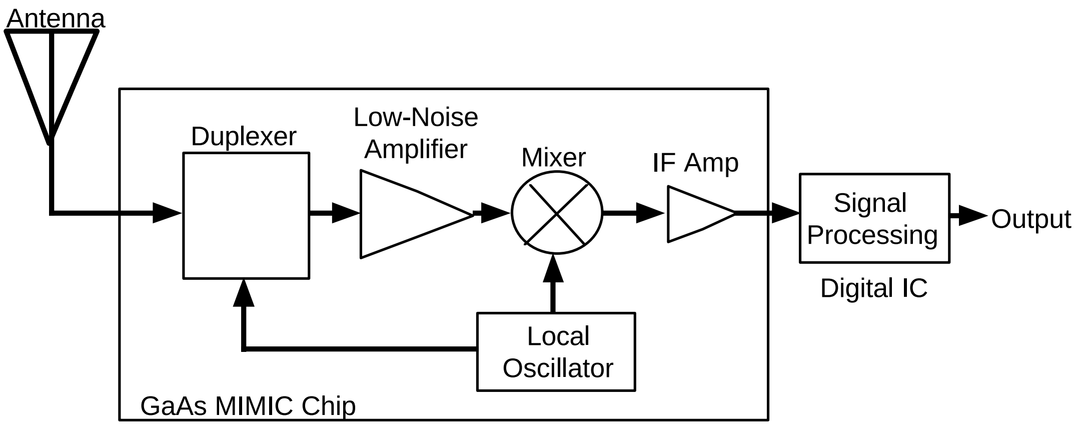


Figure 42. Radio Mechanization

PROBABILITY OF FAILURE CALCULATION

The safety diagram for communications assumes that both the transponder and the radio are necessary for proper performance. An emergency broadcast to the entire system may have better reliability, but at the cost of stopping every vehicle when an emergency occurs, even those ahead of the failed one.

As with the other vehicle subsystems, triple redundancy is required to keep the failure probability below the limits set by our overall system goals. Figure 43 shows the safety diagram for triple redundant communications. Figure 44 shows the resulting failure probabilities for the 100% and 95% test coverage cases.

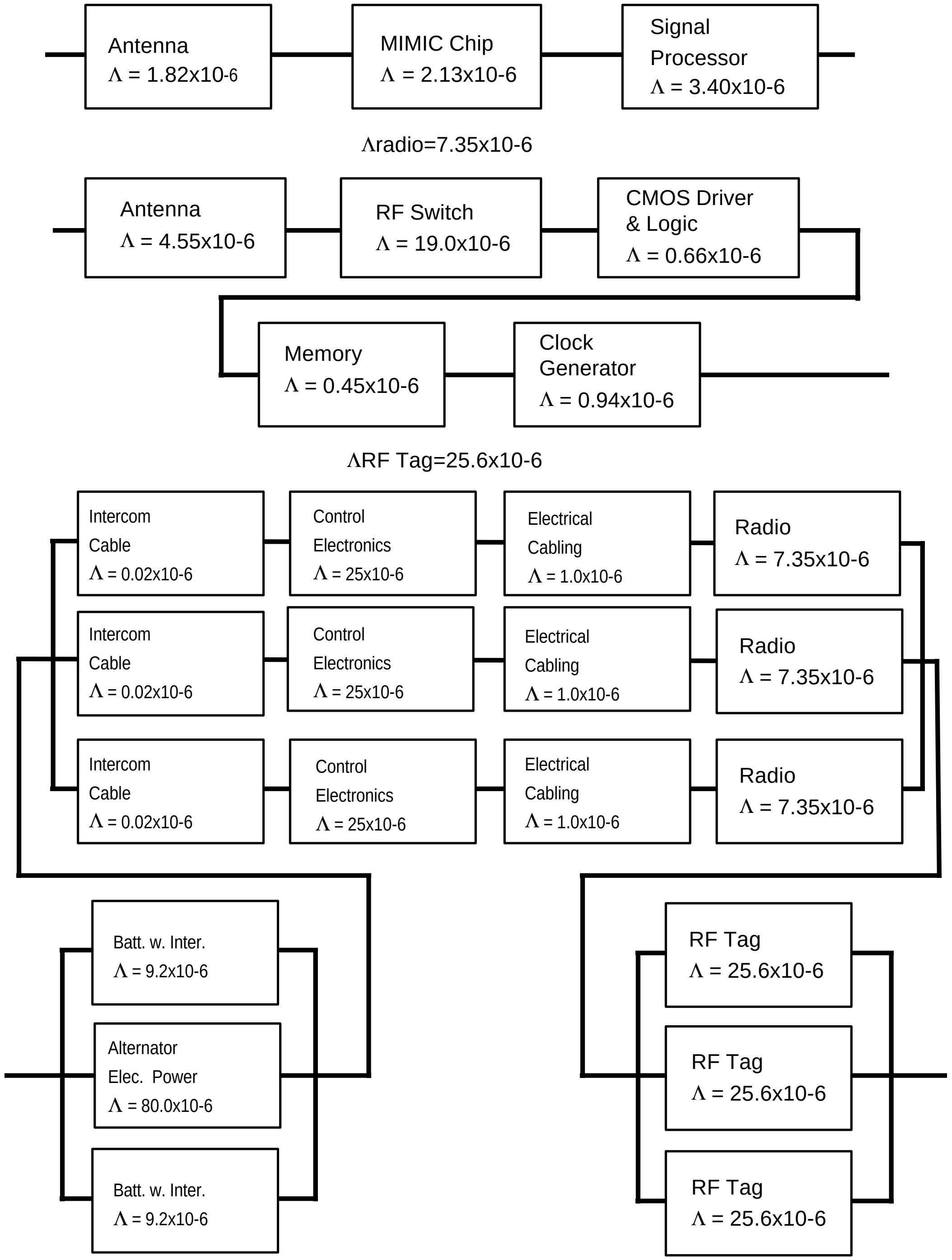


Figure 43. Communications Safety Diagram

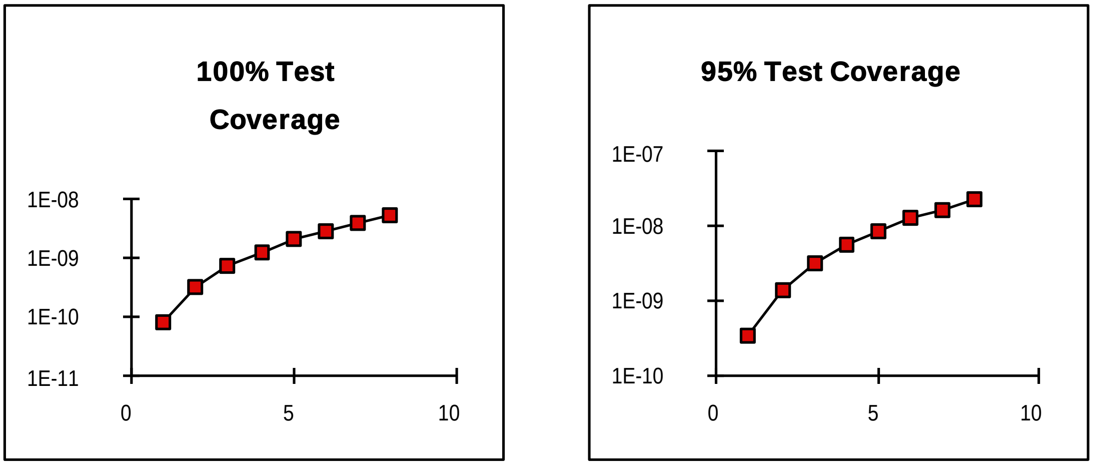


Figure 44. Communications Probability of Failure vs. Time (hrs)

Displays and Controls

MECHANIZATION

The displays and controls mechanization covers all the interfaces with the driver. Some are already present on vehicles, others are specific to automation functions or to driver checkout. Figure 45 shows a likely arrangement. All the functions provided by the displays and controls subsystem can be considered noncritical if the roadway is properly equipped and certain malfunction management strategies are followed.

The first critical message is to inform the driver that admission to the AHS has been denied. If vehicles are only brought into the AHS lanes after the transfer of control to the automation, then a failure of this message to get through will constitute a message of no admission.

The second critical message to the driver is to request that the driver resume manual control. If the system is designed so that the driver is required to send notice of readiness to the AHS, then the function becomes noncritical. If the driver does not receive the request to resume manual control, then the driver cannot respond and the vehicle remains under automatic control. Under these conditions, it would be driven to a repository where the driver could retake control after the vehicle had been stopped and shut off.

A mechanization of this subsystem is shown in figure 45 to illustrate the types of displays and controls that might be found in an AHS-equipped vehicle. Although this function is considered noncritical, redundancy may be desirable for improving overall system performance.

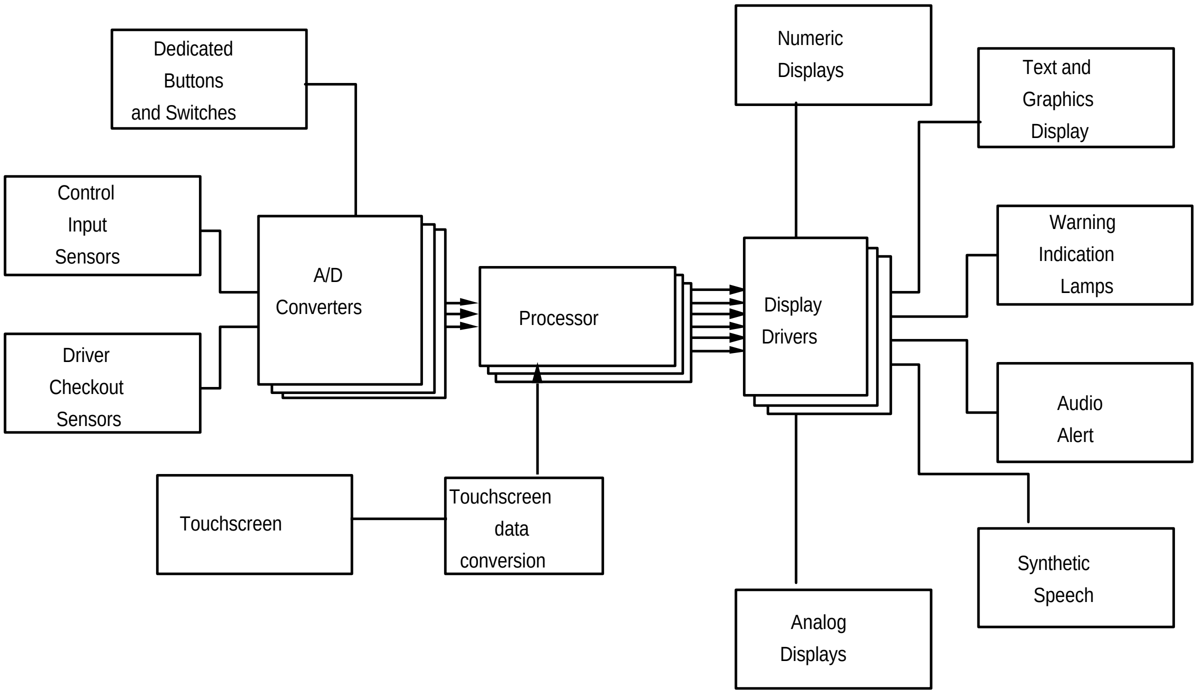


Figure 45. Displays and Controls Mechanization

DISPLAYS

Numeric: These are digital readouts of data like speed or time.

Text and Graphics: Large format displays, capable of graphics. The most likely candidates are CRT's or liquid crystal flat panels.

Warning Indication Lamps: Idiot lights and flashers.

Audio Alerts: Buzzers and beepers.

Synthetic Speech: This may range from playing back canned segments of recorded speech to full generation of synthetic speech.

Analog: Moving bars and dials, as for speed and tachometer.

CONTROLS

Dedicated Buttons and Switches: controls having a permanent limited function, radio power on/off, etc.

Control Input Sensors: Sensors that detect the positions of the manual vehicle controls.

Driver Checkout Sensors: Sensors for the specific purpose of driver readiness evaluation, heart-rate, etc.

Touchscreen: In general, this represents a means of doing random text entry. A touchscreen was selected because it is the input device under consideration by the Human Factors Design for AHS contract.

Engine

MECHANIZATION

Figure 46 is a representative engine mechanization. Although recent analysis has determined that the engine has only one critical function, requiring no special mechanization, a drawing is shown in Figure 46, since it is available. It is a standard, fuel-injected internal combustion engine, with a few additions for automatic control. Very little modification was actually necessary. Modern engines are already computer controlled.

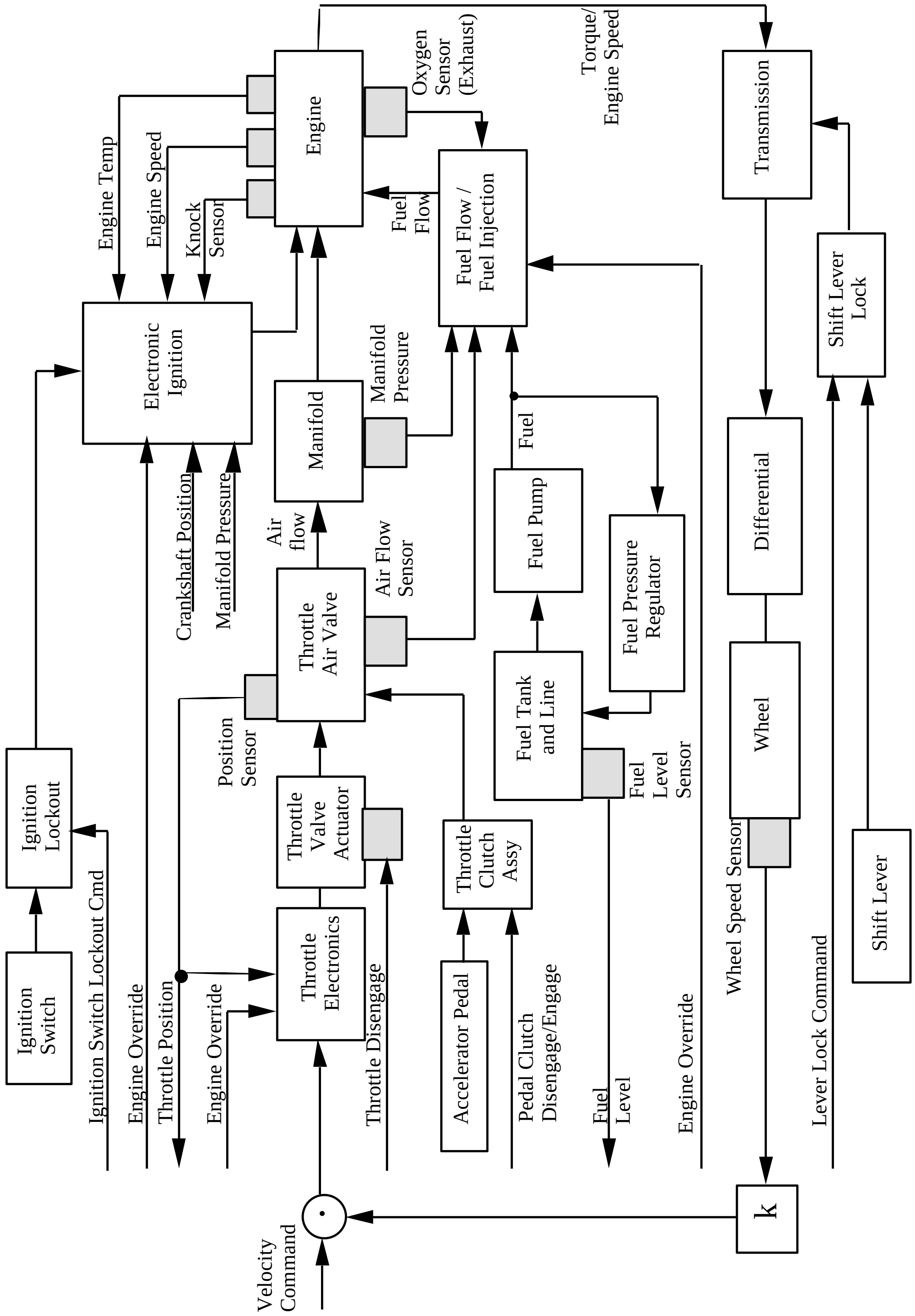


Figure 46. Engine Mechanization

MONITORING AND TESTING

The engine failure modes reflect the performance of a modern, fuel-injected, internal combustion engine. Although the vehicle will lose motive power, backups in the power supply system will provide for on-board processing, communications, and emergency braking and steering.

Table 7. Engine Component Failure Modes

Throttle valve actuator freeze (stuck at) hard open hard close sticky (slow rate)	Oxygen sensor open fail high fail low	Ignition coil low voltage open
Throttle valve freeze (stuck at) hard open hard close sticky (slow rate)	Fuel injectors/drivers poor spray incorrect delivery stuck open stuck closed	Fuel tank and line leaks rupture
Manifold leaks	Fuel pump low flow or pressure failure	Fuel pressure regulator incorrect pressure leaks or rupture
Engine mechanical failures (expand)	Spark plugs shorted open incorrect gap	Knock sensor no response low response
Air flow sensor calibration shift (dirty) electrical failure	Crankshaft position no signal erratic signal	Camshaft position no signal phase shift
Manifold pressure sensor no signal high or low signal	Manifold temperature sensor no signal high or low signal	Coolant temperature sensor no signal high or low signal

Table 8. Engine Sensor Data and Control Inputs

Throttle valve actuator
Throttle valve
Manifold
Engine
Air flow sensor
Fuel injectors/drivers
Oxygen sensor
Fuel tank and line
Fuel pump
Fuel pressure regulator
Knock sensor
Crankshaft position
Camshaft position
Manifold pressure sensor
Manifold temperature sensor
Coolant temperature sensor
Ignition coil
Spark plugs
Engine control module

ENGINE SHUTDOWN

The only critical engine function is emergency shutdown. This is required to prevent brake fade during emergency braking. Fortunately, this function requires no additional mechanization to accomplish.

There are three levels of shutdown:

- Shut down the fuel injection drivers
- Shut off the ignition coil driver
- Hard closure of the throttle valve

All three of these steps can be accomplished with the current level of engine control.

POWER SUPPLY MECHANIZATION

The power supply subsystem is included in the engine section because the engine is the primary source of power for the vehicle. Figure 47 shows how the engine fits into this subsystem mechanization.

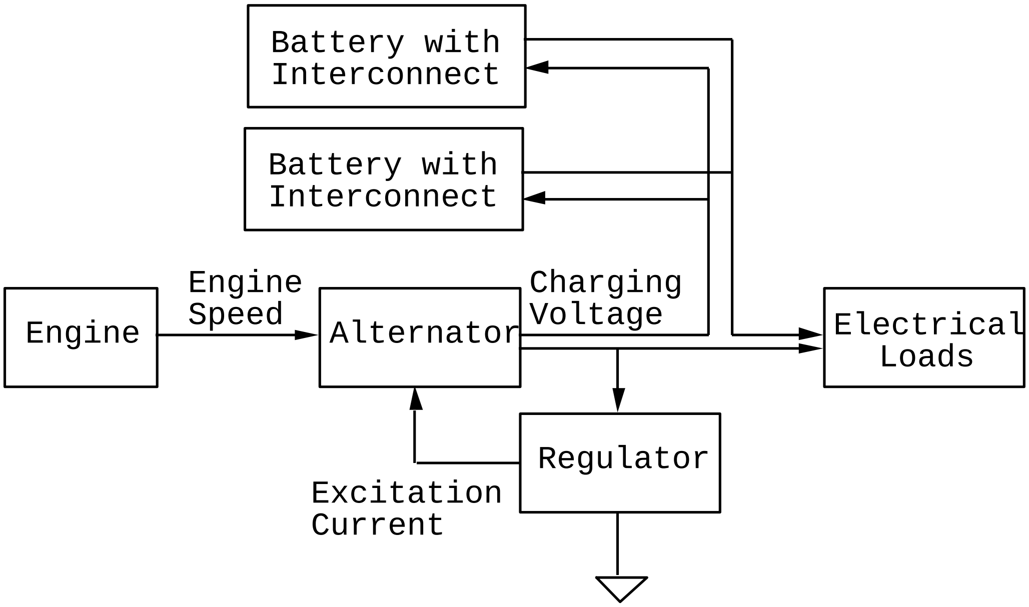


Figure 47. Power Supply Mechanization

PROBABILITY OF FAILURE CALCULATION

This system is critical since it supports so many other systems on the vehicle. As determined in the steering and braking subsystem analyses, it is triply redundant. Figure 48 shows the performance of the system with 100% and 95% test coverage.

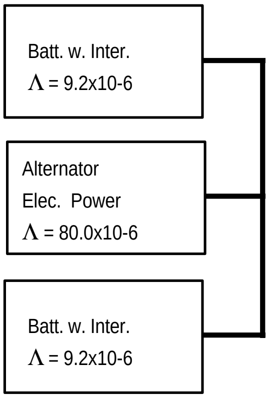


Figure 48. Power Supply Safety Diagram

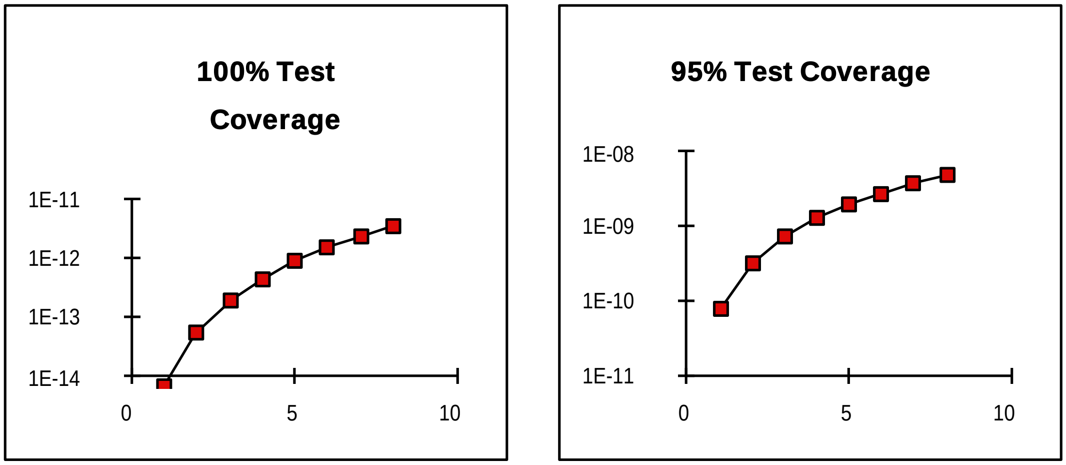


Figure 49. Power Supply Probability of Failure vs. Time (hrs)

General Vehicle Architecture

The general architecture, shown in Figure 50, illustrates the redundancy in vehicle systems.

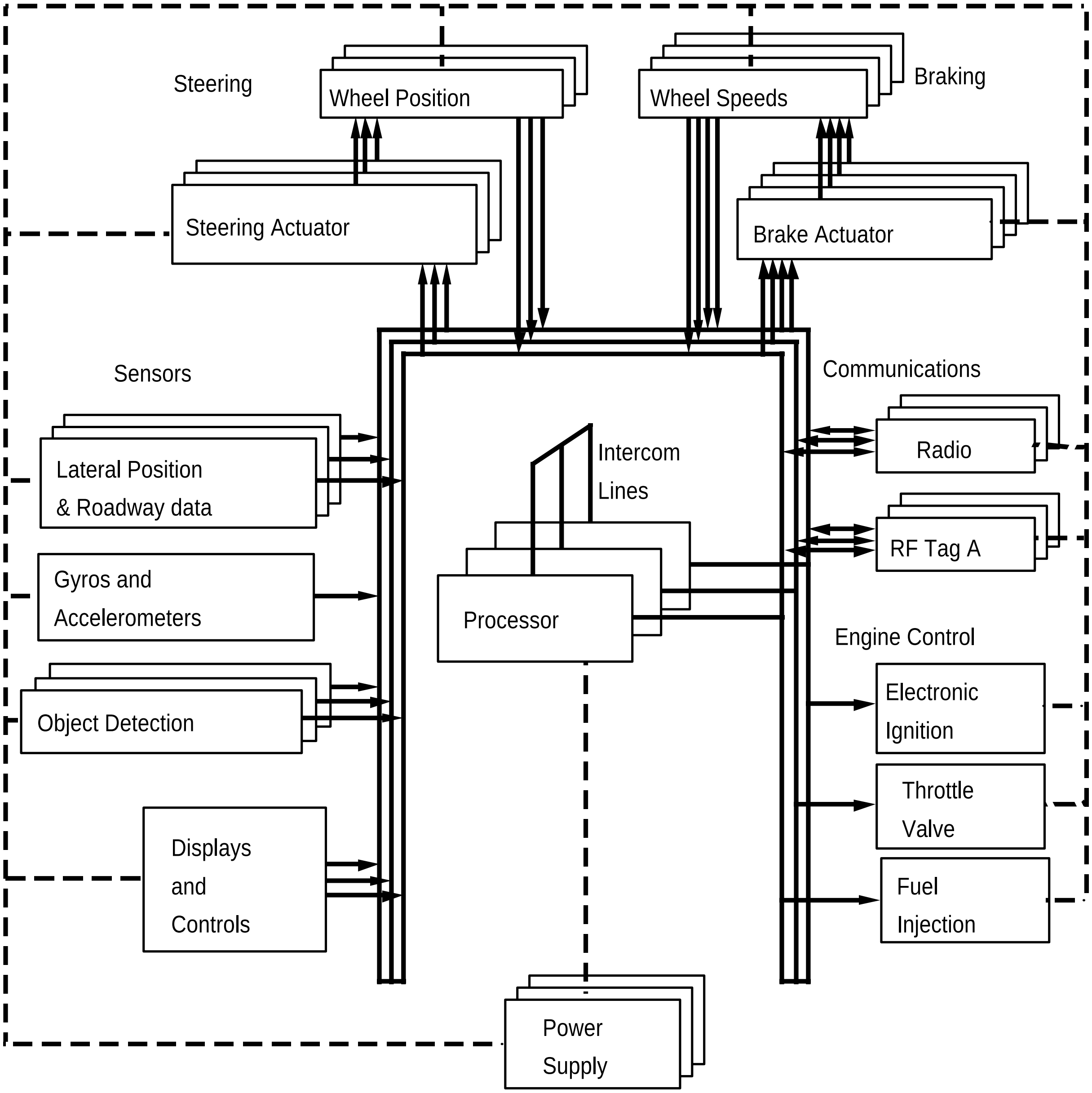


Figure 50. General Architecture

PROBABILITY OF FAILURE CALCULATION

Up till this point, each subsystem has been examined as a standalone system. Now, it is necessary to determine the probability of failure for the entire system. The failure probabilities are added as follows:

Power Supply (triple) + Steering (triple) + Braking (triple) + Object Detection (triple) + Communications (triple) + Lateral Position (triple) + Gyros and Accelerometers + Processing (triple) + Engine control + Displays and Controls.

The safety diagram in figure 51 shows how probabilities are summed across subsystems. Data were obtained for all systems except: lateral position, gyros and accelerometers, engine control, and displays and controls. Even by arguing that displays and controls are not critical, the final probability of failure will likely be higher than what is shown in the plots in figure 52.

For the systems that we have data on, the vehicle probability of failure is $5.0x10^{-7}$ after 8 hours of continuous use, without additional testing. The goal for the vehicle was $6.0x10^{-7}$, so we have succeeded in our design goals, for the most part. What we can say for certain is that if the remaining, undefined subsystems can be brought to the same level as the others, then it will be possible to meet reliability goals.

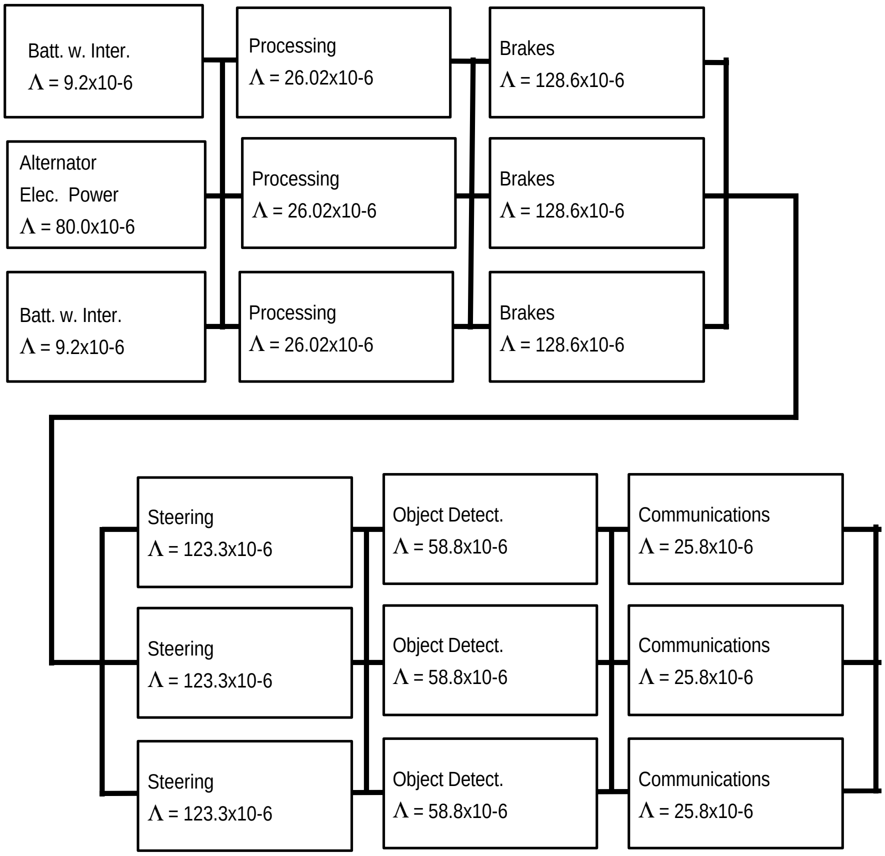


Figure 51. Vehicle Safety Diagram

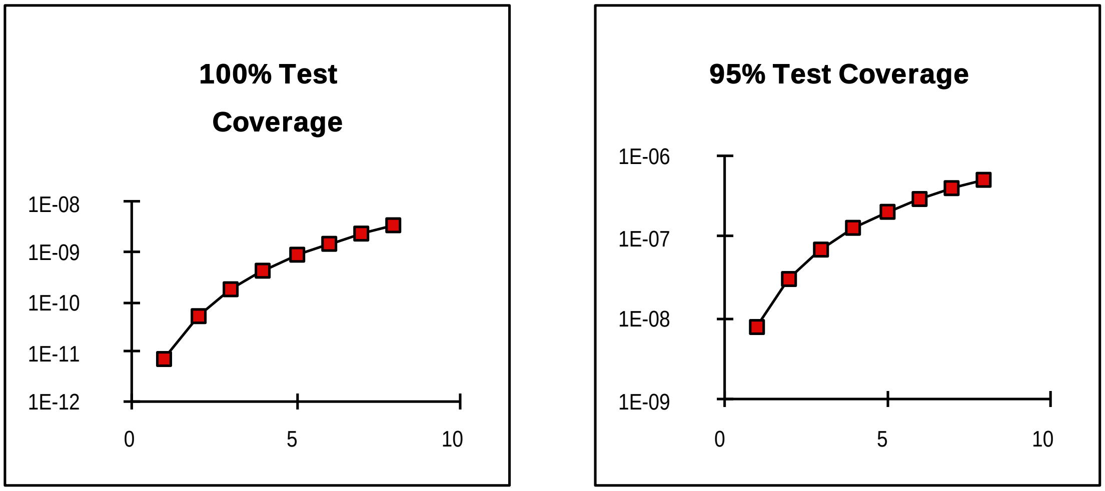


Figure 52. Vehicle Probability of Failure vs. Time (hrs)

Roadside

Mapping from Functions to Hardware

To ensure reasonable completeness at this stage in the analysis, all functions were enumerated without concern for their criticality or where they would be performed. For the purposes of the current study, however, only functions whose loss could cause death, personal injury or property damage (i.e., critical functions) need to be considered further. The next stage in the analysis is to determine a reasonable implementation or *mechanization* for those functions. The mechanization of an analyzable AHS implementation was split into the roadside and vehicle segments, which correspond roughly to the abstract functional decomposition as shown in figure 53.

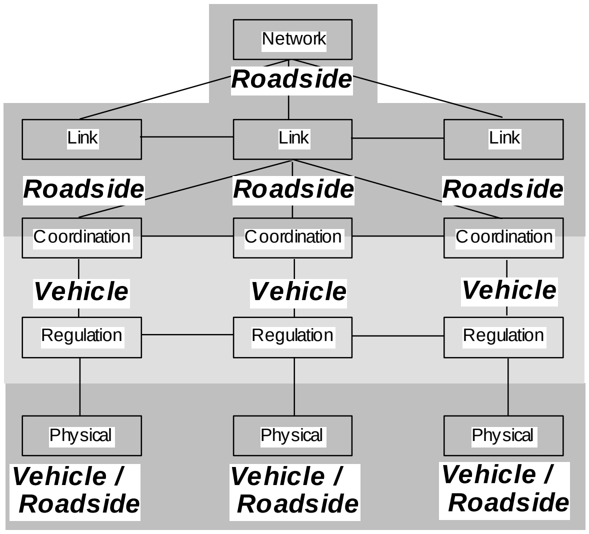
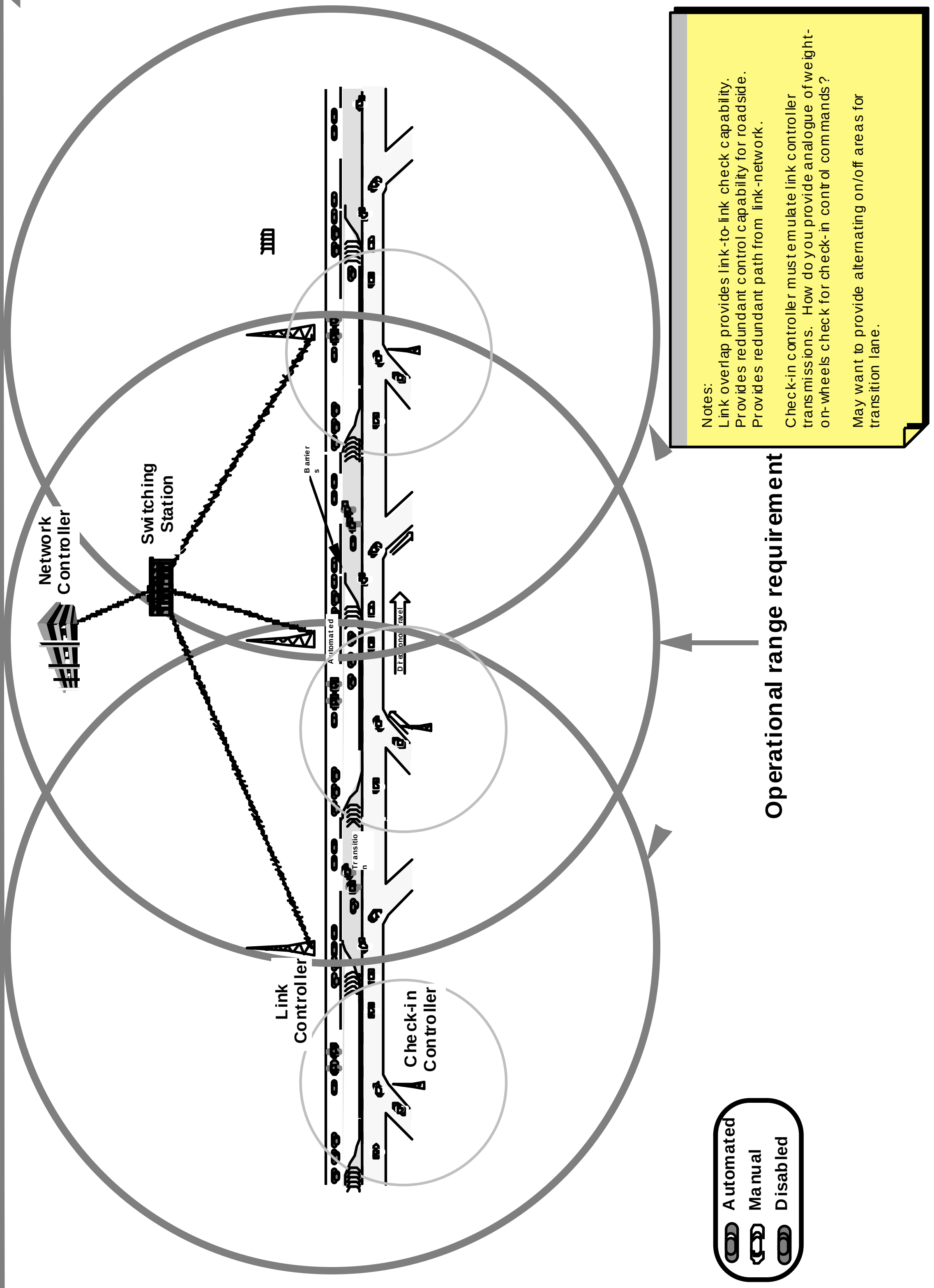


Figure 53. Abstract to Physical Mapping.

In this diagram, network and link layer functions are performed exclusively by the roadside. Coordination functions are performed by some mix of the roadside and vehicle. Regulation functions are performed on the vehicle, and the physical layer exists of course for both the roadside and vehicle. The mechanization we have assumed for the roadside is detailed here, starting at a very high level view depicted in figure 54.



Notes:
Link overlap provides link-to-link check capability.
Provides redundant control capability for roadside.
Provides redundant path from link-network.

Check-in controller must emulate link controller transmissions. How do you provide analogue of weight-on-wheels check for check-in control commands?

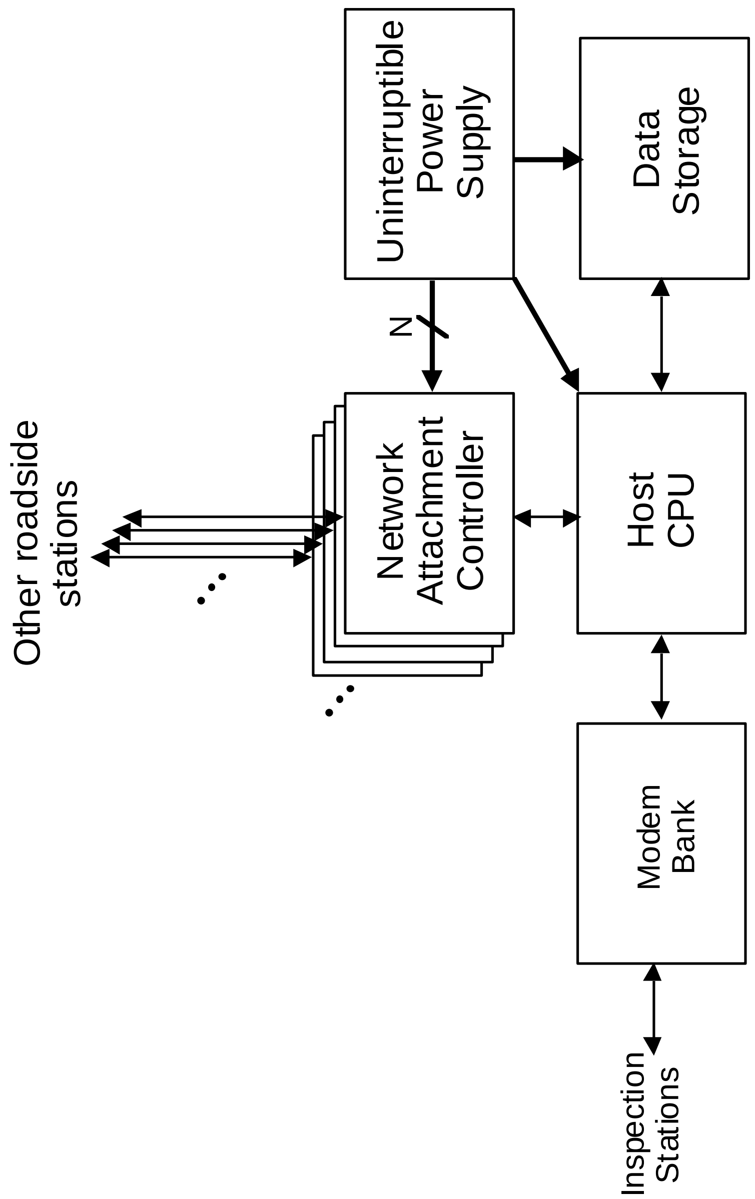
May want to provide alternating on/off areas for transition lane.

Figure 54. Roadside Overview

Common Components

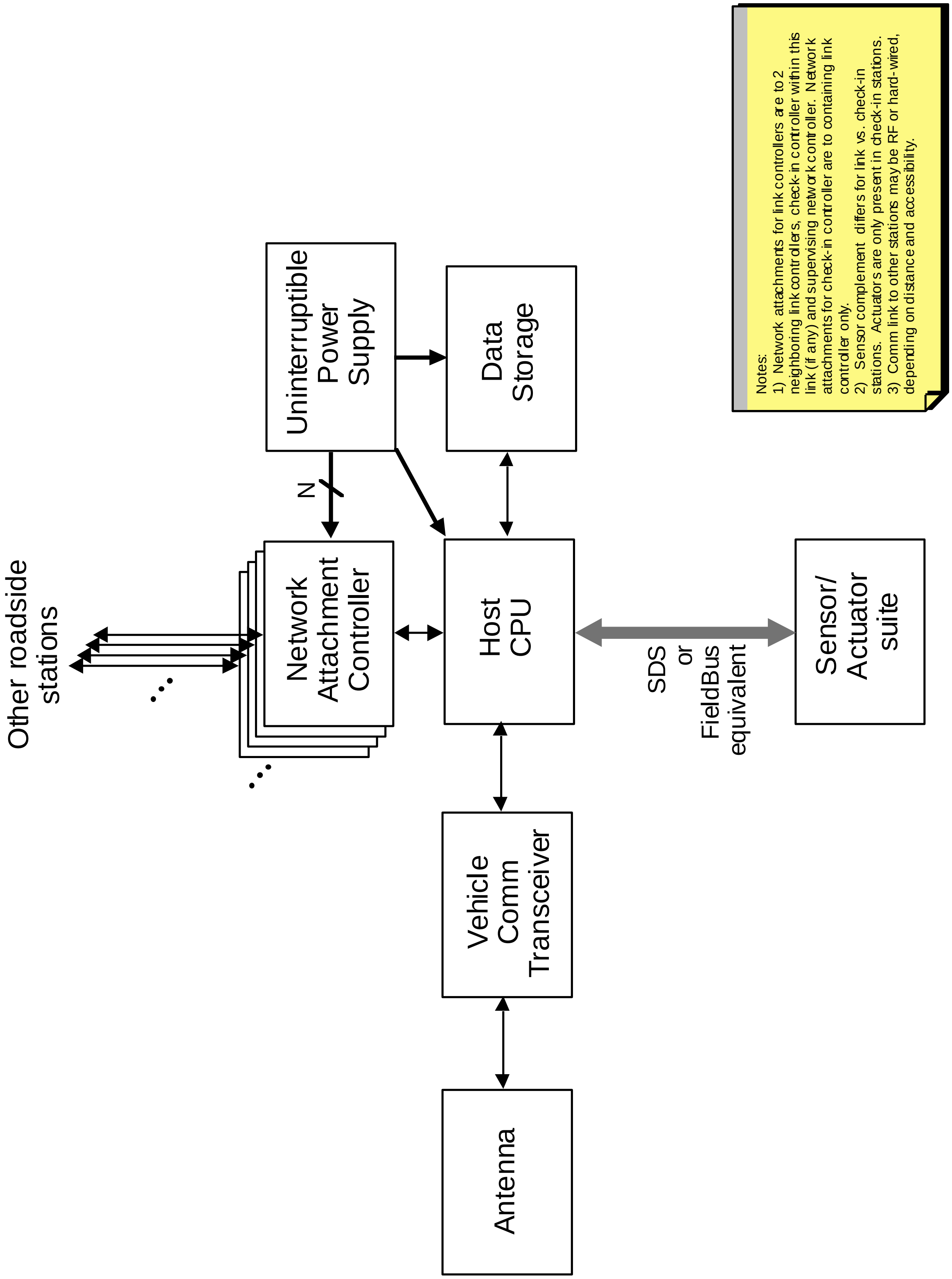
As shown in figure 54, there are three distinct types of roadside controllers, for the network, link, and checkin roles respectively. The controller mechanizations are quite similar, both possessing a core CPU with associated data store, an uninterruptible power supply, and a network attachment controller. The complex elements of this mechanization (CPU and network attachment controller) are developed in greater detail below.

The link/check-in controllers differ from the network controller in terms of the communications requirements (vehicle communication vs. modem bank), and the presence of a sensor/actuator module. The modem bank within the network controller is intended to handle a scenario in which off-road inspection stations report the results of inspections to a central authority. While this is not necessarily the best approach, it makes the mechanization less reliable (hence more challenging), and so was included.



Notes:
1) Network attachments are to adjacent network controllers, subsidiary link controllers, and check-in controllers.
2) Inspection stations report to the central network node, who is then responsible for answering queries from the check-in station controllers.

Figure 55a. Network Controller Mechanization



Notes:
1) Network attachments for link controllers are to 2 neighboring link controllers, check-in controller within this link (if any) and supervising network controller. Network attachments for check-in controller are to containing link controller only.
2) Sensor complement differs for link vs. check-in stations. Actuators are only present in check-in stations.
3) Comm link to other stations may be RF or hard-wired, depending on distance and accessibility.

Figure 55b. Link/Check-in Controller Mechanization

Figure 56 shows increased detail for the Host CPU block. Rather than develop a mechanization from scratch, we have pulled an architecture that is representative of state of the art embedded processors from the current literature that will serve to assess the reliability for such subsystems. [1] For this (or any other) mechanization, the representation of the architecture does not imply its endorsement as the correct choice for AHS application, merely an appropriate candidate for reliability/failure mode examination.

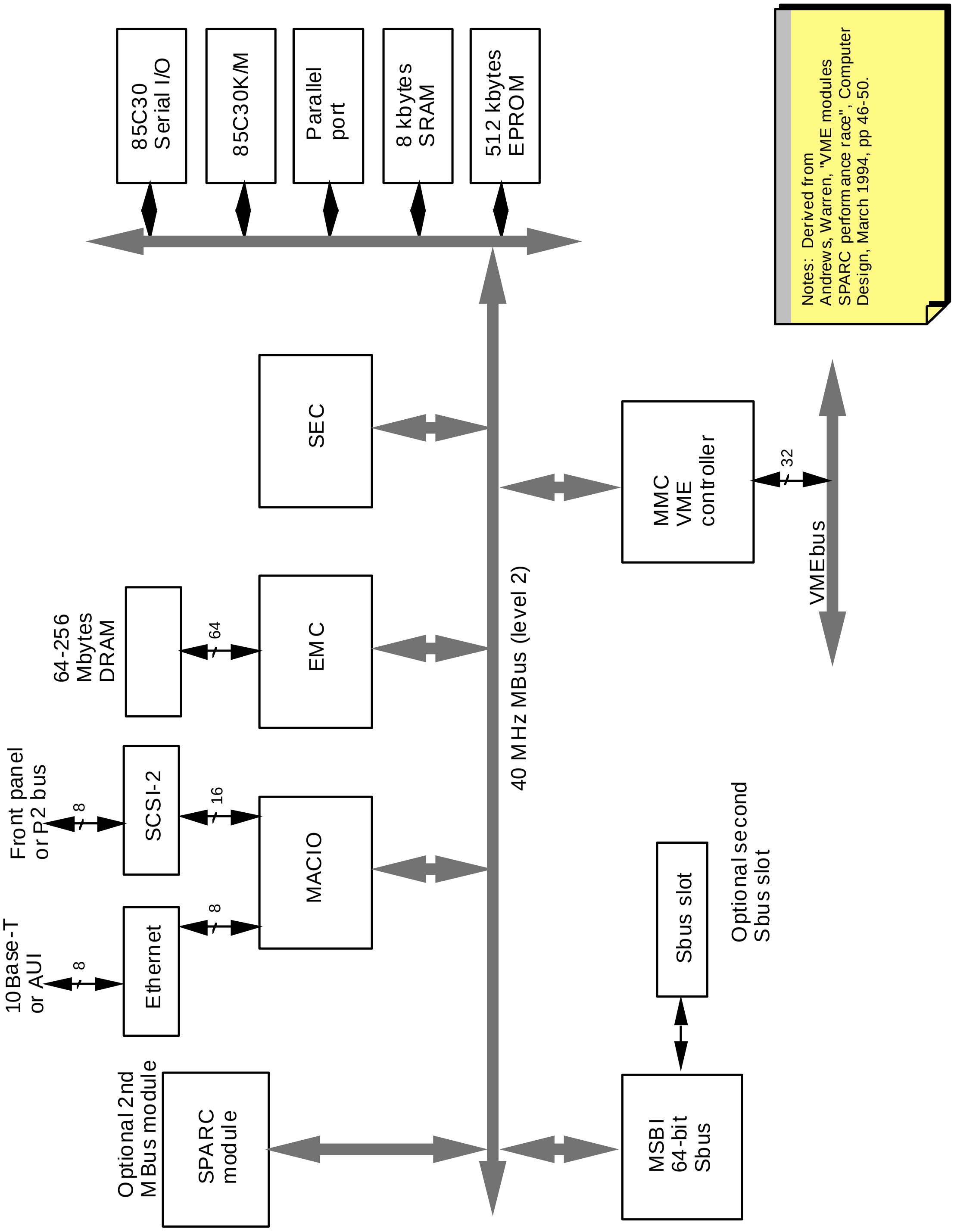
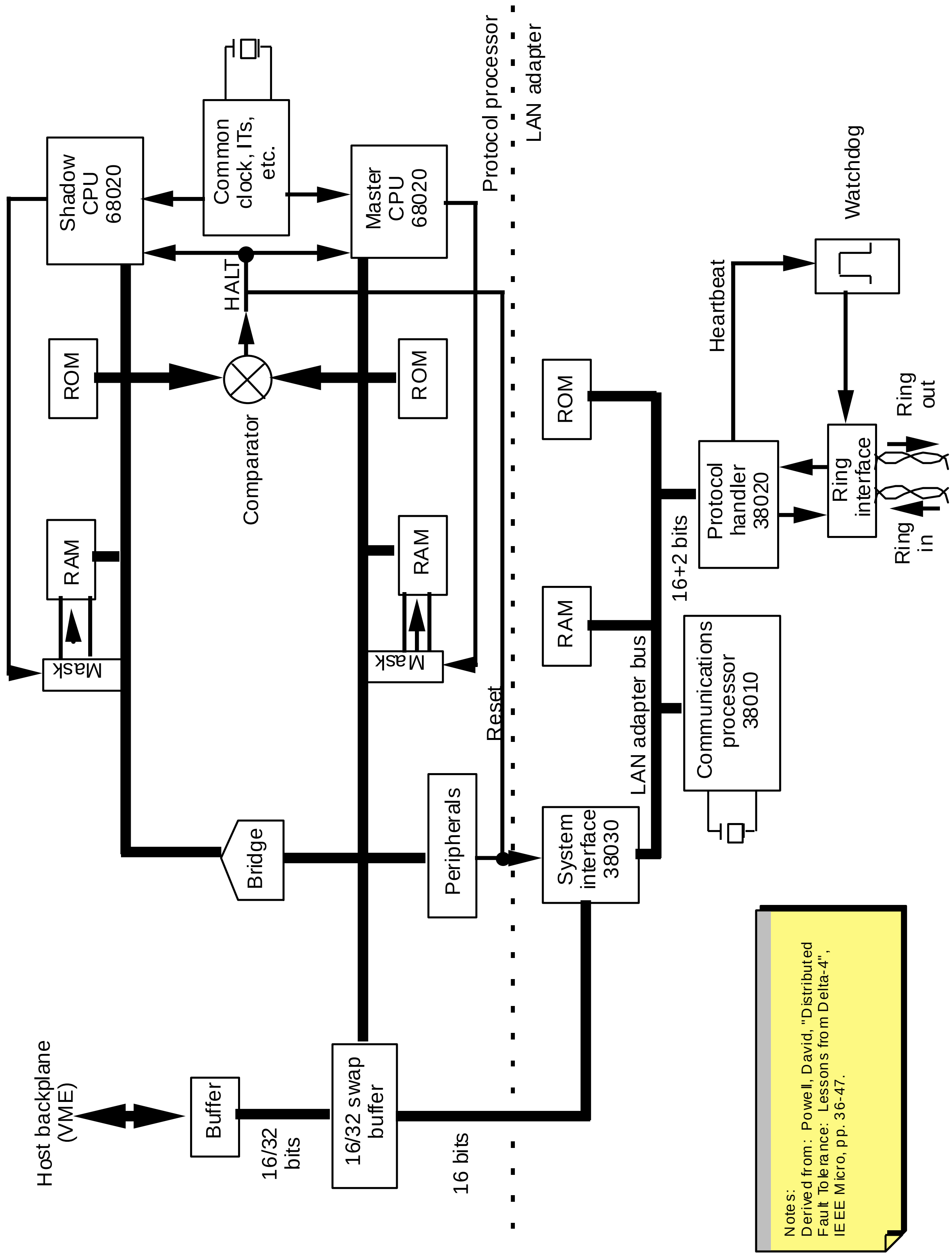


Figure 56. Host CPU Mechanization

This roadside node's connection to other roadside nodes is mediated by a Network Attachment Controller (NAC), which ensures that the roadside node fails silent (i.e., does not flood the network). A separate connection to network level controllers is not shown, since it is no different than the connection to other roadside controllers, and may in fact be achieved in a distributed fashion on those controllers. Figure 57 details the Network Attachment Controller.[17] The NAC diagram shows a twisted pair connection to other nodes, this could be adapted to RF communication if necessary.



Notes:
Derived from: Powell, David, "Distributed Fault Tolerance: Lessons from Delta-4",
IEEE Micro, pp. 36-47.

Figure 57. Network Attachment Controller Mechanization

The final element of the link controller mechanization which needs to be developed in greater detail is the sensor/actuator suite. This is shown in Figure 58. Of course, the vehicles traveling on a link also serve as distributed sensors for the roadside; their sensor complement is detailed in the vehicle section. Note that much of the sensor complement for the roadside is directed towards providing a safe environment for the vehicle: ensuring that no intruders are present, that vehicles are at the spacings and speeds that have been commanded for the link, and that the roadway surface conditions have not become hazardous. This last consideration is particularly difficult for standoff sensors, so in this mechanization we have addressed the presence of slick surfaces through two parallel means, the thermal/rainfall detector pair, and the reflectivity sensor (presumably radar). This is included as a part of the critical equipment, since relying on vehicle-based sensing (for example, entering a reduced traction turn with too high a velocity) would result in the first car sensing the condition being unable to respond.

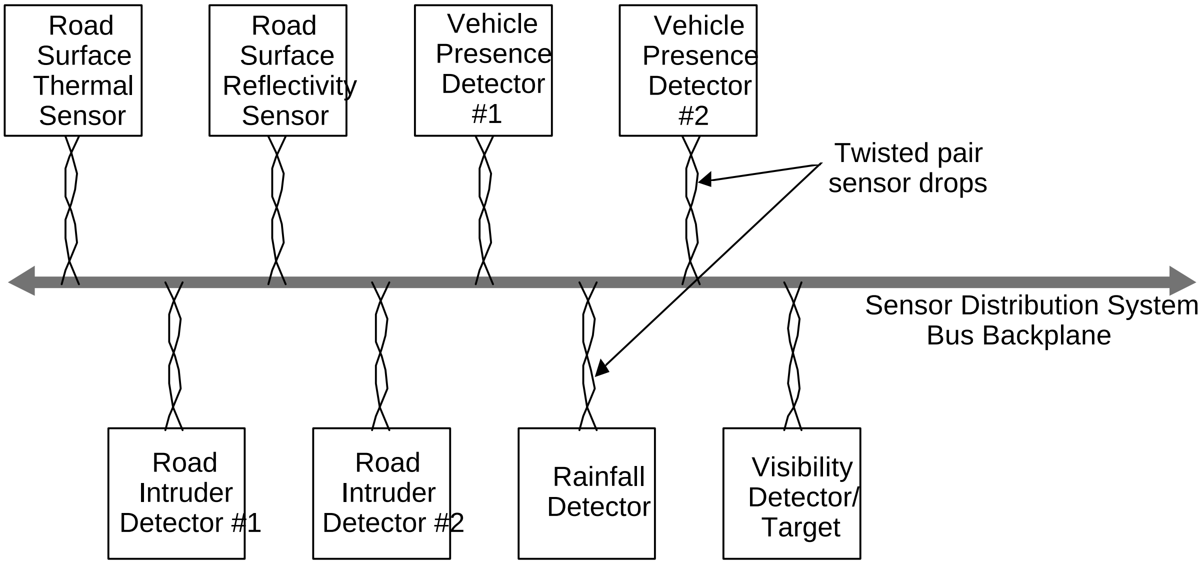

Road Surface Thermal Sensor
Road Surface Reflectivity Sensor
Vehicle Presence Detector #1
Vehicle Presence Detector #2
Twisted pair sensor drops
Sensor Distribution System Bus Backplane
Road Intruder Detector #1
Road Intruder Detector #2
Rainfall Detector
Visibility Detector/ Target

Figure 58. Sensor/Actuator Complement: Link Controller

PROBABILITY OF FAILURE CALCULATION

We have assumed a different form of redundancy for the link controller than those previously seen for the vehicle. In this case, the redundancy is provided by a "zone of control" overlap between adjacent link control stations, shown in figure 59. Note that in the scheme pictured, a malfunctioning link controller can be viewed by two adjoining stations. This is intended to address the case in which two adjacent stations will each vote that the other has failed. The other neighbor of the failed station can "verify" the vote of the functioning station. Each link station, then, is viewed as a single string implementation. The safety diagram for the link controller is shown in figure 59.

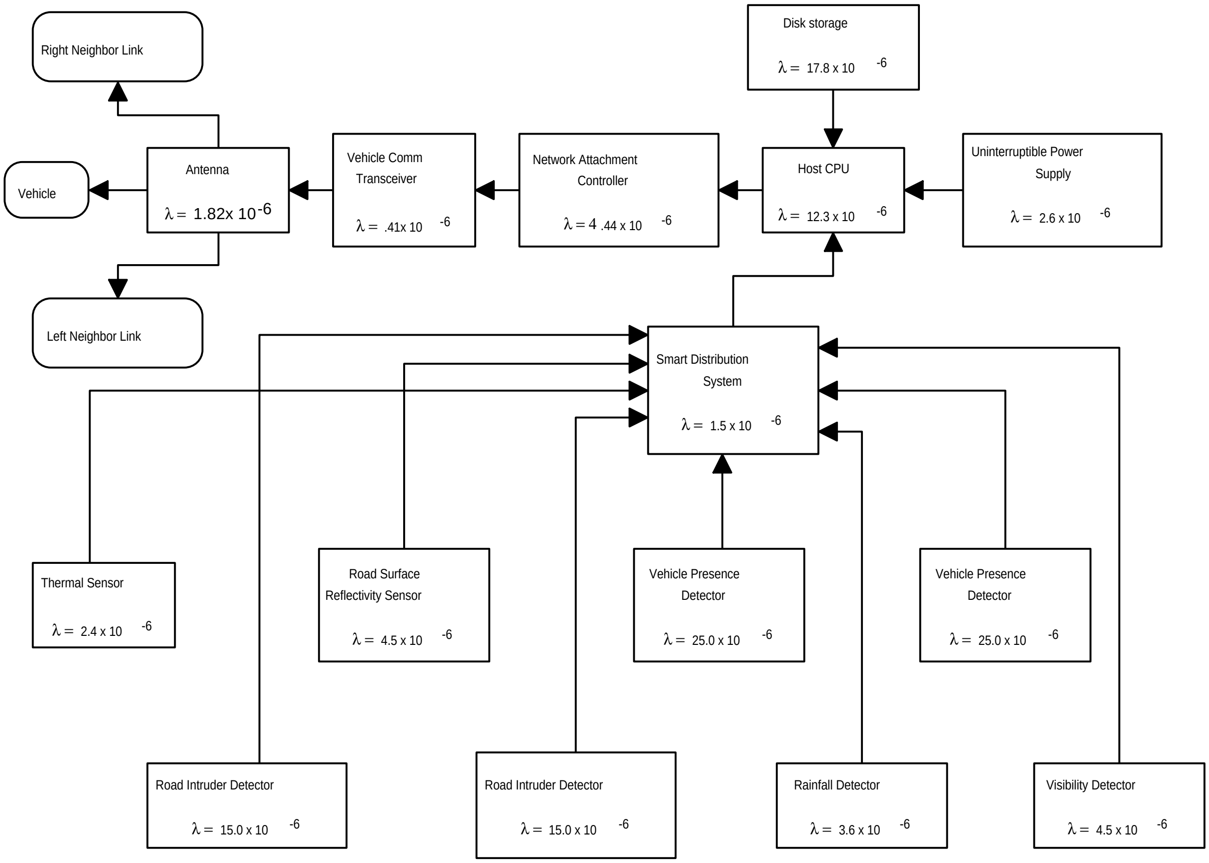


Figure 59. Safety Diagram for Link Controller.

The probability of failure calculation for this mechanization is shown in figure 60.

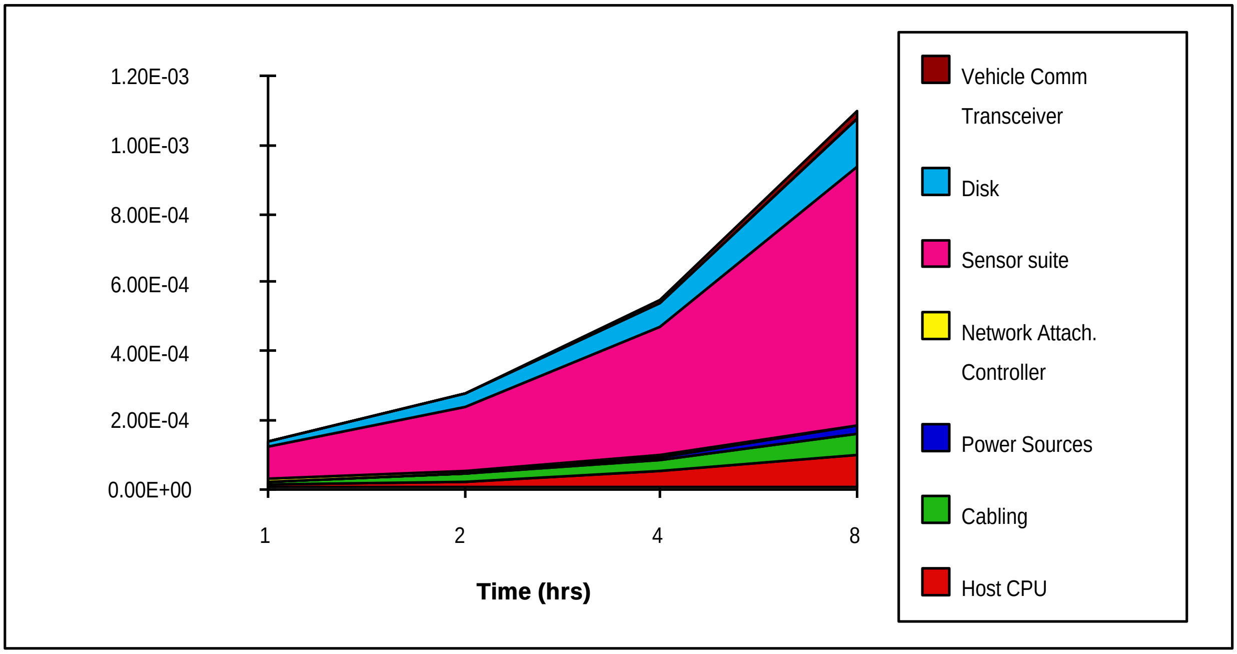


Figure 60. Probability of failure for Link Controller

Note that this probability of failure greatly exceeds the allotment for the roadside. The bulk of this contribution is from the sensor suite, due to the complex nature of some of the sensor elements. However, taking the redundancy provided by adjacent controllers into account, the picture improves markedly, as shown in figure 61.

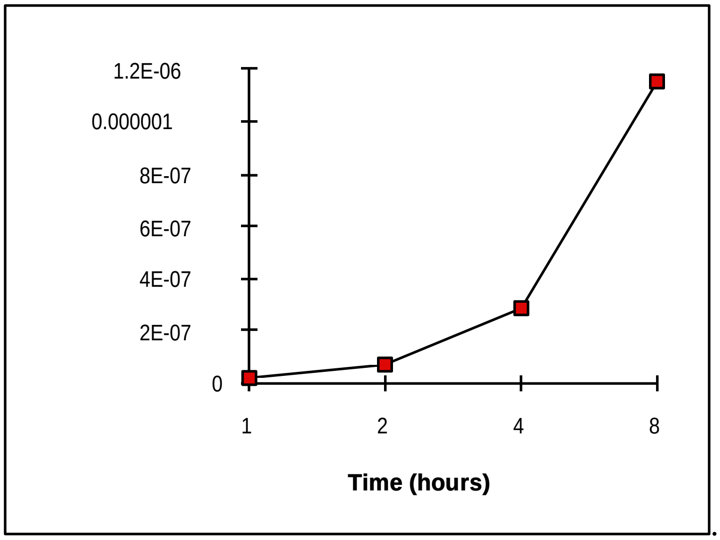


Figure 61. Mixed Coverage, Overlapping Link Controller Reliability

Dissimilar Components

FUNCTIONAL BASIS

The driving influence for dissimilarity in the mechanizations of the various controllers is, of course, the difference in the functions they perform. Since a majority of critical functions are mechanized on the vehicle, a focus of the mechanization effort on the roadside has been the portion of the roadside which checks the vehicle functions. This equipment does not contribute to the reliability of the vehicle systems in the normal manner, either by increasing the reliability of individual components, or by increasing redundancy. Rather, the roadside equipment increases *coverage* (see the section on reliability definitions) by providing in many cases an end-to-end test capability. Figure 62 shows the effect of coverage on the probability of catastrophic failure.

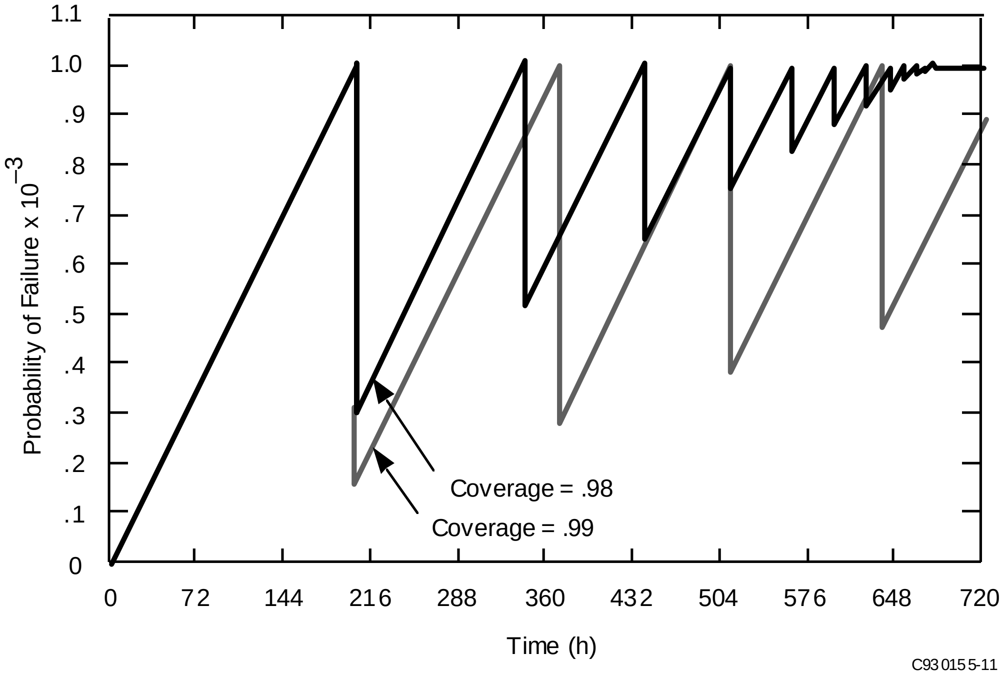


Figure 62. Coverage Effect on Probability of Failure

Table 9 shows the functions tested during the checkin process, and the associated test which challenges the function.

Table 9. Vehicle Functions Tested at Check-In

	Function to check	**Test**
P1.1	lateral displacement sensor	Calibrated driving test - lane keeping
P1.2	bearing sensor	Calibrated driving test - lane keeping
P1.5	velocity sensor	Calibrated driving test - target speed tracking
P1.6	lateral accel. sensor	Calibrated driving test - lane keeping
P1.7	long. accel. sensor	Calibrated driving test - target speed tracking
P1.8	yaw rate sensor	Calibrated driving test - lane keeping
P1.9	roll rate sensor	Calibrated driving test - lane keeping
P1.10	pitch rate sensor	Calibrated driving test - target speed tracking
P1.11	range to a frontal object/vehicle sensor	Target test
P1.12	closing rate to a front object/vehicle sensor/computation	Target test
P1.13	range to a neighboring (side) object/vehicle sensor	Target test
P1.14	closing rate to a neighboring object/vehicle sensor/computation	Target test
P1.15	range to a rear object/vehicle sensor	Target test
P1.16	closing rate to a rear object/vehicle sensor/computation	Target test
P1.19	curvature sensor/reader	Calibrated driving test or mag code wrap-around
P1.20	grade sensor/reader	Calibrated driving test or mag code wrap-around
P1.21	bank sensor/reader	Calibrated driving test or mag code wrap-around
P1.22	configuration and location of entrance/exit gates sensor/reader	Calibrated driving test or mag code wrap-around
P1.23	road surface condition sensor	Calibrated driving test - modified road surface
P1.24	visibility sensor	Target test
P1.25	wind characterization sensor/system	Inspection test
P1.26	traffic signal information channel	Comm test
P1.27	traffic sign information channel	Comm test
P2.1	steering actuation	Calibrated driving test - lane keeping
P2.3	brake actuation	Calibrated driving test
P2.4	propulsion system shutdown	Ignition system shutdown test.
P3.1	operator displays	Driver wraparound test
P3.2	switch. mech. for alternating btw auto and manual control	Last use record. Note auto-> manual and reverse
P3.3	emergency switching mechanism for human backup operation	Last use record. Note auto-> manual and reverse
P3.4	manual steering capability	In use prior to AHS, download parameters to road. Requires additional sensor.
P3.5	manual propulsion control capability	In use prior to AHS, download parameters to road. Requires additional sensor.
P3.6	manual brake control capability	In use prior to AHS, download parameters to road. Requires additional sensor.
P3.7	operator AHS input capability	Driver wraparound test.
P5	information from the regulation layer channel	Comm test
P6	information to the regulation layer channel	Comm test
P7	information from adjacent vehicle channel	Simulate vehicle on roadside
P8	information to adjacent vehicle channel	Simulate vehicle on roadside
P9	secondary functions	Current flow for headlights. Sign readability test for wipers/defroster.

In order to determine the equipment requirements to support the check-in testing, a more detailed understanding of the checkin process was required. To develop this understanding, we again created a scenario description of the relevant AHS operations. As the reader will note in table 9, the most commonly referenced test is a calibrated driving test. This test is shown graphically in figure 63, with the curvature in the test area greatly enhanced for effect. In fact, the extent of this curvature is on the order of a foot of lateral deviation from the centerline (see the simulation section on "Check-In"). Note that the road extent need not be modified for this sort of test, rather, the magnetic track that is laid within the existing road surface (or other guidance mechanism) changes direction. The lateral rangefinder array provides an independent assessment of vehicle function during the tracking segment, and the longitudinal rangefinder provides independent verification of the acceleration/deceleration capability. Other segments of the test challenge the collision avoidance system(s) and road edge detection system.

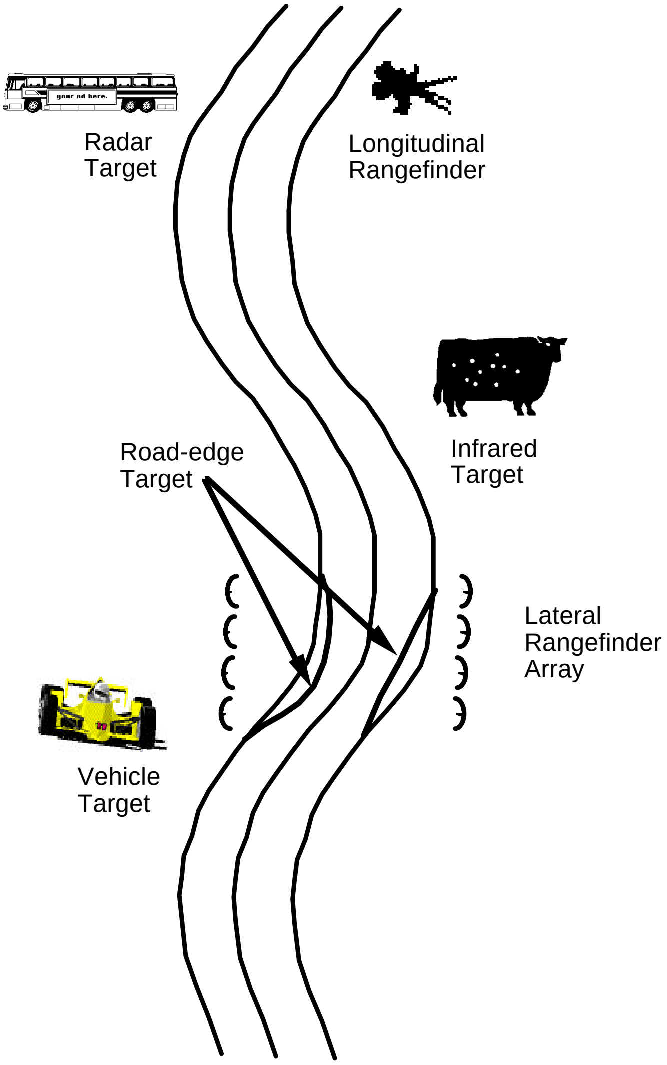


Figure 63. Caricature of Check-In Calibrated Driving Test

Roadside Test of Vehicle

This section of the report describes the sequence of tests performed by the roadside on the vehicle. Roadside, as the term is used here, applies to auxiliary, or off-vehicle equipment which is located either alongside the roadway, or at remote inspection stations whose reports are conveyed to the equipment along the roadway. Tests of the driver are described in the section on check-out. While testing may be performed on the driver upon check-in, if the driver fails testing, it is reasonable (and, we argue, necessary) to assume automated control of the vehicle anyway in order to take it to a safe repository. If this is not done, the vehicle control is given to an unqualified driver, who then exposes the AHS to risk for the time that s/he is in control. If automated control is engaged, note that the driver may be capable of controlling the vehicle by the time manual control is again required (i.e., he may have recovered from an impaired state.)

The roadside performs independent testing of the vehicle's health. Both the vehicle and the roadside must concur the vehicle is healthy for the vehicle to participate in automated operations. We assume a "no dispatch with fail" philosophy, meaning that any identified failure in a (system which performs) a critical function is grounds for refusal. Note that other philosophies, such as intentional redundancy beyond that required to meet the operational safety requirements in order to reduce the need for frequent maintenance, would introduce the idea of a "Minimum Equipment List", the set of systems which must be operational to allow participation in automated operations. This level of redundancy would drive the acquisition cost up, and hence has not been considered for purposes of the current study.

The tests described are separated into two classes, those performed on-road, and those performed off-road. The determination of where to perform the test is based on several factors:

1) An estimate of the frequency of testing required to ensure reliable operation of the functions tested.
2) An examination of the dynamic factors involved in the test (e.g., the collision avoidance sensor may be affected by adverse weather conditions present during this test).
3) An estimate of for how long the test results are valid (e.g., the load integrity applies to this trip only).

ON-ROAD TESTS

On-road tests are those that are performed on the vehicle while operating on the roadway. As discussed here, these tests are assumed to be performed prior to each use of automated mode. This assumption could be relaxed to a regular inspection schedule (every 10 hours of AHS operation, or every 10 days of calendar time, for example) if the test equipment proved costly in terms of, acquisition, maintenance or land use, *and* it could be demonstrated that the test interval was sufficient to provide the needed reliability. A discussion of the relationship of test coverage, test frequency and reliability can be found.

The tests presented here are ordered according to their presumed order of occurrence. That is, a successful communications test must occur before any of the other tests can be effectively performed, a test of the collision avoidance sensor system and braking system should occur before other systems are tested, and so forth.

COMMUNICATIONS TEST

The communications test ensures that all parts of the system are able to convey information. There are three parts to the test, corresponding to the three communications pathways involved.

Vehicle - Roadside Communication

This is the initial test, in which the roadside establishes that a viable communications channel exists to the vehicle. This is a staged protocol, starting with a standard, unencoded challenge/test response which tests the transceiver and power, along with minimal circuitry, followed by a encoded challenge response which tests the communication channel's security provisions. It is reasonable to incorporate obtaining the vehicle's ID into this test. If the communications paths and protocols are different for check-in stations and link controllers, the check-in station will have the capability to emulate the link controller to test that capability. Part of the link communication test will include the download of speed defaults which are set artificially low during the check-in phase.

Vehicle - Vehicle Communication

The roadside emulates a vehicle, modifying signal strength and protocol to fit. Signal strength, error rate and any other necessary parameters are evaluated by both sides of the interchange. If vehicle proximity sensing is by means of this vehicle-vehicle communications, this is also the first stage of target testing.

PREVIOUS USE REPORT ANALYSIS

Results of the last use of various functions are obtained from on-board records and examined to reveal potential impending failures.

Auto to Manual Switching

This is examined both for the check-out time use, and to ensure that this function is available as a backup during check-in testing.

Manual to Auto Switching

This function is assessed before the system attempts to assume control of any functions for check-in testing.

Manual Control for Steering

This is examined both for the check-out time use, and to ensure that this function is available as a backup during check-in testing. Note that certain patterns in the steering command under manual conditions, such as high variability, might indicate an incapacitated driver, which might affect check-out testing. This pattern would presumably occur across all manual input channels.

Manual Control for Braking

This is examined both for the check-out time use, and to ensure that this function is available as a backup during check-in testing.

Manual Control for Propulsion

This is examined both for the check-out time use, and to ensure that this function is available as a backup during check-in testing.

DRIVER WRAPAROUND

The driver displays, input facility, and driver alertness are assessed by means of a challenge/response test. The test must be simple (to not overload the driver, since she/he is still operating in full manual mode), brief (to not require long head-down periods), and variable (so that display function is actually required.) This test is performed first to ensure that the driver expects (and does not interfere with) test function, and is alert and ready to assume control if necessary.

PROPULSION SYSTEM SHUTDOWN

The ability to disengage or shut down the propulsion system is ensured by a brief interruption of service. This test precedes assumption of fully automated control so that if a runaway propulsion system command is experienced, there is a known backup to the braking system, which by itself could experience fade.

CALIBRATED DRIVING TEST

The driving test is an end-to-end test of the three primary system position keeping functions.

Braking

The vehicle's automated braking function is engaged. The braking test receives a braking force command, then applies braking force to each independent braking system in accordance with the command until a desired deceleration has been achieved. In order to maximize ride comfort, this test may either be of short duration, and/or may be balanced with propulsion commands to achieve a net zero deceleration. Results of the braking test as assessed by the on-board sensors are compared to the roadside equipment measured values (differentiated rangefinder readings). System defaults for maximum permissible braking and own-vehicle braking capability (used to set permissible values for group-braking commands) are downloaded and verified.

Steering/Tracking

The vehicle's automated steering function is engaged. The vehicle tracks a variable radius S-turn defined by means of the passive infrastructure lane marking (e.g., magnetic tape). Performance in tracking this marked path is assessed on-board, and relayed to the roadside for comparison to the roadside assessed performance. This may require several vehicle models to be stored on the roadside, retrieved by associating the vehicle ID obtained above with the appropriate vehicle type.

Target Test

Simultaneously with the steering test above, the collision avoidance sensing system is tested. This test is performed under automated steering control to ensure accurate positioning of the sensor on the target. A series of "targets" are positioned alongside the road corresponding to the sensor types found in the collision avoidance systems. For example, these targets might include a vehicle target (transmitting RF), an IR warm-body target, and a radar-reflective target. A special purpose target is used for road-edge detection during the steering test described below. There is a rangefinder on the roadside which reports the range to vehicle, this is used to calibrate the range-to-target reports for the various sensors. Bearing of the vehicle is used to assess the field of view of the sensor. A combination of range and bearing corresponding to the target allows the roadside to issue a "ignore target at <location>" command. This command is disabled at all times other than entrance test, to preclude sabotage opportunities.

Propulsion/Headway Control

The vehicle's performance in tracking a commanded target speed. Commands are issued above and below the system defaults to ensure that such commands are appropriately disregarded (and errors flagged.) The roadside emulates a lead vehicle to assess headway keeping capability. Again, this capability is disabled except during the check-in test. The headway sensor data stream may need to be able to accept an alternate source (roadside transmissions of simulated position) for this test.

LOAD INTEGRITY

The boundaries of the vehicle are assessed by driving through a sensor "box" which provides lateral and longitudinal cross-section. These are compared to the vehicle type to identify non-contained loads.

VEHICLE SYSTEMS REPORT ANALYSIS

The vehicle transfers BITE status and performance data to roadside for all reporting systems. Roadside analyzes this data to verify vehicle on-board assessment.

INSPECTIONS REPORT ANALYSIS

The results of off-road testing are accessed (by vehicle ID obtained above if stored on roadside) and assessed.

OFF-ROAD TESTS

WIND CHARACTERIZATION

In a static test facility, wind forces are applied to the car from various directions, and the sensors debriefed to obtain bias and accuracy indications, which are recorded.

TIRE TREAD

Remaining tread is assessed and recorded. Tire traction capability is evaluated and recorded.

EMISSIONS

This test can only marginally be considered safety related (in a long-term sense), but is included here for completeness.

STRUCTURAL INTEGRITY

The vehicle's body rigidity and connectedness is assessed and recorded to prevent vehicle parts from contaminating the AHS (e.g., the roadside muffler).

OCCUPANT RESTRAINT SYSTEMS

Proper configuration, operation, and sensor system performance for the occupant restraint systems are assessed and recorded.

Check-In Mechanization

Given this functional description, and the assumption that the roadside should have an independent means of assessing the vehicle's performance as it negotiates this sequence of tests, a mechanization for the dissimilar elements of the checkin controller is straightforward. The roadside must provide challenges and assess responses for communication (addressed in the common elements), longitudinal control (by means of roadside commands and a longitudinal sensor), lateral control (by means of roadside "commands" provided by embedded guidance markers), collision avoidance (by means of targets and emissions sensors) and load extent (by means of lateral and longitudinal sensors). In addition, some means must be provided to communicate rejection to the driver. Following the guidance of the Human Factors Design for AHS contractors, we have mechanized a two-gate system, one prior to checkin, and one prior to AHS entry, driven by actuators on the sensor/actuator bus. Figure 64 shows this configuration.

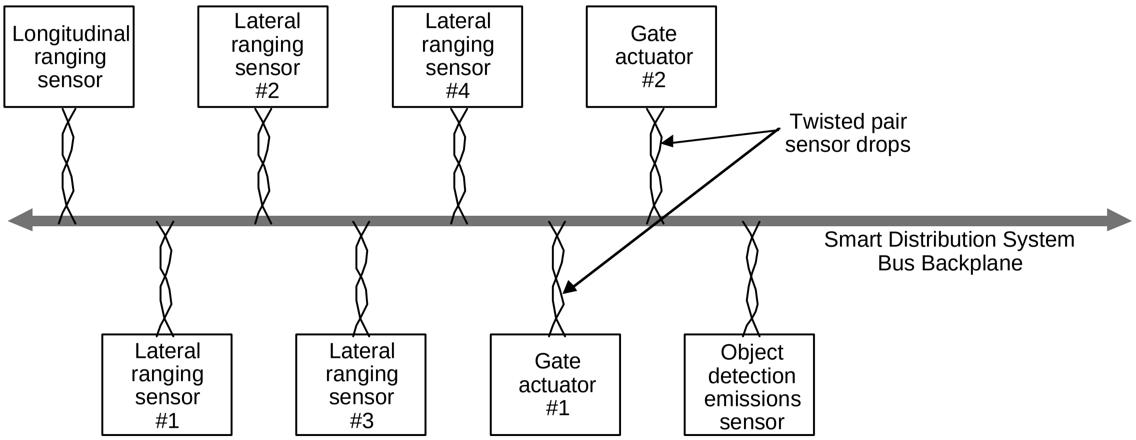
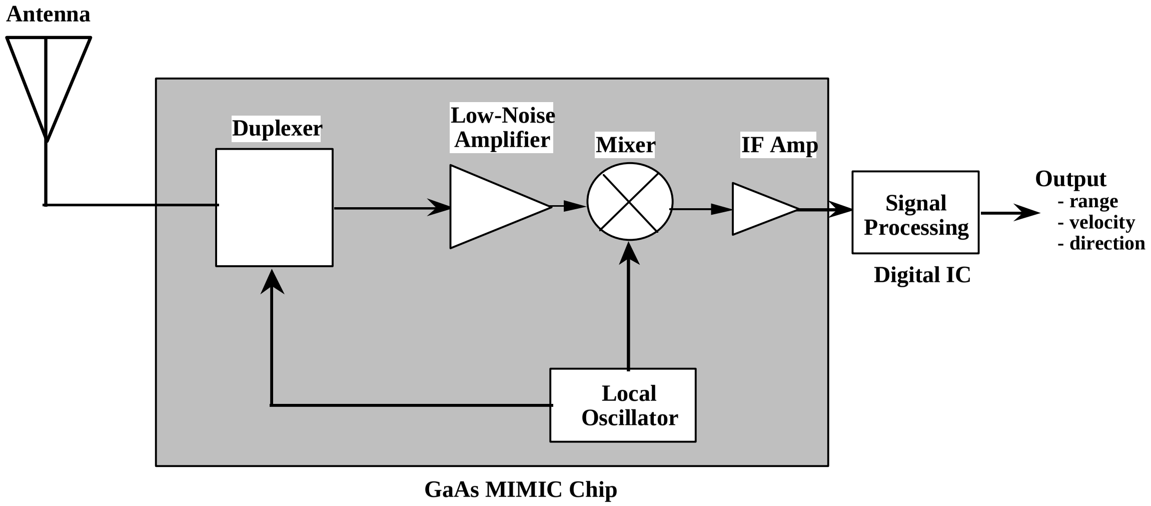

Longitudinal ranging sensor
Lateral ranging sensor #2
Lateral ranging sensor #4
Gate actuator #2
Twisted pair sensor drops
Smart Distribution System Bus Backplane
Lateral ranging sensor #1
Lateral ranging sensor #3
Gate actuator #1
Object detection emissions sensor

Figure 64. Sensor/Actuator Suite

One of the most common elements is the range and range-rate sensing element needed for both longitudinal and lateral sensing. We have chosen a radar sensor to fill these roles, shown in figure 65. Again, we emphasize that this is not necessarily an optimal or recommended mechanization, merely one which allows us to assess reliability of the system taken as a whole.



MIMIC: Microwave & Millimeter Monolithic Integrated Circuit
Antenna: Planar Microstrip Switched Array

Figure 65. Range/Range-Rate Sensor (radar)

PROBABILITY OF FAILURE CALCULATION

The safety diagram, shown in figure 66, closely resembles that for the link controller, with the exception of the sensor actuator suite. The communications links to the link controllers are shown, since it was considered reasonable that the check-in controller would announce to the link controller the presence of a new vehicle as a back-up measure.

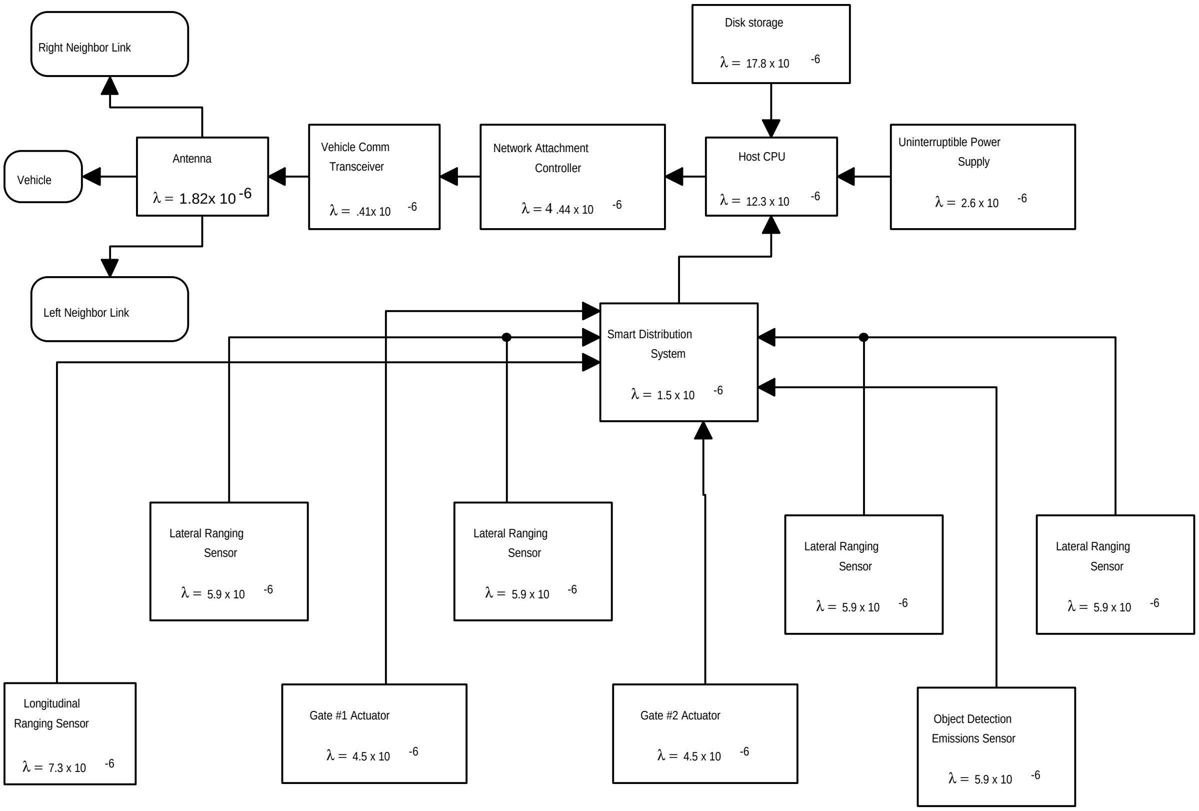


Figure 66. Safety Diagram for Check-In Controller.

Again, the probability of failure calculation closely resembles that shown for the link controller, with the sensor/actuator suite again having a dominant contribution.

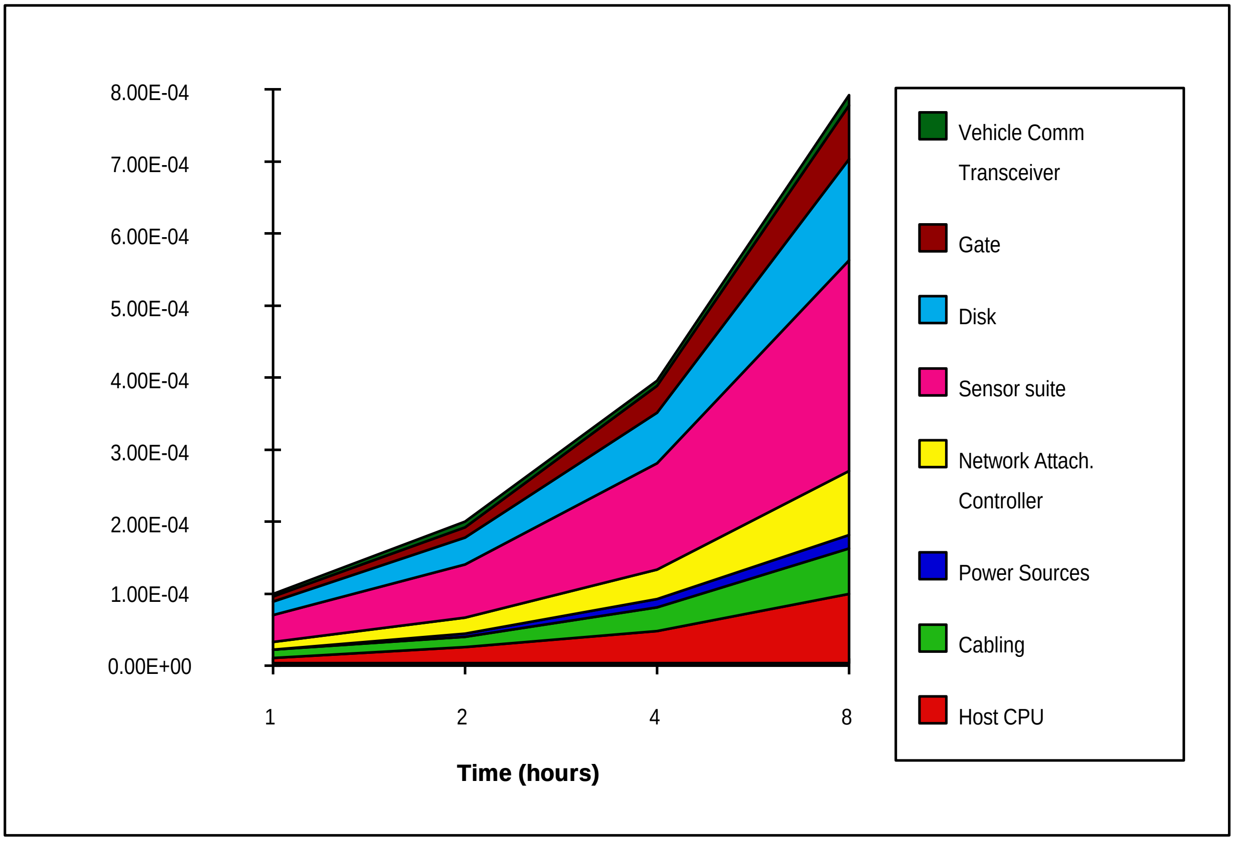


Figure 67. Probability of Failure for Check-In Controller.

Note that this probability of failure is higher than that allowed for the roadside. In this case, this is acceptable, since the critical functions being performed by the check-in controller are vehicle inspection and monitoring, along with issuing the permission/rejection for the vehicle. We have adopted a default assumption in which the vehicle and the roadside must agree to admit the vehicle, with the default mode that the vehicle is rejected. Therefore, the probability that a failed vehicle will be admitted is a combined function of the probability of failure of the vehicle monitoring and the roadside monitoring. This combined inspection puts us well within the required limit.

At the conclusion of the mechanization of critical functions, a check is done against the critical functions to ensure that all critical functions have been mechanized. A rough check of this coverage is provided in table 10. Note that some functions (roll, pitch, and yaw sensing) were judged to be too expensive or difficult to independently verify on check-in, and are thus not covered.

Table 10. Critical Roadside Functions X Mechanization

	Perform off-vehicle inspection and monitoring	Issue permission/rejection	Obtain vehicle ID	Receive information from the regulation layer	Provide information to the regulation layer	Determine roadway operational limits	Sense lateral displacement	Sense bearing	Sense velocity	Sense lateral acceleration	Sense longitudinal acceleration	Sense yaw rate	Sense roll rate	Sense pitch rate	Sense road surface condition	Sense visibility	Characterize wind	Store/provide maintenance history	Provide receiver channel from the roadside	Provide transmitter channel to the roadside	Provide electrical power	Obtain ID
Link Contr.																						
CPU						■									■	■	■	■	■	■		■
Disk/Memory						■									■	■	■	■	■	■		■
UPS						■									■	■	■	■	■	■	■	■
Sensor Bus						░									■	■	■					
Radar						░									░	■						░
IR Sensor						░									░							
RF Comm						■									░				■	■		░
Net. Attach. Contr.						■											■	■				
Land Line						■											■	■				
Check-in Contr.																						
CPU	■	■	■	■	■		■	■	■	■	■											
Disk/Memory	■	■	■	■	■		■	■	■	■	■											
UPS	■	■	■	■	■		■	■	■	■	■											
Sensor Bus	■						■	■	■	■	■											
Radar	■						■	■	■	■	■											
IR Sensor	■		░				■	■	■	■	■											
RF Comm	■	░	░	■	■																	
Net. Attach. Contr.	■																					
Land Line	■																					

MALFUNCTION SIMULATION

AHS Vehicle Lateral Motion Simulation

Overview

The AHS vehicle lateral motion simulation is a FORTRAN program which models the steering mechanization of an AHS vehicle and simulates its motion. The central concern and output of the simulation is the deviation of the vehicle from the center of the automated highway lane under both normal and failure conditions. Hence, the simulation seeks to find:

- normal operating errors that determine monitor tolerance,
- normal errors due to wind gusts that may trip a monitor,
- errors under dynamic failure conditions, and
- other lateral error related parameters.

Most of the simulation models were formulated in an earlier controls study described in the literature at pp. 33-42. [11] The study sought to determine what type of lateral controls design would be needed for the AHS vehicle based on vehicle response in varying circumstances. In the basic controls design, with only lateral position information fed back to the controller, high lateral position errors occurred during a moderately severe S-curve maneuver. The study also looked into vehicle response to wind gusts and steering actuation failures, and considered methods for reducing the normal position errors by adding additional information to the compensator.

This simulation seeks to apply the methodology in the context of failure mode analysis. In addition to employing the linear compensator/vehicle motion system, this simulation adds failure mode logic and sophisticated actuator dynamics. It is also more adaptable to simulating non-linearities in the system.

Modeling

The schematic below outlines the simulation. A more detailed description of each part of the schematic follows.

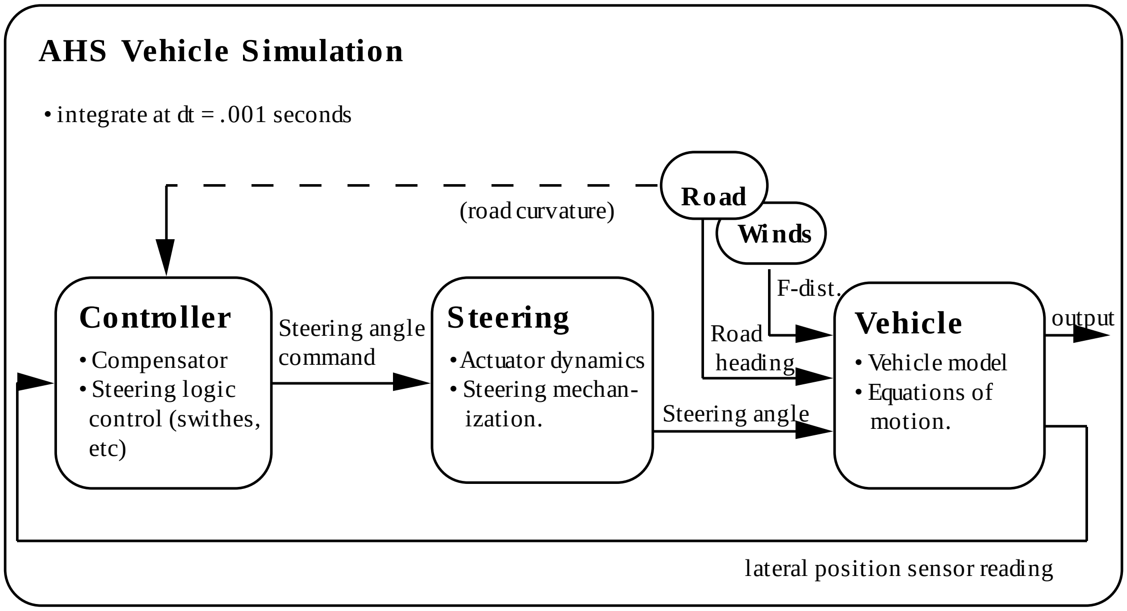


Figure 68. Simulation Schematic

VEHICLE

The "vehicle" routine stores most the vehicle model parameters and performs the basic function of integrating the equations of motion . The input parameters are steering angle (δ_w), force due to disturbance (F_d), and road heading (ψ_r). The basic output is lateral position error as read by the sensor.

Like the study mentioned above, this simulation uses the Weir model for its automobile lateral equations of motion. The states are lateral velocity (v), lateral position relative to the lane center (y), rotation rate about the z-axis (r), and heading in an earth-fixed coordinate system (ψ). [21] The inputs are front wheel steer angle ($_w$), disturbance force (F_d), and road heading (ψ_r). The states and inputs are related by the following equations of motion:

$$\boldsymbol{v}\acute{Y} = -2\frac{C_f + C_r}{MU}\boldsymbol{v} + \left(2\frac{C_r b - C_f a}{MU} - U\right)\boldsymbol{r} + 2\frac{C_f}{M}\ _{\boldsymbol{w}} + \frac{1}{M}\boldsymbol{F_d}, \qquad (13)$$

$$\boldsymbol{y}\acute{Y} = \boldsymbol{v} + U(\quad - \quad_{\boldsymbol{r}}), \qquad (14)$$

$$\boldsymbol{r}\acute{Y} = 2\frac{C_r b - C_f a}{I_z U}\boldsymbol{v} - 2\frac{C_f a^2 + C_r b^2}{I_z U}\boldsymbol{r} + 2\frac{C_f a}{I_z}\ _{\boldsymbol{w}}, \text{ and} \qquad (15)$$

$$\acute{Y} = \boldsymbol{r}, \qquad (16)$$

where

U = vehicle forward velocity,
M = Vehicle mass,

I_z = Vehicle inertia about the vertical axis,
a = Distance from cg to front axle,
b = Distance from cg to rear axle,
c = Distance from cg to lateral position sensor,
C_f = Cornering stiffness for each front tire, and
C_r = Cornering stiffness for each rear tire.

These equations were developed from the earlier controls study and can be shown to be completely equivalent to those of Peng and Tomizuka of PATH (see Weir 79) by eliminating v and r and rewriting them in terms of y and ψ.

Other outputs of interest include lateral sensor position (y_s), lateral acceleration (a_y), jerk, and heading error (ψ_e), which are

$$y_s = \boldsymbol{y} + c(\quad - \quad_{\boldsymbol{r}}), \tag{17}$$

$$a_y = \mathbf{v} + U\mathbf{r}, \tag{18}$$

$$\text{jerk} = a\acute{Y}, \text{ and} \tag{19}$$

$$_e = \quad - \quad _r . \tag{20}$$

AUTOMOBILE MODEL

This simulation has implemented two automobile models. The first is that used by Peng and Tomizuka, pp. 3090-95, and is referred to as the "Path Vehicle". [16] Its parameters are:

M = 100 slugs,
I_z = 2140 slug-feet squared,
a = 3.67 feet,
b = 4.59 feet,
c = a,
C_f = 9442 lb/rad, and
C_r = 9442 lb/rad.

The simulation also employs a 1984 Honda Accord model. Parameters for this vehicle were principally obtained from Xia, X. and E.H. Law.[30] Its parameters are:

M = 89.09 slugs,
I_z = 1200 slug-feet squared,
a = 3.28 feet,
b = 4.77 feet,
c = a or c=6.12 feet for bumper placement,
C_f = 7321.5 lb/rad, and
C_r = 6084 lb/rad, and

A_{lat} = 41.1 square feet, where A_{lat} is the lateral surface area of the car for use in modeling wind shear drag.

Use of the Honda Accord parameters were found preferable to the PATH parameters, which were used in the earlier study, because of the availability of the c (cg - bumper distance) and A_{lat} (side area) values and our familiarity with the vehicle.

CONTROLLER

The "controller" subroutine consists of the logic for controlling the vehicle through the steering command.

Note that the vehicle attempts to follow $_r$, the road heading, by controlling $_w$, the steering angle. The basic controls design contemplates calculating a steering angle command δ_{wc} based solely on information from the lateral position sensor. Hence the basic controller consists simply of a compensator with δ_{wc} as the output and lateral position error as read by the sensor (y_s) as input. The compensator employed in the simulation is a four-state dynamic compensator based on the LQG/LTR (linear quadratic gaussian with loop transfer recovery) synthesis methodology, used by Barrett for his earlier controls study.[11]

The compensator is pre-formed as a matrix outside the program based on the LQG/LTR methodology. It is dependent on the vehicle model, vehicle parameters, and longitudinal velocity. Note the dependence on longitudinal velocity. Hence, for the simulation to run at multiple vehicle velocities, a scheduled compensator would have to be employed.

The output of the controller is always steering angle command (δ_{wc}). For the initial studies, the input to the compensator was solely lateral position error as read by the sensor (y_s). As with Barrett's study, and as shown below, this control design leads to position deviations which are too high to be considered realistic.

In order to reduce the position errors during normal operation, it is desirable to introduce a new controls design which passes more information to the controller. Such a method is to exploit curvature information that could be embedded in the roadway (e.g., as a digital code stored by magnetic nail used for the position sensor). A feedforward control based on this concept was developed for an assumed ideal roadway coding scheme that provides continuous curvature information that is then combined with existing lateral sensor information. The feedforward compensator employs lateral acceleration of the roadway passed through a second-order filter with frequency and damping that approximate that of the closed loop vehicle, as described by

$${}^{ff}_{w} = K_{ff} \frac{{}^{2}_{f}}{s^2 + 2\,{}_{f}\,{}_{f} + {}^{2}_{f}} \frac{U^2}{} \qquad {}_{f} = 3 \text{ r/s}, \quad {}_{f} = 0.6 \tag{21}$$

K_f is dependent upon longitudinal velocity. This equation is the feedforward compensator, and the ${}_w^{ff}$ value is added to the value of existing lateral position compensator to achieve an overall steering command (δ_{wc}).

STEERING ACTUATION

The "steering" subroutine simulates actuator dynamics as well as failures in the actuator components. Two separate actuator models are contained within the routine. The first is a simple, second order servo-actuator model which was used prior to the more fully developed dual actuator model.

SIMPLE MODEL

The simple model can be described by

$$_w = \frac{{}_o^2}{s^2 + 2 \; _o \; _o + {}_o^2} \; _{wc}\text{, where} \qquad (22)$$

$$_o = 30\,\text{rad / sec}, \quad \text{and} \quad _o = 0.5.$$

A rate limit of 30 deg/sec is also part of the model. Hence, steering angle command enters the subroutine and passes through a second order filter, which models the steering actuation, to become the actual steering angle. The steering angle is then passed to the vehicle routine for use in the equations of motion.

This model works well for simulating a "stand-by" redundant system during failure, but is inadequate for simulating a "force summed" redundant system.

DUAL, FORCE SUMMED ACTUATOR MODEL

The primary purpose in introducing an actuator that is force summed at the output is the significant improvement in failure transients experienced during either a failure in the drive electronics or within the actuator itself. The model is depicted in figure 69, and represents a dual configuration. The actuator can be mechanized as a dual tandem configuration which has in effect two power pistons on a single shaft, or as two separate actuators driving the steering linkage.

The model is typical of those used in aircraft actuation modeling, and has proven very accurate for use in performance prediction and design, as well as monitor design.

a. Load

Working from the right side of the diagram, $1/K_{steer}$ is a conversion factor from linear to angular units. The actual load is represented by a spring term K_L simulating the increasing force on the steering actuation as the wheel is turned. Some damping is provided in the term B_L. This is an arbitrary load, modeled to provide a suitable force on the actuators, and therefore to give a more realistic condition for the transients due to actuation failure.

b. Actuator

The two actuator force outputs F_1 and F_2 sum together to provide the total steering force. The actuators are designed such that either one could provide the steering force required to safely control the vehicle. The stiffness of the fluid/actuator combination is modeled as part of the force equation, and is represented by $/ L$, the bulk modulus over the fluid column length.

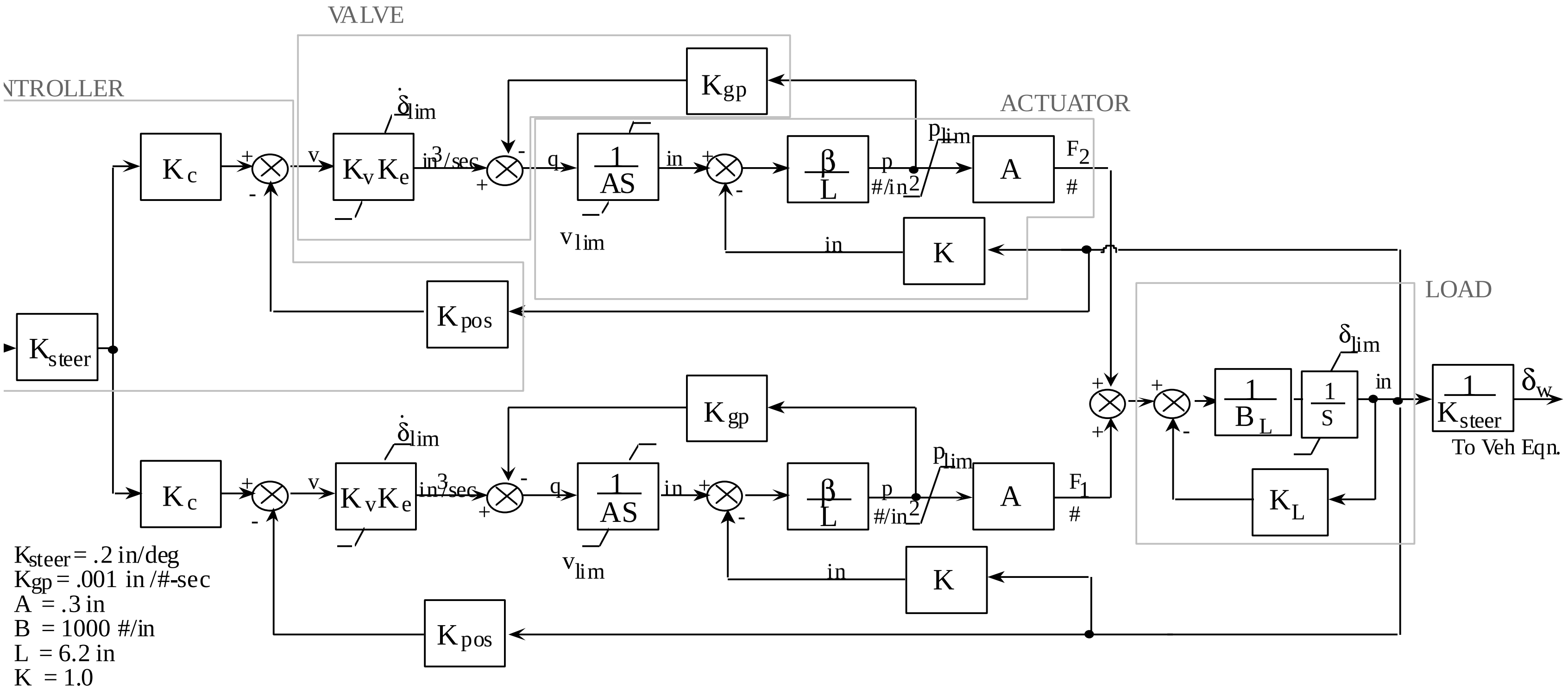
c. Valve

The valve is modeled as a simple flow gain term, modified by the load pressure through a pressure gain term. The assumptions here are operation around the null region of the valve, which is appropriate for slow steering commands, and some transient faults. A more detailed simulation with a nonlinear valve representation would yield very accurate results, and is standard practice for these types of hydraulic systems.

d. Controller

These terms represent scaling and loop error generation from the computer command and the position feedback sensor. Since the intent was not to optimize the control, no dynamic loop compensation was added. This is a relatively stable control loop, and only minimum compensation is anticipated. In any case, the transient performance will only improve.

Dual Force Summed Actuators



K_{steer} = .2 in/deg
K_{gp} = .001 in /#-sec
A = .3 in
B = 1000 #/in
L = 6.2 in
K = 1.0
K_{pos} = 1.6 v/in
K_v = 1.24 in /sec/ma
K_e = 8 ma/v

K_c = 1.6 v/in
K_L = 50 #/in
B_L = 0.5

p_{lim} = ± 1000 #/in
d_{lim} = ± 1.24 in /sec
(30°/sec)

v_{lim} = ± 6.2 in
d_{lim} = ± 6.2 in

The step response of each actuator system appears figure 70, below. In each plot the commanded steering angle is set equal to a constant 1 degree, and the actual steering angle is the response.

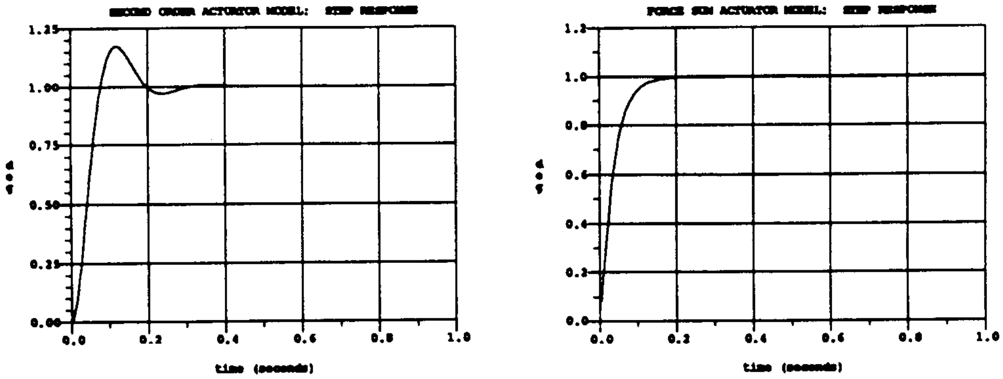


Figure 70. Actuator Step Responses

The plot at left shows the simple actuator and appears, as expected, to be a second order response. The force summed response, at right, approaches the step asymptotically. Note that the response of each of the individual actuators within the force summed system has nearly as tight a response, and if plotted would appear similar to that of the force summed at right.

ROAD

The "road" subroutine models the roadway, outputting the road heading as a function of the distance traveled. This road heading is not "known" by the vehicle itself, but is transformed via the equations of motion into the lateral position error.

The road heading is set before running the program, and is usually set as a straight road ($_r = 0$) or as an S-curve with specified length and width. No superelevation in the roadway is assumed. Note that for the feedforward control model, this subroutine will pass road curvature information to the controller.

WINDS

The "winds" subroutine models wind gusts and biases acting laterally on the vehicle. Wind disturbances can be modeled as step disturbances of magnitude

$$F_d = \tfrac{1}{2}\ {}_{air}V_{wind}^2 C_{D_{lat}} A_{lat} \qquad (23)$$

where

ρ_{air} = Atmospheric density at sea level (=0.0024 slug/ft^3),
V_{wind} = Wind velocity (ft/sec),
$C_{D_{lat}}$ = Lateral coefficient of drag (= 1.2), and
A_{lat} = Lateral area (= 41 ft^2).

The programmer specifies the speed of the winds and their duration, and the subroutine equations calculate the lateral force, outputting that value to the vehicle routine.

Error Analysis

As noted above, the primary purpose for creating this lateral motion model is to study the magnitude of position errors under both normal and dynamic actuator conditions.

In this context, health management analysis looks to the relationship between these errors. Normal operating errors in this study include position errors induced by turning through curves in the roadway and those induced by steady state winds and wind gusts. These position errors define monitor tolerance: any deviation from the lane-center less than or equal to these errors must be considered normal. In other words, a lateral deviation monitor which signals a failure must be higher than what we consider normal errors. Hence, with these normal errors established, the success of various AHS vehicles steering configurations during an actuator failure can be studied.

Actuator failures are simulated by setting one actuator onto the rate limit (30 degrees per second) in a dual-redundant system. Failures with both stand-by and force summed actuator models are evaluated.

In addition to the above error analysis, miscellaneous tests which are related to the lateral position of a single AHS vehicle are also performed. These tests relate to lane change, check-in, and sensor position.

NORMAL OPERATING ERRORS

Normal operating errors for this study include those lane-center deviations caused by winds and those caused by turning. These deviations, or errors, are calculated for both a basic controls design and for the "feedforward" controls design.

BASIC CONTROLS DESIGN

This design features one input to the controller: deviation from the lane-center. As described earlier, this deviation is read by the lateral position sensor and passes directly into the compensator, which calculates steering angle command.

a. S-curve

The S-curve is the basic turning maneuver implemented by the simulation. Figure 71 below, shows a plot of the position of the S-curve for this test (at left), and a plot of road heading vs. time as the car travels along the road.

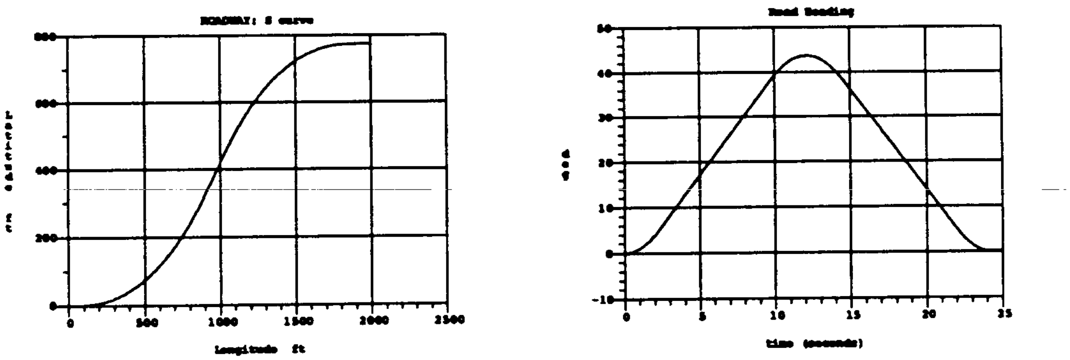


Figure 71. The S-curve

The forward velocity of the car for the basic scenario is 60 mph. (Most tests in this study use a forward velocity of 60 mph, but sometimes a 120mph forward velocity is employed. Unless otherwise specified the velocity is 60 mph.)

The size of the S-curve (as shown in the plot above) was determined so as to give the 60 mph car about .2 g's lateral acceleration. This acceleration, and hence the curve depicted here, is thought to be moderately severe, and should thus represent a good guess at the upper end of normal error levels. These errors will, in turn, define monitor tolerance for failure detection.

The five plots of Figure 72, below, shows the results of this run. The first plot (upper left) shows a time history of the steering angle ("Delta-W"). The plot shows that the car first turns left (positive steering angle) and then right (negative) in order to follow the S-curve. The maximum steering angles obtained are between 0.6 and 0.7 degrees. The periods of the plot where the steering angle is constant and near its maximum are referred to as "steady state" turning periods. Note that the plot contains two lines, one for commanded and one for actual steering angle. Here those lines are almost too close to distinguish.

The second plot of figure 72 (upper right) shows rotation rate of the vehicle about the z-axis. Rotation rate is one of the vehicle model states and closely correlates to the steering angle, which is a model input.

The third plot (middle left) shows vehicle lateral velocity, another state. Note that the integral of lateral velocity is only one term in the lateral position equation. This is because lateral position is relative to the road, while lateral velocity is relative to the alignment of the car. Hence, in the equations of motion for lateral position there is also a forward velocity times heading error term ($U\ _e$).

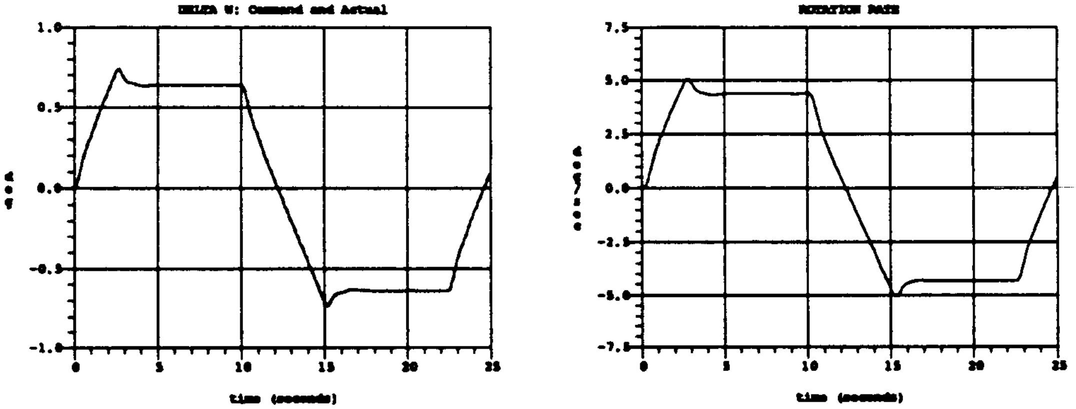


Figure 72a. S-curve Plots

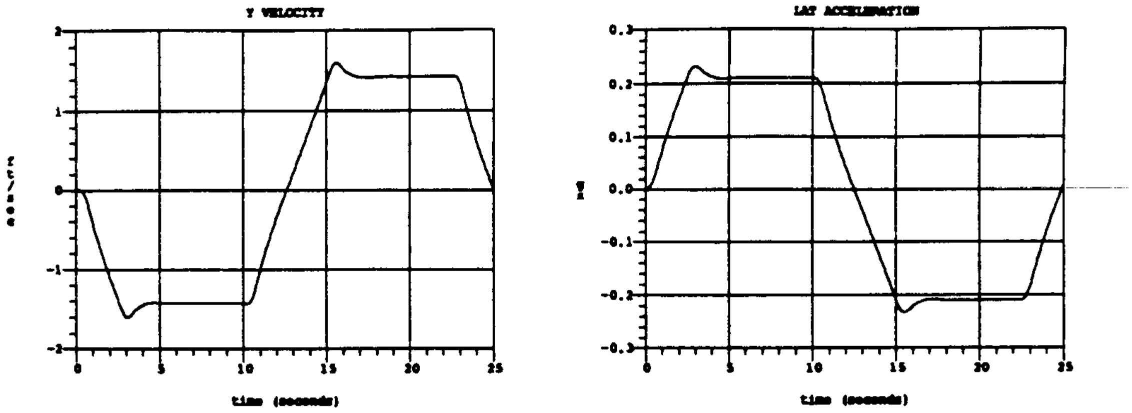


Figure 72b. S-curve Plots

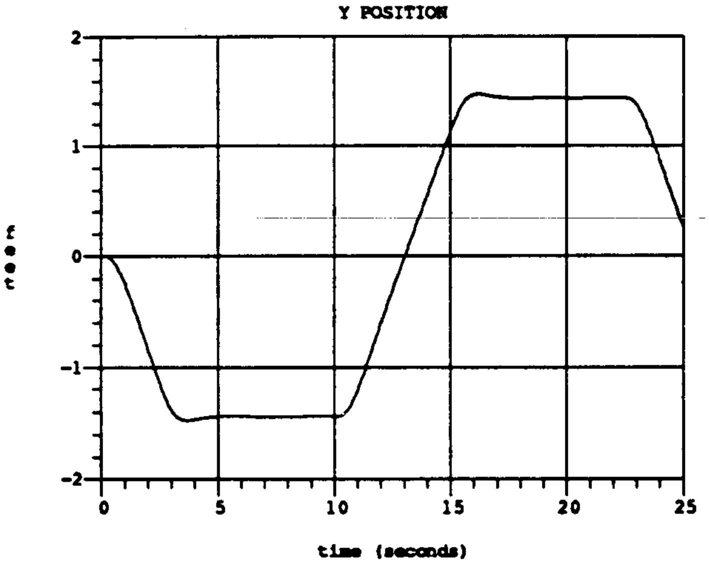


Figure 72c. S-curve Plots

The fourth plot (middle right) is lateral acceleration. Note that this plot is not simply the derivative of lateral velocity, which would be the vehicle's actual lateral acceleration, but is rather the centripetal acceleration as *felt* by the vehicle. In terms of actual motion, most of this acceleration is offset by the friction between the road surface and the tires.

During steady state turn periods the lateral acceleration has a value of approximately 0.2 g's. This value is taken to be a measure of the turn's severity.

The fifth and final plot (bottom) is lateral deviation, the key output of the run. For this run we see that maximum errors reach 1.5 feet. This error is quite large. since proposed maximum lane width corresponds to a maximum deviation of 1.0 foot. 1.5 feet, even under failure conditions, would be unacceptable.

Two possible solutions to this problem are 1) making roadway curves less severe and 2) making lanes wider. Neither of these solutions is desirable since AHS roadway is likely to be built over existing roadway and roadway curvature is then not so easily manipulable. Formulating a roadway curve for a 0.1 g lateral acceleration was a simple task, as acceleration is inversely proportional to radius of curvature. The plots in figure 73, below, show acceleration of the new, moderate 0.1 g curve and a time history of position.

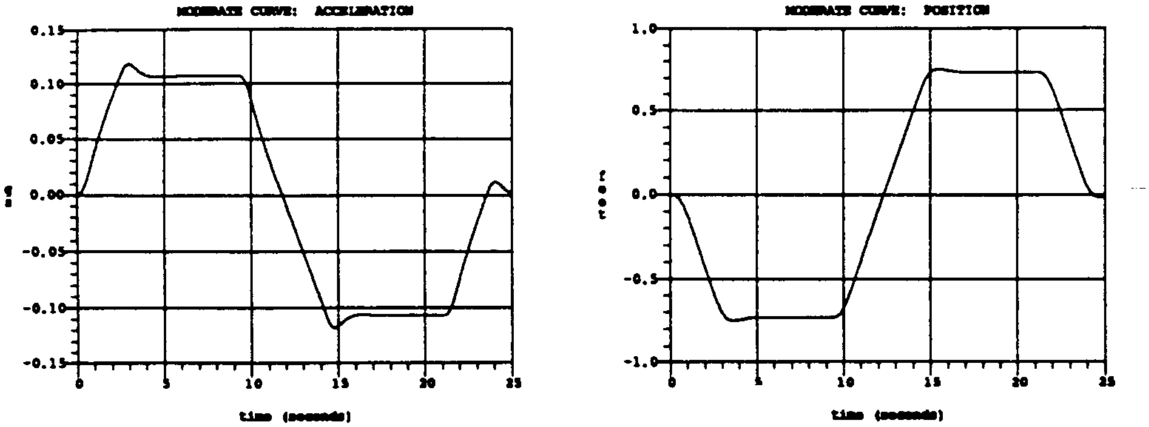


Figure 73. Moderate Curve

Note that the position deviations from the center of the lane are half the size, roughly proportional to the difference in lateral acceleration and radius of curvature. Hence, moderating the severity of curves would indeed be a way to solve the deficiencies of the position feedback-only controller. However, since AHS roadways are to be built on existing highway, this solution may not be an alternative.

Likewise, the solution of increasing lane width also runs contrary to AHS goals, as decreased lane size is one of the advantages AHS technology seeks to realize.

FEEDFORWARD DESIGN

As we have seen, the normal operating errors associated with the basic controls design are unrealistically high. The AHS system will need to have smaller lateral position errors, and a controls method which accomplishes this, as described in section 2-C, is the feedforward design. The feedforward design uses additional information, roadway curvature, in attempting to minimize position errors while controlling the vehicle. As we saw above, errors during turning were always proportional to lateral acceleration. Mathematically, we expect lateral acceleration to be proportional to $V^2 /$, where ρ is the radius of curvature of the roadway. Indeed we saw this result during the 0.1 g test. The feedforward design assumes that roadway radius of the curvature is known, and that the controller takes advantage of this information by compensating for expected lateral accelerations. Therefore, operating errors associated with turning are expected to be less.

a. S-curve

As expected, errors are significantly less. All things being equal, the feedforward design reduced errors by almost a factor of ten. Figure 74, below, shows steering angle and deviation for the vehicle going through the same 0.2 g S-curve used previously, but with the new controls design.

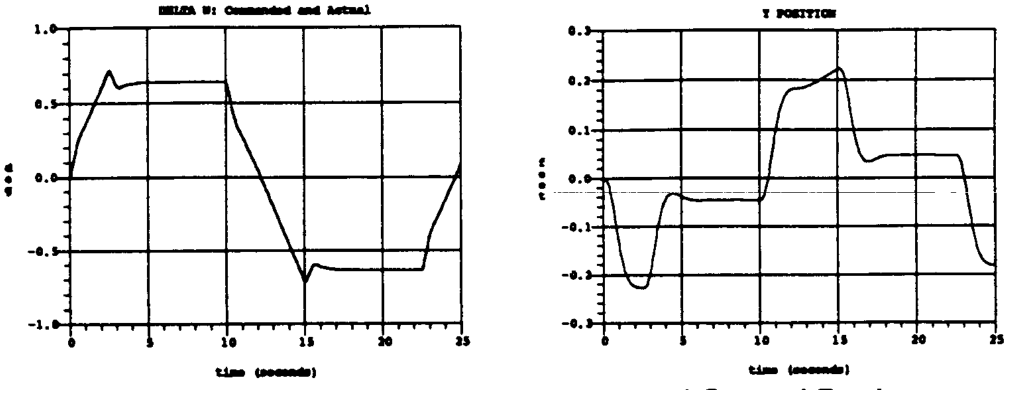


Figure 74. S-curve with Feedforward Control Design

Note that the highest errors occur during changes in lateral acceleration, whereas before the highest errors occurred during steady state turns (constant acceleration). This demonstrates how as new design works: roadway curvature information predicts a lateral acceleration for which the vehicle corrects.

In controls analysis, the high performance of the design is offset by its sensitivity to model parameter uncertainty. It is expected that actual errors in the feedforward design might grow to 0.5 feet.[11] Although this simulation does not attempt to simulate that sensitivity, overall errors are increased by implementation of a new lateral position compensator. The new compensator is designed with the same methodology as the old compensator(four-state, LQG/LTR synthesis methodology) but has increased stability near poles in the compensator frequency response. Such stability comes with the cost of increased position errors, but for our purposes the increased errors serve as a more realistic estimates of lane deviations in the feedforward design.

Figure 75 shows position errors and accelerations in this latest and "most realistic" controls design.

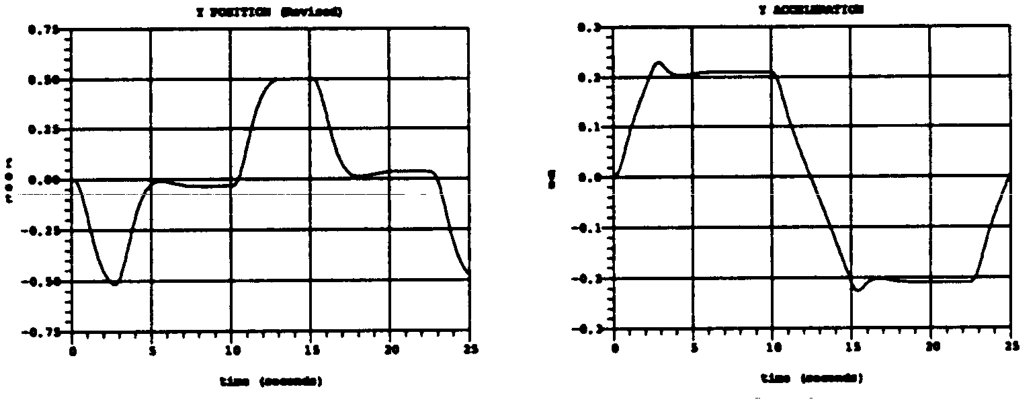


Figure 75. Results, Final Controls Design

Hence, maximum position for this controls design is approximately 0.5 feet, while maximum acceleration due to turns still depends on severity of the curves, and is taken to be about 0.2 feet.

b. Winds

These tests analyze the vehicle response to momentary wind gusts and steady wind biases. With knowledge of vehicle behavior under these conditions, failure monitors can be designed so as not to trip erroneously due to winds.

The modeled winds include two cases: a 0.5 second lateral wind of 50 mph and a 10 second wind bias of 25 mph. Figure 76, below, shows the forces acting on the vehicle due to these winds. The plot at left shows the wind gust and at right the wind bias.

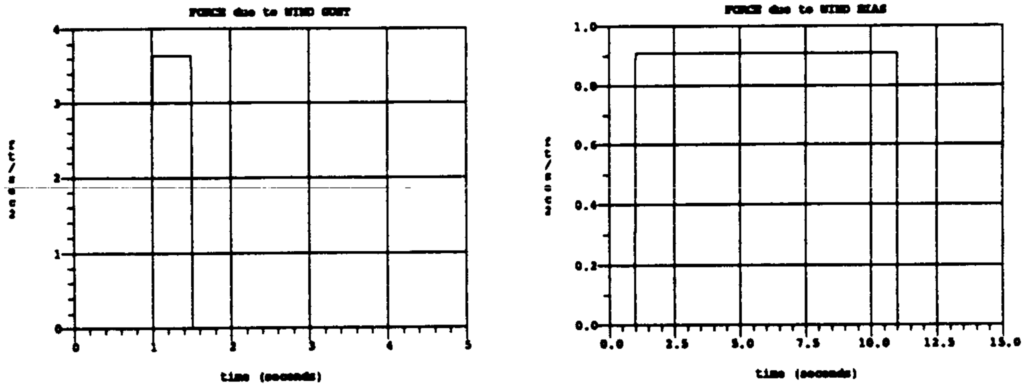


Figure 76. Winds

Steady-state position errors for these cases are 0.32 and 0.20 (figure 78). For the wind gust, a heading (crab) angle generated by a steady-state steering angle is needed to counteract the wind. As shown in figure 77, below, the wind causes an initial acceleration of .11 g's which then falls to zero as the vehicle compensates for the wind.

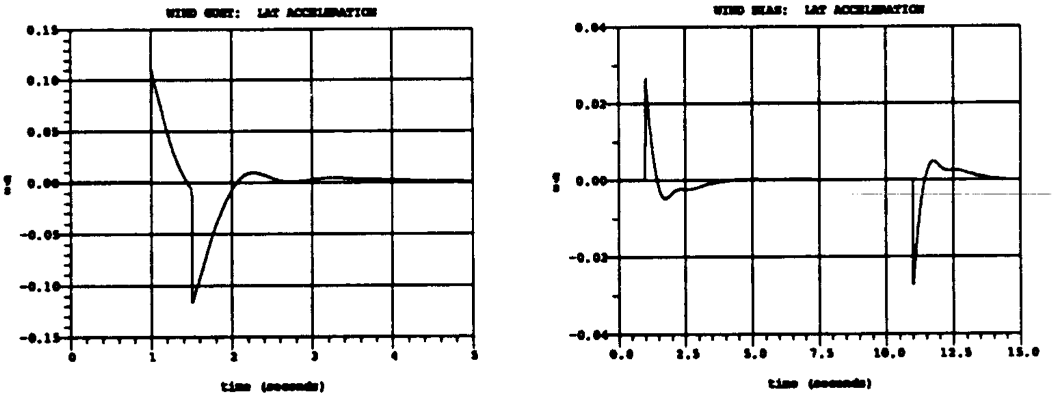


Figure 77. Accelerations due to Winds

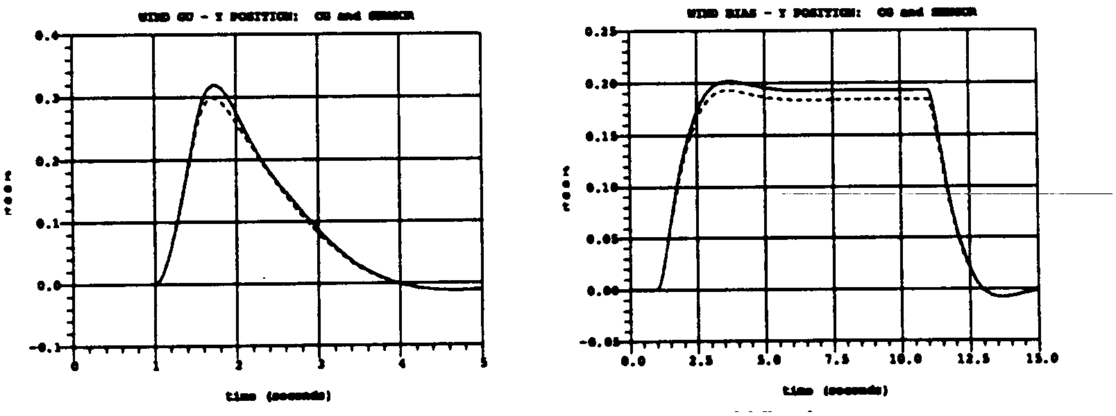


Figure 78. Deviations due to Winds

The position errors may pose significant challenges for failure mode analysis. These errors are less predictable than errors caused by roadway turns and at times errors due to winds and those due to turns may combine. Also, the 0.11 g acceleration due to the wind gust must be accounted for in any sort of monitoring of acceleration. In terms of mitigating these wind-based problems, Barrett's study points out that an accelerometer will be of little help, and hence a wind sensor might prove valuable. The accelerometer won't be able to detect winds since, as shown in figure 77, above, the lateral acceleration falls off quickly. A wind sensor, however, could possible allow the controller to compensate for winds.

CONCLUSION

Normal operating errors have been established for a "typical" system, which includes a controller with lateral position error and road curvature information, but no wind sensor. The highest expected lateral accelerations due to road curvature are 0.2 g's, and the corresponding lane deviations are 0.5 feet. Steering angle climbs up to 0.7 degrees in that scenario.

The highest anticipated wind gust disturbance acting directly on the side of the vehicle is 50 mph, lasting of 0.5 seconds. Under such a situation, a position error will have to be tolerated. Under the steady wind bias of 25 mph, the lane deviation is 0.2 feet. Profiles of resultant accelerations are shown in figure 77 above, with a maximum 0.11 g's.

All of these normal operating errors must be within monitor tolerance.

ACTUATOR FAILURES

These tests seek to determine how well the vehicle reacts to actuator failures and how failure detection can be made in order to keep the vehicle from deviating to unacceptable distances from the center of the lane. Detection may be based on lane deviation, lateral acceleration, and steering angle, as well as abnormalities within the actuator itself. Monitor of vehicle parameters must, of course, include tolerance for normal operating errors.

The steering actuator system is assumed to be dual redundant. In the first set of tests, a "stand-by" redundant model is employed. In the stand-by system, only one of the redundant actuators operates on the steering: the other is dormant but "stands by" in case the first actuator fails. In the second set of tests, we use a "force summed" redundant model. Here, both actuators operate on the steering at the same time, with the forces of each individual actuator sum together to create a total force acting on the system. (See above for detailed description of system.)

For each of the failure simulations in this study, the vehicle is assumed to be driving along a straight road

STAND-BY

The modeling of the actuator hardover failure for this test involves causing the steering angle command to begin ramping up along the rate limit at the time of failure. The rate limit is 30 degrees per second. This action models a hardover failure of the active actuator. At a specified time, the vehicle "detects" the failure, and the system switches to the stand-by actuator. Controls and steering are allowed to operate uninhibited, allowing the vehicle to recover from lane deviation caused by the failure. Nonetheless, deviation from the center of the lane continues to grow while the car makes its recovery.

Figure 79, below, illustrates the car's reaction to a failure with a detection time of 0.1 seconds. The failure occurs at 1.0 seconds; the detection at 1.1 seconds. At left are plots of steering angle command (solid) and actual steering angle (dashed). Notice the steering angle ramps up along the rate limit and reaches an angle of 3 degrees at the time of detection. At that point the steering angle ramps down at the rate limit toward the commanded (desired) steering angle as determined by the controller.

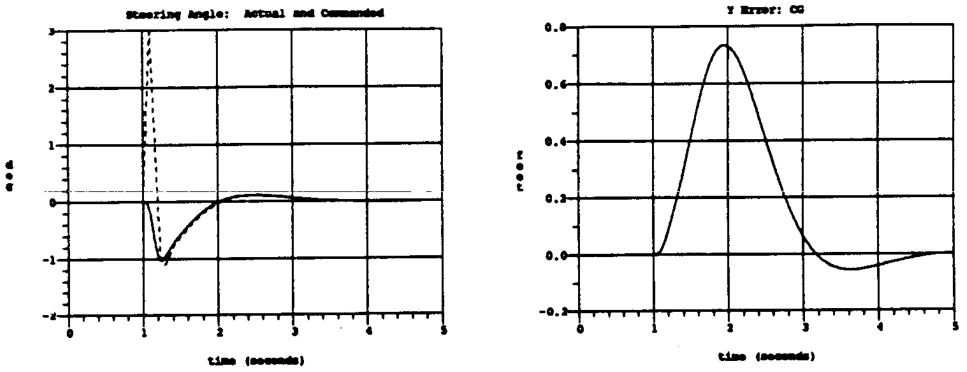


Figure 79. Steering Angles and Position Error for Actuator Failure and Detection

The plot at right shows position error at the vehicle cg. Note that at the 0.1 second time of detection the error is still small, and only during the full second as the vehicle recovers does the error climb to 0.7 feet. In addition to this total deviation, the deviation of the vehicle at the time of detection is also important, as it represents the hypothetical "trigger" of the failure detection. Here, that value is 0.015 feet. Hence, if the failure monitor level were in reality 0.015 feet for this specific vehicle, the net error would be 0.7 feet.

a. Lane position as monitor

This set of tests was completed by simulating a family of failures, increasing the time of detection for each run under otherwise the same conditions. In this way, we generated a plot of total deviation vs. failure detection level. See figure 80, below.

Note that increased time of detection increases the probability that the anomaly is a true failure, therefore decreasing false alarms. On the other hand, the transient due to the failure increases, impacting roadway width and ultimate controllability.

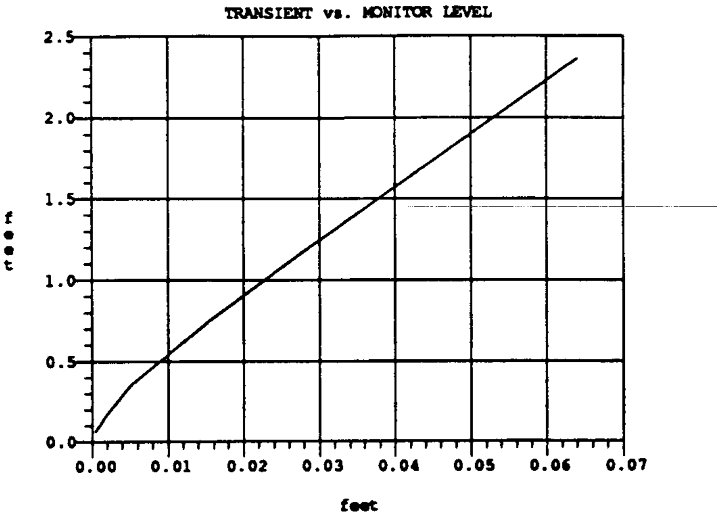


Figure 80. Total deviation vs. Monitor level

If the maximum allowable error is equal to the sensor width, and that value is 1.5 feet, that would mean the failure detection level would have to be 0.035 feet. This value is far below normal operating errors and indicates that for a stand-by system, actuator failure detection cannot be based on a position monitor alone.

b. Alternate rate limits

Note that in these tests a high rate limit will cause the errors to grow more rapidly during the failure, but will also allow the car to correct more rapidly upon detection. Conversely, a lower rate limit will results in slower developing errors, but will force a weaker response by the car. This trade-off was examined in a series of tests using both lower and higher rate limits than the normal 30 degrees per second. Rate limits of 15, 20, 25, 35, and 40 degrees per second were tested in the context of actuator failures. None of these rate limits was found be more effective at reducing total transients across the range of detection times as the 30 degree per second rate limit. The smaller rate limits of 15 and 20 degrees, which allow for significantly slower ramping of the steering angle during failure, actually showed demonstrably worse results. Hence, 30 degrees is a desirable rate limit, and rate limit modification will apparently not improve the stand-by system actuator failure response.

c. Acceleration as monitor

Another possible solution is to use lateral acceleration as a monitor. We can easily examine the practicality of using acceleration by plotting the total transient vs. acceleration at time of detection rather than deviation at time of detection. See figure 81, below.

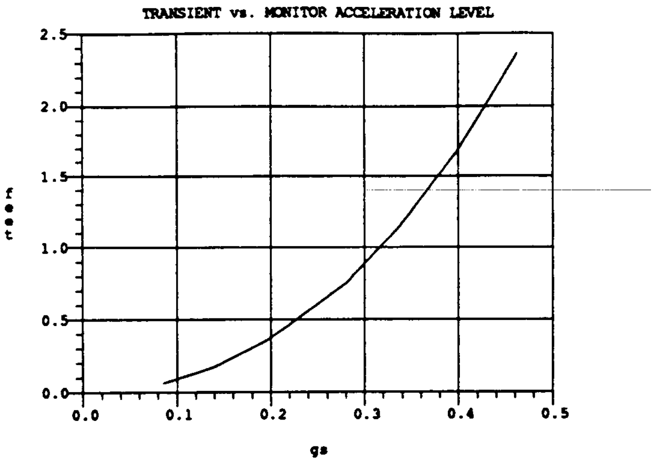


Figure 81. Total Deviation vs. Acceleration Monitor Level.

Note that to keep the maximum transient at 1.5 feet, a detection level of about .36 g's would need to be employed. To keep the transient under 1.0 feet, a detection monitor of about .31 g's is desired.

This level appears to be above the normal operating errors for turns and winds, and shows that in the stand-by case acceleration is indeed a more appropriate monitor parameter than initial deviation.

FORCE-SUMMED

The failure for an actuator in the force summed model, which is more complex then the stand-by model, is initiated by allowing maximum flow through the valve of one of the actuators in the two-actuator system. The maximum flow limit was initially modeled to give the actuator as a whole a steering angle rate limit of approximately 30 degrees per second. Hence, by allowing maximum flow we are putting the actuator "on the rate limit". As noted, this rate limit is by design similar to that of the simpler model.

When the one actuator fails in the force summed system, the other attempts to compensate. This action can be discerned in the plot of actuator forces (figure 82) for the first failure run. In this run, failure occurs at time = 0.1 seconds. Note that the force of actuator 1 (solid line) begins rising at a constant rate.

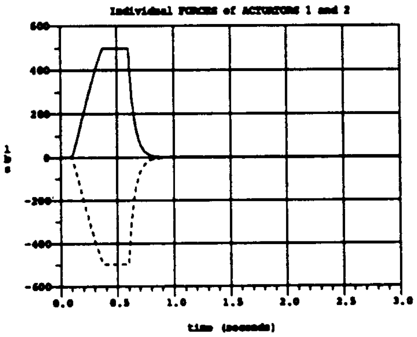


Figure 82. Forces of Actuators during Failure

When the force on actuator 1 rises, actuator 2 (dashed line) begins to compensate. Though there is some lag, the actuator 2 force is opposite and nearly equal to the actuator 1 force. At approximately time = 0.4 seconds, the force hits a limit at 500 lbs. This limit is caused by the 1000 lbs/inch pressure limit acting on the 2 inch actuator surface. Note that this limiting of actuator 1 force allows the actuator 2 force to "catch up" and fully offset the failure induced force on actuator 1. This full compensation is reflected in the fact that the steering angle falls back to zero at this time. Figure 83, below, shows steering angle.

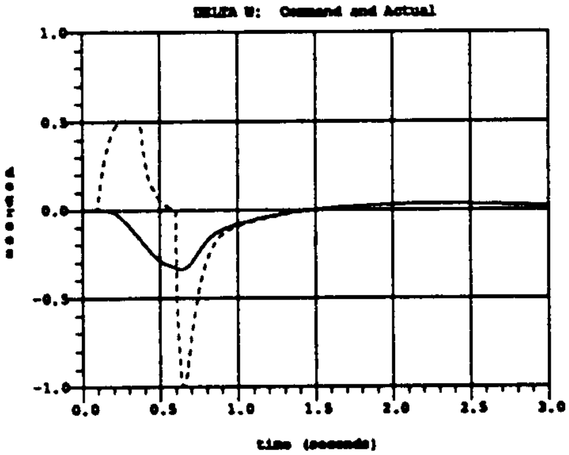


Figure 83. Steering Angle during Failure

Note that during the time while the forces are ramping up (time = 0.1 to 0.4 seconds), the steering angle is also ramping up. During this ramping, the steering angle slowly reaches the level which corresponds the difference in force between actuator 1 and actuator 2. Remember that this difference is due to the time lag inherent in the system between actuator 1's failure and actuator 2's response to the failure. The net force from the actuators acts on the spring nature of the load creating an equilibrium condition at 0.5 degrees. Of course, a constant steering angle of 0.5 degrees is not exactly desirable, since it indicates that the vehicle is still turning *away* from the center of the lane.

As noted, when the forces reach the pressure limit, the lag disappears and they are equal. This causes the steering angle to begin falling off to zero, reflecting the zero force acting on the spring between the actuators and steering angle. Note that at zero steering angle the vehicle will still be veering away from the center of the lane since it has already built up a heading error between itself and the roadway. Actuator 2 cannot make up for this difference by exerting greater force than actuator 1 since it, too, is at its maximum value.

The vehicle stays locked in this condition until the failure detection at time = 0.6 seconds. At detection, actuator 1 is switch off, and its force falls quickly (though not instantly) to zero. Actuator 2's force follows, but during this time it now has the lee-way to correctly compensate for the vehicle's lane deviation. Hence, the force on actuator 2 is here slightly greater than that on actuator 1, causing the steering angle to jump down to as far as -1.0 degrees, correcting the vehicle's heading and later steering it back to the center of the lane. Figure 84, below, shows vehicle deviation from the lane center.

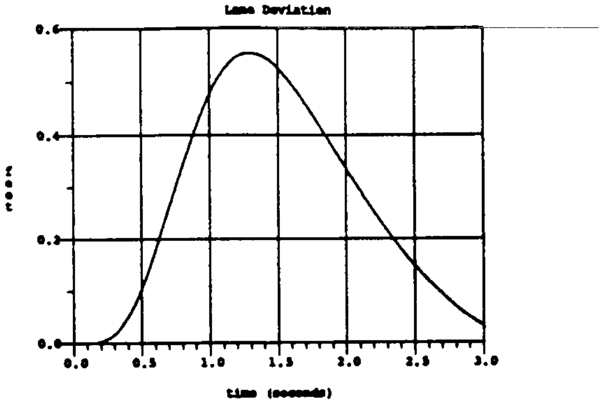


Figure 84. Vehicle Deviation during Failure

The maximum deviation for this run is approximately 0.55 feet. This value is well below the 1.0 foot maximum. A family of similar runs with varying detection time completed this test, the results of which are represented in figure 85, below. The plots show total deviation vs. detection time and vs. detection position.

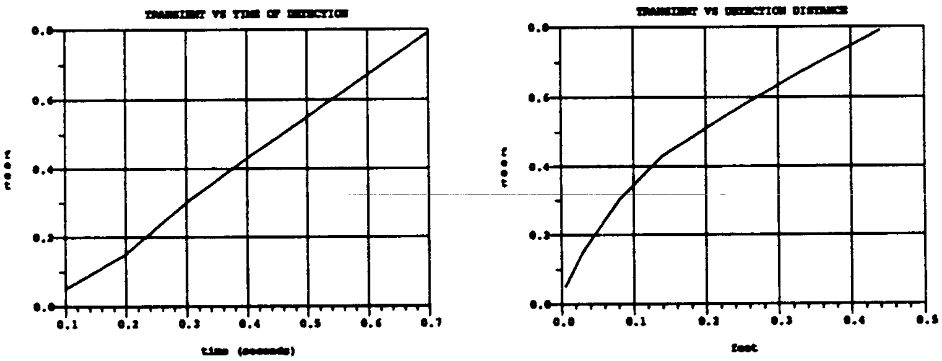


Figure 85. Force-Summed Failure Results

Note the transient never reaches the critical limit of 1.0 feet. Hence, we cannot be certain the of the exact detection deviation (plot of right) necessary to keep the vehicle from reaching the critical 1 foot distance. We do know that the detection deviation will be at least 0.45 feet, which approaches the maximum normal operating error of 0.5 feet. The reason that detection time runs of greater then 0.7 seconds were not run, however, is that it is expected that within this time the sensor itself would have detected the failure and switched itself off. We expect failure detection from internal actuator sensors within 0.5 seconds, and at that time, as shown in the plot at right in figure 85, the lane deviation is only 0.55 feet.

The above results essentially demonstrate that the dual redundant, force summed actuator system would be successful in the single actuator hardover scenario at 60 mph. With this success, another test was run at 120 mph. The results of this test are shown in figure 86, and show similar success.

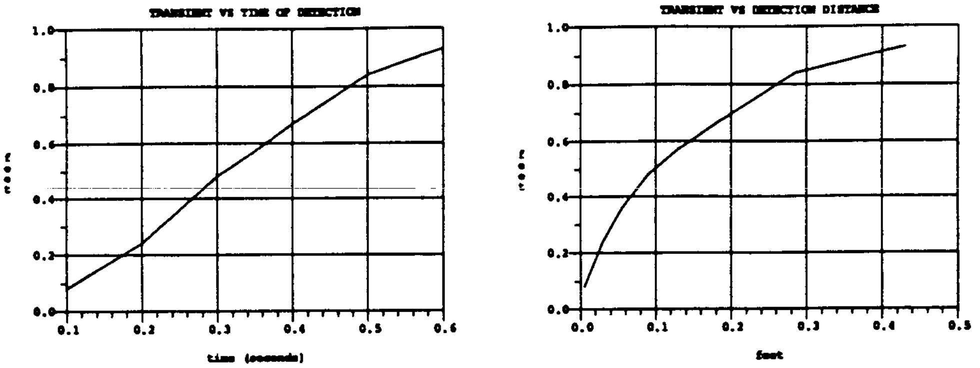


Figure 86. Force Summed Failure at 120 mph

Hence, at the time = 0.5, we expect the transient to be an acceptable 0.85 feet. The deviation plot at right is similar to the corresponding plot in the 60 mph scenario. The required detection deviation would be near the 0.5 feet, which is very near the maximum normal operating error.

The force summed redundant system demonstrates a significant improvement over the stand-by system, which is demonstrated by the systems' responses to failures. In allowing for detection times of 0.5 seconds and greater, the force summed system is orders of magnitude more proficient in this scenario, and, if the probability of both actuators in the system failing is significantly small, appears feasible as a safe actuator design.

MISCELLANEOUS TESTS

VARIOUS SENSOR LOCATIONS

This test seeks to determine what advantage can be gained by locating the position sensor further towards the front of the car. If such a placement could reduce the general lateral deviation, it would be logical to assume that such would be the placement of the sensor in the actual vehicle.

Both the AHS vehicle with sensor location at the axle and the same vehicle but with the sensor location at the bumper are put through the standard S-curve.

Keep in mind that each time a model parameter, such as sensor location, is changed, the compensator model needs to be re-calculated. This is not a problem for the actual vehicle since vehicle parameters will be constant.

The results for the sensor location tests are surprising at first but logical upon second glance. Vehicle performance remained unchanged with the forward sensor location. The two plots below (figure 87) show position errors of the sensor(dashed) and cg(solid) for the two vehicle configurations.

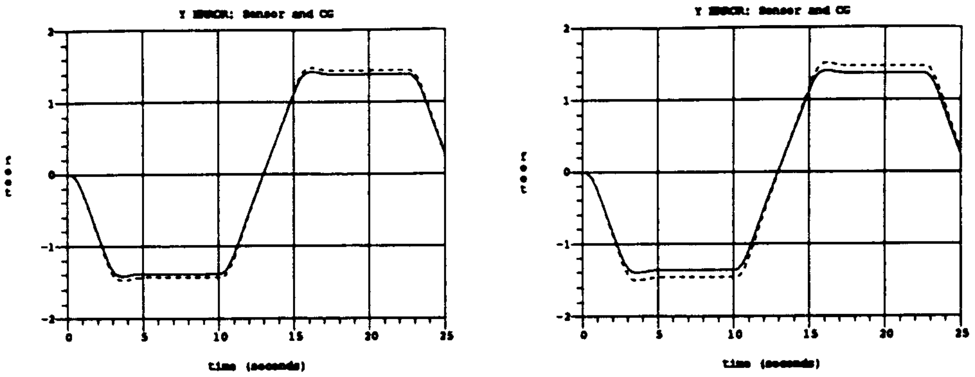


Figure 87. Position Errors for Axle and Bumper Sensor Locations

The plot at left in figure 88 shows rotation rate as a function of time and indicates that the steady state position errors occur during continuous turning periods.

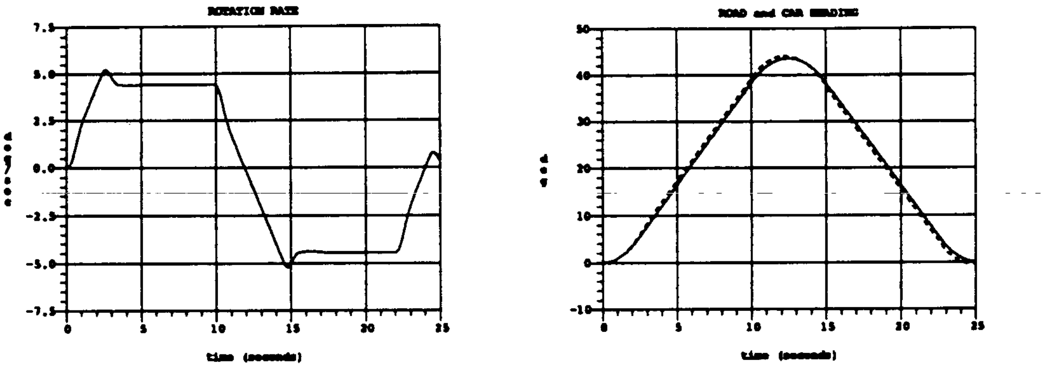


Figure 88. Rotation Rate and Heading for S-curve Maneuver.

Notice in figure 87 that the difference between sensor distance and cg distance in the plots above is greater for the bumper-sensor vehicle. This is expected since the bumper sensor is further from the cg than the axle sensor. Note also, however, that during the steady state turns, it is the sensor which is closer to the center of the lane. This appears to be the correct result, as the vehicle is attempting the narrow the gap on the continuously turning road. The vehicle, as evidenced by the dashed line in the figure 70 heading plot, has a greater heading then the road (solid) during the steady turn. It is therefore expected that the front of the vehicle would be closer to the center of the road then the rest of the car. As a result the remainder of the car is further away form the center line.

Another way the explain the result is that the controller inputs and is dependent on the sensor error, and has no knowledge of the cg error. In conclusion, this study indicates that sensor location on the car has little effect on controller performance.

A more in depth controls study, focusing on such problems as sensor sensitivity to white noise and other errors, is not included here and remains an area of concern.

CHECK-IN

This test seeks to determine what the dimensions of a check-in S-curve need to be to adequately test the vehicle. Tests have been completed for both full speed vehicle and on-ramp speed (20-30 mph).

The vehicle is put through S-curves of 0.5 x 30 feet, 1 x 30 feet, and 3 x 30 feet. Modeling the S-curves was easily accomplished in the road subroutine where the S-curve size is parameterized.

The plots below (figure 89) show y-acceleration and y-error for the 0.5 x 30 case.

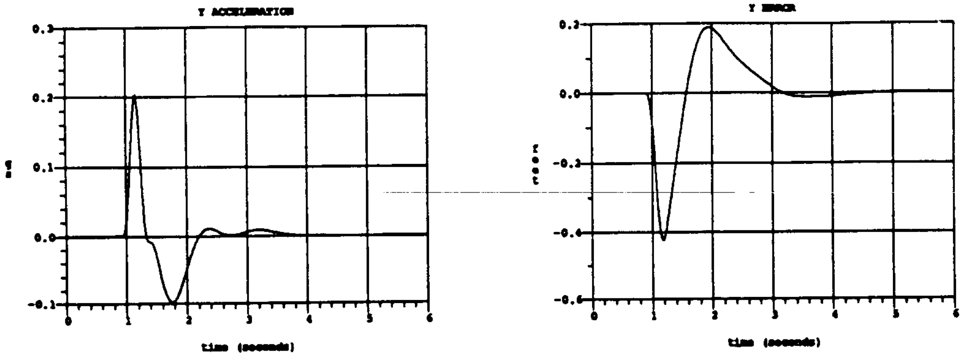


Figure 89. Check-In S-curve.

For proper testing forces the vehicle should be at 10 to 25 percent of normal operating forces. It appears from the plots that adequate forces on the vehicle for testing purposes. Another area of concern in this study is the acceleration changes ("jerk") experienced within the vehicle. There are certain limits on jerk placed on the vehicle due to discomfort by the passengers. High values on jerk are easily attainable on small S-curve designs on on ramp check-in maneuvers. Figure 90, below, shows jerk for the normal sized S-curve used in the normal operating error studies.

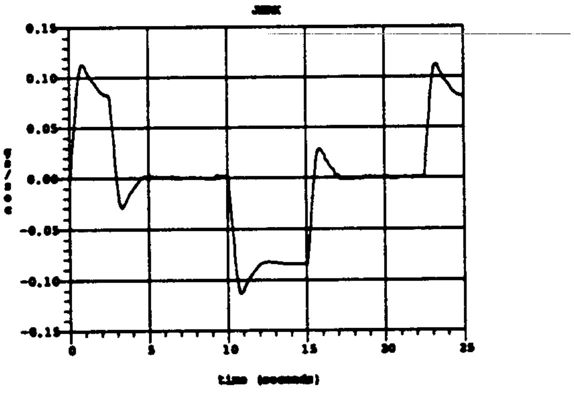


Figure 90. Jerk During Moderately Severe S-curve

LANE CHANGE

We completed a set of runs which attempted to model a vehicle lane change maneuver, attempting to discover the best way to achieve a lane change and some of the problems and parameters associated with that maneuver.

All models assumed that the lane centers were 10 feet apart, that the vehicle velocity was 60 mph, and that the lane roadways were straight.

The first model initiated a lane change maneuver by placing a 10 foot error on the sensor reading, as if the vehicle sensor could read its displacement from the future lane. For the sake of this test it was assumed that the position sensors sense the center line, even at this distance. Nonetheless, this test failed because the steering angle ramped up so high in attempting to close the 10 foot margin that it intersected the adjacent lane at nearly a perpendicular angle.

The second model involved a series of runs in which the vehicle was commanded to some initial heading which steered it towards the new lane. Upon achieving the commanded heading, the steering angle was set to zero in order to maintain that constant heading. Upon reaching a distance of 1.5 feet from the new lane center, the steering controls were switched back on, allowing the vehicle to position itself back on the center of the lane.

This second model suffered from a problem similar to that of the first. At the critical 1.5 feet distance, the vehicle was already heading towards the new lane center. Yet when the controls were switched on at that point, the compensator's initial reaction was to increase the steering angle in order to steer more towards the lane. Hence, the vehicle heading increased, and the vehicle severely overshot the lane center.

This controls problem is an area of concern. It is beyond the scope of this study and perhaps suggests that an alternate method of lane change should be used.

Such an alternate method is the third model of this set. This model involves pre-programming an S-curve within the vehicle to be used as a lane change maneuver. Hence, the vehicle guides itself with a guess of where it should be. Such guidance could be assisted by accelerometers and or gyros on board to navigate the vehicle. In any case, when the vehicle has finished its pre-programmed maneuver, it switches back to the center-lane based control. The situation at that point is anomalous to the vehicle having some initial displacement in position and perhaps heading, rate, and lateral velocity. Runs performed under this study which simulated such initial displacements showed that the vehicle could easily control itself back to the center of the lane.

Lateral Margins for False Alarm

Introduction

The purpose of this part of the study is to determine the margin of failure detection in lateral position error necessary to avoid excessive false alarms when detecting failures in the lateral control system.

Background

REQUIREMENTS

We assume a false alarm rate of 5 percent. Assuming a failure rate of 10^{-6}/hour, that implies a false alarm probability of less than $5*10^{-8}$.

MODELS

VEHICLE

The vehicle chosen for the study was a 1984 Honda Accord. As documented elsewhere, the basic parameters are:

mass	1300 kg
moment of inertia about vertical axis	1629 kg*m^2
distance from CG to forward axle	1.00 m
distance from CG to back axle	1.45 m
distance from CG to lateral sensor	1.87 m
forward cornering stiffness	32.6 kN/rad
back cornering stiffness	27.1 kN/rad
forward speed	27.1 m/s
lateral coefficient of drag	1.2
lateral area	3.81 m^2

The following parameters are estimated for use in the models below:

tread width	1.52 m
suspension unsprung mass per wheel	45.4 kg
suspension stiffness	17.5 kN/m
tire stiffness	175 kN/m

suspension damping	0.3

WIND

As documented elsewhere, the force due to wind is given by the following:

$$F_d = \tfrac{1}{2} \; V^2 C_D A \qquad (24)$$

where:

F_d	force (slugs)
	density at sea level (slug/ft^3)
	= 0.0024
V	wind speed (ft/s)
C_D	lateral coefficient of drag (unitless)
A	lateral area (ft^2)

The worst-case wind speed was chosen to be V = 80 kph, which is compatible with the other studies. This roughly represents a 1 percent extreme wind speed. Thus we have:

V	= 22.6 m/s (74 ft/s)

An alternative would be V = 52 * 0.723 mph, where 52 mph is the 1 percent risk hourly wind speed in Shemya, Alaska normalized to 50 ft altitude, and 0.723 is the normalization ratio to normalize to 5 ft altitude from 50 ft altitude for daytime. (Adapted from the literature; tables 4-5 and 4-19.[19])

TURBULENCE

Turbulence is defined as the moment to moment variation in wind speed about the mean wind speed. The force equation is:

$$F_d = \; V C_D A \cdot v \qquad (25)$$

where everything is defined as in the wind model, with the addition of:

v	turbulence intensity (ft/s)

The turbulence intensity is modeled as a second-order linear filter applied to white noise with the form:

$$x_1\!\!\acute{Y} = -\frac{x_1}{L} + \frac{}{\sqrt{L}} dW$$

$$x_2\!\!\acute{Y} = -\frac{x_2}{L} + \frac{x_1}{L} \qquad (26), (27),$$

$$v = \sqrt{3} x_1 + (1 - \sqrt{3}) x_2$$

(28)

where:

dW	pure white noise
	root-mean-square gust velocity *v* (ft/sec)
L	integral scale (sec)
	= 1000 ft / vehicle-speed
	= 11.26

This model yields the power spectral density:

$$(\Omega) = \frac{{}^{2}L}{2}\,\frac{1+3\Omega^{2}L^{2}}{(1+\Omega^{2}L^{2})^{2}} \qquad (29)$$

where:

	wave number (rad/unit)

which is presented in equation 10-3,12 of the literature.[7]

The probability distribution of the root-mean-square gust velocity at 0-10,000 ft altitude, which closely fits the equation:[7]

$$f(\ ) = 0.54e^{-0.54} \qquad (30)$$

where:

f( )	probability density of gust intensity (1/(ft/sec))

The resulting plot is given by the following.

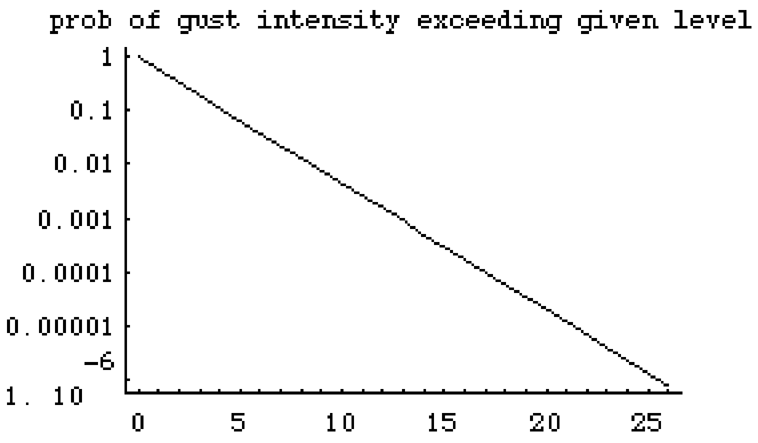


Figure 91. Probability of Gust Intensity Exceeding Given Level

From this we choose the 1 percent extreme gust intensity which is given by σ = 2.74 m/s (9 ft/s) as our worst case gust intensity for 0-3048 m (0-10,000 ft) altitude.

Another choice would have been the 10^{-6} extreme gust intensity given by σ = 26 ft/sec.

That value is then normalized to a 5 ft altitude using the factor of normalization 0.662 given in Table 4-19 of the literature for the ratio of wind speeds at greater than 300 ft to wind speeds at 5 ft during the daytime.[19] The result is:

σ	= 1.82 m/s (5.958 ft/s)

A discrete simulation yielded the following time trace of the wind force in slugs (divide by 8.7 to get ft/sec).

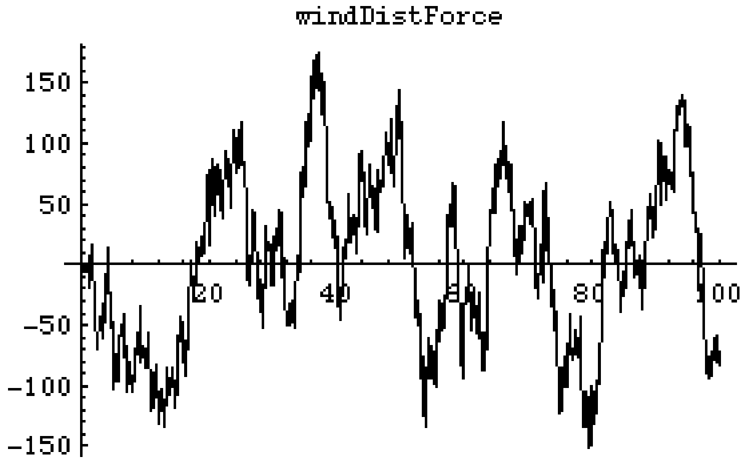


Figure 92. Wind Force

SUPERELEVATION FORCE

Superelevation is the lateral slope of a road. It is used on curves to counter the centrifugal force of the turn when made at the design speed. The force equation is given by:

$$F_d = \frac{gM}{w} Z \tag{31}$$

where:

F_d	force (slugs)
g	gravity (ft/sec^2) = 32.17
M	mass of vehicle (slugs) (see above)
w	tread width (ft) (see above)
Z	lateral height difference of vehicle (ft)

The worst case superelevation is assumed to correspond to a 0.1 g turn, or a lateral height difference of 0.5 ft:

Z = 0.152 m (0.5 ft)

ROAD DISTURBANCES

Equation 5-1 in the literature states that the power spectral density (PSD) of road elevations is given by:[10]

$$G(\;)=\frac{G_0}{(2\;)^2}\frac{1+(\;_0/\;)^2}{\;^2} \qquad (32)$$

where:

G0 roughness (ft^2/(cycle/ft))

= 1.25*10^{-5} rough road

0 length cutoff (cycle/ft)

= 0.02 PCC (Portland Cement concrete)

This is for the longitudinal direction. The ratio of the PSD of the lateral height deviation to the PSD of the longitudinal direction is shown in figure 93. A fit can be attained for a rough PCC road by using the PSD form:

$$G_r(\;)=\frac{G_0}{(2\;)^2}\frac{\;_0^2+\;^2}{\;_r^4+\;^4+(4\;_r^2-2)\;_r^2\;^2} \qquad (33)$$

where:

r lateral cutoff (cycle/ft)

= 0.006

r lateral damping

= 4.0

A plot both of the longitudinal PSD and the lateral PSD is as follows. The solid line is lateral and the dashed line is the longitudinal. Note that the PSD's above are two-sided (include contributions from positive and negative wave numbers) whereas the plots are one-sided (e.g. , show the sum of the positive and negative contributions).

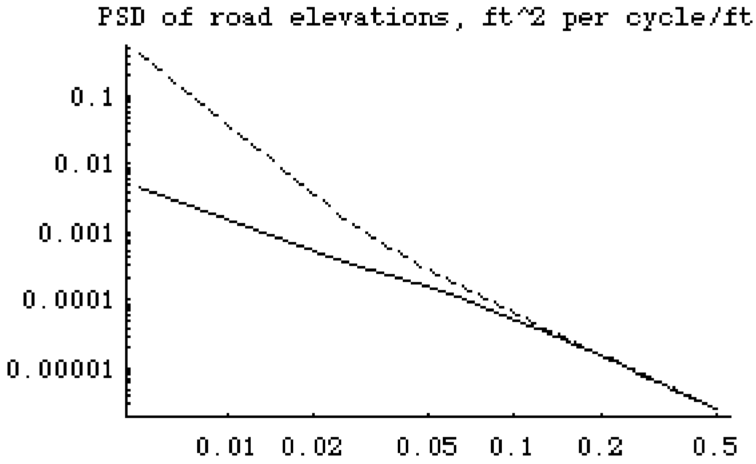


Figure 93. PSD of Road Elevations

After scaling to use time instead of distance, the resulting linear system has the form:

$$\acute{\dot{v}} = -2 \quad _r \quad _r v - \quad _r^2 x + \sqrt{G_0} dW$$

$$\acute{\dot{x}} = v \qquad \text{(34), (35),}$$

$$z = v + \quad _0 x$$

(36)

where (note that all these have been rescaled from cycle/ft to rad/sec using the road speed defined above):

Z	lateral height difference of vehicle (ft)
dW	pure white noise
G0	roughness (ft^2/(rad/sec))
	= 0.00111 rough road @ 88.8 ft/sec
0	length cutoff (rad/sec)
	= 11.16 PCC @ 88.8 ft/sec
r	lateral cutoff (rad/sec)
	= 3.35 @ 88.8 ft/sec
r	lateral damping (unitless)
	= 4.0

The resulting standard deviation for the lateral road deviations is 0.00488 m (0.016 ft).

A discrete simulation yielded the following time trace of the road lateral deviation in feet for 100 seconds of travel.

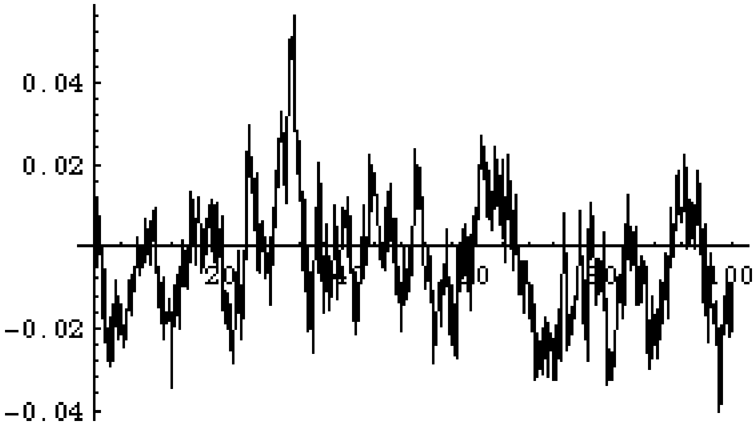


Figure 94. Road Lateral Deviation

LATERAL STEERING

The lateral steering dynamics model used is based on the literature.[21] These are:

$$vÝ = -2\frac{C_r - C_f}{MU}v + (2\frac{bC_r - aC_f}{MU} - U)r + \frac{C_f}{M}\ {}_w + \frac{1}{M}F_d$$

$$rÝ = 2\frac{bC_r - aC_f}{I_z U}v - 2\frac{b^2 C_r + a^2 C_f}{I_z U}r + 2\frac{aC_f}{I_z}\ {}_w$$

$$yÝ = v + U(\ \ - \ {}_r) \qquad (37), (38), (39), (40), (41)$$

$$Ý = r$$

$$y_s = y + c(\ \ - \ {}_r)$$

where:

v	lateral velocity (ft/sec)
r	rotation rate (rad/sec)
y	lateral position (ft)
	heading (rad)
y_s	lateral sensor position (ft)
${}_w$	steering angle (rad)
F_d	lateral disturbance forces (lb)
${}_r$	road heading (rad)
M	mass (slugs)
	= 89.09
U	forward speed (ft/sec)
	= 88.8
I_z	vertical intertial moment (slug-ft^2)

	= 1200
a	distance to forward axle (ft)
	= 3.28
b	distance to back axle (ft)
	= 4.77
c	distance to sensor (ft)
	= 6.12
C_f	forward cornering stiffness (lb/rad)
	= 7321.5
C_b	back cornering stiffness (lb/rad)
	= 6084

CONTROL

The control used is a four state filter using lateral sensor position to generate a command steering angle and is a preliminary design by one of the authors.

$$x\acute{Y}_c = Ax_c + By_s$$
$$_{wc} = Cx_c + Dy_s \qquad (42), (43)$$

where:

x_c	control state vector
y_s	lateral sensor position (ft)
$_{wc}$	commanded steering angle (rad)

$$\left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{cccc|c} -3.96312 & -97.0842 & -665.200 & -4169.00 & -663.8 \\ -0.0374909 & -6.6366 & -319.265 & -1977.76 & -318.9 \\ 1 & 0 & -32.8662 & -113.141 & -32.87 \\ 0 & 1 & -7.93138 & -48.5401 & -7.931 \\ \hline 0.00330586 & 0.0630439 & 0.00872665 & 0.649545 & 0 \end{array}\right]$$

ACTUATOR

The actuator model used is:

$$\ddot{Y}_w = -2\ {}_0\ {}_0\acute{Y}_w - {}_0^2\ {}_w + {}_0^2\ {}_{wc} \qquad (44)$$

where:

$_w$	steering angle (rad)

wc	commanded steering angle (rad)
	actuator frequency (rad/sec)
	= 30
0	actuator damping
	= 0.5

SUSPENSION

The suspension model is based upon the quarter-car model presented in the literature, chapter 5.[10] The linear model is:

$$M_s \ddot{z} + C_s \dot{z} + K_s z = C_s \dot{z}_u + K_s z_u$$
$$M_u \ddot{z}_u + C_s \dot{z}_u + (K_s + K_t) z_u = C_s \dot{z} + K_s z + K_t z_r \qquad (45), (46)$$

where:

z	height of sprung mass (body) (ft)
z_u	height of unsprung mass (wheel) (ft)
z_r	height of road (ft)
M_s	sprung mass (slugs)
	= *M*/4 = 22.27
M_u	unsprung mass (slugs)
	= 100/g = 3.108
K_s	suspension stiffness (lb/ft)
	= 1200
K_t	tire stiffness (lb/ft)
	= 12000
C_s	suspension damping
	= 98.1

All values are either for the 1984 Honda Accord, or nominal values from the reference, except for the suspension damping, which was chosen so as to generate a typical suspension damping ratio of 0.3.

The resulting suspension has a natural undamped frequency of 1.11 Hz, a damping ratio of 0.3, and a wheel hop undamped frequency of 10 Hz.

Results

ERROR IN ROAD FOLLOWING

The following simulation run shows the time trace of the lateral sensor error when the vehicle executes an "S"-turn of the type defined elsewhere in this study.

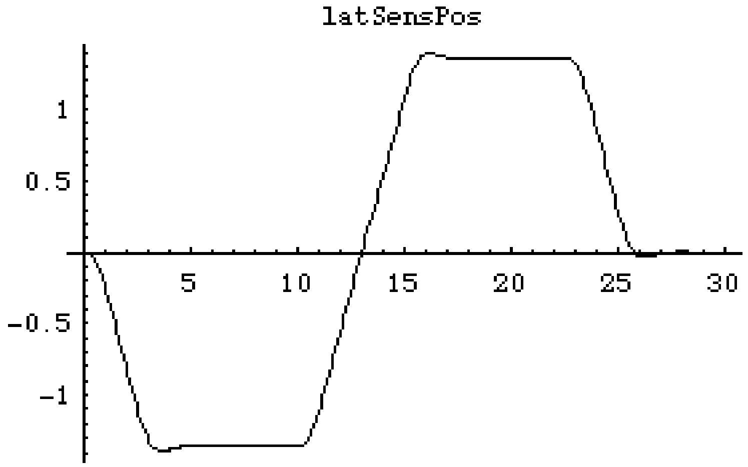


Figure 95. S-Turn Lateral Sensor Position

The following plot shows the road heading in radians for the "S"-turn.

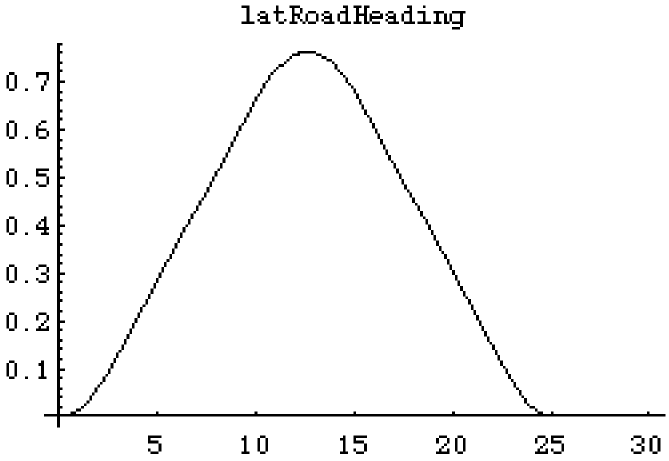


Figure 96. S-Turn Lateral Road Heading

ERROR DUE TO WIND BIAS

The following plot shows the lateral sensor error for a 80 kph wind gust applied at t=10 seconds.

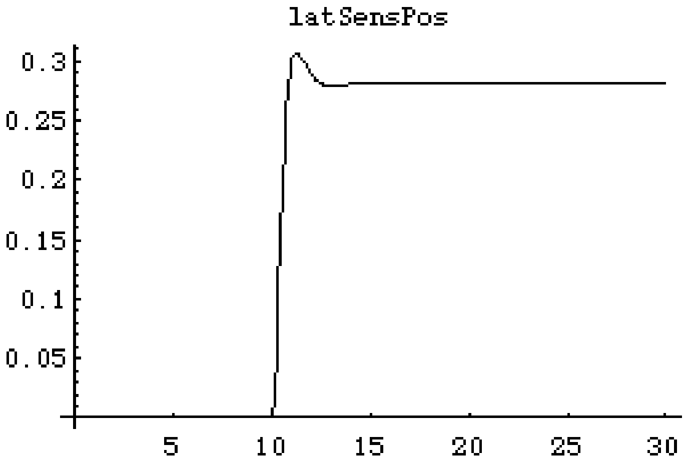


Figure 97. Wind Gust Lateral Sensor Position

ERROR DUE TO SUPERELEVATION

The following plot shows the lateral sensor error for a 0.152 m (0.5 ft) superelevation applied at t=10 seconds.

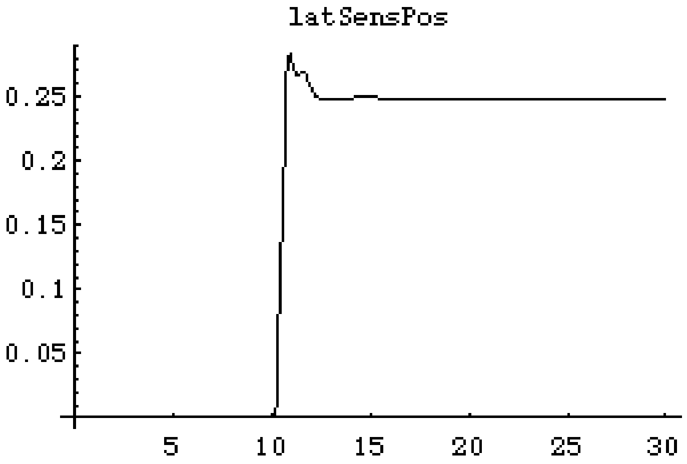


Figure 98. Superelevation Lateral Sensor Position

FALSE ALARM PROBABILITY DUE TO GUSTS

The following shows a typical time trace of a simulated run under the gust model discussed above.

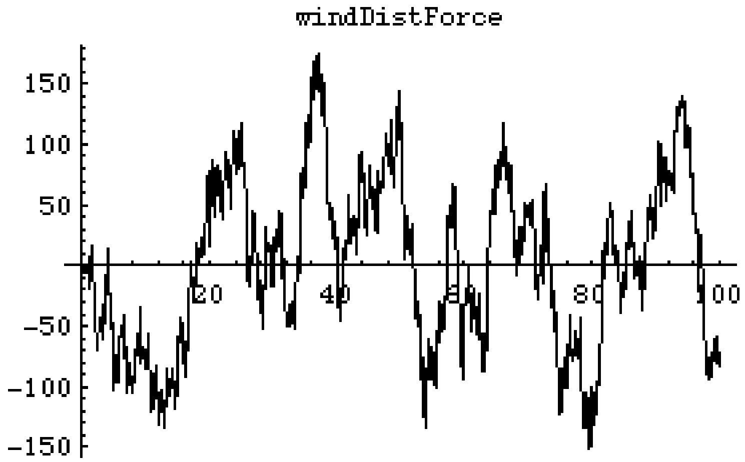


Figure 99. Wind Force

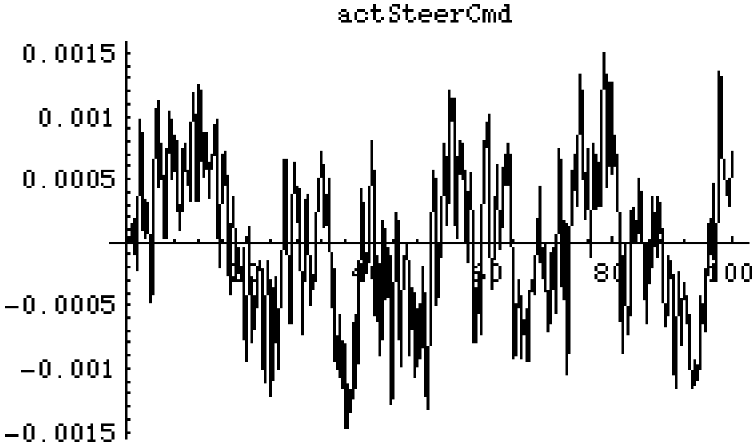


Figure 100. Wind Gust Steering Command

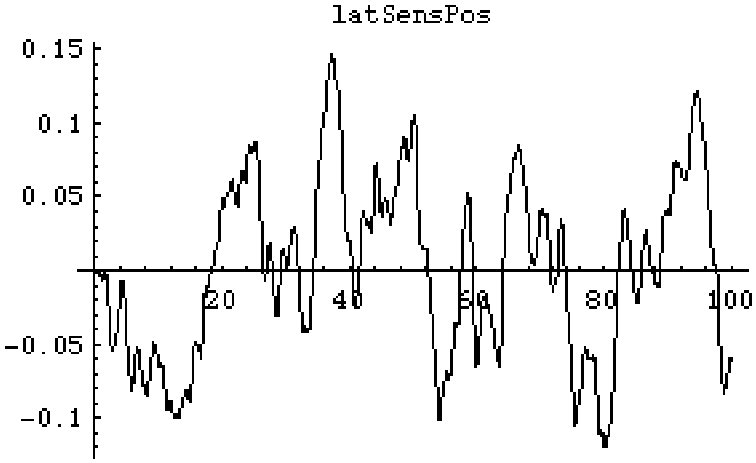


Figure 101. Wind Gust Lateral Sensor Position

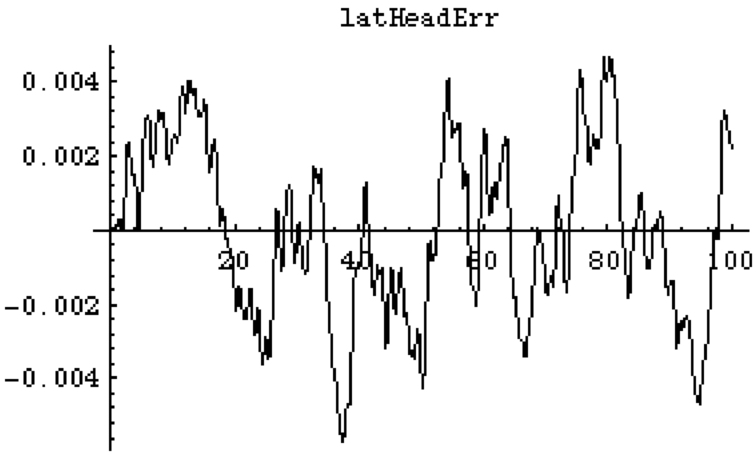


Figure 102. Wind Gust Lateral Heading Error

Direct analysis of the linear models shows the following standard deviations under gusts:

Output	**Standard Deviation**
gust speed	3.22 m/s (10.58 ft/s)
gust force	1349 kg (92.43 slugs)
steering angle	0.000744 rad
lateral error	0.0244 m (0.0799 ft)
heading error	0.003 rad

In addition for the analysis below, we note that the self-correlation of the lateral error over an interval of 0.1 seconds is 0.99821.

The following formulas determine the probability of having a false alarm in one hour:

$$P_A = T\!/\!h \quad \frac{1}{\sqrt{2}} \frac{1}{A} e^{\frac{1}{4}\ {}^{2}A^{2}} erf(\tfrac{1}{2}\quad A\ )e^{-\frac{1}{2}A^{2}} \tag{47}$$

where:

P_A	probability of false alarm per hour
A	alarm threshold (ft)
h	time sample interval (sec)
T	total interval (sec)
	= 3600
	correlation over interval h
	$= \dfrac{\mathrm{E}(X(t)X(t+h))}{\mathrm{E}(X(t)^2)}$
	= 0.99821

^{2} variance of $X(t)$

$= \mathrm{E}(X(t)^{2})$

$= 0.799^{2} = 0.00638$

δ_{ρ} $= \sqrt{\frac{2(1- \quad)}{1+}}$

A_{ρ} $\sqrt{\frac{2}{1+}}\ A/$

The following graph shows how the probability of false alarm falls with increasing threshold.

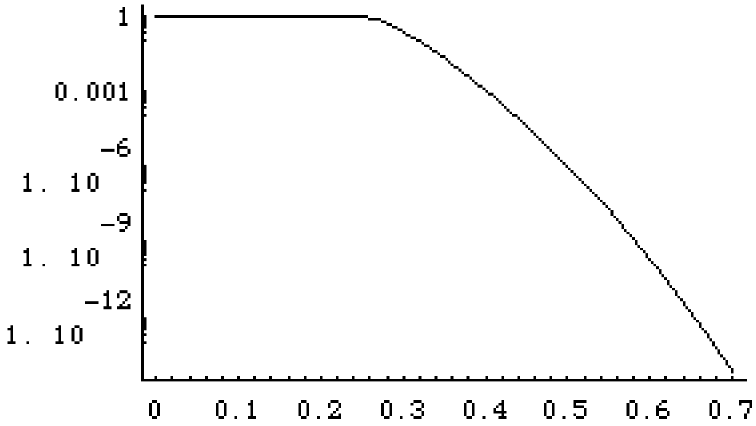


Figure 103. False Alarm Probability with Increasing Threshold

The following data shows the values more precisely:

Threshold Margin (ft)	**Probability of False Alarm per Hour**
0	1
0.1	1
0.2	0.9999997
0.3	0.26
0.4	0.0012
0.5	$1.1 \cdot 10^{-6}$
0.6	$1.9 \cdot 10^{-10}$
0.7	$7.1 \cdot 10^{-15}$
0.8	$5.4 \cdot 10^{-20}$

FALSE ALARM PROBABILITY DUE TO ROAD NOISE

The following shows a typical time trace of a simulated run under the gust model discussed above.

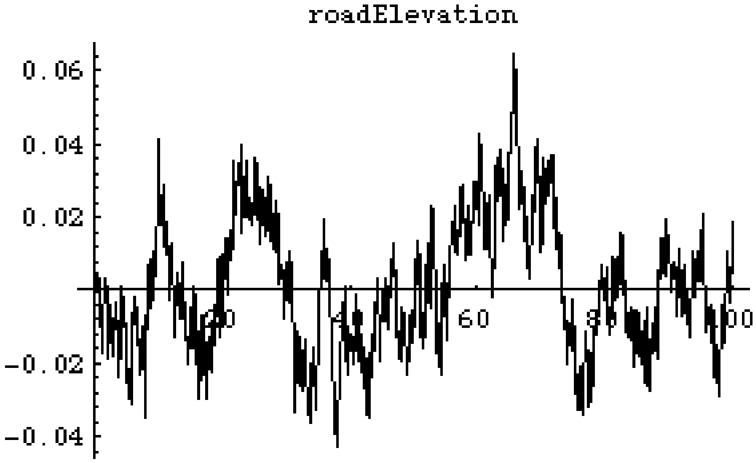


Figure 104. Road Elevation Model

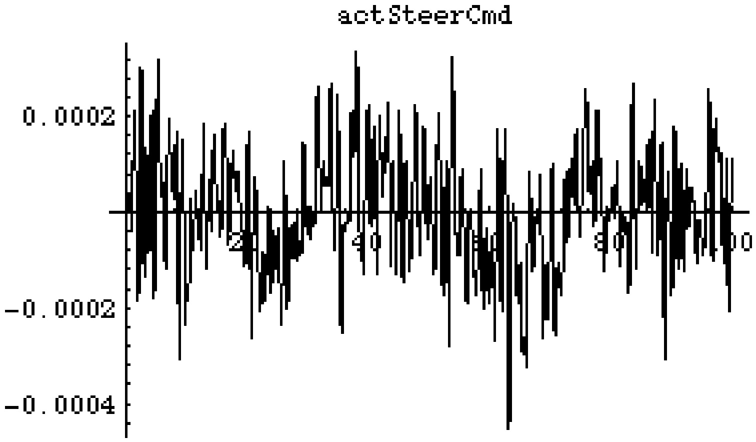


Figure 105. Road Noise Steering Command

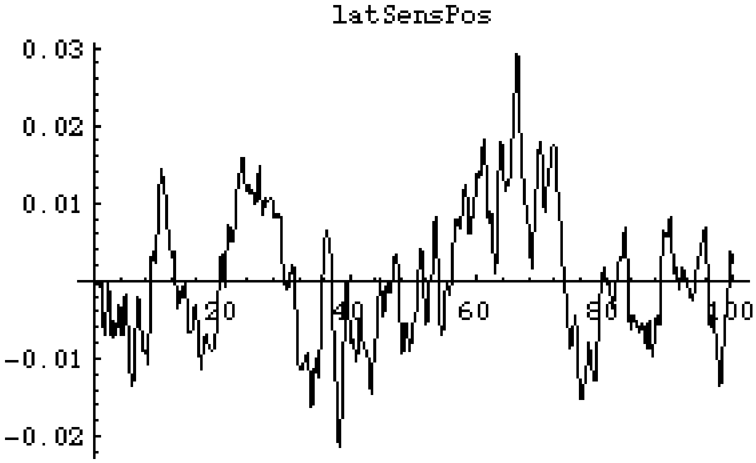


Figure 106. Road Noise Lateral Sensor Position

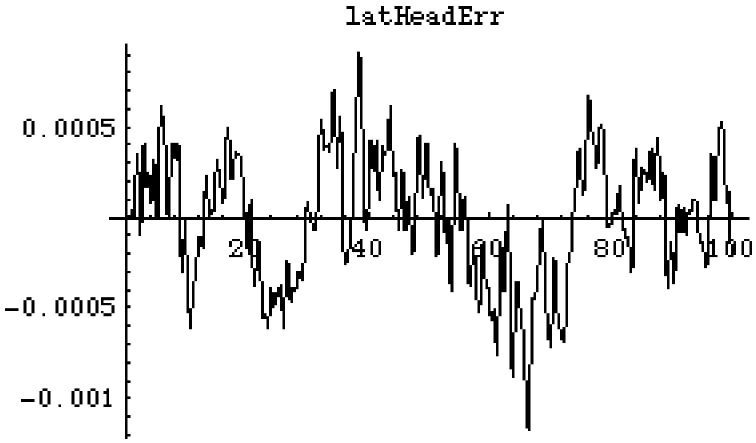


Figure 107. Road Noise Lateral Heading Error

Direct analysis of the linear models show the following standard deviations under gusts:

Output	**Standard Deviation**
road elevation	0.00482 m (0.0158 ft)
body elevation	0.00235 m (0.0077 ft)
lateral force	138 kg (9.46 slugs)
steering angle	0.00012 rad
lateral error	0.00235 m (0.0077 ft)
heading error	0.0003 rad

In addition for the analysis below, note that the self-correlation of the lateral error over an interval of 0.1 seconds is 0.99115.

The following formulas determine the probability of having a false alarm in one hour:

$$P_A = {}^{T}\!/_{h} \quad \frac{1}{\sqrt{2}} \frac{1}{A} e^{\frac{1}{4} \quad {}^{2} A^{2}} erf(\tfrac{1}{2} \quad A\ )e^{-\frac{1}{2} A^{2}} \qquad (48)$$

where:

P_A	probability of false alarm per hour
A	alarm threshold (ft)
h	time sample interval (sec)
T	total interval (sec)
	= 3600
	correlation over interval h
	$= \frac{\mathrm{E}(X(t)X(t+h))}{\mathrm{E}(X(t)^{2})}$

$= 0.99115$

^{2} variance of $X(t)$

$= \mathrm{E}(X(t)^2)$

$= 0.0077^2 = 0.00006$

$\delta_\rho \quad = \sqrt{\frac{2(1- \ )}{1+}}$

$A_\rho \quad \sqrt{\frac{2}{1+}}\ A/$

The following graph shows how the probability of false alarm falls with increasing threshold.

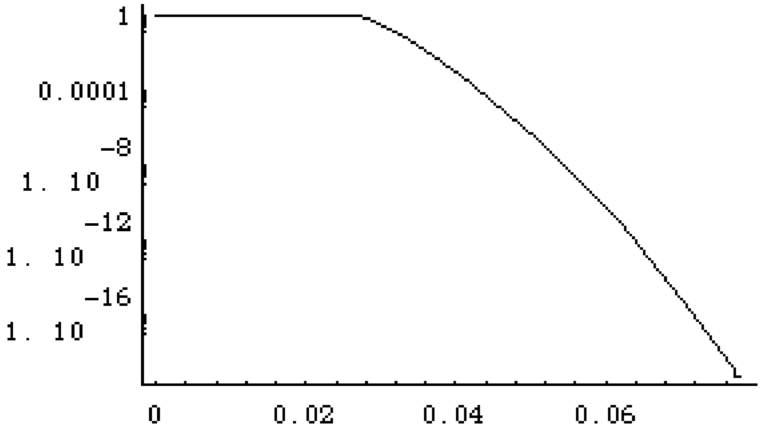


Figure 108. Road Noise False Alarm Probability with Increasing Threshold

The following shows the values more precisely:

Threshold Margin (ft)	**Probability of False Alarm per Hour**
0	1
0.01	1
0.02	0.999999999994
0.03	0.31
0.04	0.00099
0.05	$4.8 \cdot 10^{-7}$
0.06	$4.3 \cdot 10^{-11}$
0.07	$7.1 \cdot 10^{-16}$

Summary

CONCLUSIONS

The following are the currently estimated margins to prevent excessive false alarm.

Required Margin in Lateral Position to Avoid False Alarms

bias due to wind	0.0914 m (0.3 ft)
bias due to superelevation	0.0762 m (0.25 ft)
error in road following	0.457 m (1.5 ft)
margin to accommodate gust turbulence	0.183 m (0.6 ft)
margin to accommodate road noise	0.0183 m (0.06 ft)
Total required margin	0.823 m (2.7 ft)

The final margin is designed to meet a false alarm rate of no more than 5 percent. The actual deviations found are listed below.

Deviations in Lateral Position due to Sources Other Than Failure

bias due to wind	0.0914 m (0.3 ft) (worst-case-deviation)
bias due to superelevation	0.0762 m (0.25 ft) (worst-case-deviation)
error in road following	0.457 m (1.5 ft) (worst-case-deviation)
gust turbulence	0.0244 m (0.08 ft) (root-mean-deviation)
road noise	0.00244 m (0.008 ft) (root-mean-deviation)

CAVEATS

The lateral control design used in this study is a preliminary design. A better control filter is likely in the final design, and that would affect the results of this study.

Not included in the studies to date are the deviations due to mechanical tolerances in the control system itself.

Not included in the wind disturbances is the effect of the moment generated by the center of pressure not coinciding with the center of gravity.

The model of road noise implies a standard deviation in road elevation along the lateral direction which is only 0.00488 m (0.2 in). Intuitively, this seems too small for the average road. Further investigations into road elevation models would be necessary to resolve this issue.

DERIVATION OF FORMULAS FOR PROBABILITY OF UPCROSSING FOR DISCRETELY SAMPLED STATIONARY ONE-DIMENSIONAL GAUSSIAN PROCESSES

See the appendix for this derivation.

DRIVER CHECK-OUT

Many of the AHS scenarios under consideration require that, following a period of automated driving and prior to exit, control of the vehicle be passed back to the driver while the vehicle is moving at highway speeds. A significant concern is that the lack of driving-related activity required of the driver during fully automated driving will tend to induce attentional impairment, with associated decrements in driving skills. Control of the vehicle cannot be transferred back in a safe manner to a driver that is so impaired. Therefore, in these “checkout on the fly” scenarios for AHS, some checkout test is needed that can discriminate attentionally impaired from unimpaired drivers and decide whether or not control can be safely transferred back to the human from the automation.

Issues

The literature is replete with attempts over the years to devise measures for detecting driver fatigue, drowsiness, intoxication, and inattention. A review of this literature revealed some specific issues that AHS driver checkout testing must address:

How Will People Drive After Periods of Automated Driving?

Currently, we do not know how automated driving will affect the skills of subject drivers. However, we must consider the likelihood that more than simple control behaviors, such as lane following, will be affected. For example, safe driving requires the skills of dividing attention to detect vehicles, objects, signs, etc., make judgments about speeds and spacings, plan and execute emergency responses. Also, the driver’s expectancies about continuity and regularity in the traffic situation may well be altered by automated driving. Thus, the AHS driver may become habituated to the regularities of automated driving, only to find himself incapable of rapidly altering those expectations when faced with the unpredictable behavior of manual traffic. His reaction time increased by the lack of anticipation, he becomes vulnerable to the actions of the unsafe driver. All of these skills could, conceivably be affected by periods of automated driving. Moreover, these different skills may degrade differentially over time. That is, some skills may be affected more rapidly by automated driving than others.

Several conclusions can be drawn relative to this issue. First and foremost, an essential precursor to specifying checkout tests is to understand exactly what behaviors and symptoms we are looking for. We must quantify the behavioral effects of automated driving. Second, we should not be surprised if the effects are complex, affecting higher level driving skills, a s well as control behaviors. The corollary of this is that the checkout tests will likely not be simple and one dimensional.

Checkout Tests Will Not Be Perfect

The challenge of driver checkout testing will be that of detecting small differences amid high random variability in people who will be highly motivated to either pass or defeat the test in whatever manner they can (the consequences of failure being a missed exit, lost time and money, missed appointments, etc.). Unfortunately, given these conditions, a perfect test most likely cannot be devised. Some impaired drivers will pass the test and be given control of their vehicle. Some unimpaired drivers will fail and receive an unwarranted trip to the repository. Where we set the acceptable levels for each of these types of classification errors will have a great deal to do with the complexity of tests required and with the time required to conduct them. In fact, given the success (or lack thereof) of tests to screen other types of impaired drivers (drunk, fatigued, etc.), it is possible that we may never be able to meet testing error standards that are acceptable to the public. In that case, other options would have to be considered. These include applying more active monitoring and drowsiness intervention during the period of automated driving, or perhaps forcing the driver to greatly reduce speeds or even halt before control is transferred back.

Can We Ever Get a "Post-Test" to Work in the AHS Context?

Psychomotor tests, simply by being administered, typically produce a temporary increase in the subject's state of arousal or alertness. Drivers in a reduced state of arousal following a prolonged period of driving often manage to rally or mobilize their resources briefly and perform normally on tests, before lapsing back into their pre-test state of arousal. In the AHS checkout context, it is possible that a driver, suffering some attentional deficit due to a long automated drive, might still manage to pass a short readiness test, only to lapse back into his previous state about the time control is transferred back to him. Several studies indicate that through careful test construction, this effect might be avoided. The more extended the testing period, the less the effect. Also, if the test is designed to prevent the driver from knowing how he/she is performing on the test, this "rallying" effect can be reduced.

Test Requirements And Approaches

The following characteristics should guide the selection of testing approaches:

1. Sensitivity to impairment (low type 1 and type 2 error rates).
2. Tests behaviors directly relatable to driving skills.
3. Tests range of behaviors known to be affected by automated driving.
4. Immune to "Broadbent" or rallying effect discussed in (3) above.
5. Adaptive to individual differences with minimal amount of training.
6. Usable within the time frame and real estate available for checkout.
7. Relatively unobtrusive.
8. Inexpensive.

If, for present purposes, one assumes that attempts to detect driver fatigue and driver intoxication provide models for driver checkout testing, then the following three testing approaches can be considered:

- Physiological.
- Control behavior.
- Psychomotor.

Physiological

A great deal of research has been done over the past 20 years on physiological correlates of fatigue, drowsiness, and inattention in drivers. They have met with varying success.

EEG

The electroencephalogram can provide a good indicator of inattention, with Delta and Theta patterns signaling transition to sleep. EEGs have been correlated with behavioral indicators of impaired driving such as missed signals and coarse vehicle control. Unfortunately, EEG measures require continuous monitoring of the driver with obtrusive instrumentation. Also, a significant period of inattentiveness normally precedes any detectable changes in the signal patterns.

HEART RATE

Variability of heart rate tends to increase during extended times of low workload under uneventful conditions. It can be easily measured as a finger pulse using a small, unobtrusive optical sensor. On the negative side, detection of changes requires continuous monitoring. Also, heart rate measures are affected by many other factors unrelated to the driving situation.

CRITICAL FLICKER FUSION

This is the frequency at which a pulsating light is perceived as steady or fused into one continuous signal (i.e. the critical flicker fusion frequency or CFF). As arousal decreases, the CFF also decreases. While it could easily be incorporated into the vehicle dash panel, the CFF has numerous problems as a checkout test. First, the magnitude of the change due to arousal level is small (about 5 percent) and must be extracted from larger background variations caused by human circadian rhythms. To determine a stable estimate of the CFF, a strict psychophysical measurement procedure must be used, requiring approximately 30 repetitions of the test.

EYELID CLOSURE

The slow, ramp-like closure of the eyelid (as opposed to a blink) has been shown to be a stable and reliable indicator of driver drowsiness. In fact, a commercial product, called *Onguard*, is produced by Xanadu Ltd. of Israel, and measures eyelid closure by means of a small infrared sensor and processor that can be mounted to eyeglasses. While eyelid closure measures may have some potential in checkout testing, it is likely limited to that of continuous driver monitoring and alerting. Also, it is not capable of detecting intermediate stages of driver inattentiveness such as those preceding an actual state of drowsiness.

In summary, then, the less obtrusive of the physiological measures physiological measures (heart rate and eyelid closure) may have a role in some sort of continuous monitoring scheme to detect driver impairment. However, they are not nearly sensitive enough to detect intermediate levels of attentional impairment, nor are they predictive enough of specific driving skill deficits to stand alone as readiness tests.

Control Behavior

Among the better attempts to detect driver impairment are those that measuring various aspects of driver control behavior.

STEERING BEHAVIOR

During prolonged periods of driving, steering becomes “coarse”, with fewer small corrections and more large corrections, but fewer corrections overall.

LATERAL POSITION

Errors and variability in lateral position increase with some reliability under various conditions causing inattention or drowsiness. However, lateral position also is affected by situational variables, such as the presence of other cars, road conditions, etc. Inferences about driver state must take into account these variables to correctly classify the behavior.

While measures of control behavior are appealing in that they assess directly a key component of driving skill, they have some problems when considered in the context of AHS checkout requirements. First and foremost, the driver must actually be in control of the vehicle in order to make the measurements. Perhaps control could indeed be returned to the driver during a checkout period if the automatic control system provided a “safety net”, preventing any dangerous manual deviations in lane following. However, the evaluation would not be simple. The steering behavior would have to be assessed against the driver’s baseline steering habits, learned by the system during a period of manual driving immediately preceding entry into the AHS. Second, even if steering behavior can be safely assessed during checkout, it still represents only one component of driving behavior--in fact a rather low-level and nearly autonomous one--that may be affected by automated driving. Thus, at best, this approach might represent one portion of an overall checkout testing scheme.

Psychomotor Tests

Much of the recent research on detection of impaired drivers has focused on the use of psychomotor or human performance tests. The more successful of these are discussed below.

CRITICAL INSTABILITY TRACKING TEST (CTT)

Developed at STI, this test measures eye-hand coordination and performance. The CTT requires the driver to control a first-order dynamically-unstable element. Instability is gradually increased until the driver loses control. The CTT has been implemented as a driving task using a steering wheel and dash panel display of the road ahead. The instabilities are experienced by the driver as “crosswind gusts” as he/she attempts to steer. The characteristics of the test in regard to the driving population are very well known.

DIVIDED ATTENTION TEST

A common symptom of driver impairment is “stickiness of attention”, as Broadbent calls it, i.e. maintaining a high level of attention to one portion of a task at the expense of others. this typically results in missed signals, cues, information, etc. Divided attention can be tested by adding a second, peripheral visual task to a primary tracking task such as the CTT.

TRUCK OPERATOR PROFICIENCY SYSTEM (TOPS)

This is a portable system developed by STI and the Arizona State Patrol for screening truck drivers for fatigue. It combines both the CTT and a driving-related divided attention task (monitoring unexpected events in side view mirrors) into a small driving simulator device that can be installed in a patrol car. It is a good example of using multiple psychomotor tests that are driving skill-related to achieve a fairly high level of impairment discriminability.

In general, the psychomotor tests are appealing in that they are directly related to specific driving skills and deficits associated with attentional impairments (i.e. they have high face validity). Tests can be constructed to measure a range of driving skills including control behavior, as well as higher order attentional and cognitive driving behaviors. They can be administered at the end of a period of automated driving without actually returning control of the vehicle to the driver.

Although the use of psychomotor tests has seen recent success in the screening of drunk or fatigued drivers, they are not sufficiently sensitive in their present form to achieve the error levels likely required on the AHS. More research is needed to identify techniques for enhancing their ability to discriminate impaired from unimpaired AHS drivers.

Driver Check-Out Conclusions

The following conclusions can be made as a result of this initial review and analysis:

- Basic simulator data are needed to identify the specific effects of automated driving on driving skills.
- Criteria for passing/failing checkout tests must be established (i.e. levels of acceptable classification error).
- No single testing approach appears to have the breadth nor the sensitivity to meet the demands of checkout testing by itself. Rather, a more complex model, combining several measures will probably be required.
- As an alternative to checkout on the fly, some configurations should be considered in which checkout and control transfer can be done at very slow speeds or a complete halt.

CONCLUSIONS

FIRM RESULTS

Critical Functions Mechanization

Vehicle

Some critical functions will need to be triple redundant or better in order to satisfy system safety requirements.

Test coverage (the ability to detect failures) has significant effects on probability of failure for catastrophic events. A realistic number for test coverage, like 95%, causes the probability of failure for single or dual systems to rise above our baseline system safety number almost immediately.

Collision avoidance is a basic critical function. When it works correctly, it simplifies the mechanization of many other functions by moving them from a critical to an essential category. If the reliability of collision avoidance cannot be made high enough, many other functions will need to be improved.

Both the steering and braking function reliability numbers are severely constrained by the reliability of axles, wheels, and tires. Improvements in these vehicle components are critical to the safety of the AHS. In particular, run-flat tires will be a requirement.

An uncontrolled engine failure may overpower the brakes. It is necessary to provide a means to kill the engine in this scenario. Luckily, multiple means are present in current engine designs. Electronic ignition and fuel injection provide ready made shut off points.

Road surface condition monitoring is difficult to do from the roadside, due to the large areas needing to be covered. However, if it is performed solely by on-vehicle systems, it will result in a sacrificial lead vehicle scenario. (e.g. the first vehicle to detect reduced traction due to ice on a turn may crash, but warn all the following vehicles.)

Groups have been described as being safe due to the small velocity difference between vehicles with small headways. Join/Split maneuvers, as groups are formed up and dissolved, introduce transient unsafe conditions, as vehicles move from safe long headways to safe short headways. These maneuvers should be minimized.

Roadside

Most of the reliability calculations are based on determining the reliability of a subsystem which provides a critical function. The check-in equipment complement is different, in that its correct operation aids in ensuring the correct operation of another set of critical functions. Stated another way, the check-in test has the effect of increasing vehicle test coverage.

Continuous BIT cannot interfere with system function, and therefore needs to be supplemented with power-on self-test or other non-operational test.

Malfunction Simulation

Using steering as an example, it is not possible to distinguish failure conditions from nominal operation in the presence of environmentally induced errors by simple monitoring of lateral position. A more sophisticated monitoring scheme is required.

A car cannot remain within an 8 foot lane when a failure occurs, given reasonable assumptions about detection and response time.

High speeds in the automated lanes (e.g., 95 mph) require large acceleration and deceleration times, and actually reduce overall throughput for all but the lowest insertion/removal rates.

The driver cannot reasonably act as a backup system for an automation failure. With the speeds, lane widths, and headways proposed for the AHS, the automation cannot detect and verify a failure in time for the driver to add any useful inputs, even if they are attentive to conditions and capable of driving, which is an unsafe assumption. This does not preclude having the driver take over some control after the vehicle has been stopped and the driver tested. This does, however, introduce problems associated with having a manually controlled vehicle in the automated lanes, a very unpredictable factor.

Driver Check-out

It is not possible to predict how people will drive after long periods of automated driving. The AHS presents a new situation, in which a population with widely varying physical capabilities and driving skills is presented with a high speed driving task after a prolonged period of inactivity or distraction.

No driver readiness test will work perfectly. We will be trying to detect small differences amid high random variability in people who are highly motivated to fool us. Acceptable percentages of false negative and positive test results need to be established. Too many false negatives results in user annoyance as capable drivers are shunted to a repository. Too many false positives will result in an unacceptable number of accidents as incapable drivers are given control.

Short duration tests have little validity in fatigue testing. people who know that they are being tested can marshal their faculties in order to carry out a short term task, and then lapse back into a fatigued or otherwise impaired state. This is known as the Broadbent Effect.

No single testing approach will meet the needs of driver readiness testing. Current research indicates that a test combining several different aspects has the best chance of attaining the accuracy necessary for the AHS. However, there are some indications that a useful test may not be achievable.

Driving consists of more than simple motor behaviors such as steering. Tests which only address motor behaviors do not address necessary cognitive skills such as situation awareness.

INDICATIONS

Critical functions Mechanization

Vehicle

Communications with adjacent vehicles poses the problem of restricting the target of the transmission. For example, how do you broadcast a lane change message to the adjacent vehicles only?

On-vehicle contingency planning may lead to the situation where every vehicle on the system chooses the same response, at the same time. There may be a need to randomize algorithmic response to a given situation e.g. to prevent congestion.

Many sensor functions become critical if groups are proposed. Vehicle to vehicle communications is not a critical function in an independent vehicle scenario, but with the tight control required by groups, it becomes a safety critical system.

Roadside

It is difficult to provide a sensing capability sensitive enough to distinguish random error (due to road roughness, wind, ...) from failures without performing maneuvers that would be severe and unacceptable to the occupants. Checkin test may therefore be low payoff.

Vehicle parameters transmitted during checkin need to be correlated with external check, so a timestamp may be required. Speed, heading, acceleration, position, (rollover, acoustic and known vertical (with respect to antenna position)) are among the parameters which need to be passed.

Note that there is a need to calibrate speed so that on-board speed sensor can be adjusted for inflation, tread wear, etc. Assuming sensed lateral guidance (e.g. magnetic) is a discrete signal with known spacing, this also provides speed.

Roadside control of vehicle maneuvers requires that the roadside have knowledge of all vehicle positions with sub-meter accuracy. We judge this requirement to be too difficult and expensive to satisfy, and have used a model of vehicle autonomous control in an environment which the roadside controller makes "benign" by controlling speed and gap.

Safety critical comm (which implies time-critical communication) should be minimized, unless there is a way to ensure that messages are not dropped. The Two Generals Paradox states that there can be no fixed length protocol in the presence of dropped messages.

Approximately 30 ft by 0.5 ft (center of gravity track) is a sufficient maneuvering envelope for the check-in steering test.

The required check-in time is on the order of 30 seconds for the transition lane scenario, which translates to approximately 1/2 mile at 60mph.

Malfunction Simulation

It is difficult if not impossible to insure safety in mixed traffic scenarios, due to the introduction of unpredictable vehicle behavior.

Barriers, if present, need to be transparent to collision avoidance sensors. The use of barriers implies openings, for lane changes, of finite length. Vehicles will commence lane changes at the first available moment. Vehicles in the adjacent lane, previously hidden by the barrier, will cause on-board collision avoidance systems to abort the lane change.

Sensors will need to be tolerant to some variation from desired value due to environmental disturbances and plant model inaccuracies. For example, the lateral position sensor margin to achieve 5% false alarm rate is on the order of 0.8 meter (2.7 ft)

Driver Check-out

No indications.

FURTHER STUDY REQUIRED TO REACH CONCLUSIONS

Check-in tests may require ignoring objects/obstacles. How is this accomplished without providing an opportunity for sabotage or for a real collision if something is in the transition lane?

How do you prevent/assess vehicle structural and load integrity to prevent drop-off events? What about flat-bed trucks? Car top carriers? Unprofessionally secured loads (the roadside mattress)? Long pipe? And if we allow flat-beds, how do we assess how well the load is tied off?)

Can you assume reasonable maintenance behavior? How do you motivate that? If you can't, how do you monitor maintenance? Are there patterns of bad maintenance where you could check one element (oil debris, tire pressure, ...) and assume that others have the same (bad) pattern?

Is the inspections database on the road or on the car? Roadside storage will be easier to protect from sabotage and tampering. Costs equal? Cost of memory on the car vs. database complexity issues. Inspections are relatively local, so database is not nationwide, more local in scope. Could have a call-in service to service non-local inspections. Assume roadside storage.

How can we enforce rejection? The Human Factors Design study has proposed a two stage process with gates prior to each stage of the process. Barrier down means rejection, and control is the responsibility of the human. At the second gate, this means the human must resume control. There is then the issue of how long you're in automated mode before you return control: we should try to minimize this time, since you'll not be doing a readiness test. (Last "readiness test" was manual operation prior to automated mode.)

We have assumed that acquisition cost is a bigger driver than availability (i.e., whether my car is capable of using AHS today). Hence, we have assumed a "no dispatch with fail" philosophy, meaning that redundancy is kept to the minimum needed for safe operation if you start with all systems operational.

If grouping concepts are used, why not take headway to zero, i.e. use a hard linkage as in railroads?

Is the low delta-V impact assumption for group collisions valid? In particular, can a jackknife of the leading cars cause violation of this assumption?

Basic simulator data are needed to identify the specific effects of automated driving on driving skills.

Criteria for passing /failing checkout tests must be established, and levels of acceptable error defined.

As an alternative to checkout on the fly, consider some configurations in which checkout and control transfer can be done at very slow speeds or a complete stop (toll booth scenario).
Detecting objects is easy. Distinguishing obstacles from objects is tougher.

Firm Conclusions/ General Engineering Principles

There is a basic tradeoff between safety and efficiency (a perfectly safe AHS moves no cars).

APPENDICES

FUNCTION DEFINITIONS

For each function in the current system definition, table 11 identifies:

- Function identifier - a unique ID that combines the level in the AHS model architecture (one of: Network, Link, Coordination, Regulation, Physical) with a counter. Some functions have been subdivided, in this case the counter will have subsidiary fields, e.g., "P2.1".
- Name - a brief descriptive string.
- Description - a more lengthy explication of the function role.
- Function criticality - an assignment of the function's criticality, one of Critical, Essential, Non-Essential, and Not Applicable.
- Criticality justification - a record of the rationale for the assignment.
- Allocation - an assignment of the system element(s) that will perform the function in our hypothesized implementation, one of Vehicle, Roadside, Driver, Other.

#	Function Name	Description	Crit.	Criticality Justification/Notes	Alloc.	Allocation Justification/Notes
General Notes:				Criticality Key: C=Critical, E=Essential, NE=Non-essential, N/A=Not Assigned/Applicable		Allocation key: R=Roadside, V=Vehicle, D=Driver, O=Other (e.g., inspections). In dual designation (e.g. R/V), primary player goes first.
N1	Monitor traffic condition and predict congestion	The network layer manages network traffic data and predicts when and where congestion will occur based on real-time traffic information.	E	Judgement call. Loss of this function results in possibly directing traffic into congestion.	R	
N2	Recommend route	Upon receiving the location and the destination of a vehicle, the network layer may recommend the shortest/fastest route. Route recommendation may be provided at the beginning of a trip or anytime during the trip.	E	Judgement call. Loss of this function results in possibility of selecting route through known congestion.	R	If all 3000 vehicles react to the announcement of crash the same way, just create a jam somewhere else.
N3	Receive information from link layer	The network layer receives information regarding regional traffic condition and route selection request from the link layer.	E	Comm link is same criticality as the functions it conveys information to/from.	R	
N4	Provide information to/via link layer	The route recommendation, traffic prediction information, and vehicle ID assignment will be sent to the requester via link layer.	E	Comm link is same criticality as the functions it conveys information to/from.	R	
L1	Assign lane 1	The link layer may provide lane assignments in accordance with the selected route and traffic conditions. Lane assignments may be given before lane-changing is needed, and at locations such as entrance, exit, or diverging points where decisions are needed for choosing a path.	E	No way to assign lanes "by default". Move left until no space?	R	Have a big win in terms of deciding which lane if the roadside knows the destiation/route.
L2	Assign target speed	The target speed is provided in accordance with the local traffic conditions.	E	Assume default maximum "burned in" to vehicle controller. Too low a value degrades performance.	R	
L3	Set maximum group size	When groups are used, the maximum size of group is provided based on the current traffic conditions.	E	Assume default maximum "burned in" to vehicle controller. Too low a value degrades performance.	R	Same argument. Best knowledge of the tradeoff between density and merge/demerge operations.
L4	Set minimal separations	The required minimal headway is provided in accordance with the weather and roadway conditions. In a system with groups the required minimum spacing between groups is provided.	E	Assume default minimum "burned in" to vehicle controller. Too high a value degrades performance.	R	Requires an assumption of standardized capability that everyone has and uses.
L5	Prioritize vehicle operations	Vehicles with special missions, such as ambulances or fire engines or high occupancy vehicles, are given priority over other vehicles.	E	Incident management considered essential	R	Has greater advanced notice of need for maneuver.

L6	Monitor regional traffic condition and manage incidents	Traffic conditions are monitored. Under incident conditions, the link layer selects paths for vehicles, adjusts target speed, or instructs vehicles to changes lane for diversion around incidents.	E	Driven by ambulance/ emergency vehicle requirement.	R	Again, greater global view. Handoff problem? Includes roadside telling other vehicles of vehicle reporting (forced) slowdown.
L7	Monitor road surface conditions and weather	The link layer determines weather and road surface conditions, based in part on vehicle traction reports.	E	Assume vehicle function road surface sensing is critical.	R	Has predictive capability due to knowledge of weather.
L8	Receive information from the coordination layer	The link layer receives information regarding traffic condition of the subsections within the link and vehicle's destination from the coordination layer. The link layer also receives information addressing the network layer from the coordination layer.	E	Driven by lane assignment and incident management functions (what info do they receive from coord?)	R	Since all functions are roadside, all comm is on roadside.
L9	Receive information from the network layer	The link layer receives information regarding the traffic condition predictions and route recommendations from the network layer. The link layer may also receive information addressing the vehicle from the network layer.	E	Comm link is same criticality as the functions it conveys information to/from.	R	Since all functions are roadside, all comm is on roadside.
L10	Receive information from neighboring link	Receive handoff information as vehicle passes from one link to the next.	E	Comm link is same criticality as the functions it conveys information to/from.	R	Since all functions are roadside, all comm is on roadside.
L11	Provide information to the network layer	The link layer provides information regarding regional traffic condition to the network layer. The link layer also transfers the information intended for the network layer from the coordination layer.	E	Comm link is same criticality as the functions it conveys information to/from.	R	Since all functions are roadside, all comm is on roadside.
L12	Provide information to the coordination layer	The link layer provides information regarding vehicle operation parameters such as target speed and minimal separation to the coordination layer. The link layer also transfers the information intended for the coordination layer from the network layer.	E	Driven by lane assignment and incident management functions (what info do they send to coord?)	R	Since all functions are roadside, all comm is on roadside.
L13	Provide information to neighboring link	Provide handoff information as vehicle passes from one link to the next.	E		R	Since all functions are roadside, all comm is on roadside.
C1	Perform off-vehicle inspection and monitoring	Vehicle inspection requiring supplemental off-vehicle equipment could be performed before the vehicle enters the AHS, or while the vehicle is on the AHS. These inspection and monitoring functions, which may work together with on-vehicle detection/diagnosis devices, provide vehicle health or condition reports	C	E.g., tire tread measurement (inspections that are important, but whose results do not change rapidly.)	R	If function includes inspection, must be done. Has to be some quality control outside the vehicle. What's the calibration source if the function is on-vehicle?
C2	Issue permission/rejection	Based on the inspection/monitoring outcome, traffic flow and destination parameters, the coordination layer issues permission for entering or remaining on the AHS. Should a fault(s) be detected, a rejection command will be issued.	C	If this function has failed, AHS allows non-capable vehicles to enter.	R	Has ultimate authority. Car can check out some stuff to prevent wasted time. Roadside is independent authority. Both must agree to grant permission.

C3	Plan maneuver coordination	Maneuver coordination planning determines the sequence of events for a number of vehicles performing a coordinated maneuver. Maneuvering coordination planning is performed for both normal and abnormal conditions.	N/A	Use roadside to command densities by means of speed and headway. Vehicles figure out where in stream to self-insert.	N/A	Add joining/splitting group to this function.

C3.1	Plan maneuver coordination for normal conditions	Normal maneuvers that require coordination between vehicles, such as lane-changing, merging, entering or exiting an AHS, or joining or splitting a group, are handled by the coordination layer. The coordination layer sets up coordination protocols among the involved vehicles and determines commanded speed, location, and condition for maneuvering action.	E	Assume barriers transparent to collision avoidance sensors. Otherwise, critical function.	V/R	Having the roadside know car positions within meters at all times seems unlikely. Roadside will know lane ends. Set of right-of-way rules that determine precedence of vehicle merge.
C3.2	Plan maneuver coordination for hazardous conditions	Under hazardous conditions, the coordination layer provides information regarding specific hazards to vehicles which are potentially affected, and provides instructions for avoiding collisions.	E	Assume barriers transparent to collision avoidance sensors. Otherwise, critical function.	V/R	Do emergency conditions allow violation of headway temporarily? Seems like a temporary introduction of unsafe condition, you could compare that to the condition where the lane change is not allowed.
C4	Supervise the sequences of coordinated maneuvers	The coordination maneuvers will be monitored by the coordination layer.	E	Assume barriers transparent to collision avoidance sensors. Otherwise, critical function.	V/R	Monitoring has to be in vehicle. What do you do if right of way rules arenÕt working? Slow down traffic, or execute rules earlier. How/when do you change right-of-way rules? New time-coded ROM burned in inspection
C5	Obtain vehicle ID	Obtain identification address used to communicate with a particular vehicle.	C	For permission/rejection. Use existing because any billing will require association of temp with perm. ID.	R/V	Vehicle knows its ID, roadside gets it and uses it for any vehicle specific addressing needed. Shows on both because of implicit comm.
C6	Receive information from the link layer	The coordination layer receives information regarding the vehicle operation parameters such as target speed and minimal separation from the link layer. The coordination layer also receives information intended for the regulation layer from the link layer.	E		R/V	Because sending/receiving functions (may) reside on both.
C7	Receive information from the regulation layer	Two types of information will be acquired by the coordination layer, including the requests for a maneuver that will require coordination, such as lane-changing, and status information about vehicles.	C		R/V	Because sending/receiving functions (may) reside on both.
C8	Receive information from neighboring coord. element	Receive information on coordination maneuvers planned for neighboring coordination element's span of control.	E	Permission/rejection and inspection are local functions, and results need not be communicated	R/V	Because sending/receiving functions (may) reside on both.
C9	Provide information to the link layer	The coordination layer provides information regarding traffic condition of the subsections within the link and vehicle's destination. The coordination layer also transfers the information intended for the link layer or the network layer from the regulation layer.	E		R/V	Because sending/receiving functions (may) reside on both.

C10	Provide information to the regulation layer	The coordination layer provides operation commands defining the sequences of coordination maneuvers and information such as road surface condition and weather to the regulation layer.	C		R/V	Because sending/receiving functions (may) reside on both.
C11	Provide information to neighboring coord. element	Provide information on coordination maneuvers planned for this coordination element's span of control.	E	Permission/rejection and inspection are local functions, and results need not be communicated	R/V	Because sending/receiving functions (may) reside on both.
C12	Determine roadway operational limits	Determine the maximum safe speed and minimum safe gap for this segment of roadway based on road surface conditions, known curvature, anticipated weather including wind, temperature and rain/snow.	C	Car will run off road unless limited to safe behavior.	R	Roadside has lookahead view of road surface conditions unavailable to car.
R1	Provide steering control command	Commands for providing the required lateral motion are constantly updated based on information regarding the vehicle's lateral position, yaw motions, lateral acceleration, and upcoming road geometry.	C		V	Could conceivably be on roadside for emergency, huge comm/processing rqt.
R2	Provide speed regulation command	The speed control command is issued based on the instruction provided by the coordination layer and sensor and vehicle performance feedback from the physical layer.	N/A	Assumes about .5g deceleration out of braking system. Makes engine shutoff critical.	N/A	N/A
R2.1	Provide headway keeping command	Headway keeping (for groups only) forms an "inner loop" of the speed regulation command, overriding target speed considerations	C	What's the reason not to take headway to zero, i.e., hard linkage?	V	Could conceivably be on roadside for emergency, huge comm/processing rqt
R2.2	Provide target speed tracking command	Maintain speed commanded by coordination layer. Overridden by headway keeping and collision avoidance.	E	IF collision avoidance, brakes, road curvature, and monitoring of target/commanded difference are critical.	V	Could conceivably be on roadside for emergency, large comm/processing rqt
R3	Provide braking command	The braking command is issued when reduction of the vehicle speed is required. The braking command can be issued in combination with the speed control command.	C		V	Could conceivably be on roadside for emergency, large surge comm/processing rqt
R4	Manage vehicle health	Vehicle conditions are monitored using the sensory information provided by the physical layer. Failure detection and diagnosis are performed when a system fault is discovered. Failure response actions are determined. On-board actions are performed. Failure response actions requiring roadside involvement are communicated.	N/A	Diagnosis and malf. mgmt. minus similar string redundancy management (which is performed by fcn.)	N/A	N/A
R4.1	Monitor propulsion system	Several parameters such as temperature, pressure (for an internal combustion system), or current (for an electrical system) are selected to represent the health of the propulsion system .	C	Assessment of redundancy for checkin makes these critical. Note: Assume no dispatch with fail philosophy.	V/R/O	Test probably primarily on-vehicle continuous test, supported by roadside periodic, inspections, periodic bit.
R4.2	Monitor braking system	Several parameters such as temperature of brake discs or shoes and pressure of brake hydraulic system are selected to characterize the health of the braking system.	C		V/R/O	"

R4.3	Monitor steering system	Several parameters such as hydraulic pressure (for a hydraulic steering actuator) or current (for an electrical steering actuator) and temperature will be used to characterize the health of the steering system.	C		V/R/O	"
R4.4	Monitor electrical system	Several parameters such as voltage, current, and temperature will be used to characterize the electrical system.	C	Separate electronics/actuator power?	V/R/O	"
R4.5	Monitor energy supply	Determine remaining energy, e.g., fuel level, battery voltage, ...	E	gas or voltage or .... Power for, e.g., brakes is critical, but covered by saying brakes critical.	V/O	Effects of loss not likely to be visible to roadside or driver
R4.6	Monitor displays	Determine correct function of displays.	C	Assume displays used to convey permission/rejection to driver	V/D/O	Effects of loss not likely to be visible to roadside.
R4.7	Monitor controls	Determine correct function of controls.	C	Controls used to steer/brake/accel the vehicle. Others (destination select) only essential.	V/D/O	Effects of loss not likely to be visible to roadside.
R4.8	Monitor comm	Determine correct function of the communications subsystem.	C	At least mechanism used to convey permission/rejection and data for off-vehicle inspection	V/R/O	Effects of loss not likely to be visible to driver.
R5	Monitor driver health/readiness	Ensure driver is prepared to undertake manual operation	C	If human is part of backup strategy. Also applies to mixed traffic scenarios.	V/O	Infrastructure assigns license.
R6	Monitor roadside health	Roadside function is monitored using sensory information from monitored functions and (potentially) vehicle cross-checks.	N/A	N/A	N/A	N/A
R6.1	Monitor roadside comm	Determine correct function of the communications subsystem.	C	At least mechanism used to convey permission/rejection and data for off-vehicle inspection	R/V	Vehicle only works as detector for R-V comm, not roadside internal comm.
R6.2	Monitor roadside computing equipment	Determine correct function of the computers & associated peripheral equipment.	C	Vehicle permission/rejection function only.	R/V	Flawed commands received by several vehicles may provide backup detection. Unclear how vehicle could isolate this failure.
R6.3	Monitor roadside sensors	Determine correct function of the roadside sensing equipment.	C	Vehicle permission/rejection function only.	R	"
R7	Monitor trip progress	The trip progress is monitored by reporting to the operator the information regarding vehicle location and traffic condition and estimated arrival time.	E	If you miss your exit, the system hasn't worked.	V	Roadside only needs to know presence not progress.
R8	Receive information from the coordination layer	The regulation layer receives information regarding operation commands which defines the sequences of coordination maneuvers and information such as road surface condition and weather from the coordination layer.	C	Depends on status of vehicle ID and maneuver functions.	V/R	
R9	Receive information from physical layer	The regulation layer receives information regarding sensory measurements and user's requests from the physical layer.	C	Consider Two Generals Paradox for comm (no fixed length with dropped messages).	V/R	
R10	Provide information to the coordination layer	The regulation layer provides information about maneuvers requiring coordination, such as lane-changes, and the status of vehicles.	C	Depends on status of vehicle ID and maneuver functions.	V/R	

R11	Provide information to the physical layer	The regulation layer provides control commands to the physical layer.	C	Note: Reg-Reg comm not yet identified as necessary.	V/R	
R12	Detect obstacle	Determine whether information from physical layer concerning front/rear/side detections constitutes obstacle. Includes loss of road.	C	Note distinction of obstacle/object between this and P	V	Need to inform roadside of speed change
R13	Determine dynamic response of propulsion system	The dynamic response of the propulsion system is characterized by the time interval required for accelerating the vehicle to a target speed from a specified initial speed.	E	Assume braking response greater than propulsion loss effect. Part of platoon dynamics, using least capable vehicle?	V	If not required for controller and not needed often, may be cheaper on roadside or via inspection.
R14	Determine dynamic response of braking system	The dynamic response of the braking system is characterized by the time interval required for decelerating a vehicle from certain speed to a stop.	C	Only parts that have no manual backup? Part of platoon dynamics, using least capable vehicle?	V	If not required for controller and not needed often, may be cheaper on roadside or via inspection.
R15	Determine dynamic response of steering system	The dynamic response of the steering system is characterized by the frequency response of the steering system and the deadband.	C	Only parts that have no manual backup? Part of platoon dynamics, using least capable vehicle?	V	If not required for controller and not needed often, may be cheaper on roadside or via inspection.
R16	Determine traction	The parameters which affect the vehicle's slip or traction will be monitored.	C	Required to calibrate braking. Lock one wheel? Steering vs. slip angle?	V	C5 is roadside fusion of information.
R17	Determine visibility	The visibility (e.g., of the collision avoidance sensor) will be monitored and graded.	C	Required to set collision avoidance distance/speed limit	V/R	Use VPD for roadway to tell vehicle distance to lead car. Then use different headways to calibrate distance to unacceptable S/N or absolute signal.
R18	Convey information to driver	Format information for display.	N/A	See diagram "AHS-Human comm paths" for graphical depiction of convey/request/provide/receive distinction.	N/A	N/A
R18.1	Convey vehicle speed	Convey speed information	E	Headway is overriding influence.	V	Different than existing speedometer?
R18.2	Convey headway	Convey distance to leading vehicle	E	Including out-the-window view. Acclimatization problem?	V	How accurately doesn human need this?
R18.3	Convey energy level	Convey remaining energy (fuel, voltage)	E	Part of standard vehicle instrumentation.	V	Standard vehicle equipment
R18.4	Convey diagnosis information and warning signals	Alert driver to problems with vehicle that reduce capability or reserve.	C	Required for safe transition and manual operation	V	How much detail required?
R18.5	Convey mode status	Effectively tell driver what mode the vehicle is in, e.g., auto, manual, emergency.	C	Including permission/rejection	V/R	Could be roadside signage either primary or backup.

R18.6	Convey route recommendation information	Effectively tell driver what route is optimal in the estimation of network layer.	E	Part of driver situation awareness.	V	Display resolution required?
R18.7	Convey yellow page information	Effectively tell driver relevant local (business?)information	NE	Not considered a core AHS function	V	Distraction? Block under certain conditions?
R18.8	Convey trip progress report	Effectively tell driver progress of vehicle	E	Part of driver situation awareness.	V	-
R18.9	Convey location	Effectively tell driver current location.	E	Part of driver situation awareness.	V	-
R18.10	Convey lane recognition	Effectively tell driver current lane.	E	Part of driver situation awareness.	V	-
R19	Request information	The driver or other system elements may request various kinds of information from the system.	N/A	N/A	N/A	N/A
R19.1	Request vehicle status	Driver or other system element may request vehicle status.	NE	System still works correctly if human requests no info. Issue of human operator comfort level if broken?	D	This function is performed by other system elements for different purposes.
R19.2	Request system status	Driver asks for roadside health info.	NE	System still works correctly if human requests no info. Issue of human operator comfort level if broken?	D	"
R19.3	Request trip progress	Driver asks for progress of vehicle.	NE	System still works correctly if human requests no info. Issue of human operator comfort level if broken?	D	"
R19.4	Request traffic condition	Driver requests network level view of system status.	NE	System still works correctly if human requests no info. Issue of human operator comfort level if broken?	D	"
R19.5	Request performance adjustment	Driver may request that vehicle perform within certain constraints on acceleration, headway, etc.			D	This may be coded in to driver profile.
R20	Receive information	The driver will receive information from the vehicle, the roadside, and the traffic management center.	C	Control handoff must be accurately conveyed so that human does not relinquish control prematurely.	D	Not clear how you "guarantee" this function.
R21	Provide information/acknowledgements	The driver will be required to provide information to the system. This includes the following:	N/A	N/A	N/A	N/A
R21.1	Provide requests to enter the AHS	The vehicle operator requests permission to enter the AHS	E	Lack of function implies low AHS utilization	D	-
R21.2	Provide destination	The driver will be required to designate a destination for his/her trip. This function also will allow the driver to change that destination during the trip.	E	Without function, driver exits at low fuel status, or goes to repository.	D	Workload issue if must be done while under manual.

R21.3	Provide requests to immediately exit AHS	The driver may request to leave the system at the closest possible exit or to leave the transition lane prior to entering the automated lane.	E	Function provided for user comfort and, e.g. medical emergency handling	D	Must be simple (redundant mode?) for emergency.
R21.4	Grant authorization for change from manual to automated mode	The driver must provide a final authorization in order for the manual to automated control transition to proceed.	E	If system times out waiting for this, can go auto, or leave with manual.	D	-
R21.5	Provide responses to manual control readiness tests	The driver will have to make some input when cued by the system to indicate his/her readiness to resume manual control.	E	If function unavailable, assume incapacitated driver and dump in repository.	D	False positives would be a significant problem.
R22	Perform mode selection	Determine and initiate the appropriate mode of operation for the vehicle, including automatic, manual, and crisis operational status.		Tied to L5 "Prioritize vehicle operations"	V	Will not allow driver to command manual or emergency mode.
R23	Configure for manual operation	Ensure that the vehicle has all functions necessary for manual operation enabled (e.g., wipers, lights, defroster...)	C	Short exposure time after handoff if mixed traffic.	V/D	Driver could configure most secondary equipment. Health management system must be able to verify/ensure correct configuration. Control handoff?
P1	Sensing	Four groups of sensory information are needed. The sensory information can be obtained through direct sensing or combined sensing and signal processing. The following information may be entirely or partially needed for any specific AHS design.	N/A	N/A	N/A	N/A
P1.1	Sense lateral displacement	The distance from a point along the longitudinal center line of the vehicle to a reference line or marker. The reference can be a roadway reference which delineates the center or the edge of a traffic lane or a roadside reference which retains a constant	C	Do you also need lateral "velocity"?	V	Could perform on roadside for limited spans.
P1.2	Sense bearing	Determine bearing of vehicle.	C	Needed for accurate lane-following if sensor is not at the center of gravity.	V	-
P1.3	Sense longitudinal position	The vehicle acquires its longitudinal position of the vehicle relative to a milepost.	E	How do off-ramps work? Assume collision avoidance will prevent exit at inappropriate time.	V/R	Only interesting at certain points, and roadside announces?
P1.4	Recognize lane	The vehicle recognizes the number of the lane on which the vehicle is traveling.	E	Superceded by collision avoidance and run-off-road avoidance.	V	Knowing which lane your vehicle is in allows announcements of "Lane 3 blocked"
P1.5	Sense velocity	The vehicle measures its velocity as the distance traveled in a specified time interval.	C	Critical for groups only.	V	Could perform on roadside for limited spans.
P1.6	Sense lateral acceleration	The lateral acceleration is measured as the variation in velocity in the lateral direction during a specified time interval at the mass center.	C	Critical for groups only.	V	", limited accuracy.

P1.7	Sense longitudinal acceleration	The longitudinal acceleration is measured as the variation in velocity in the longitudinal direction during a specified time interval at the mass center.	C	Critical for groups only.	V	", limited accuracy.
P1.8	Sense yaw rate	Yaw rate is measured as the angular change in a specified time interval along the axis perpendicular to the road surface.	C	Critical for groups only.	V	-
P1.9	Sense roll rate	Roll rate is measured as the angular change in a specified time interval along the longitudinal axis through the center of gravity of the vehicle	C	Critical for groups only.	V	-
P1.10	Sense pitch rate	Pitch rate is measured as the angular change in a specified time interval along the lateral axis through the center of gravity of the vehicle.	C	Critical for groups only.	V	-
P1.11	Sense range to a frontal object/vehicle	The distance to a frontal vehicle is measured as the separation between the controlled vehicle and the frontal vehicle.	C	Part of headway maintenance/collision avoidance.	V	Vehicle detection may use different method than for other objects.
P1.12	Determine closing rate to a front object/vehicle	The closing rate to a frontal vehicle is measured as the variation in distance between the controlled vehicle and the frontal vehicle in a specified time interval.	C	Part of headway maintenance/collision avoidance.	V	Object becomes obstacle when projected paths overlap, only true for positive closing rate.
P1.13	Sense range to a neighboring (side) object/vehicle	The distance to a neighboring vehicle is measured as the separation between the controlled vehicle and the neighboring vehicle.	C	Encroachment only with broken vehicle/maneuver function. Overlap with this and lateral displacement? (Auto only.)	V	-
P1.14	Determine closing rate to a neighboring object/vehicle.	The closing rate to a neighboring vehicle is measured as the variation in distance between the controlled vehicle and the neighboring vehicle in a specified time interval.	C	Part of collision avoidance.	V	-
P1.15	Sense range to a rear object/vehicle	The distance to a rear vehicle is measured as the separation between the controlled vehicle and the rear vehicle.	C	Encroachment only with broken vehicle/maneuver function. Overlap with this and lateral displacement? (Auto only.)	V	-
P1.16	Determine closing rate to a rear object/vehicle	The closing rate to a read vehicle/obstacle is measured as the variation in distance between the controlled vehicle and the rear vehicle/obstacle in a specified time interval.	C	Part of collision avoidance.	V	-
P1.17	Determine tire pressure	Tire pressure can be physical measurements or estimation based on dynamic performance.	NE	Assume run-flat tires. How long can you run-flat?	V	Do run flat tires act the same (traction, handling) when flat?
P1.18	Sense energy level	Energy level can be fuel level (for an internal combustion propulsion system) or voltage (for an electrical propulsion system) or both (for an hybrid vehicle).	E	Assume braking response of trailing vehicles greater than propulsion loss effect. Drivetrain lockup? Separate elec/act. power?	V	
P1.19	Sense or read curvature	A horizontal curve is characterized by several parameters, i.e. radius and length of the curvature, and the distance to the curvature.	C	Critical to determine if speed exceeds safe conditions.	V	May be directly sensed, or roadside may convey by magnetic coding or transmission.
P1.20	Sense or read grade	A vertical curvature is characterized by gradient and the length of the curvature and the distance to the curvature.	C	Only critical for tight positional control	V	"

P1.21	Sense or read bank	A bank is characterized by length of the bank, bank angle, and distance to bank.	C	Critical to determine if speed exceeds safe conditions.	V	"
P1.22	Sense or read configuration and location of entrance/exit gates	When entrance/exit gates are present, the distance to a gate, the direction of the gate, and the size of the gate will be given.	C	Critical to determine if safe exit possible.	V	"
P1.23	Sense road surface condition	The condition of the road, particularly the parameters which will affect the vehicle cornering force, will be monitored.	C	Required to calibrate braking	V	"
P1.24	Sense visibility	The visibility will be monitored and graded.	C	Required to set collision avoidance distance/speed limit	V	Some technologies can assume unlimited vis.
P1.25	Characterize wind	The direction and magnitude of the wind will be measured.	C?	required for steering? Probably not. Design steering to be robust to disturbances not to exceed...	R	-
P1.26	Obtain traffic signal information	Traffic signals for speed control will be transmitted to or recognized by the vehicle.	C?	Depends on nature of signal information.	V	Are all standard signage/signals superceded by AHS transmissions for auto mode?
P1.27	Obtain traffic sign information	Traffic signs will be transmitted or recognized by the vehicle.	e/c ?	Depends on nature of sign information.	V	"
P2	Actuation	Actuation is provided in two dimensions, steering and speed control. The speed control includes control of both the propulsion and the braking systems.	N/A	N/A	N/A	N/A
P2.1	Perform steering actuation	The steering actuation causes the wheels to turn forcing the vehicle to change its direction of motion.	C	Critical to lane-keeping, collision avoidance	V	Simulation indicates hard over of > 5 degrees causes skid
P2.2	Perform propulsion actuation	The propulsion actuation causes a vehicle accelerate or decelerate (using engine brake).	E	Assume braking response greater than propulsion loss effect. Drivetrain lockup?	V	-
P2.3	Perform brake actuation	The brake actuation causes a vehicle to decelerate.	C	Critical to collision avoidance, run-off-road crash avoidance.	V	-
P2.4	Shutdown propulsion system	In the event of an overspeed condition, the propulsion system must be capable of being deactivated	C	Braking response greater than propulsion for some limited time period. Brake fade effects require shutdown.	V/D	Does turning the key off count? What does that do on AHS?
P3	Human-machine interface	The human-machine interface enables the human operator to monitor the performance of the vehicle, to adjust performance parameters within a reasonable working range, to be aware of hazardous conditions, and to take over control tasks if necessary. It may	N/A	N/A	N/A	N/A
P3.1	Provide operator displays	The operator requires some set of devices which will be used to convey information to him/her. Audio, lights, flat panel displays are all possible examples.	C	Critical in mixed traffic, and for conveyance of accept/reject.	V/R	Accept/reject may be roadside primary or backup.

P3.2	Provide switch. mech. for alternating btw auto and manual control	Engagement/disengagement of automated commands.	C	Note: only available in transition lane/exit/entry	V	-
P3.3	Provide emergency switching mechanism for human backup operation	Disengagement of auto functions for emergency conditions.	C	Critical during transition to/from automated mode while in mixed traffic.	V	-
P3.4	Provide manual steering capability	Standard functions. Criticality implications for AHS in mixed traffic.	C	Critical during transition to/from automated mode while in mixed traffic.	V	-
P3.5	Provide manual propulsion control capability	"	C	Critical during transition to/from automated mode while in mixed traffic.	V	-
P3.6	Provide manual brake control capability	"	C	Critical during transition to/from automated mode while in mixed traffic.	V	-
P3.7	Provide operator AHS input capability	Provide means for operator to convey information to AHS. Keypad, voice recognition, etc., are all examples.	C	If responses to manual readiness tests are false positives, can revert to manual mode in error.	V	-
P4	Store/provide maintenance history	Maintain record of when maintenanceand or inspection was last performed on given system elements.	?E?	Only an isolation function? I.e., tire tread depth knowledge is a nicety if you can determine inadequate traction, irrespective of cause.	R/V	Could be on-board, with more opportunity for spoofing.
P5	Provide receiver channel from the roadside	The physical layer receives control commands from the regulation layer.	C		V/R	Mostly vehicle functions.
P6	Provide transmitter channel to the roadside	The physical layer provides sensory information and user's request to the regulation layer.	C		V/R	"
P7	Provide receiver channel from adjacent vehicle	Obtain information on neighboring vehicles, such as location and potential actions.	C	Depends on whether information required for lat/long control loop. Critical if part of vehicle obstacle detection. Implies mechanization.	V	-
P8	Provide transmitter channel to adjacent vehicle	Information on existence, upcoming commands and actions are conveyed.	C	Depends on whether information required for lat/long control loop. Critical if part of vehicle obstacle detection. Implies mechanization.	V	-

P9	Perform secondary functions	The secondary functions that exist on the existing vehicles such as windshield wipers, defroster and lights will be incorporated in the AHS.	C	Short exposure time for mixed traffic conditions. Critical secondary functions identified to date are those which affect driver visual performance. Other systems have been exercised in auto mode, except manual input modes, noted above.	V	
P10	Provide electrical power	Provide power for electronics, any electrically powered actuators, lights, displays, etc.	C	Criticality is determined by the subsystem consuming the power. Since some of these subsystems are critical (e.g. brakes), power supplied to them must be.	V	
P11	Obtain ID	Provide means for roadside to obtain ID of vehicle. Presence of this function implies that the ID is not trasmitted via the standard comm link.	E	Loss of ID will result in denied check-in	R	Assumes roadside uses ID to look up inspection records on check-in
P12	Provide ID	Provide a unique vehicle identifier to the roadside. This identifier is used to key inspection records and past performance history.	E	Same as above	V	-

DERIVATION OF FORMULAS FOR PROBABILITY OF UPCROSSING FOR DISCRETELY SAMPLED STATIONARY ONE-DIMENSIONAL GAUSSIAN PROCESSES

Let $X(t)$ be a continuous one-dimensional stationary, gaussian stochastic process. Let $\{0, h, 2h, \ldots, Nh = T\}$ be the discrete times at which we are interested. We wish to derive formulas for the expected number of times the sampled process crosses a threshold A over the time interval $\{0, T\}$.

The two-dimensional process $\{ X(t), X(t+h) \}$ is a stationary bi-gaussian distribution. Hence we can derive the following for the upcrossing expectation:

expected number of upcrossings = $\mathrm{E}(\#i\text{: } X(ih) < A < X((i+1)h) \textit{ for } i = 0 \ldots N-1)$

(49)

$$= \sum_{i=0}^{N-1} \Pr(X(ih) < A < X(ih+h))$$

$$= {}^{T}\!\!/_{h} \cdot \Pr(X(0) < A < X(h))$$

Let us define:

^{2} variance of $X(t)$

$= \mathrm{E}(X(t)^2)$

(50)

correlation over interval h

$$= \frac{\mathrm{E}(X(t)X(t+h))}{\mathrm{E}(X(t)^2)}$$

(51)

P_0 single interval probability of upcrossing

$= \Pr(X(0) < A < X(h))$

(52)

a normalized threshold

$= A\!\!/$

(53)

The distributions $X(t)$ and $X(t+h)$ are correlated and jointly-gaussian with variance ^{2} and correlation . By looking at normalizing them , we see that if we let x and y be correlated jointly-gaussian distributions with unit variance and a correlation coefficient of , we will have:

$P_0 = \Pr(x < a < y)$.

(54)

The joint probability density of x and y has the general form:

$f(x,y)$ joint density of x and y

$$= \frac{1}{2} \frac{1}{\sqrt{1-\ {}^{2}}} \exp\left(-\tfrac{1}{2} \frac{x^2 - 2\ \ xy + y^2}{1-\ {}^{2}} \right).$$

(55)

Therefore we can write P_0 as a two-dimensional integral

$$P_0 = \iint_R \frac{1}{2} \frac{1}{\sqrt{1-\ {}^{2}}} \exp\left(-\tfrac{1}{2} \frac{x^2 - 2\ \ xy + y^2}{1-\ {}^{2}} \right) dx\, dy$$

(56)

over the region

$$R = \left[\{x,y\} : x < a < y \right].$$

(57)

Through the bilinear transformation

$$u = \frac{1}{\sqrt{1+\ }} \frac{1}{\sqrt{2}} (y+x), \qquad v = \frac{1}{\sqrt{1-\ }} \frac{1}{\sqrt{2}} (y-x),$$

(58), (59)

the new distributions u and v will be independent unit gaussian distributions, and so we have

$$P_0 = \iint_S \frac{1}{2} \exp\left(-\tfrac{1}{2} (u^2 + v^2) \right) du\, dv$$

(60)

over the region

$$S = \left[\{u,v\} : v > \sqrt{\tfrac{1+}{1-}} \cdot \left| u - \sqrt{\tfrac{2}{1+}}\ a \right| \right].$$

(61)

We can now write the double integral as two iterated integrals

$$P_0 = \int_{u=\sqrt{\frac{2}{1+}}a}^{\infty} \int_{v=\sqrt{\frac{1+}{1-}}u-\sqrt{\frac{2}{1-}}a}^{\infty} \frac{1}{\sqrt{2}} e^{-\frac{1}{2}v^2} dv \cdot \frac{1}{\sqrt{2}} e^{-\frac{1}{2}u^2} du$$

(62)

$$+ \int_{u=-\infty}^{u=\sqrt{\frac{2}{1+}}a} \int_{v=\sqrt{\frac{2}{1-}}a-\sqrt{\frac{1+}{1-}}u}^{\infty} \frac{1}{\sqrt{2}} e^{-\frac{1}{2}v^2} dv \cdot \frac{1}{\sqrt{2}} e^{-\frac{1}{2}u^2} du .$$

(63)

The inner integrals can be solved in terms of the special error function

$$\operatorname{erf}(x) = \frac{2}{\sqrt{\ }} \int_0^x e^{-t^2} dt$$

(64)

which yields:

$$P_0 = \int_{u=\sqrt{\frac{2}{1+}}a}^{\infty} \tfrac{1}{2} \left(1 - \operatorname{erf}\left(\tfrac{1}{\sqrt{2}}\left(\sqrt{\tfrac{1+}{1-}}u - \sqrt{\tfrac{2}{1-}}a\right)\right)\right) \frac{1}{\sqrt{2}} e^{-\frac{1}{2}u^2} du$$

(65)

$$+ \int_{u=-\infty}^{u=\sqrt{\frac{2}{1+}}a} \tfrac{1}{2} \left(1 - \operatorname{erf}\left(\tfrac{1}{\sqrt{2}}\left(\sqrt{\tfrac{2}{1-}}a - \sqrt{\tfrac{1+}{1-}}u\right)\right)\right) \frac{1}{\sqrt{2}} e^{-\frac{1}{2}u^2} du .$$

(66)

If we use the change of variable

$$u_{new} = \tfrac{1}{\sqrt{2}}\left(\sqrt{\tfrac{1+}{1-}}u - \sqrt{\tfrac{2}{1-}}a\right)$$

(67)

for the first integral, and the change of variable

$$u_{new} = \tfrac{1}{\sqrt{2}}\left(\sqrt{\tfrac{2}{1-}}a - \sqrt{\tfrac{1+}{1-}}u\right)$$

(68)

for the second integral, we can consolidate the integrals into one integral with the form:

$$P_0 = \sqrt{\tfrac{2(1-\ )}{1+}} \int_0^{\infty} \tfrac{1}{2}(1 - \operatorname{erf}(u)) \tfrac{1}{\sqrt{2}} \Big(\exp\left(-\tfrac{1}{2}\left(\sqrt{\tfrac{2}{1+}}a + \sqrt{\tfrac{2(1-\ )}{1+}}u\right)^2\right)$$
$$+ \exp\left(-\tfrac{1}{2}\left(\sqrt{\tfrac{2}{1+}}a - \sqrt{\tfrac{2(1-\ )}{1+}}u\right)^2\right)\Big) du .$$

(69)

Define normalizations

$$= \sqrt{\frac{2(1-\ )}{1+}}$$

(70)

$$A \;\; = \sqrt{\frac{2}{1+\;}}\; a = \sqrt{\frac{2}{1+\;}}\; A\!\!/ \qquad .$$

(71)

Then

$$P_0 \;\; = \int_0^\infty \tfrac{1}{2}(1-\mathrm{erf}\,(u))\,\frac{1}{\sqrt{2}}\Big(\exp(-\tfrac{1}{2}(A \;\; + \quad u)^2)+\exp(-\tfrac{1}{2}(A \;\; - \quad u)^2)\Big)du\,.$$

(72)

Note that asymptotically, as $h \to 0$, we will have $\;\; \to 1$, $\;\; \to 0$, and $A \;\; \to A\!\!/$. We now introduce some lower and upper bounds:

$$2e^{-\frac{1}{2}A^2} \quad 2\; \exp(-\tfrac{1}{2}(A \;\; + \quad u)^2)+\exp(-\tfrac{1}{2}(A \;\; - \quad u)^2)$$

$$2\; e^{-\frac{1}{2}A^2}\,(e^{- \quad A\; u} + e^{\quad A\; u}).$$

(73)

Substituting the bounds into the basic integral gives bounding integrals that can be integrated exactly. The resulting formulas are:

$$\frac{1}{\sqrt{2}}\,\frac{1}{\sqrt{\;}}\,e^{-\frac{1}{2}A^2} \quad 2\;\; P_0 \;\; 2 \qquad \frac{1}{\sqrt{2}}\,\frac{1}{\;A}\,e^{\frac{1}{4}\;\;{}^2A^2}\,erf(\tfrac{1}{2} \quad A\;)e^{-\frac{1}{2}A^2}\;\; .$$

(74)

Upper and lower bounds on the total expected number of upcrossings can then be expressed as:

$$T\!\!/\!h \qquad \frac{1}{\sqrt{2}}\,\frac{1}{\sqrt{\;}}\,e^{-\frac{1}{2}A^2} \quad 2 \text{ expected number of upcrossings}$$

$$2\; T\!\!/\!h \qquad \frac{1}{\sqrt{2}}\,\frac{1}{\;A}\,e^{\frac{1}{4}\;\;{}^2A^2}\,erf(\tfrac{1}{2} \quad A\;)e^{-\frac{1}{2}A^2}\;\; .$$

(75)

The actual integral mentioned above can also be solved numerically to give an accurate expected number of crossings. Numerical studies of the motion detection processes indicated that the upper bound is quite close to the actual values.

AHS COMPONENT FAILURE RATE DATA

QUANTIFYING SYSTEM RELIABILITY

Introduction

System design of AHS health management involves identifying and quantifying the primary contributors to AHS reliability and safety. This process depends to some degree on failure rate data of AHS components. This section of the report describes the methodology employed by project personnel to generate the necessary data and the results of this effort. Failure rates for both the vehicle and roadside subsystems have been generated. In addition, results illustrate graphically the impact of certain environmental factors on failure rate for those vehicle components where factors are obtainable from technical literature.

Procedure

For the vehicle subsystem, began by generating a listing of all automotive component types for which failure rate values were needed from a review of the block diagrams for steering, throttle, ABS, cooling, engine lube and electrical power. When the project began, what was considered the best failure rate source -- NPRD-91 -- was consulted first.[13] However, during the project a copy of NPRD-95,[26] the successor to NPRD-91, was obtained. This document contains 56% more data than presented in its predecessor, NPRD-91, so all previous data was reviewed and updated whenever improved data was found in NPRD-95. After this updating was completed, of a total of 62 vehicle component types, 42 were found listed in NPRD-95. MIL-HDBK-217F was data source for 8 component types.[12] A search of GIDEP R/M Databooks was then performed for component types not found either in NPRD-95 or MIL-HDBK-217F.[9] This yielded failure rate data for 5 more. For the remaining 7, use of judgment values determined from ranking by experts was the technique employed. These experts used their experience with automotive failures to rank components in order by failure rate. S ince failure rates for some of these ranked components were available from NPRD-95, MIL-HDBK-217F or GIDEP, assigning failure rates to the rest by the "bracketing" process was accomplished in a fairly straightforward manner.

A literature search for vehicle failure rate data was performed, with essentially negative results. All knowledgeable people contacted stated that there were no industry-wide sources of automotive failure rates.

The use of generalized data bases such as NPRD-91, NPRD-95 and GIDEP involved considerable engineering judgment. Care had to be taken to select that data source which best fit the commercial automotive environment. Some of the criteria used in this selection process were as follows:

- Commercial preferred over military
- Ground mobile preferred over other environments

- Preference given to larger number of operating hours to reduce risk of picking a data-limited source

- Failure rate preferred over replacement rate for GIDEP data

- Failure rate had to meet reasonableness test

For the roadside subsystem, the process was somewhat similar to that for the vehicle subsystem. The starting point involved block diagrams for protocol processor, LAN adapter, longitudinal sensor, sensor suite, line/check-in controllers, network controller, host typical architecture and link controller. MIL-HDBK-217F was the primary data source for roadside component failure rates due to these components being primarily electronic in nature. Of a total of 51 items, MIL-HDBK-217F was data source for 34. Of the remaining 17, NPRD-91 was data source for 9, GIDEP was data source for 3, Honeywell Microwave Systems was data source for 3 and judgment was used for 2. Of the criteria used for judgment in the selection process, Ground Fixed sources were preferred for roadside failure rates.

Results

Vehicle component failure rates are shown in table 12. Failure rates in this table are applicable to the G_M environment as described in MIL-HDBK-217F. In this listing, there are three items where the component failure rate calculation was based on the assumption that the average speed of a military truck is 30 miles per hour; these items are water pump, fuel flow/injection and radiator. (NOTE: Failure rate for these 3 items are directly proportional to the assumed value of speed in miles per hour).

Roadside component failure rates are shown in table 13, "Component Failure Rates for AHS Roadside Subsystem (G_F Environment). Failure rates in this table are applicable to the G_F environment as described in MIL-HDBK-217F.

Environmental Factors for Vehicle Components

This section of the report covers all effort to develop factors (for vehicle components) which alter the failure rate including environmental factors and factors for off-design characteristics.

PROCEDURE

A literature search was not successful, which is most likely due to the same reason that automotive failure rate data could not be obtained in the first place (see above). In view of this, a decision was made to use data from "Handbook of Reliability Prediction Procedures for Mechanical Equipment" and adapt it for the purpose intended for non-electronic components in table 12.[27] For those table 12 items which are also found in MIL-HDBK-217F (for example, electric motors) in general the failure rate/temperature relationships found therein were used. In all, curves were plotted for 14 component types. Data sources used in developing these curves are identified in detail in table 14.

Results

Failure rate environmental factor results are provided in the form of characteristic curves. These curves are figures 109 through 124 of this report.

Literature Search Methodology and Results

The literature search task was carried out by the Honeywell MA/MO Technical Library, by contacting various parties both (1) directly by telephone and (2) indirectly through DTIC and NERAC. This was a major effort by the librarian, with many man-hours spent in what turned out to be essentially a fruitless task.

The major difficulty was the proprietary nature of the information sought. All of the manufacturers who were contacted, both domestic and foreign, admitted to possessing proprietary data bases on automotive component failure rates and tire tread wear rates but had absolutely no knowledge of any independent data base source. They would not, of course, disclose any of their own proprietary information. In fact, phone inquiries were immediately referred to Customer Service in most cases, with the impression left that attempts to obtain data of this nature were not welcomed. In addition to automotive manufacturers, other potential data sources contacted were as follows:

U. S. Department of Transportation (DOT), Society of Automotive Engineers (SAE), J. D. Power and Associates and the Detroit Public Library. No one contacted knew of any existing source of automotive component failure rate data.

The Ford Motor Company provided the best lead of all for similar efforts in the future. Ford supplied the name and address of a leasing company, Peterson, Howell and Heather (PHH). They lease cars, trucks and other vehicles. They initiated a data base compilation effort in the 1980's, which has since been discontinued. When contacted, PHH stated they were planning to re-initiate this effort and resume the service of providing this data (for a price).

A listing of contacts follows:

(1) <u>Automotive Manufacturers</u>

(a) Domestic

1. General Motors (GMC)
   - William Kerscher (810)-257-8686

2. Ford Motor Company
   - Patrick Daum (313)-845-8991
   - Bob Samas (313)-258-5836 (Compiles data base)
   - Ed Russell (313)-322-3000

3. Chrysler
   - Reliability/Quality (313)-556-6163
   - Technical Center (313)-956-5252

(b) Foreign

1. Honda (310)-783-2000 (Public

Relations)

2. Nissan (310-532-3111
[Norma Romo- Public Affairs (310)-719-3264]

3. Diamond Star (309)-888-8000
(Quality - Dave)

4. Nummi (Geo and Toyota) (510)-498-5500

5. Subaru (609)-488-8500
(800)-782-2783 (Customer
Service)

6. Toyota (502-868-2000
(502)-868-2072 (Legal -
Patrick)

7. Association of International Automobile Manufacturesrs
(AIAM) - All other foreign
(703)-525-7788 (Technical
Dept. - Laura)

(2) <u>Government - Department of Transportation (DOT)</u>

National Highway Traffic and Safety Administration (NHTSA)

(202)-366-9550
(800)-424-9393 Hot Line
(Recalls and collects information on failures; initiates analysis, does <u>not</u>
disseminate this information)

(a) Research & Development Dept.
(202)-366-4862

(b) Office of Defects Investigation
(202)-366-2850

(c) Special Traffic Safety Investigation
(202)-366-6359 (Julie Abrahamson - Investigates customer
complaints as evidence to frame a case)

(d) National Center For Statistical Analysis
(202)-366-5380
(202)-366-1503 (Deals with fatal accident statistics)

(e) Rule-Making
(202)-366-4805

(202)-366-1810

(f) Technical Reference Library
(202)-366-2768

(3) <u>Other Sources</u>

(a) Highway Loss Data Institute (HLDI)
(703)-247-1600 (Investigates only injury/collision by model).

(b) Insurance Institute for Highway Safety (IIHS)
(703)-247-1500 Communications Dept. (Investigates effectiveness of seat belts, air bags, etc.)

(c) Auto Safety Hotline
(800)-424-9393 (Model defect recall reports)

(d) Consumer Reports
(914)-378-2562 (Does not do ratings)

(e) J. D. Power & Associates
(818)-889-6330 Lance Wilcox (Auto consumer survey - releases information on problerm cars)

(f) Peterson, Howell and Heather (PHH)
(410)-711-2945 Joe Silvestri & John Callahan
(410)-771-3600 (Leasing of cars and trucks - had such database in 1980's - planning to resume in near future, but nothing right now. This was the most promising lead. Referred to them by Ford Motor Co. - Did at one time sell this information to Ford.)

(g) American Automobile Manufacturers (AAM)
(202)-326-5500 (No data)

(h) AAA
(407)-444-7000 (No data)

(i) Automotive Engine Rebuilders Association (AERA)
(708()541-0250 (No data)

(j) Automotive Parts Rebuilders Association
(703)-968-2772 (Machine shops)
(216)-535-6117 Scott Hachman

(k) Auto Research labs

(708)-210-9987 Fred Blatz (No data)

(l) Society of Automotive Engineers (SAE)
(412)-776-4841 Arlan Stehney (IVHS) Develops
standards
Ext. 156

(m) Detroit Public Library
(303)-833-1456 (Mark Patrick - Curator)

(4) Tire Manufacturers

NERAC contacted major tire companies.

(5) Tire Associations - Domestic

(a) National Tire Dealers and Retreaders Association (NTDRA)
(202)-789-2300

(b) Tire and Rim Association (TRA)
(216)-666-8121

(c) Motor Vehicle Manufacturers Association of the United States
(MVMA)
(313)-872-4311

(6) Professional Literature Search Groups

(a) Defense Technical Information Center (DTIC)

(b) NERAC, Inc. Search experts - contacted various sources either
themselves or provided names to Honeywell.
(203)-872-7000 Joe Thopsey
NOTE:J. Thopsey of NERAC called PHH and FHA with negative
results.

Table 12. Failure Rate Data

Component	Failure Per10^6 Hrs.	Subsystems						F.R. Source
		Steering	Throttle	ABS	Cooling	Engine Lube	Elect. Power	NPRD-95 Page No.
Pump Clutch	5.0	X						2-43
Hydraulic Reservoir	6.6	X						2-213
Brake Fluid Reservoir	6.6			X				2-213
Oil Reservoir	2.6					X		2-213
Hydraulic Pump	40.4	X		X				2-159
Fuel Pump	11.2		X					2-160
Oil Pump	28.2					X		2-160
Water Pump	77.9				X			2-162
Level Sensor	2.6	X		X				2-182
Pressure Sensor	5.9	X	X	X		X		2-219
Position Sensor	15.4	X		XX				2-219
Knock Sensor	7.0		X					Judgment
Air Flow Sensor	8.0		X					Judgment
Oxygen Sensor	20.0		X					Judgment
Speed Sensor	21.3		X	XX				2-182
Temperature Sensor	4.2				X			p.A7(217F)
Steering Wheel & Column	10.0	X						GIDEP
Power Steering Unit	50.0	X						Judgment
Wheel	2.0	X	X	X				GIDEP
Tie Rod (and other mech. links)	4.0	X						Judgment
Hydraulic Actuator	76.3	X						2-4
Throttle Valve Actuator	1.7		X					2-3
Wheel Brake Actuator (#2)	76.3			X				2-4
Actuator #1	25.8			X				2-3
Bypass Valve	5.1	X						2-226
Control Valve	5.1	X						2-226
Exhaust Gas Recircle Valve	8.8		X					2-235
Throttle Air Valve	4.0		X					2-232
Modulator (supply/disch. valve)	5.1			X				2-226
Isolation Valve	5.1			X				2-226
Relief Valve	8.8					X		2-235
Spark Plug/Coil	7.1		X					2-153 &
Cylinder/Piston/Rod	2.3		X					2-74
Electronic Ignition	40.0		X					Judgment
Crankshaft	33.3		X					2-73
Manifold	7.2		X					2-132
Transmission	25.0		X					GIDEP
Differential	4.6		X					2-76
Fuel Flow/Injection	5.8		X					2-122
Fuel Tank and Line	8.9		X					2-95 &
Actuator Drive	1.0			X				GIDEP
Brake Pedal	12.5			X				2-148
Vacuum Booster	28.2			X				2-161
Master Cylinder	40.0			X				GIDEP
*Motor *(217F)*	3.3			X				P. A9 *
Radiator	6.6				X			2-112
Thermostat	2.3				X			2-217
Oil Cooler	13.5					X		2-68
Oil Filter	6.7					X		2-134
Alternator	6.8						X	2-8

Battery	30.0						X	2-13
Regulator	29.5						X	2-165
Short throw solenoid actuator	22.5							2-4
Hydraulic accumulator	13.7							2-2
Antenna	4.55							Judgment
RF switch (217F)	19.0							pp A5/A6
CMOS driver and logic (217F)	0.66							p. A2
ROM memory (217F)	0.45							p. A3
Clock generator (217F)	0.94							pp. A2,A4,
Intercom line - cable only	0.02							2-30
Intercom line - cable plus IC chip	0.47							p. A2

Table 13. Component Failure Rates for AHS Roadside Subsystem (GF Environment)

Assembly	**Component Type**	**λ (Fail/10^6 hrs.)**	**Failure Rate Source**
Protocol Processor	Master CPU 68020	1.7	MIL-HDBK-217F
	Shadow CPU 68020	1.7	MIL-HDBK-217F
	Common Clock, IT's, etc.	0.45	MIL-HDBK-217F
	Comparator	0.24	MIL-HDBK-217F
	Bridge	0.24	MIL-HDBK-217F
	Mask (2 x 0.15)	0.30	MIL-HDBK-217F
	RAM (2 x 0.53)	1.06	MIL-HDBK-217F
	ROM (2 x 0.65)	1.3	MIL-HDBK-217F
	Peripherals (Keyboard - 8.9 and Printer - 23.6)	32.5	GIDEP
	Buffer	0.26	MIL-HDBK-217F
	16/32 Swap buffer	0.26	MIL-HDBK-217F
	Crystal	0.20	MIL-HDBK-217F
LAN Adapter	38010	0.85	MIL-HDBK-217F
	38020	0.85	MIL-HDBK-217F
	38030	0.85	MIL-HDBK-217F
	Crystal	0.20	MIL-HDBK-217F
	RAM	0.53	MIL-HDBK-217F
	ROM	0.65	MIL-HDBK-217F
	Ring Interface	0.36	MIL-HDBK-217F
	Watchdog	0.15	MIL-HDBK-217F
Longitudinal Sensor	Antenna	1.82	HI Microwave Systems
(Radar)	MIMIC Chip	2.125	HI Microwave Systems
	Signal processor	3.4	MIL-HDBK-217F
Sensor Suite	Lateral Ranging sensor	5.9	NPRD-91
	Gate actuator	4.5	NPRD-91
	Object detection emissions sensor	5.9	NPRD-91
Link/Check-in controllers	Antenna	1.82	HI Microwave Systems
	Vehicle comm. transceiver	0.41	MIL-HDBK-217F
	Uninterruptible power supply	2.6	NPRD-91
	Data storage (disk)	17.8	GIDEP
Network controller	Modem	1.2	MIL-HDBK-217F
	Uninterruptible power supply	2.6	NPRD-91
	Data storage (disk)	17.8	GIDEP
Host typical architecture	SPARC module	3.4	MIL-HDBK-217F
	MACIO	1.7	MIL-HDBK-217F

	EMC	1.7	MIL-HDBK-217F
	SEC	1.7	MIL-HDBK-217F
	MMC VME Controller	1.7	MIL-HDBK-217F
	MSBI 64-bit S-Bus	0.36	MIL-HDBK-217F
	EPROM	0.38	MIL-HDBK-217F
	SRAM	0.23	MIL-HDBK-217F
	Parallel port	0.15	MIL-HDBK-217F
	85C30 K/M	0.36	MIL-HDBK-217F
	85C30 Serial I/O	0.36	MIL-HDBK-217F
	DRAM	0.23	MIL-HDBK-217F
Link controller	Road surface thermal sensor	2.4	NPRD-91
	Road surface reflectivity sensor	4.5	NPRD-91
	Vehicle presence detector (radar)	25	Judgment
	Road intruder detector (infrared)	15	Judgment
	Rainfall detector	3.6	NPRD-91
	Visibility detector/target	4.5	NPRD-91

Table 14. Environmental Factors - Data Sources

		Data Source:					
<u>Component</u>		**<u>NSWC-94L07</u>**	**<u>MH-217F</u>**	**<u>Other</u>**	**<u>Page No.</u>**	**<u>Notes</u>**	**<u>Figure</u>**
Pump clutch	No. of Applications	X			12-19		109
Reservoir/ Accum.	No. of Pulsations	X			1-9		110
	Temperature	X			3-22 &		111
					6-27		
Pump	Temperature	X			10-8		112
Sensors	Temperature		X		11-1		113
Valve	Temperature	X			6-27		114
	No. of Operations	X			1-9		115
Spark plug/coil	Temperature		X		11-1		116
Electronic ignition	Temperature			X	107	Note (1)	117
Crankshaft	Temperature	X			10-8		118
Actuator drive	Temperature			X	107	Note (1)	119
Electric motor	Temperature		X		12-1		120
Oil cooler	Temperature	X			3-22		121
Oil filter	Temperature	X			11-12		122
Alternator	Temperature		X		12-1		123
Hydraulic Accum.	No. of Pulsations	X			1-9		124

NOTES:

(1) Data source is page 107 of the Rome Laboratory Reliability Engineer's Toolkit. [28]

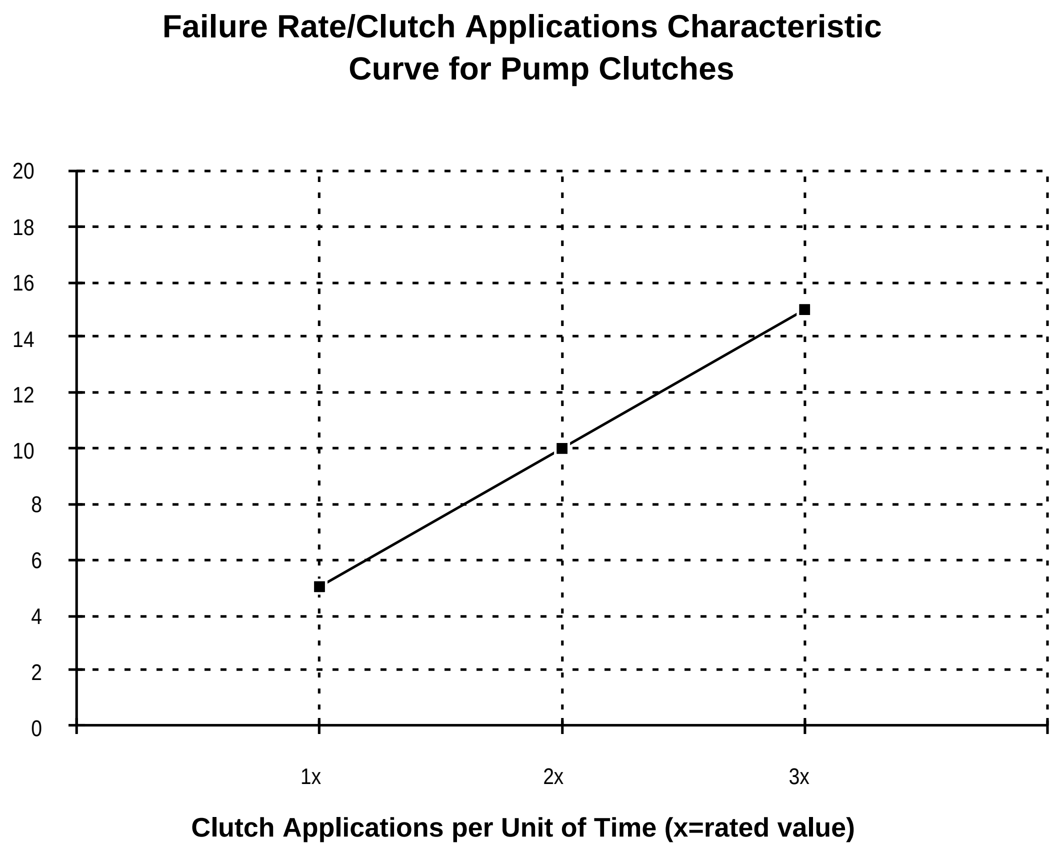


Figure 109. Failure Rate/Clutch Applications Characteristic Curve for Pump Clutches

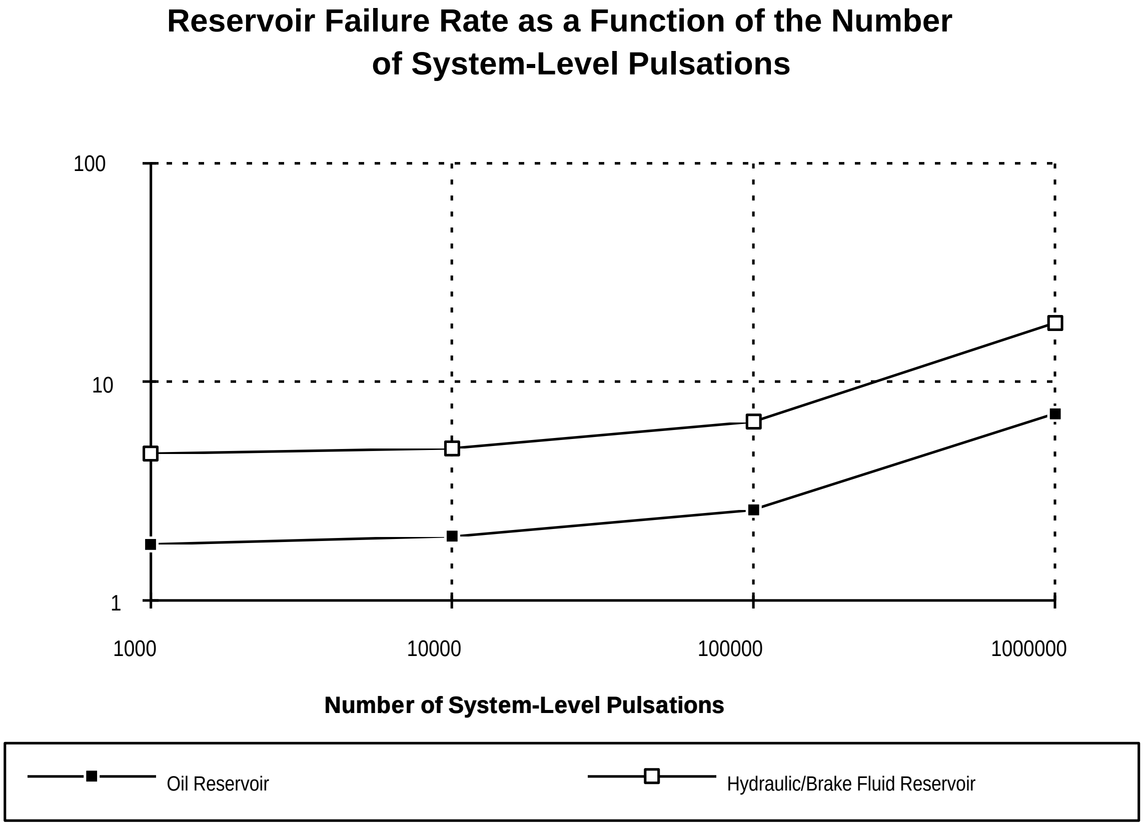


Figure 110. Reservoir Failure Rate as a Function of the Number of System-Level Pulsations

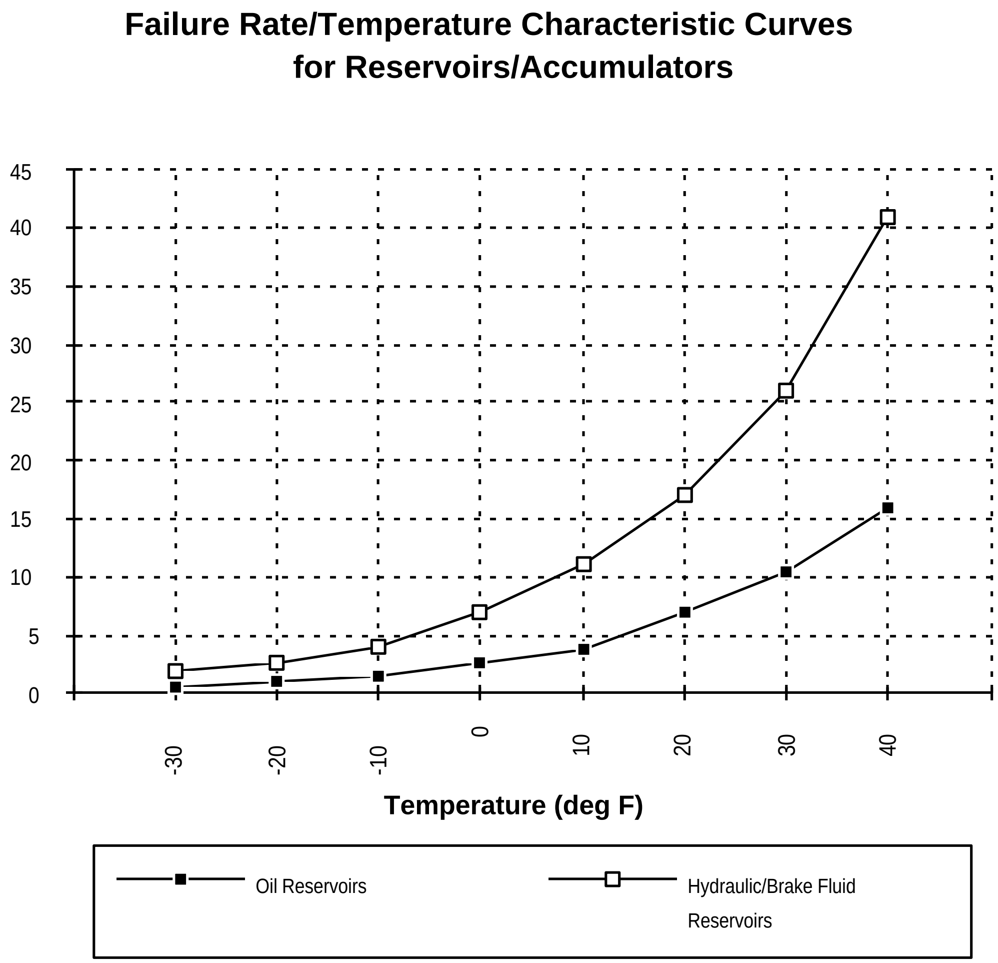


Figure 111. Failure Rate/Temperature Characteristic

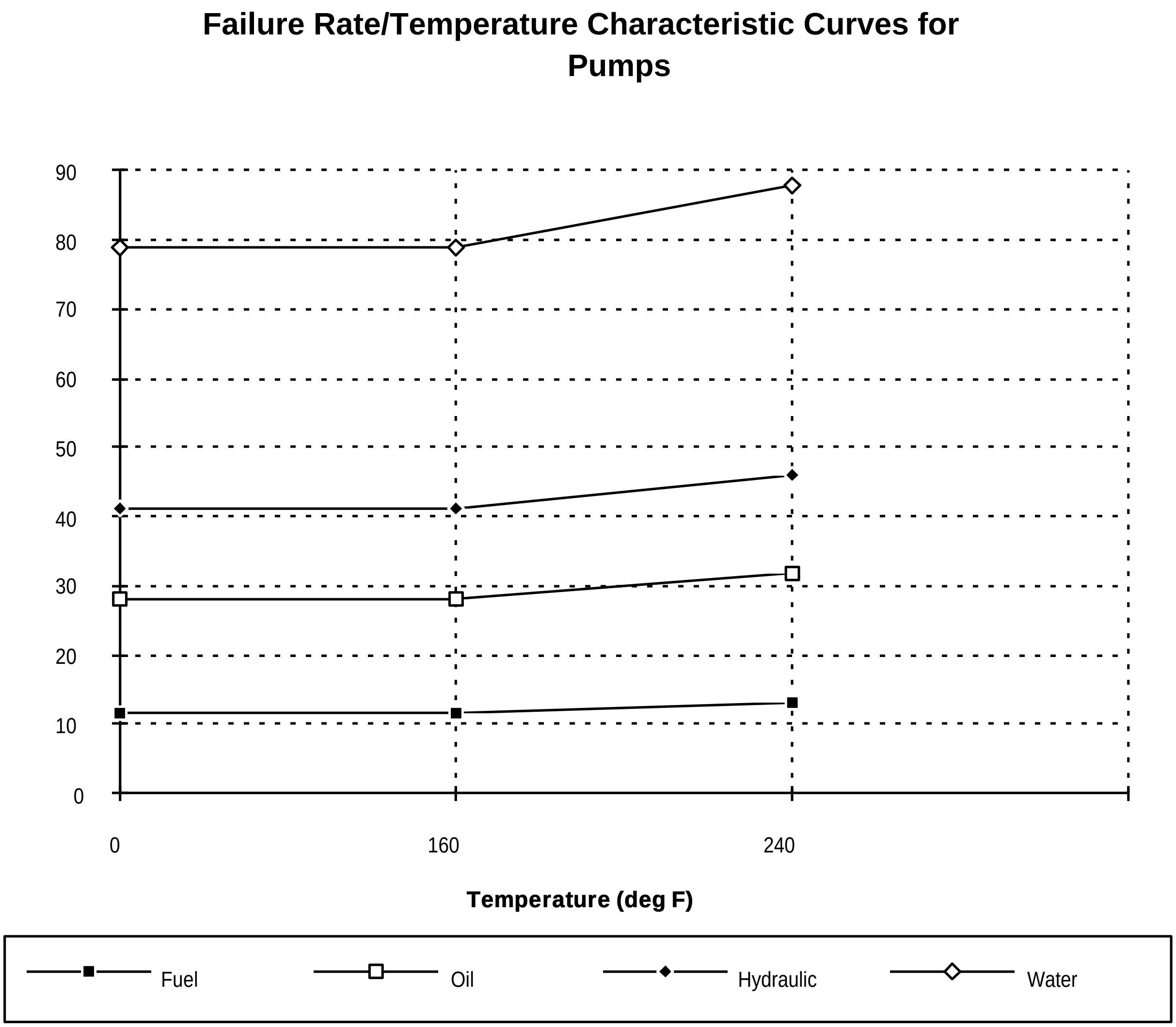


Figure 112. Failure Rate/Temperature Characteristic Curves for Pumps

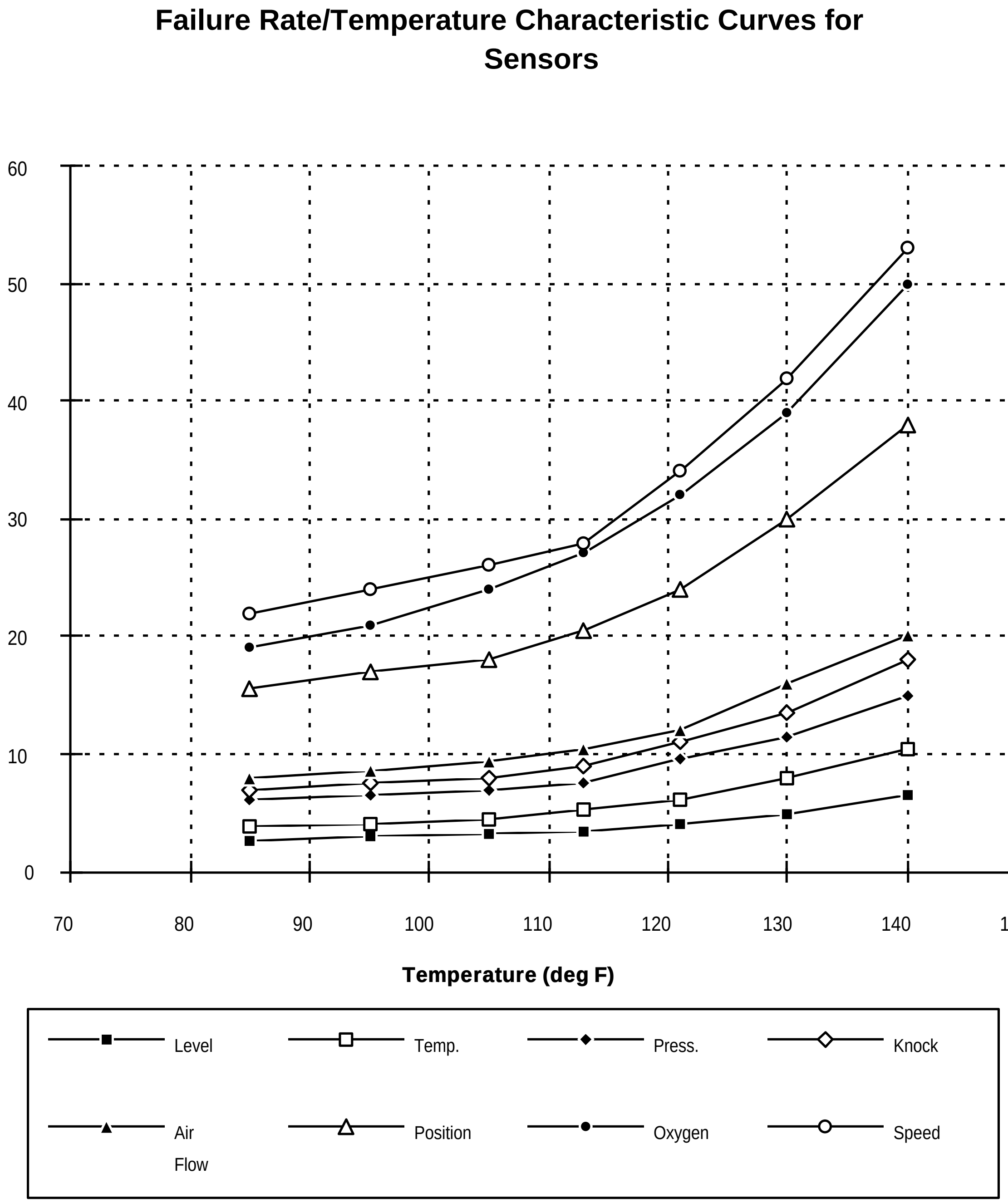


Figure 113. Failure Rate/Temperature Characteristic Curves for Sensors

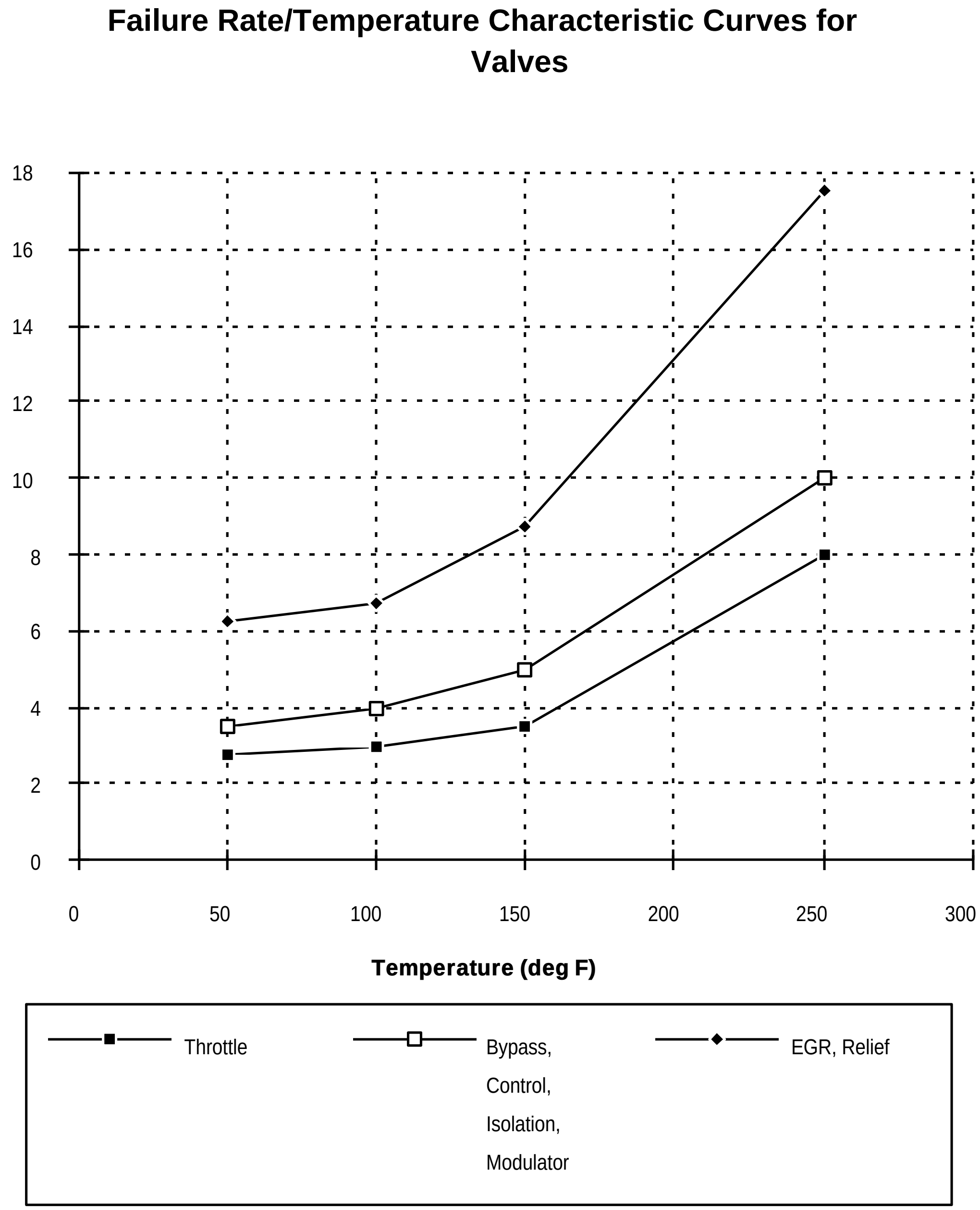


Figure 114. Failure Rate/Temperature Characteristic Curves for Valves

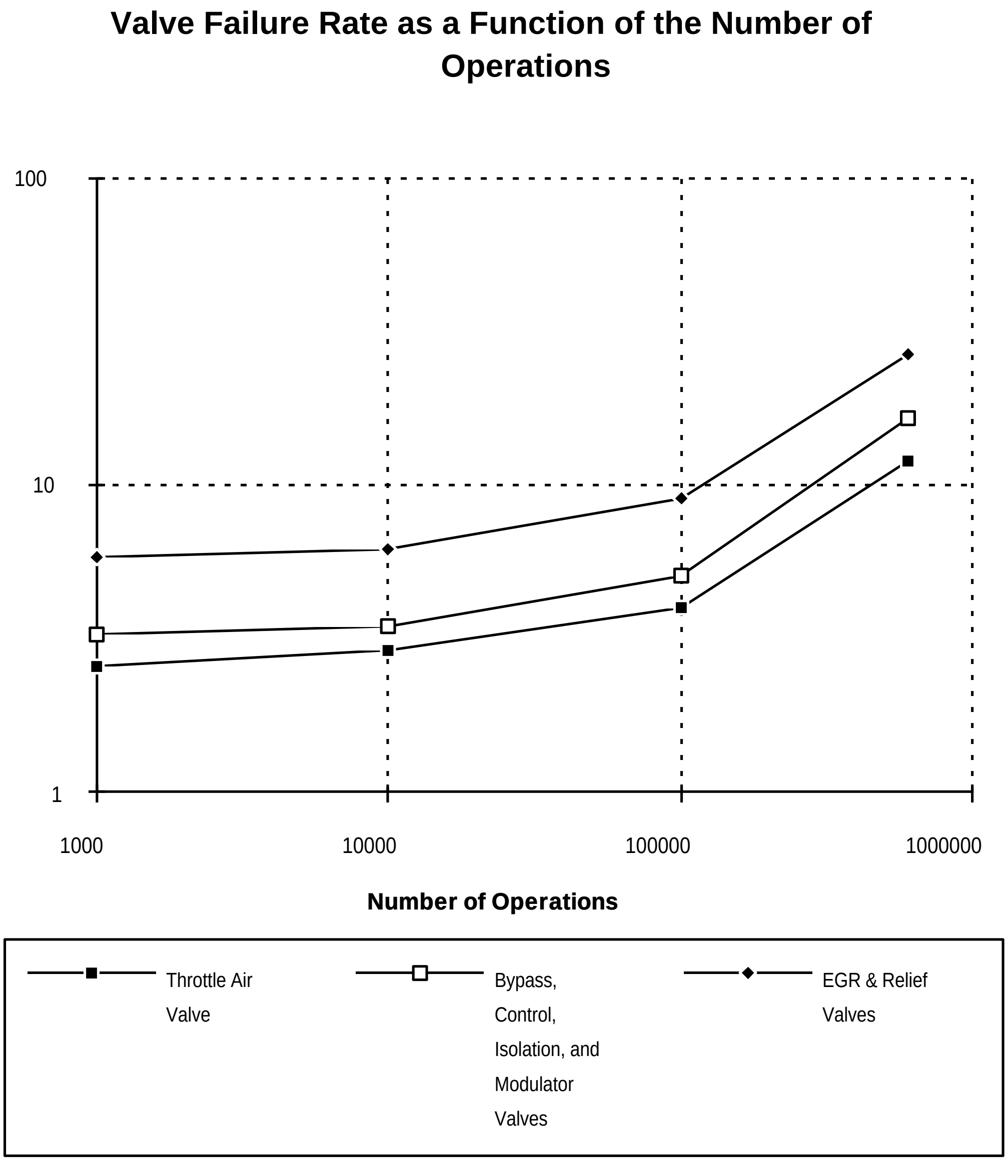


Figure 115. Valve Failure Rate as a Function of the Number of Operations

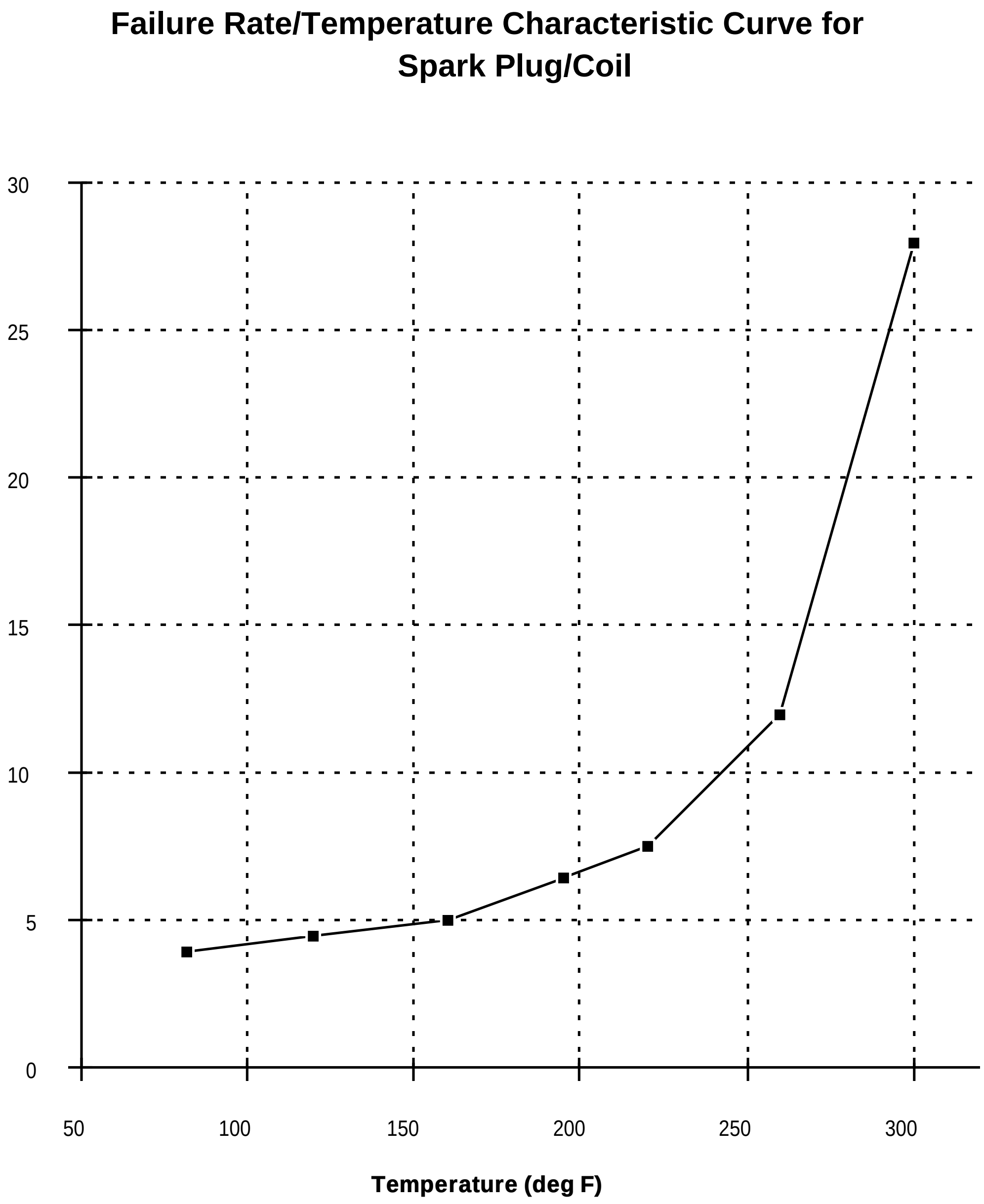


Figure 116. Failure Rate/Temperature Characteristic Curve for Spark Plug/Coil

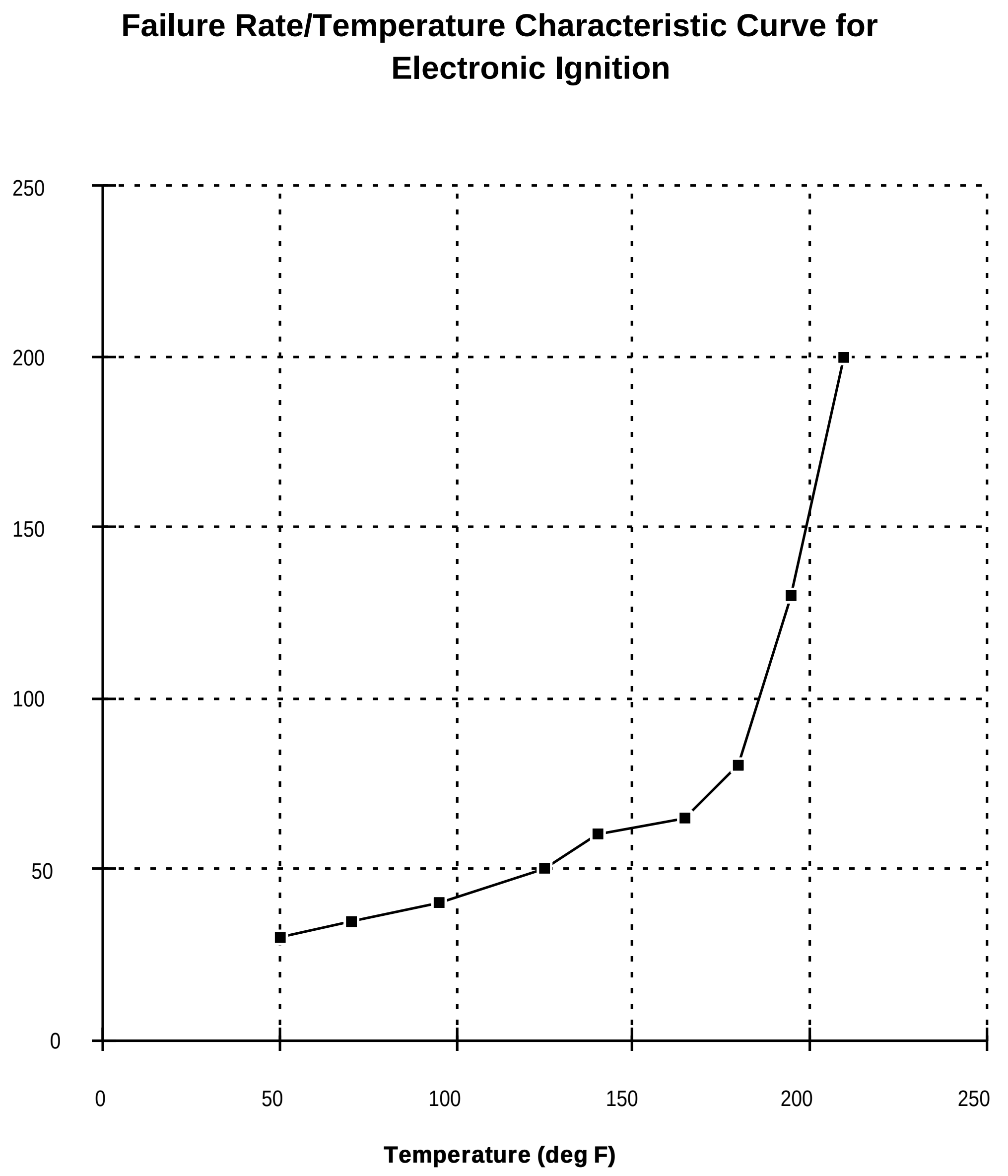


Figure 117. Failure Rate/Temperature Characteristic Curve for Electronic Ignition

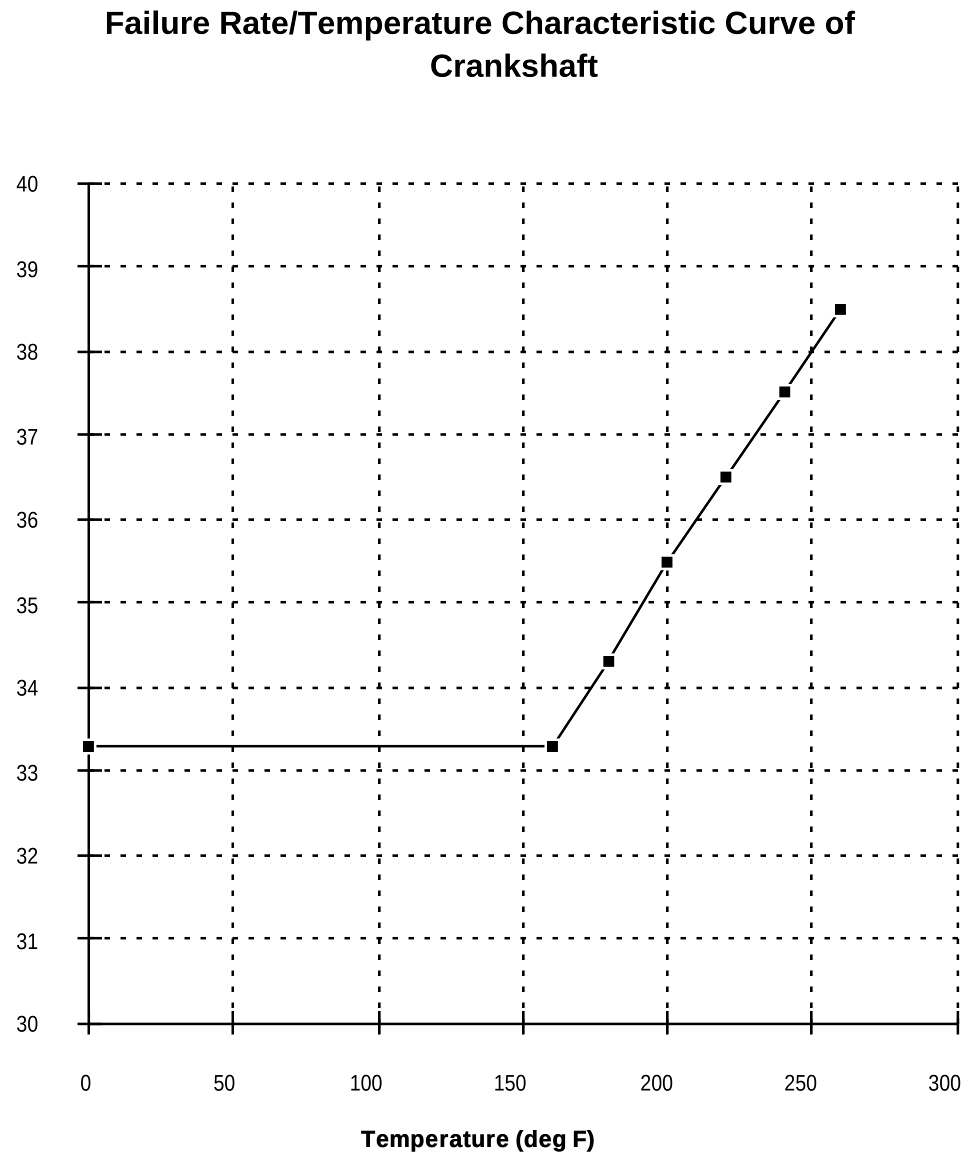


Figure 118. Failure Rate/Temperature Characteristic Curve for Crankshaft

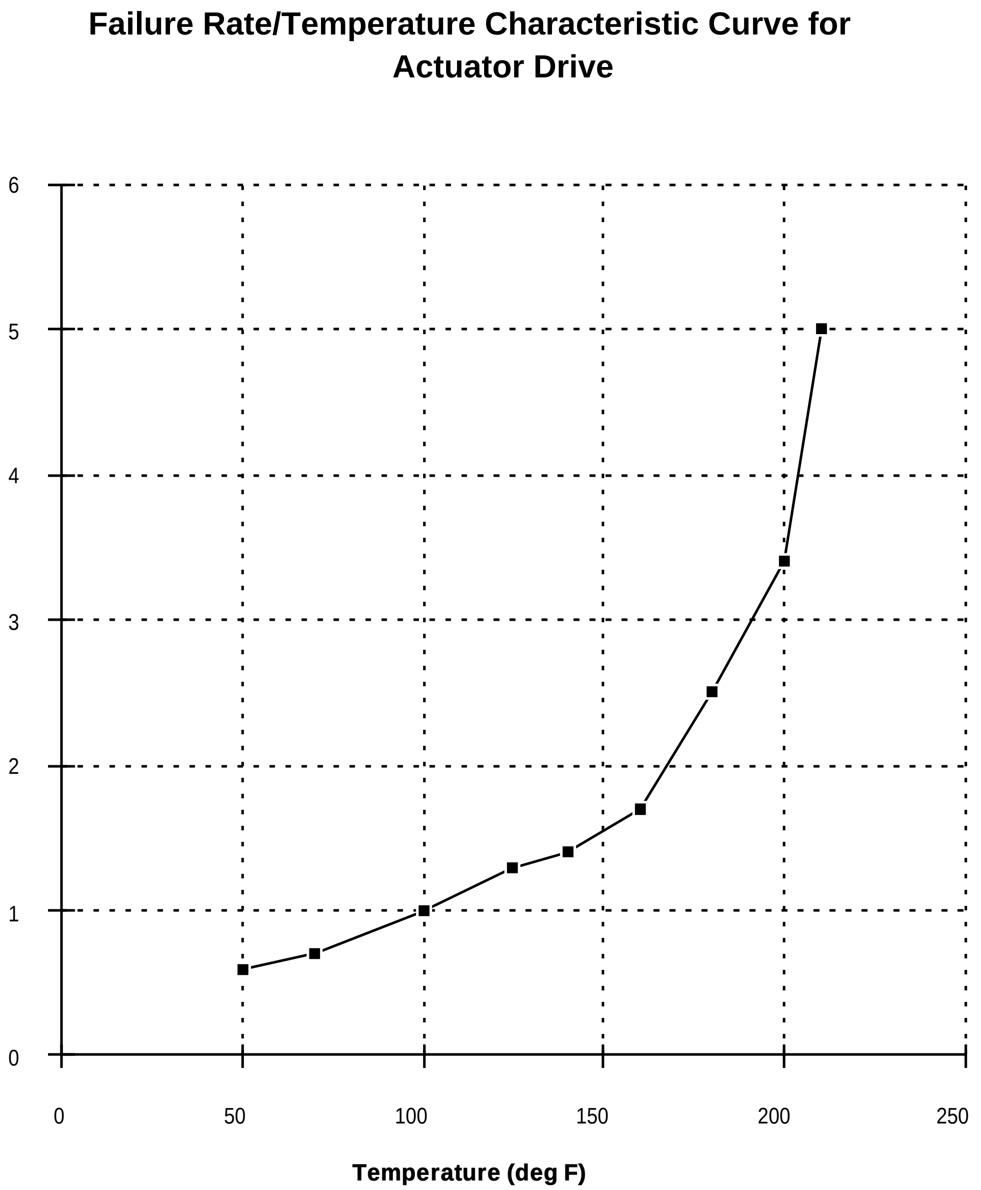


Figure 119. Failure Rate/Temperature Characteristic Curve for Actuator Drive

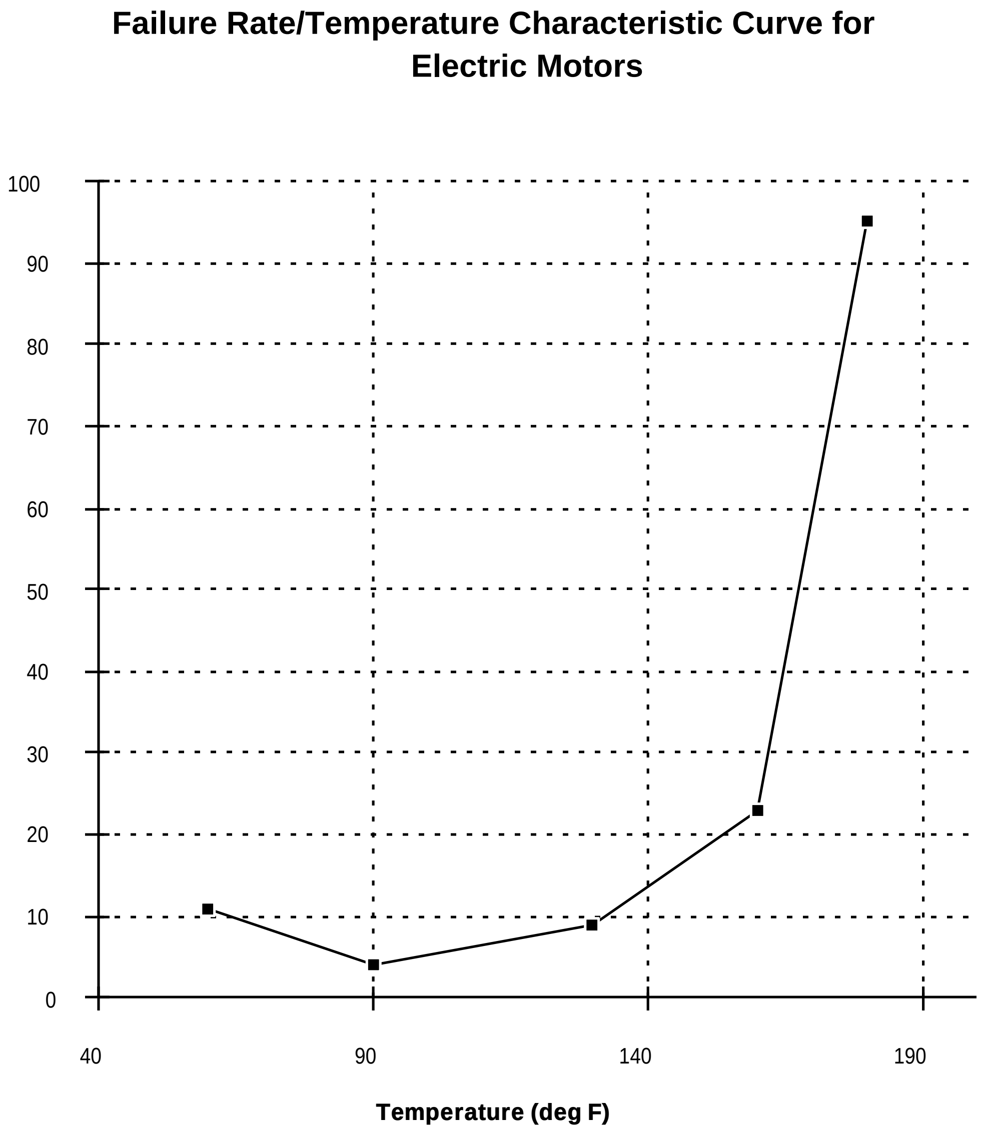


Figure 120. Failure Rate/Temperature Characteristic Curve for Electric Motors

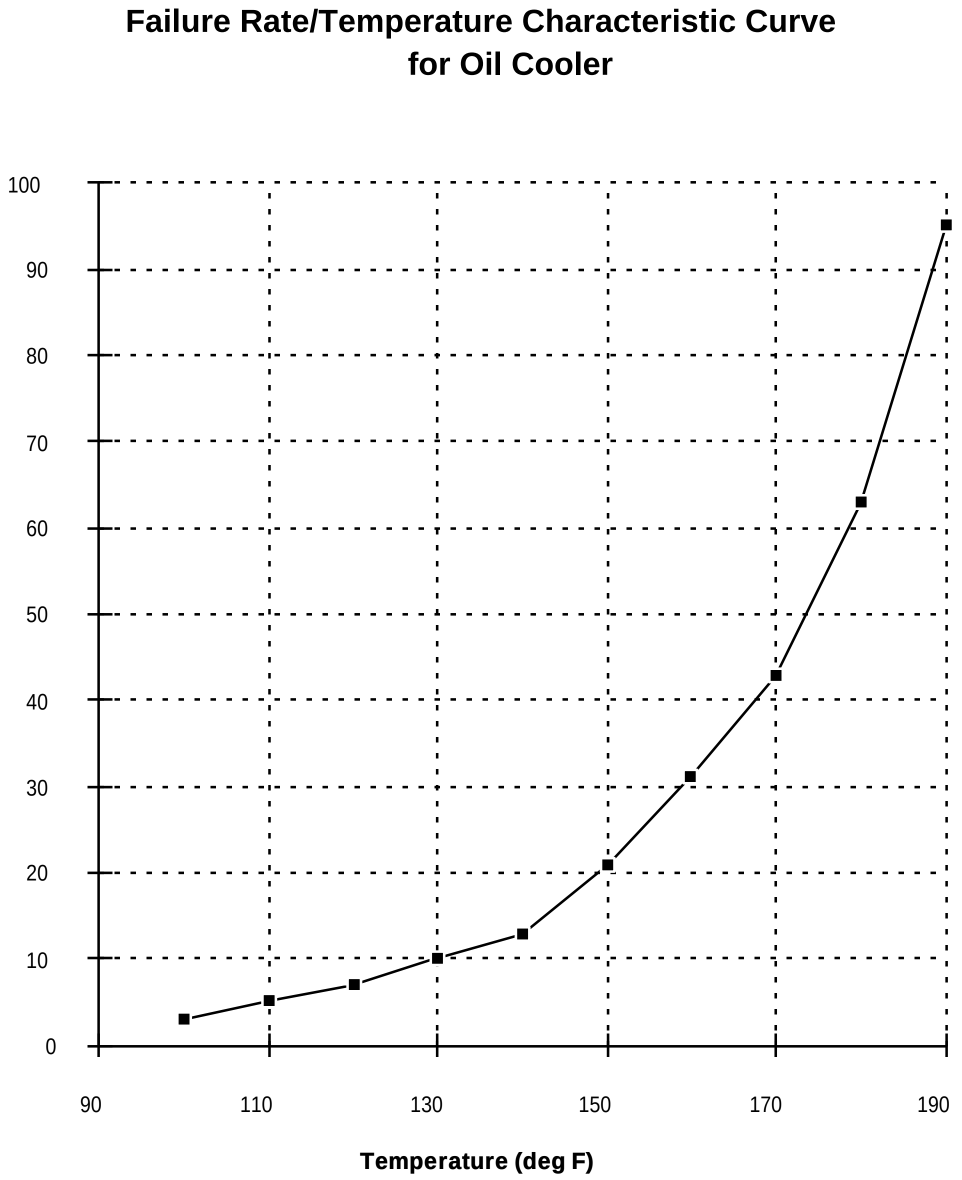


Figure 121. Failure Rate/Temperature Characteristic Curve for Oil Cooler

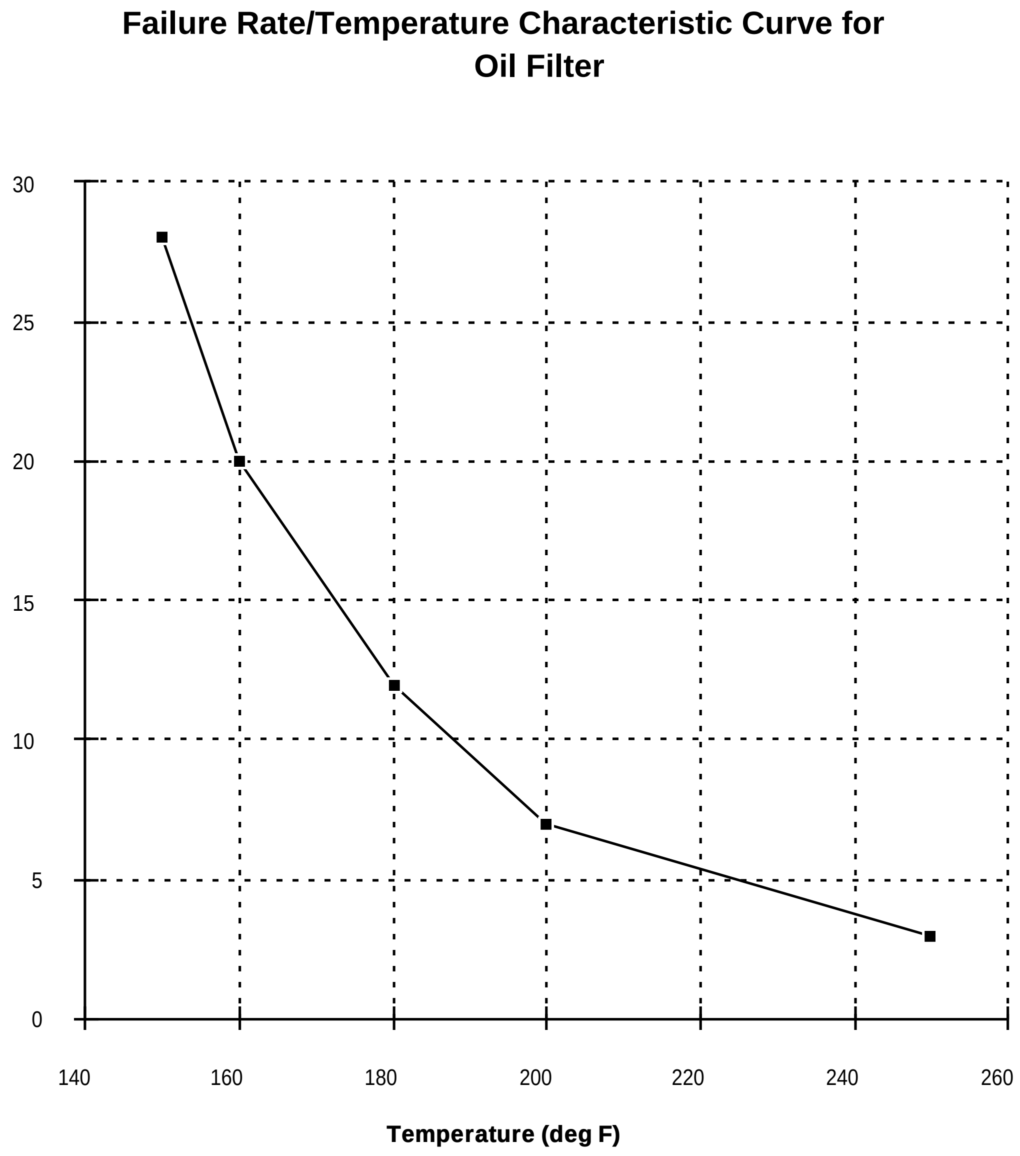


Figure 122. Failure Rate/Temperature Characteristic Curve for Oil Filter

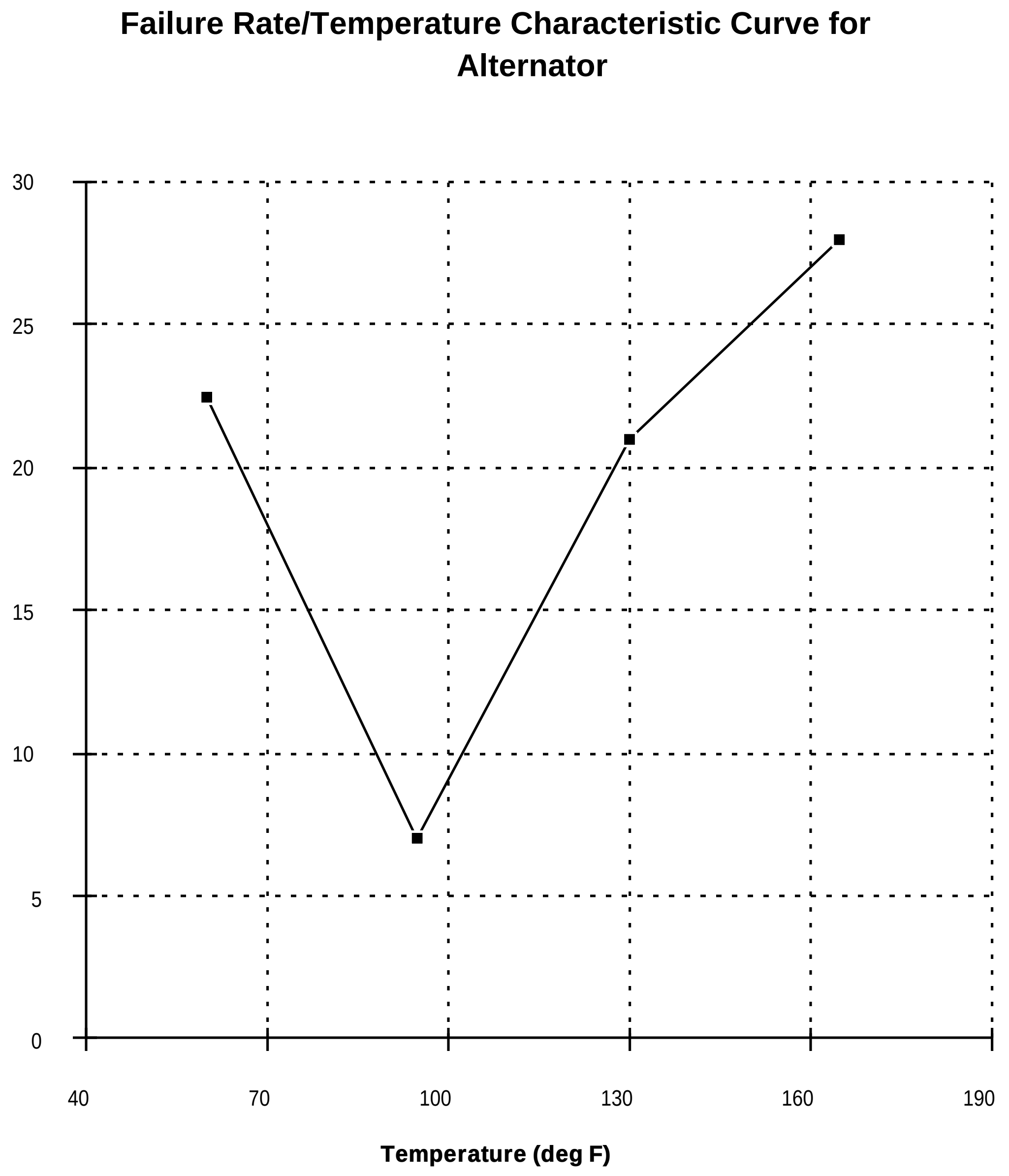


Figure 123. Failure Rate/Temperature Characteristic Curve for Alternator

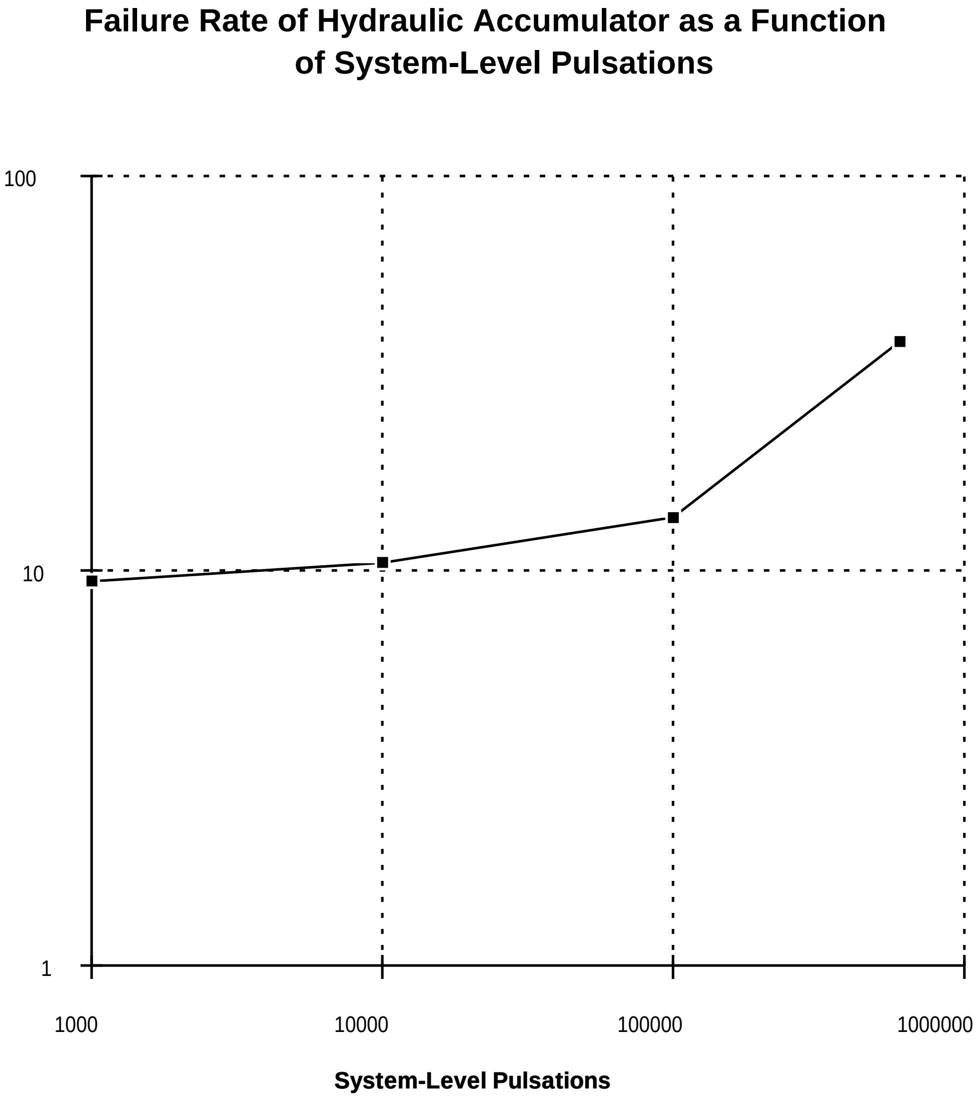


Figure 124. Failure Rate of Hydraulic Accumulator as a Function of System-Level Pulsations

REFERENCES

1. Andrews, W. "VME Modules SPARC Performance Race." Computer Design. March, 1994. pp. 46-50.

2. Babb, M. "New Sensors Have Intelligence, Will Communicate." Control Engineering. February 1994. pp. 84-85.

3. Caruthers, F. "Bus Specs Drive Packaging Technologies." Computer Design. January, 1994. pp. OEM9-OEM15.

4. Doyle, J. and G. Stein. *Multivariable Feedback Design: Concepts for a Classical/Modern Synthesis.* IEEE Transactions on Automatic Control. Vol. AC-26. Feb. 1981. pp. 4-16.

5. Doyle, J., K. Glover, P. Khargonekar and B. Francis. *State Space Solutions to Standard H2 and H-Infinity Control Problems.* IEEE Transactions on Automatic Control. Vol. AC-34. Aug. 1989. pp. 831-847.

6. Ervin, Robert D. and Fancher, Paul S. "Rationalizing the Study of Active Safety Technology." 1990.

7. Etkin, Bernard. Dynamics of Flight. John Wiley and Sons. New York. 1959.

8. Frazzini, R., Funk, H., Meisner, J., and Zhang, W.B. "System Description and Specification for AHS Health Management Precursor System Analysis." Federal Highway Administration Report FHWA/RD-93/???. Federal Highway Administration. Washington, D.C. December, 1993.

9. Government-Industry Data Exchange Program R/M Data Interchange Data Summaries. 5/83 thru 4/89.

10. Gillespie, T. D. Fundamentals of Vehicle Dynamics. 1992.

11. Meisner, J., Frazzini, R., Funk, H. and Zhang, W.B., "Function Criticality, Allocation and Mechanization for AHS Health Management Precursor System Analysis", Federal Highway Administration Report FHWA/RD-94/???, Federal Highway Administration, Washington, D.C., April, 1994.

12. MIL-HDBK-217F. "Reliability Prediction of Electronic Equipment." December 2, 1991.

13. "Nonelectric Parts Reliability Data 1991." Reliability Analysis Center. May 1, 1991.

14. California PATH Program. "Test Vehicles for AVCS Research." Request for Information. California PATH, Institute for Transportation Studies. University of California at Berkeley. Berkeley, CA. August, 1993.

15. Peng, H. and M. Tomizuka. *Vehicle Lateral Control for Highway Automation.* 1990 American Control Conference. pp. 788-794.

16. Peng, H. and M. Tomizuka. *Preview Control for Vehicle Lateral Guidance in Highway Automation.* 1991 American Control Conference. pp. 3090-3095.

17. Powell, D. "Distributed Fault Tolerance: Lessons from Delta-4." IEEE Micro. February, 1994. pp. 36-47.

18. Tsao, H. S. J., Hall, R. W., Shladover, S. E., Plocher, T. A., Levitan, L. J. "Human Factors Design of Automated Highway Systems: First Generation Scenarios." Federal Highway Administration Report FHWA/RD-93/???. Federal Highway Administration. Washington, D.C. October, 1993.

19. Valley, Shea L. Handbook of Geophysics and Space Environments. McGraw-Hill. New York. 1965.

20. Varaiya, P. and Shladover, S. “Sketch of an IVHS Systems Architecture.” Institute of Transportation Studies Report UCB-ITS-PRR-91-3 PATH. University of California, Berkeley. October 1990. revised February 1991.

21. Weir, D. H. and D. T. McRuer. *Dynamics of Driver Vehicle Steering Control.* Automatica. Vol. 6, 1979. pp. 87-98.

22. Weiss, R., "PowerPC goes after X86 PCs and embedded systems", Computer Design, pp. 32-35, June, 1994.

23. "Highway Electrification and Automation Technologies: Regional Impacts Analysis Project, Phase 1 Report". SCAG. 1990. pp 3-15. and "1987 Base Year Travel Information Digest". SCAG. 1990

24. "Supplementary Description of Automated Highway Systems". supplement to BAA for AHS Precursor Systems Analysis. 1993.

25. Levitan, Lee, et.al. "Driver Task Analyses and Driver-System Interface Designs for the Automated Highway System." Honeywell Technology Center. 1994.

26. Reliability Analysis Center document "Nonelectronic Parts Reliability Data 1995" (NPRD-95) July 1994.

27. Naval Surface Warfare Center (Carderock Division) document "Handbook of Reliability Prediction Procedures for Mechanical Equipment" (Carderock Div, NSWC-94/L07 March 1994).

28. Rome Laboratory Reliability Engineer's Toolkit. April 1993.

29. "Highway Statistics 1992", Slater, Rodney E., Federal Highway Administrator. ISBN 0-16-042970-6.

30. Xia, X. and E.H. Law, *Linear Analysis of Front and Four Wheel Steering Automobiles: Understeer, Oversteer, and Handling Qualities*.

Wurtenberger, M. *Modelling and Parameter Estimation of Nonlinear Vehicle Dynamics*. Transportation Systems. ASME. 1992. p. 53. -models describing the braking system, powertrain, and steering and suspension.

Connolly, F. T. *Modelling and Identification of the Combustion Pressure Process in Internal Combustion Engines Using Engine Speed Fluctuations*. Transportation Systems. ASME. 1992. p. 191. -model relating cylinder combustion pressure to crankshaft angular velocity.

Lewandowski, E. J. *Experimental Studies of a Model-Based Control System for an Automotive Hydrostatic Drive*. Transportation Systems. ASME. 1992. p. 223. -"drive-by-wire" control of engine and transmission.

Pianese, C. *A Dynamic Model for Control Strategy Optimization in Spark Ignition Engines*. Transportation Systems. ASME. 1992. p. 253. -dynamic model of an electronically controlled spark-ignition engine.

Choi, S. B. *Sliding Control of Automotive Engines*. Transportation Systems. ASME. 1992. p. 281. -model of engine torque production.

Narendran, V. K. *Merge Control of Vehicles in an Automated Highway System*. Transportation Systems. ASME. 1992. p. 269. -vehicle follower control approaches.

Ribbens, W. B. *Distinguishing Changes in Plant Dynamics from Actuator of Sensor Failures for Failure Detection in Non-Linear Plants*. Transportation Systems. ASME. 1992. p. 39.

Ammann, C. A. *Cleaning Up the Automotive Engine - Retrospect and Prospect*. (92C001) Vehicle Electronics Meeting Society's Needs. SAE. 1992. p. 5. -summary of emission standards.

Rodda, W. J. *Automotive Electronic Implications of OBD II*. (92C005) Vehicle Electronics Meeting Society's Needs. SAE. 1992. p. 41. -summarizes the design impact of the new OBD II standards.

McLellan, D. R. *Increasing the Safe Driving Envelope - ABS, Traction Control and Beyond*. (92C014) Vehicle Electronics Meeting Society's Needs. SAE. 1992. p. 103. -hardware emulation of driver's control strategies.

Kizu, R. *Electronic Control of Car Chassis - Present Status and Future Perspective*. Proceedings. IEEE. 1988. p. 173. -present status and future of such systems.

Ressler, N. W. *Integrated Chassis and Suspension Controls - Present and Future World of Chassis Electronic Controls*. Proceedings. IEEE. 1988. p. 213.

Inoue, T. *Future Engine Control*. (901152) Vehicle Electronics in the 90's. SAE. 1990. p. 285. -advanced sensors, controls, etc.

Baker, R. E. *Future Transportation Fuels and the Environment*. (901153). Vehicle Electronics in the 90's. SAE. 1990. p. 299.

Schwab, M. *Electronically-Controlled Transmission Systems - Current Position and Future Developements*. (901156). Vehicle Electronics in the 90's. SAE. 1990. p. 335.

Irie, N. *4WS Technology and the Prospects for Improvement of Vehicle Dynamics*. (901167). Vehicle Electronics in the 90's. SAE. 1990. p. 429. -traces the course of Nissan's HICAS system.

Wallentowitz, H. *Scope for the Integration of Powertrain and Chassis Control Systems: Traction Control - All-Wheel Drive - Active Suspension*. (901168). Vehicle Electronics in the 90's. SAE. 1990. p. 439. -functional integration of these systems.

Cummimgs, T. M. *Vehicle Diagnostics - A System View*. (901171). Vehicle Electronics in the 90's. SAE. 1990. p. 473. -vehicle multiplex systems used for raw failure data, SPC, quality improvements.

Haider, S.A. *Powertrain Torque Management*. (870081). Automotive Electronic Engine Management and Driveline Controls. SAE. 1987. p. 27. -describes a strategy to utilize high output engines without increasing transmission/drivetrain size.

Wakeman, A. C. *Adaptive Engine Controls for Fuel Consumption and Emissions Reduction*. (870083). Automotive Electronic Engine Management and Driveline Controls. SAE. 1987. p. 43. -describes a controller that can detect changes in the compression ratio.

Tamura, H. *Improvement of Performance and Reliability of Engine Electronic Controller*. (880181). Engine and Driveline Control Systems. SAE. 1988. p. 79. -Nissan's system.

Nimmo, P. E. *Shortcut to Interactive Drivetrain Simulation*. (880183). Engine and Driveline Control Systems. SAE. 1988. p. 89. -systematic description of the linear and non-linear components.

Automotive Electronics Reliability Handbook. SAE. 1987.

Baker, M. "Sensing and Systems Aspects of Fault Tolerant Electronics Applied to Vehicle Systems." SAE. (901123). 1990. -some response numbers.

Vahle, R. W. "Part Quality Trends and Requirements." SAE. (901143). 1990. -electronic component reliability.

Fayet, J. "Developements in Quality and Reliability for Automotive Electronics." SAE. (901144). 1990.

Sasaki, H. 1990. LSI Technology for Meeting The Quality Goals for Automotive Electronics. SAE. 901145.

Shiga, H. *Electronic Transmission Control.* (861032). Transportation Electronics, SAE. 1986.

Gerstenmeier, J. *Traction Control (ASR) - An Extension of the Anti-Lock Braking System (ABS)*. (861033). Transportation Electronics, SAE. 1986.

Vehicle Multiplexing Systems. SAE. 1991.

Rizzoni, G. *Application of Failure Detection Filters to the Diagnosis of Sensor and Actuator Failures in Electronically Controlled Engines*. IEEE Workshop on Automotive Applications of Electronics. 1988. p. 57.

Bastow, Donald. Car Suspension and Handling. 1987.

The Dynamics of Vehicles on Roads and Tracks. 11th IAVSD Symposium. 1989.

Chrstos, J. P. *Inclusion of Steering System Freeplay in Open-Loop Vehicle Dynamic Simulations*. The Dynamics of Vehicles on Roads and Tracks. 12th IAVSD Symposium. 1989. p. 99.

Hauschild, W. *Numerical Simulation of Characteristic Manoeuvres of Passenger Cars in the Pre-Crash Phase*. The Dynamics of Vehicles on Roads and Tracks. 10th IAVSD Symposium. 1989. p. 127.

Nagai, M. *An Adaptive Control Model of a Car-Driver and Computer Simulation of the Closed-Loop System*. The Dynamics of Vehicles on Roads and Tracks. 10th IAVSD Symposium. 1989. p. 275.

Segel, L. *The Influence of the Steering System on the Directional Response to Steering*. The Dynamics of Vehicles on Roads and Tracks. 10th IAVSD Symposium. 1989. p. 381.

Xia, X. *Linearized Analysis of Front and Four Wheel Steering Automobiles*. Transportation Systems. ASME. 1990. p. 9.

Wei-Xin, L. *Study of Optimal Matching between Automobile transmission Parameters and Engine*. Transportation Systems. ASME. 1990. p. 87.

Moskwa, J. J. *Dynamic Fuel Parameter Estimation in Automotive Engines*. Transportation Systems. ASME. 1990. p. 93.

Ashkenas, I. L. "Power Steering Failure Study." 1978.

Unruh, J. *Error Detection Analysis of Automotive Communication Protocols*. SAE Special Publications. 1990. p. 806. -identifies failure levels and vendor quality processing problems which make possible the early detection of component early life failures.

Ribbens, W.B. *Mathematical Model Based Method for Diagnosing Failures in Automotive Electronic Systems*. SAE Transactions. 1991. v 100, sec 2. -failure diagnosis and calibration of vehicle electronics.

Vollmer, R. P. "Changes in Automotive Failures." SAE Technical Paper Series (921594). 1992. -control system redundancy, human/machine interfaces, defective maintenance procedures, new designs in these areas.

Laudenbach, A. *VLSI System Design for Automotive Control. I*EEE Journal of Solid-State Circuits. July, 1992. v 27 n 7. -novel VLSI approach for combustion engine control.

Moghbelli, H. "Electronically Assisted Steering." SAE Technical Paper Series (920268). 1992. -design and implementation of EAS control hardware. Allows driver to have control if EAS fails.

Kawahashi, A. "Development of a Smart Analog IC for Electronic Control of an Automotive Variable Power Steering System." SAE Technical Paper Series (920267). February, 1992.

Ajumobi, S. O. "Model of an Automotive Power Steering System Via the Linear Graph Technique." 1987.

Garrard, W. L. *Effects of Jerk Limiting on the Stability of Automated Transit Vehicles*. Transactions of the ASME. 1978. v.100. p. 298.

Olson, D. E. *Model-Follower Longitudinal Control for Automated Guideway Transit Vehicles*. IEEE Transactions on Vehicular Technology. 1979.

Miner, D. K. *An Effective Solution to the Problem of Hydraulic Brake Line Corrosion*. Source Book on Copper and Copper Alloys. ASM. 1971. p. 348-363. -Figure 5. subdivides causes of brake failures. Sample size = 100,000 vehicles.

Lyons, P. "The Computer Takes the Wheel." Car and Driver. May 1994. p.203 -use of the computer to sense position, yaw, roll, g-forces, and a list of the companies supplying the hardware.