Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Vehicle Operational Analysis

U.S. Department of Transportation
Federal Highway Administration

Publication No. FHWA-RD-95-148
November 1994

PRECURSOR SYSTEMS ANALYSES

OF

AUTOMATED HIGHWAY SYSTEMS

Activity Area L

Vehicle Operational Analysis

Results of Research

Conducted By

Delco Systems Operations

FOREWORD

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

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

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

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

Original signed by:

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

NOTICE

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS Activity AreaL Vehicle Operational Analysis		5. Report Date 6. Performing Organization Code
7. Author(s) B. Tsuruda, A. Cochran*, F. Mangarelli*, M. Halseth, J. Tsao**, W. Lauritsen, H. Tan**		8. Performing Organization Report No.
9. Performing Organization Name and Address Delco Electronics Corporation Delco Systems Operations 6767 Hollister Avenue Goleta, CA 93117-3000		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFH61-93-C-00194
12. Sponsoring Agency Name and Address IVHS Research Division Federal Highway Administration 6300 Georgetown Pike McLean, Virginia 22101-2296		13. Type of Report and Period Covered Final Report September 1993–November 1994 14. Sponsoring Agency Code
15. Supplementary Notes Contracting Officer's Technical Representative (COTR)–J. Richard Bishop HSR 10 * Hughes Aircraft Company, San Diego, CA; ** PATH, Richmond, CA		
16. Abstract Present and future designs of automobiles, light duty trucks, and heavy trucks are discussed. The analysis relates these hardware systems to the potential critical components of the Automated Highway System (AHS) vehicle. Communications equipment and electronic control hardware and software are reviewed in detail. Reliability and retrofit issues are analyzed. Fail-soft design approaches which could be applied to the AHS vehicle system are discussed. Vehicle technologies which are common to AHS and non-AHS systems are catalogued.		
17. Key Words vehicle electronics, vehicle communications, fail-soft, vehicle, retrofit, reliability	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 / 22. Price

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

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The vehicle operational analysis addresses topics associated with the development, operation, and deployment of AHS vehicles. Each area of analysis presents a variety of aspects which affect the feasibility of the AHS from the vehicle perspective. Vehicle electronics are discussed in terms of recent trends in subsystem automation, existing state of the art, and expected future developments. The impact of subsystem reliability on the process of bringing new technology to the consumer car market is another factor. The methodologies for providing safe system operation in the event of subsystem failures is an important consideration in the design of AHS specific vehicle components. This analysis is also concerned with the ability to optimize early market penetration by supporting reverse compatibility in vehicle models as advances in automation are achieved. The benefits of AHS-specific vehicle subsystems in terms of potential user services while traveling outside of the AHS are also estimated.

Define Vehicle Factors

The development of an AHS vehicle must consider the specific system configuration in which it is to operate. Infrastructure intensive configurations in which the control loop of the vehicle's longitudinal position is closed in the infrastructure roadside equipment will tend to emphasize the functional content of the wayside system architecture. Vehicle intensive configurations which close the longitudinal control loop in the vehicle will emphasize the functional elements within the boundaries of the vehicle. The primary factors associated with definition of AHS-specific vehicle functions can be placed into three categories: development, operation, and deployment.

Issues concerning the development of AHS vehicle functionality include the state of existing vehicle instrumentation, impending equipment developments, degree of integration of components, subsystem reliability, impact to vehicle cost, and production considerations. The factors associated with successful operation of AHS-equipped vehicles include the compatibility with non-AHS roadways, manual control options for emergency maneuvers, fault tolerance, fail-safety, and maintainability. Deployment aspects regarding AHS vehicles include the ability to retrofit non-AHS vehicles with AHS instrumentation, compatibility of early AHS equipment with future upgrades, maintaining optimum capability as technology advances, and consumer acceptance of automated vehicle features.

The considerations in terms of passenger vehicles will be distinct from those of commercial truck interests. The trucking industry is motivated toward increased automation to reduce the insurance and lost productivity costs of incidents caused by human error. Profit margins can also be expected to increase through reduced transit times and reduced labor hours resulting from automated features as well as fewer highway incidents due to driver error or neglect. Drivers of passenger vehicles may rate predictable travel times and freedom to perform alternate tasks while traveling as the most important features of automated highways. The goal of this analysis is to identify the system configuration which addresses the needs of diverse users uniformly.

Hardware Research

Equipment relevant to automated vehicle control includes power train control systems, body and chassis electronics, safety related systems, and communications and infrastructure electronics. The advent of more powerful microprocessors and larger memory capacities has enabled the automotive industry to improve various vehicle control systems. Systems that have traditionally been controlled mechanically have been replaced with sophisticated electronic control systems. A prime example of the trend toward vehicle electronics is the engine control module (ECM). Carburetors have been replaced in virtually all modern automobiles with ECM's and fuel injectors. Electronic modules are currently being used to control automatic transmissions, antilock brakes, air bag deployment, suspensions, heating/ventilation/air conditioning (HVAC), display systems, entertainment systems, and security systems. On board electronics content is increasing on heavy duty trucks as well, with integrated ECM's becoming common. Safety systems such as antilock brakes have been engineered for heavy duty trucks to prevent rear wheel lock up, improve stopping distance and brake application/release timing performance.

The goals of increased automation in passenger vehicles and trucks has its basis in increased fuel economy and improved safety. The current use and future proliferation of electronic control systems will provide the enabling technology required to support full automation of vehicle control. Throttle and steering by wire are considered viable approaches to further elimination of mechanical cables. The ability to achieve a cost effective method to safely disengage the brake, steering, and throttle functions from manual control is a requirement in the feasibility of automated vehicle control.

Sensors and communications will be required to provide lateral and longitudinal position information to the vehicle control loop. Specific function include position determination, detection of nearby vehicles and obstacles, and transfer of traffic flow control information. The sensor and communication technology performance parameters must be compatible with the update rate, accuracy, and interference immunity required to provide safe vehicle control. Existing low cost options may not meet performance requirements, while state-of-the-art technologies may not be compatible with high volume vehicle manufacturing cost objectives. A balance between performance specifications and impact to vehicle cost must be achieved to provide a feasible solution which satisfies both technical requirements and economic constraints.

Reliability

The electronics content of AHS vehicles is expected to be significantly greater than current vehicle models, including equipment such as sensors, actuators, processors and transceivers. The safety of AHS is affected by the reliability and maintainability of the vehicle, which is directly related to the number of subsystems involved in safety-critical functions. Reliability of modern electronics is driven primarily by subsystem complexity and manufacturing techniques. AHS vehicle electronics are comparable in complexity to existing consumer electronics such as video camcorders and cellular telephones. This type of electronics equipment is highly reliable, tending to operate flawlessly for years, but typically fails without the warnings associated with degraded performance common to traditional vehicle subsystems such as engines or brakes. It is recommended that AHS-specific subsystems include built-in-test capability to predict impending failure and prevent sudden loss of functionality. Safety-critical subsystems may require multiple redundancy or back-up systems to ensure error free operation.

The most cost effective approach to ensuring reliable system operation is to increase the mean time between failure (MTBF) of subsystem elements. System MTBF is a function of the total number of components. High levels of integration reduce the overall complexity, minimizing interconnects and eliminating sources of error in manufacturing and assembly and reducing potential points of failure. The current trend in vehicle engine controllers toward integrating functionality will support the need to simplify electronics subsystems, setting an early precedence for highly reliable AHS equipment.

Maintainability issues include repair/replace decisions as well as self test capabilities for fault detection and isolation. Maintenance of vehicle subsystems will include fault detection and isolation as well as repair. Unit self-test capability is recommended to enhance efficient diagnostics of AHS-specific equipment. The installation of vehicle equipment will also affect the maintainability of the equipment. Modular design of electronics equipment is one method of minimizing mean-time-to-repair. This approach allows repair of failed units at the factory, while malfunctioning units are merely unplugged and replaced at service stations. This may provide economies of scale required to reduce maintenance costs of complex subsystems, reducing the need for trained technicians to the factory level.

System engineering methodologies and concurrent design processes are recommended to ensure AHS quality and reliability, and subsequent safety performance. Robust Engineering practices have been implemented across the automobile industry, with overall benefits to reliability and production costs. A large percentage of engineering and manufacturing responsibilities are currently delegated to suppliers, and this is expected to increase with the implementation of AHS. Structured engineering methodologies will provide assurance that reliability, durability, and quality requirements are coordinated closely. The level of complexity of the AHS will require a high degree of attention to this aspect of design, development and manufacturing throughout the system life cycle.

Fail-Soft Reduction In Functionality

One aspect of ensuring safe AHS operation is providing a method to fail-soft. The goal of reducing functionality in the presence of failures is to provide graceful degradation of the level of service, without causing damage or injury. The two major aspects of fault tolerant design include fault detection and fault mitigation. Fault analysis methods address progressive levels of hazard to system operation, including identification of faults, determination of potential errors, and detection of failures.

A fault is a physical defect, imperfection, or flaw which occurs within hardware or software. Examples of faults are physical damage, short circuits, open circuits and infinite software loops. Faults may also result from design errors or external environmental conditions, such as temperature, electromagnetic interference, ionizing radiation, or system misuse.

An error is a manifestation of a fault, in which the logical state of an element differs from its intended value. An error in a system is the result of a fault but not all faults cause errors. A fault is termed latent if it has not yet caused an error to occur. A failure is the nonperformance of some expected action.

Failures are caused by errors which results in the system performing one of its functions incorrectly. A fault can be characterized by its duration, nature and extent. Fault duration can be transient, intermittent or permanent. Transient faults are often due to external disturbances and are non recurring. Intermittent faults cause a system to oscillate between normal and faulty operation, resulting in marginal or unstable operation. Permanent faults result from component failures, environmental stress or design errors. Transient and intermittent faults are difficult to detect since they seem to occur at random, and present a potentially greater risk to system safety since they may not be manifest during system integration and test.

System failures may be due to hardware or software failures. Hardware subsystems may implement passive or active redundancy to mitigate faults, while software subsystems may employ code or information redundancy to improve fault tolerance. Hardware and software failure detection and mitigation techniques are discussed in general terms to provide an overview of current technology and its applicability to AHS equipment. Failure mitigation strategies regarding specific vehicle systems critical to safe AHS operation are concerned with detection and control of subsystem failures.

The vehicle control functions which are critical to safe operation are lateral position control and longitudinal position control. Lateral position control replaces the manual steering function, while longitudinal position control replaces the manual brake and throttle functions. Several safety critical aspects of the lateral control function have been identified as lacking fail-safe states, including the steering actuator, deviation sensor, and processing unit. The longitudinal processing unit also lacks a fail-safe operating state. Failures in this type of component will cause immediate interruption of a safety-critical function. Extremely reliable components or redundant elements are required in these instances to prevent failures. An alternate solution is to introduce the driver as a back-up source of control, however this solution has serious safety considerations, especially in close vehicle following modes.

Retrofit Analysis

The ability to upgrade non-AHS vehicles to AHS compatibility is a reasonable design objective. However, this capability is concluded to be very difficult unless the vehicle is built as an “AHS-ready” vehicle. An “AHS-ready” vehicle should include at a minimum, all required actuation capability and have sufficient space available to install AHS-specific vehicle equipment. Wiring, power, sensors, and mounting provision can likely be retrofitted, but would also be a desirable feature for an “AHS-ready” vehicle. The inclusion of all actuators may not be a severe requirement considering the present trend towards throttle-by wire, brake-by-wire, and steer-by-wire.

A related issue is the ability to provide upward compatibility as AHS functionality progresses. The risk of early AHS vehicles becoming rapidly obsolete is a valid concern. This is another application where modular component design will provide straightforward replacement with next generation equipment. Some retrofits could be as simple as replacement of existing microprocessor program memory chips with replacements incorporating additional functionality. Some upgrades however may require additional wiring. Such retrofits would be much easier if early designs incorporate spare capacity for anticipated input/output and wiring requirements. For best integration of systems into the vehicle all power and interface requirements should be addressed at the time of initial vehicle design. This requires that interface specifications and standards for stages of an evolving AHS be fully determined long before the specific hardware and software is produced for a given stage. The concept of a multiplexed data bus is one solution which may support increased input/output capacity without compromising the reliability of interconnects.

AHS Technologies Applied To Non-AHS Roadways

One method of developing broad user acceptance and widespread market penetration of AHS is to support evolutionary deployment of AHS functionality. The gradual introduction of component technologies will increase the likelihood of deployment success by providing valuable and self-sustained pre-AHS user services. One of the benefits of an evolutionary deployment strategy is the ability to operate vehicles with pre-AHS functions on non-AHS roadways. Several of the capabilities provided by AHS technologies, such as sensor and communications systems, may be compatible with operation on non-AHS or pre-AHS roadways.

Transition to full AHS functionality over a period of time will permit user familiarity and acceptance of AHS functions as increasing levels of technology are introduced into the vehicle. Pre-AHS functions which are compatible with evolutionary deployment as well as operation on non-AHS roadways include automated headway maintenance and obstacle detection. Control of vehicle spacing using radar sensor inputs is referred to as adaptive cruise control (ACC), and is a good candidate for use on non-AHS highways. The instrumentation required to implement obstacle detection is vehicle-based and can be exploited on arterials as well as non-AHS highways since no infrastructure modification is required.

INTRODUCTION

Motor vehicles, including private passenger vehicles, public transit vehicles, commercial vehicles, and public safety vehicles, are a major part of American civilization. Millions of commuters and business travelers journey by vehicle daily within the metropolitan areas of the U.S. More than 75 percent of the U.S. population now lives in urban areas.[1] Since 1970, travel in urban areas (predominantly passenger vehicle travel but also including truck travel) has doubled and travel on urban interstate highways has tripled. With more people working now than when the major interstates and roadways were first built, there is more concern for the problem of congestion created by motor vehicles. And the majority of households now have two or more cars. As a nation, we have more vehicles than licensed drivers.

The trucking industry and the retailing sectors that the trucking industry serves, as well as the private traveler, are being affected severely by traffic congestion. Driving on congested freeways increases driving time, fuel consumption, and wear-and-tear on trucks. These additional costs are ultimately passed on to the shippers and receivers, increasing the cost of transporting goods. The impact is sizable because the economy is very dependent upon trucking. In 1988 trucks carried 40 percent of all domestic tonnage and accounted for 78 percent of domestic freight revenues, about $240 billion dollars. Global competition has forced U.S. companies to make changes, such as the use of overseas parts suppliers, introduction of just-in-time manufacturing and distributing, and increased emphasis on quality and customer service. Carriers are being asked to provide faster, more reliable, and more cost effective services, but increasing congestion on the national highway network is making it costly to meet these service and productivity requirements.

Predictions of economic growth indicate that the U.S. will be even more reliant on fast, reliable, and cost-effective freight services in the future than ever before. There will be smaller shipments, less high volume freight deliveries, and an emphasis on individualized freight services. The criticality of just-in-time shipments will increase, which in turn puts a higher demand on reliable air and truck transportation.

One of the principal objectives of the automated highway system is to relieve this congestion and provide all transportation modes with safer, more efficient travel. However, advancement of the AHS program cannot proceed more rapidly than the progress of developments in the vehicle manufacturing industry. This report summarizes many of the current and future vehicle manufacturing activities and attempts to relate them to the development of the ‘smart’ vehicle which will be the user of the automated highway.

This report will consider in its research both heavy duty trucks and passenger automobiles. This activity will put emphasis on investigating electronic control systems, as well as advances in mechanical systems, in both vehicle types. By examining the growth of technology from the past to the present, trends in vehicle systems and vehicle electronics will be identified. This data can serve as useful information for conjecturing the state of future technology and future vehicle development necessary for operation on an AHS. An attempt will be made to compare current vehicle technology with the kind of technology that will be needed for an AHS vehicle and to highlight any significant gaps in current vehicle development.

REPRESENTATIVE SYSTEM CONFIGURATIONS

The representative system configurations (RSC's) were generated very early in this Precursor Systems Analyses of AHS program. These RSC's are used throughout the various areas of analysis whenever a diversity of system attributes is required by the analysis at hand. The RSC's identify specific alternatives for 20 AHS attributes within the context of three general RSC groups.

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

TECHNICAL DISCUSSIONS

Task 1. Define Vehicle Factors

The principle vehicle factors associated with AHS passenger cars and heavy duty trucks are identified and categorized in this task. Electronic vehicle control systems are emphasized. The list of vehicle factors is shown in table 1. The vehicle factors are categorized under the following topics:

- Development.
- Operation.
- Deployment.

The development of an AHS vehicle is somewhat dependent upon RSC in which it is to operate. Infrastructure intensive configurations, such as RSC 1, where the servo loop of the vehicle's longitudinal position is closed in the infrastructure roadside equipment, will tend to emphasize the functional content of the wayside system architecture. On the other hand, RSC 2, which places the maximum practical system content in the vehicle, will emphasize the functional elements within the vehicle.

Development

A list of some of the equipment available on present day automobiles and heavy duty trucks is presented in (table 2). This equipment, production considerations, sensors that are used in automotive technology, and general manufacturing trends will be examined in the hardware research section. As an example of trends, figure 1 shows the rising content of electronics in automobiles. Electronic content has grown about 12 percent annually and 1995 vehicles will average about $900 worth of electronics per car, up from $680 in 1990.[2] Looking back at early stages of development which led to the current day deployment of vehicle equipment (electronic control systems) can establish a baseline for predicting future AHS equipment and point to trends in technology that may allow for insight into the future. Reliability and support will be addressed in the maintainability and reliability task.

Operation

AHS vehicles will be faced with the challenge of operating on both non-AHS and AHS roadways. The AHS vehicle must operate safely, reliably, and comfortably on both highway systems. In order to justify vehicle expenditures the AHS vehicle will be expected to have improved fuel economy (or increased battery range in electric vehicles), and satisfy environmental requirements. The AHS vehicle must meet safety standards and be able to detect failures or potential failures internally, provide warning for failures or potential failures, mitigate faults and provide strategies of soft failure. Fault tolerant systems issues and the use of fail soft control strategies will be covered in task 4. The elements of vehicle and subsystems diagnostic design, redundancies, component designs and failure modes are all part of vehicle operations.

In the event of emergencies, the driver may need to take over the manual control of the vehicle. The method in which this transition takes place will be an important issue to design and implement. The automated check-in activity and the safety activity both have relevance and overlap in this area.

Table 1. Vehicle Factors

OPERATION	• Use on Non-AHS Roadway. • Optional Manual Control (Emergency). • Fault Tolerant, Fail-Soft Control Strategy. • Maintainability.
DEVELOPMENT	• Current Equipment Available. • Future Equipment. • Components. • Reliability. • Support. • Cost. • Production Considerations.
DEPLOYMENT	• Updating AHS Vehicles With Newest Equipment and Retrofitting. • Evolution of Equipment. • Public Acceptance of New Technology.

Deployment

AHS vehicles, like current vehicles, will experience continual change and refinement. In the Retrofit Analysis task the issues of updating "older" AHS vehicles and modifying non-AHS vehicles will be addressed. Aftermarket suppliers of AHS equipment will be primarily experts in vehicle electronics and must be cognizant of AHS rules, requirements, and standards. Aerospace and defense contractors may become suppliers of AHS equipment because of their experience working with and understanding Federal standards, contracts, and finance.

Table 2 presents the equipment which is available on current automobiles as well as that which should be available within the next ten years. Additional technological advances would be necessary for AHS vehicles.

In the future the motivation for the use of AHS automobiles and AHS heavy duty trucks may be very different. The trucking industry would like to reduce its reliance on the driver and put more automation into the truck. Highway incidents caused by driver error or neglect cost the trucking industry millions of dollars annually. Automation is expected to reduce the number of highway incidents as well as the total labor hours, thus increasing the profit margin of trucking companies. The future in the trucking business will belong to those lean efficient companies that can react faster by putting products or services to market faster than the competition. Businesses will also be reliant on just-in-time shipments which will benefit from the automated highway.

The motivation behind automating automobiles is distinct, but not always different, from that of the trucking industry. The public's acceptance of AHS will be based on predictable travel times, greater comfort, and a safer driving environment.

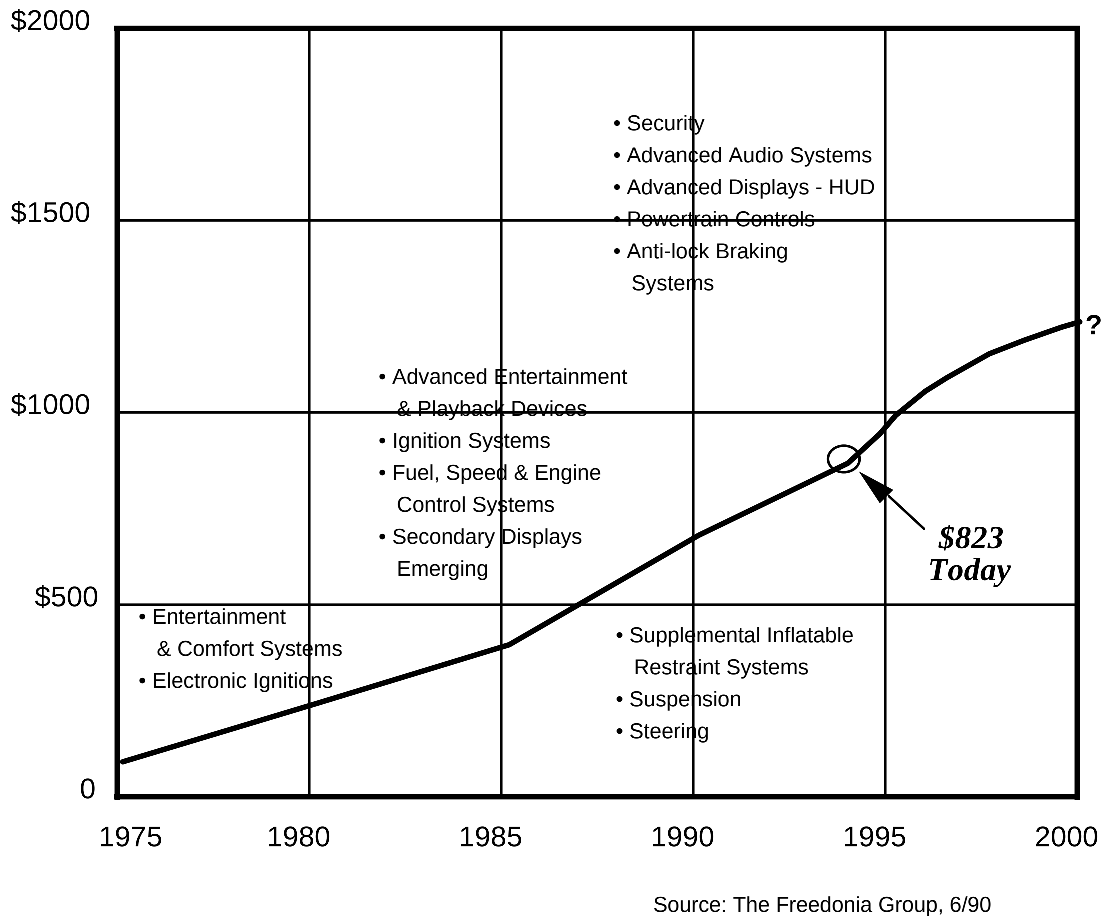

Figure 1. Electronic Content

Table 2. Hardware

Systems	**Equipment (Production and Development)**
Powertrain Control Systems	Electronic Engine Controller Electronic Transmission Controller Electronic Ignition Powertrain Controller Integration (Engine and Transmission)
Body & Chassis Control Systems	Real Time Damping Suspension Controller (Active Suspension) Electric Power Steering
Safety, Platooning, and Communication Systems	Driver Interface Anti-Lock Brake System Supplemental Inflatable Restraints (Air Bags) Adaptive Cruise Control Collision Avoidance Front/Rear Collision Avoidance (Sides) Night Vision Rear Vision Vehicle Condition and Performance Monitoring Driver Condition and Performance Monitoring Communications Systems: • Vehicle-to-Vehicle. • Vehicle-to-Infrastructure. • Inside the Vehicle (Data Bus). Hands Off Steering System Automatic Vehicle Identification Location/Mapping

Task 2. Hardware Research

The AHS infrastructure and AHS vehicle will be able to take advantage of the many proposed system architectures and products developed under the Intelligent Transportation Systems (ITS) theme. The primary focus in this activity will be directed to the research of hardware that could potentially be part of the systems architecture of an AHS vehicle. Although there may be references to the wayside infrastructure and some of it's equipment, the scope will be limited to the boundaries of the AHS vehicle. Although vehicle electrical hardware exists outside of that which has been listed (table 2), the focus is on the types of hardware that have potential relevance within an AHS vehicle system architecture.

AHS will relieve drivers of their traditional roles while traveling on the AHS, increase the traveler's safety, and improve the overall efficiency of road travel. A driver on a typical journey is continually adjusting the vehicle's lateral and longitudinal position, vehicle speed, and spacing between vehicles. There also is the element of anticipation which every driver exercises in order to execute smooth stops and starts, make judgment decisions about other drivers, and perform lane changes. All vehicle control will be provided by the AHS vehicle control system operating in conjunction with the infrastructure equipment and, in some cases, with other non-AHS vehicles. This activity will highlight the in-vehicle hardware that will be needed to achieve AHS operation with both private vehicles and heavy duty trucks

Vehicle Electronics For Passenger Cars And Heavy Duty Trucks

The use of electronic control systems in vehicles is increasing every year. The powertrains of passenger cars that were once mechanically controlled are now controlled by reliable and sophisticated electronic controllers. Distributors and mechanical fuel injection systems have been replaced with engine control modules (ECM's). ECM's are found on virtually every modern production car. General Motors, North American Operations, uses electronic controllers on all of their automatic transmissions being produced today. Mechanisms inside automatic transmissions that once controlled the hydraulically actuated clutches and bands have given way to electronically controlled solenoids. Transmission control modules (TCM's) are now common equipment in current day automobiles. Delco Electronics is now producing an integrated engine and transmission controller, the PCM or powertrain control module, for some of it's manufacturing customers. Other examples of electronic control are: the deployment of an air bag is controlled by the SIR (supplemental inflatable restraint) controller, the antilock brakes are controlled by a microprocessor based ABS unit, and the fuel mixture and transmission shift points are controlled by the engine/transmission computer. A GM car today with the newest engine control systems and state-of-the art safety systems has about five times the computing power of the on-board guidance system used in the 1969 Apollo moonshot.[3]

The heavy duty trucking industry is also finding a need to develop electronic control systems for its vehicles. Although the trucking industry is producing vehicles that have less electronics content and sophistication than private passenger vehicles, the technology push in that area and the customer demand for added functionality and performance is on the rise. Potentially there are hundreds of thousands of dollars in value in each tractor trailer rig and it's freight, so loss of a truck, even if unloaded, is a major business cost. Some truck makers have been requested to retrofit tracking systems into their product. Some shipping companies are having black box recorders retrofitted into their vehicles to track the drivers performance and log truck destination data.

Electronic powertrain controls for trucks have been developed to increase performance, decrease noise, and to meet future stringent environmental laws. Safety systems such as antilock brakes have also been engineered to improve the braking performance of trucks. Some current and future truck electronic systems will be reviewed in this activity.

Powertrain Electronics

General Motors began using electronic engine management back in 1980. Delco Electronics developed the TBI (throttle body injection) ECM and it was first used by Cadillac. The TBI used an 8-bit Motorola microprocessor that had items such as memory, I/O, and timing circuitry outside of the microprocessor on separate integrated circuits. The microprocessor was thus a multiple chip set. The requirements of controlling an engine coupled with additional functional requirements has pushed the automotive electronics industry to develop hardware that is more powerful, in terms of throughput and I/O, smaller, less expensive, more durable, more efficient, and more reliable. Today, 32 bit microprocessors are finding their way into several automotive electronics applications.

Up integration is a current trend in powertrain electronics. The engine and transmission control functions are now being integrated together into one control module. Both the engine and transmission control strategies are executed by a single microprocessor. It has been demonstrated that the antilock brake function can also be added. The amount of bandwidth and I/O to accomplish these tasks far exceeds the capability of the electronic hardware of a decade ago, which explains why 32-bit microprocessors are being developed. The AHS vehicle will require more powerful electronic control systems capable of processing large amounts of data at higher speed.

Automotive Electronic Transmission Control

The entry of electronic transmission control into the market place lagged production electronic engine controls by a few years. The desire to have better control over shift points and to improve the shift quality brought on the need for TCM's . Now, to meet stringent environmental regulations, the TCM has become a necessary component. The TCM and the ECM communicate with each other to control torque management, shift points, torque converter clutch lock, and many other coordinated vehicle functions. The results are lower emissions and better fuel economy which meet current Federal regulations.
Today's automatic transmissions are designed to have very little resistance or drag under coasting and down hill conditions. Thus the vehicle may coast much further and fuel consumption is improved. Powertrains and powertrain controllers developed for an AHS vehicle could potentially further reduce the drag of the drive train. Heavy duty trucks use the Jake Brake which utilizes the powertrain inertia to absorb the energy of motion and slow down the truck. It reduces brake wear and brake maintenance costs. This would be an interesting alternative method to control the speed of an AHS vehicle.

Drive-By-Wire Throttle

The drive-by-wire electronic throttle is being considered to eliminate vehicle hardware such as the throttle cables and brackets. The accelerator will not be hooked up to the engine via a throttle cable. Instead, a sensor which measures the gas pedal position couples to a controller which activates an electric motor that precisely adjusts fueling. This approach improves engine emissions and affords space savings within the engine compartment.

Future Vehicle Electronics Improvements

The University of Michigan Delphi Forecast and Analysis of Intelligent Vehicle Highway Systems predicts a 20 percent hike in CAFE by 2003. Automakers and importers in the year 2003 will combat tougher fuel economy standards, environmental pressures and moderately higher gasoline prices with the expanded use of lighter, more recyclable materials and the development of more efficient powertrains. The corporate average fuel economy standards will increase from 8.6 L/100 km today to 7.4 L/100 km. That 20 percent jump compares with a 5.8 percent boost during the previous 10 years. The U.S. Big Three/ U.S. Government "supercar" deal will lead to a 5.2 L/100 km car by the year 2020. More than 50 percent of the engine systems will be redesigned during the next 10 years, and electronic controls will be added to all automatic transmissions. A slight shift toward engines with fewer cylinders will occur. Nearly all of the North American cars produced will have antilock brakes. Electronic componentry will account for roughly 20 percent of the vehicles cost.[4]

Heavy Duty Truck Powertrain Control

Electronic Engine Control

Today's heavy duty diesel trucks share some of the same requirements for electronic engine control as today's passenger cars. Requirements for diesel engines include lower cost, increased user friendliness, noise reduction, and the need to protect our environment. One example of electronic engine control is the Caterpillar Incorporated Hydraulic Electronic Unit Injector (HEUI). It requires no mechanical actuating or mechanical control devices. The fuel system maintains injection pressure control independent of engine load or speed, it has totally flexible injection timing, and it provides full electronic control of injection parameters. The HEUI development began as a joint effort between Caterpillar Inc. and an engine customer, Navistar International Transportation Corporation. Navistar's development of the T444E diesel engine required the development of a highly advanced fuel system.

Heavy Duty Truck Electronic Transmission Controls

Electronic TCM's for heavy duty truck transmissions are currently available, but they are not as widely used as they are in the automotive industry. The majority of heavy trucks used for long distance freight still use manual transmissions to achieve maximum fuel economy. Heavy equipment, like garbage trucks, used for stop and go driving do use automatic transmissions, largely because of the decreased wear on the trucks. It is expected that automatic transmissions will become more prevalent in the future for all applications except the longest haul.

Allison Transmission Division of GM and Eaton have both developed automatic transmissions (the Allison HD Transmission and the Eaton Ceemat Ate Transmission) that are electronically controlled. Both companies have targeted a range of customers and applications in the heavy duty truck market. Since the release of the first Allison commercial, on-highway transmission in 1972, market requirements have continued to become more stringent. The Allison HD transmission is slated for use in applications that will have very different performance and feature requirements. For example, the refuse truck may spend a great deal of time at low vehicle speeds with a proportionately high amount of reverse operation. This vehicle may also need a top mounted engine driven power take off to operate the packing mechanism. On the other hand, the motorhome will probably operate at high vehicle speeds and require very good shift quality for passenger comfort. The key to providing for these different requirements is to provide a flexible product design.[5]

Body And Chassis Electronics

The advent and success of automotive powertrain electronic control systems set the tone for the automotive electronics business. The application of electronic controls on automobiles has found it's way to the chassis from the powertrain. Ride and handling characteristics for automobiles can be greatly improved and to this end electronic suspension control has been installed on selected production automobiles. The computational capability necessary to process data for suspension algorithms is greater than what is necessary to control the engine and transmission of a production automobile. Suspension controllers usually contain a digital signal processor (DSP) along with a microprocessor to execute the mathematically intensive algorithms. This push to process more information is driving the electronics industry to provide more powerful and efficient components for automotive applications. Advancement in electronics technology, more so than advances in the vehicle handling attributes, makes this subject relevant to technology for AHS.

Electric Power Steering

Electric power steering is making it's way into production automobiles now. Electronic power steering can be thought of as electronic power assist. There still is a mechanical linkage between the steering wheel and the front wheels. TRW is developing an electronic power steering system that will be installed on the next generation Volkswagen Golf and the 1997 Mazda Lantis compact for Japan. TRW also has been encouraged to develop the system for electric vehicles. The challenges for TRW, which has invested heavily in development of the electric power steering system for ten years, are to reduce the cost of the electronics package that controls the rack from $120 to about $80, design the steering rack to handle forces up to 10,000 Newtons, develop small 12 volt electric motors able to handle the high forces in the system, and insulate the electronics from radio frequency interference.

The potential advantages are weight savings, better fuel efficiency, less load on the engine, lower cost, less parts, easy integration into active collision avoidance system, no maintenance, and no hydraulic fluid leaks. The hydraulic pump and hoses necessary in a traditional hydraulically mechanized power steering system can be eliminated. Before electric power steering is accepted, electronically powered hydraulic steering may be offered. In this system the hydraulic pump is powered by an electric motor. The advantages are cost effective power steering for small cars and greater fuel efficiency for larger cars.[6]

Steer By Wire

Electric steering, or steer by wire, is totally different from electric power steering. Electronic steering has no mechanical linkage between the steering wheel and front wheels. In this type of system a steering wheel sensor is used to determine steering wheel position. The controller, based off this information commands the wheels to the proper steering position via electric motors. Noise immunity to RF and reliable performance are paramount in this system since there is no mechanical linkage from the steering wheel to the wheels.

In 1985 GM Truck and Bus began the design of the Pegasus concept vehicle for Chevrolet. It was also known as the Blazer XT-1 and it made several appearances at auto shows across the nation in 1986. This vehicle was designed to demonstrate the state of the art in automotive electronics and to demonstrate future electronics. One of the featured systems was steer by wire. This system was developed by GM’s Saginaw Steering Division. This system controlled the steering by sensing steering wheel position and it had the capability to turn all four wheels. This system was a concept system and was not to be considered ready for production.

Steer By Brakes

Mercedes Benz is currently working on a production intent handling control system with Bosch. Sensors and computer logic calculate and compare the actual vehicle direction with the steering angle, the direction the car is being steered. If any differences are detected then the system makes corrections by applying the left- or right-hand side brakes. According to the company, it is effective during acceleration, deceleration, and coasting. This system may prove to be a fail-safe back-up system for the nominal steer-by-wire system that will be used in every vehicle on the automated highway. Even if the mechanical steering system fails, there would still be some residual steering capability resident in the brake system.

Safety And Platooning Systems

Electronics has evolved from powertrain controls into a variety of different areas. Some of the systems that will be on board AHS cars are in automobiles and trucks today. Systems such as collision warning and collision avoidance that will be necessary for AHS cars are on the drawing board and have some time to go before they will be in production. Air bags are common place in current day vehicles. By the year 2000 virtually every car and light duty truck produced in North America will be equipped with both driver and passenger side airbags.[7]

Antilock brake systems (ABS) have been available on vehicles for several years. By the end of this century almost every production car should have ABS as standard equipment or as an option. Some design approaches utilize the ABS system and the ECM for traction control. Traction control will probably not see the market penetration as ABS. But it is expected that by the year 2000 about 20 percent to 25 percent of cars and light trucks will have traction control.[8]

Many systems are in various states of development. Those that are important for AHS are discussed in the following sections.

Forward Collision Warning

This system will warn the vehicle operator of a potential collision with another vehicle or of an obstruction in front of the vehicle. A fault indicator inside the vehicle on the dashboard or instrumentation display panel or a collision warning alarm will alert the driver that a potential danger is ahead. The frontal looking sensor can be radar, sonar, infrared, or laser technology.

Back Up And Blind Spot Detection

Rear obstacle and blind zone detection systems are similar to the frontal collision warning type in that a sensor is used to detect obstacles and to warn the driver. In this system the sensors are positioned in the rear and in the blind zones off to the sides of the car where visibility is bad. School buses are currently outfitted with the NODS (Near Obstacle Detection System), that use Doppler technology called 2FD radar. Future systems will probably use the FMCW (frequency modulated carrier wavelength) approach. FMCW does not require motion to operate, however the 2FD approach does require motion.

Roadway Imaging Infrared

Roadway imaging provides drivers with an enhanced image of the roadway ahead under adverse weather and visibility conditions at night. It is predicted that some implementation of this system will have a 50 percent market penetration in automobiles and light duty trucks by the year 2020.

Adaptive Cruise Control

Adaptive Cruise Control is similar to the present standard cruise control, except that the vehicle engine adapts automatically to maintain an appropriate speed which preserves the headway to the lead vehicle that the driver dialed in. The forward looking sensor can be any of the sensors mentioned in the forward collision warning system. This feature is anticipated to be popular and will probably cost under $500 to purchase. It could be in production shortly after the year 2000 and be installed in 50 percent of the cars 10 to 15 years after introduction.

Automatic Braking

This system applies brakes when the driver does not provide safe headway distance or in an emergency when a roadway obstruction suddenly appears. The actuation would be determined by the automatic braking control algorithm and the actuation drive signals from the ABS controller. This system could be used in conjunction with adaptive cruise control and lane keeping for platooning on an automated highway.

Autonomous Lane Keeping

Lane keeping systems supplement driver control with the capability to automatically maintain lateral vehicle position. Various lane tracking methods can be used to accomplish lateral positioning such as magnetic embedded markers, video, and radar. This system will be an integral part of the automated highway vehicle control system. It's control algorithm will be coupled with the steering system which controls the direction of the vehicle when it is under automated control.

Communications And Infrastructure Electronics Hardware Research

Implementation of AHS will require instrumentation of the vehicle to support vehicle control functions, sensing of neighboring vehicles and objects, and communication of vehicle and traffic flow control information. This topic will address the vehicle electronics associated with sensors interacting with objects external to the vehicle, and communications between vehicles and with the roadside. The degree of impact which various technologies have on the vehicle instrumentation are evaluated. The relative cost of specific approaches to system solutions are estimated. The capabilities of available technologies are highlighted in terms of their advantages and disadvantages in AHS applications.

Sensor Technology Overview and Applications

Table 3 contains a summary of various sensor technologies which may contribute to enabling AHS implementation and which are described in the accompanying text.

Absolute Position Location

Determination of vehicle position is an integral part of the automated control loop. Accurate position location can be used to evaluate vehicle spacing and assist in maneuvers. It is also a key input to vehicle navigation and route planning operations. The most common alternatives available for implementing automatic vehicle location include global positioning system (GPS) and beacons. The relative features and issues involved with AHS application are discussed in the following paragraphs.

GPS

GPS is a radio-navigation system that employs radio frequency (RF) transmitters in 24 satellites. GPS receivers decode signals from the satellites to calculate the latitude and longitude of a specific position. The accuracy ranges from 40 m to better than 1 cm.

Table 3. Summary Of Sensor Technology

TECHNOLOGY	FEATURES	ADVANTAGES	DISADVANTAGES	COST
PositionLocation				
GPS	Satellite based	Established coverage	Adequate accuracy requires differential Beacons for tunnels	Medium
Roadway Beacons	High frequency Directional	Directional High data rate	Sensitive to alignment	Tag - Low Beacon-High
Lateral Position				
Side Radar	Similar to microwave radar	Good sensitivity	Multiple units may interfere with each other	High
Magnetic Markers	Permanent magnets in road	Insensitive to environment	Markers must be installed in road bed	Low
EMF	Buried wire	Insensitive to environment	Wire must be installed along center line	Low
GPS	Satellite based	Infrastructure largely in place	Requires differential signal to get required accuracy	Middle
Ultrasonic	Sound wave reflected off side barrier	Inexpensive, proven technology	Requires barriers	Low
Vision	Single or dual camera systems	Passive sensing COTS	Night operation problems exist	Middle
Roadside Beacons	High frequency Directional	Directional High data rate	Precise clock alignment needed	Tag - Low Beacon-High

Table 3. Summary Of Sensor Technology (Continued)

TECHNOLOGY	FEATURES	ADVANTAGES	DISADVANTAGES	COST
HeadwayMaintenance				
Doppler Radar	Measures frequency shift	Insensitive to environment	Sensitive to road surface variations	Medium
Microwave Radar	Relies on TOA to find position	Good sensitivity	Cost	High
Laser	Triangulation based processing	Passive sensing Night operation	Complex Cost	High
Cellular	Multi-lateration	Add to existing infrastructure	Complex signal processing, timing	Medium
Obstacle Detection				
Infrared	Point to point High data rate	Inexpensive, proven	Affected by weather	Low
Microwave Radar	Several frequency ranges developed	Insensitive to environment	Resolution of small objects increases cost	High
Ultra Wideband Radar	Time domain approach	Low power energy spread	FCC approval an issue	Low
Vision	Dual camera systems	Concurrent lateral position	Poor operation in bad weather	Middle

For complete and continuous global coverage, GPS requires 21 satellites and three spares circling the earth once every 12 hours. The satellite configuration guarantees that a GPS receiver located anywhere on earth can receive RF signals from at least four satellites 24 hours a day. The entire constellation of 24 GPS satellites became operational in early 1994. A key issue in the availability of GPS is the funding of operating costs, which are currently born by the Federal Government.

GPS receivers are commercially available in a variety of formats including units small enough to be housed in handheld portable products. The price of GPS integrated circuits is dropping rapidly, causing multiple channel receivers capable of tracking as many as eight satellites to become more common. Multi-channel receivers have greater accuracy because single channel models lose phase-tracking information while breaking and re-acquiring lock with several satellites. Differential GPS is currently a viable option for fleet management of commercial vehicles, and applications for private vehicle location are becoming prevalent.

Beacons

Measurements of absolute position can be made using beacons at the roadside which communicate with passive tags located in the vehicle. This method of navigation places beacons at intervals along the roadway. Each beacon is initialized with its position. The vehicles interrogate each beacon as it passes the beacon, and the beacon returns the absolute position. The vehicle can employ dead reckoning between beacon updates. The position accuracy achievable with passive tags is compatible with navigation but not longitudinal control requirements.

Headway Maintenance

Information regarding vehicle velocity and acceleration is required to maintain lateral and longitudinal control of AHS vehicles. Velocity and acceleration inputs along with positon are used to determine the adjustments necessary to maintain specified headways between vehicles.

Microwave Radar

The velocity of a vehicle relative to the subject vehicle can be determined by successive measurements of relative target location and dividing the position difference by the time difference between measurements. Relative acceleration can be determined from a third set of measurements in a similar manner. This technique relies on continuously measuring the relative location of the vehicle and calculating the rate at which the location changes.

Performance degradation associated with problems such as false alarms and signal dropout can be significantly reduced by employing a technique known as cooperative ranging. The radar responds only to targets which are specifically identified by a tag, providing a clean reliable return signal which can be processed to yield stable, accurate range readings.

Doppler Radar

Another method employs measurement of the vehicle's Doppler frequency, which is directly proportional to the relative velocity. The Doppler frequency is determined by filtering the reflected signal and measuring the offset between signals applied in two parallel filters. The Doppler method can be extremely precise because errors in the measured location are not inadvertently included in the differentiation calculations made to determine relative velocity and acceleration. The result of Doppler measurements is nearly instantaneous, minimizing signal processing delays associated with measuring the rate of change of location.

Laser

Infrared laser communication between vehicles has the advantage of avoiding the issues of frequency congestion and electromagnetic interference (EMI). Data rates of up to 100 Mbps are compatible with automatic control loop update requirements. The primary drawback of this signaling architecture is the limitation to point-to-point communications. Platoon-based system configurations will suffer delays in data transfers from the lead vehicle to each following vehicle as the messages are handed from one vehicle to the next. This will have a significant impact on the safety of platoon dynamics in emergency maneuvers and will cause greater deviations in headway as the number of hops from the lead vehicle increases. Another concern is the effect of alignment on receiver/transmitter pairs, which is of importance on curves and in instances of dissimilar vehicle body styles. Weather also affects performance. In fog, snow, or dust the signal attenuation may be so severe that the system is innoperable.

Cellular

Absolute position, velocity, and acceleration can also be determined using a dedicated cellular system for supplying mobile service. Localization accuracies are currently compatible with navigation and map-matching applications. Determination of the lateral and longitudinal position compatible with automatic vehicle control require timing measurements with synchronization errors on the order of 1 nsec and sample rates on the order of one billion samples per second. The feasibility of this measurement and communications technique will rely on the complexity and related cost of implementation of the signal processing algorithms. The technology is not mature at this time.

Lateral Position

Lateral position hardware includes those systems which allow vehicles to maintain their position within a lane and to perform a lane change. The techniques for lateral position determination vary greatly, with each technique having its own strengths and weaknesses. Lateral position strategies employing two independent systems for redundancy have also been proposed. By using two independent techniques for lateral position measurements, the weaknesses of one system (e.g. poor performance of video based systems at night) are offset by the other system.

Magnetic Markers

This technique uses magnetic markers embedded in the roadway along the center line of the lane along with magnetic sensors in the vehicle for lateral position control. Because the strength of the magnetic field varies as the vehicle approaches each sensor, field strength alone cannot be used to maintain the vehicle in the lane. Instead, two magnetic sensors are positioned equidistant from the center line of the car. The difference in the field strength measured by the two sensors is used to determine the correct lateral position.

The magnetic markers are maintenance free once they are installed, although installation may be relatively expensive. The sensors on the vehicles are also relatively inexpensive and reliable. Other advantages of magnetic markers include the accuracy of the measurement, the ability to maintain adequate performance when a single marker is damaged or destroyed, their tolerance to inclement weather and road conditions (although raised markers may be susceptible to snow plow damage and sunken markers provide less sensitivity), and the fact that no power is required on the roadway.

Another feature of magnetic markers is that they can be used to convey information such as an upcoming curve or grade change, or a speed change. This information is used by the vehicle to help maintain a smooth ride. By embedding the magnetic markers with the positive or negative polarity facing up, each marker can convey one bit of information to the vehicle. As the vehicle passes over a string of markers, the corresponding string of bits can be read by the vehicle and the information processed.

Buried Wire

Electrical current is applied to a wire buried in the roadway, causing the wire to act as a transmitter. The induced voltage of two coils integral to an antenna system on the underside of the vehicle is measured. The induced voltage is equal when the two coils are equidistant from the wire, indicating the vehicle is positioned correctly in the lateral direction. The system is currently in use in construction and maintenance applications where barriers must be aligned with the center line of lanes. The primary disadvantage of this method is the extensive modification of the roadway, requiring every linear meter of AHS lanes to be instrumented.

Ultrasonic

Ultrasonic systems can also be used to measure lateral position for AHS. In an ultrasonic system, a pulse of ultrasound is transmitted, and the time between the transmission and the return is measured to determine distance. The concept is the same as microwave radar, except that the frequency is much lower. The lower frequency leads to lesser accuracy and a very inexpensive unit. The major technical issues are interference with multiple users on the same frequency and the need for a barrier or other physical reflector along the roadway in order to reflect the ultrasonic signal.

Vision

Vision sensing systems use a vehicle mounted camera or other optical sensor to maintain lateral position. Systems range from a camera mounted on the side of the vehicle and looking down at the lane marker to a camera mounted on the roof looking straight ahead at the lane markers to the left and right of the vehicle. Advantages of vision sensing systems include the fact that no roadway modifications are required and that preview information (curves, grades, etc.) is directly acquired from the front looking systems. Disadvantages include deteriorated performance in bad weather, the high computational power required for the system and the potential low reliability of a video system. Regular maintenance of the lane markings is also required for video systems. Video systems may not be effective in a platoon environment where the preceding vehicle blocks the lane markings unless the viewing unit is mounted to the side.

Beacons

Measurements of lateral position can be made using beacons at the roadside which communicate with passive tags located in the vehicle. The link is a bi-directional microwave path similar to the poll-response method used for electronic toll and traffic management technologies. One implementation of this infrastructure-based system which relies on active vehicle transponders supports both open-road and lane-based strategies. The technology is referred to as VRC, and existing designs support up to four lanes of traffic moving at speeds up to 160 km/h with vehicle spacing of 7.6 m.

In order for a VRC to measure distances in inches, it must have a clock accurate to fractions of a nanosecond, and that clock must be synchronized to a fraction of a nanosecond with the beacon clock. Hardware designs which compensate for multipath and fading may be required. When the VRC technology is used to exchange velocity and acceleration information for a control loop, the data must be correctly received for each control loop cycle (20 msec to 50 msec rate). These requirements add to the complexity of the VRC, which leads directly to additional cost.

Side Radar

Another method of determining vehicle lateral position uses radar ranging techniques. Existing vehicle lateral control techniques place the radar in the vehicle. Two major technical issues with this approach include the problem of interference with multiple users on the same frequency, as well as the cost of placing ranging radar in all vehicles. Another consideration is the establishment of a consistent roadside reference for the radar to track. A barrier or other constant physical reflector must be present to echo the radar signal. However, this marker could also be set along the divider stripe between lanes, thus removing several ambiguities but requiring a high precision radar system. The effect of anomalies such as disabled vehicles at the roadside on range measurements is not well known.

Obstacle Detection

Individual vehicles must also be capable of detecting foreign objects in the roadway such as debris or unauthorized vehicles. The primary concerns of obstacle detection sensors employed in an automotive environment include the following:

- Performance with respect to diverse targets and clutter.
- Frequency allocation and licensing requirements.
- All-weather operation.
- Susceptibility to contaminants.

There exist several sensor technologies capable of detecting and localizing obstacles in a forward sector, including radar, sonar, laser, video imaging, and infrared imaging.

Infrared Radar

Coherent laser radars afford three dimensional imaging capability by collecting reflected light from a series of short laser pulses. One issue involved in obstacle detection is the identification of foreign objects in cluttered backgrounds which include legitimate targets such as other vehicles in the same travel lane. Data processing algorithms incorporating statistical detection theory are used to discriminate legitimate obstacles. Laser radar beams are relatively narrow and have limited capability to scan a solid angle, and like all optical systems, they have limited utility in bad visibility conditions. The advantage of the narrow beamwidth is the elimination of ambiguity due to multiple reflections to which conventional radar is susceptible.

Microwave Radar

One approach to providing obstacle detection capability is forward-looking radar (FLR). Microwave Doppler-based FLR technology makes it possible to detect objects within 100 meters and current implementations can detect objects falling from leading vehicles. The high resolution is obtained using narrow beam scanning techniques. Switched beam or fixed beam approaches have a wider beamwidth and cannot achieve the degree of resolution demonstrated by the scanning FLR. The scanning FLR uses a more focused beam and electronically steers the beam to survey the entire field of view rather than relying on one or two wide beams.

The scanning FLR operates in the W band. The high operating frequency leads to smaller antennas and improves the signal return performance from small targets. Another advantage of microwave radar is its superior performance over alternate technologies in adverse conditions including snow, rain, ice, or mud. Infrared radar systems often fail to detect certain colors, and the sensors have a relatively short life. Laser radar relies heavily on the light reflectivity of objects, and the sensors have a narrow field of view.

Ultra Wideband Radar

UWB radar systems rely on short duration pulses referred to as impulses having very high peak power and a frequency spectrum that extends from near DC to several gigahertz and translates directly into very high range resolution. Each of the individual frequency channels in the pulse has very low power. Collision avoidance applications use a receiver which detects echoes from reflected objects from zero to 75 m. Range gating (separating return signals by the relative distance from the transmitting radar) is used to discern the reflect signal, so signal strength variations are not an issue with this approach. Frequency reuse is also an advantage with UWB, allowing many users to operate simultaneously without interference. The primary disadvantage of UWB is FCC hesitance to approve its use. The concern is that the UWB signal would jam narrowband users. Rather than being disruptive, impulse waveforms go virtually unnoticed by conventional narrowband users because the energy of the impulse waveform is spread instantaneously over a wide band of frequencies and the average power at a single frequency is low.

Video Systems

Dual camera video systems have been tested by PATH for obstacle detection. These systems use the stereo image to distinguish objects above the road from the roadway itself. Experiments have shown that systems of this type can detect obstacles as small as 15 cm above the road. Video systems are not practical as the sole method of object detection, since night and fog can virtually disable the entire system. They offer some strong possibilities as a secondary or redundant system, since a video system can be used to back up both lateral positioning and obstacle detection sensors.

Communications Technology Overview And Applications

Table 4 contains a summary of various communications technologies which may contribute to enabling AHS implementation. The communications link for individual RSC's may be structured using vehicle-vehicle, vehicle-roadside, and roadside-vehicle paths. The definition of the RSC will determine what combination of links are necessary to support the communications requirements. The following text provides an overview of the key features of each of the technologies in each of the categories. The applicability to the RSC's is also indicated in the discussions.

Table 4. Summary Of Vehicle Communication Hardware

TECHNOLOGY	FEATURES	ADVANTAGES	DISADVANTAGES	COST
VEHICLE-VEHICLE				
Ultrasonic	Low frequency	Directional	Low data rate-Not for platoon control	Low
Infrared	High frequency	Directional High data rate	Sensitive to alignment	Low
SS Data Radio	Spread spectrum Unique network protocol	Good multipath performance Immune to noise Unlicensed band Supports coordinated platoon control	Limited nonLOS range-Not for platoon control	Middle
Cellular	Voice Data becoming more prevalent	Extensive infrastructure	Frequency reuse and system capacity problems. -Not for platoon control	$.80 per minute
PCS	Voice and data Position location	Designated spectrum Rural coverage	Lack of seamless domestic conductivity-Not for platoon control	$3.00 per minute
VEHICLE-ROADSIDE				
VRC	Tag-beacon approach using active vehicle transponders	Line-Of-Sight not required	Added reliability requirements of AHS increase cost	Low
220 MHz	Band recently allocated for ITS application	Different message for each direction	Roadside transmitter installation required-Not for platoon control	<$75 per unit
SS Data Radio	Spread spectrum Unique network protocol	No new bandwidth allocation needed	Self-jamming by other users	Middle
Satellite	LEO or MEO	Existing infrastructure	Low data rate-Not for platoon control	Middle

Vehicle-Vehicle Communications

Communications between vehicles is a primary feature of the vehicle-centered platoon control defined in RSC 2. Close vehicle spacing requires tight coordination among vehicles within the platoon, mandating high update rates of headway spacing, braking, and acceleration information between the lead and following vehicles.

Spread Spectrum Radio

One candidate technology which meets the high update rate requirements of the vehicle-vehicle link is spread-spectrum radio using time division multiple access (TDMA). TDMA provides the benefit of assigning individual vehicles unique time slots, allowing vital control information to be transmitted reliably and conflict free. The spread spectrum waveform is also capable of providing interference rejection. Direct sequence spread spectrum systems modulate the data signal with a wideband high rate spreading code. The higher rate is referred to as the chip rate, and the lower rate information signal carries the data message bits.

Spread spectrum modulation is inherently resistant to multipath signal variations because signals which are delayed by more than one code chip are treated as an uncorrelated input. The higher the code chip rate, the smaller its susceptibility to multipath. The direct sequence spread spectrum waveform also offers enhanced interference rejection. The measure of interference rejection is made in terms of the system's processing gain developed by spreading and despreading the message signal. The spread spectrum receiver recovers the desired signal while suppressing the effects of all other inputs.

The relatively high capacity of the spread spectrum radio enables it to support several modes of operation, including the vehicle-roadside and roadside-vehicle link, but it is not intended for use in vehicle-to-vehicle operations because the sophisticated processing makes it too slow and line-of-sight ranging reduces interference from other vehicles more efficiently. The network protocol which is used to manage data traffic over the three data paths is a prime factor in reliable and timely communications. The assignment of transmission time slots in a manner which gives priority to emergency data and processes longitudinal control information efficiently provides the key to this capability.

Advanced Train Control Radio

Based on a position-location and reporting system with enhanced data communications, the EPLRS system employs a TDMA communications network. The system is slated to provide headway control for the Bay Area Rapid Transit (BART) system trains. The BART application requires that the position of trains be measured and reported to control stations using spread spectrum transceivers, where speed commands will be selected and relayed to the trains via the same transceivers. The EPLRS radio relies on a time slot multiple access protocol and employs spread spectrum modulation for robustness to multipath fading. The radio has the advantage of position location capability combined with data communications, and was designed for rugged environments compatible with outdoor mobile applications. Expensive modifications of the existing hardware would be necessary to achieve accuracies compatible with the requirements for close vehicle following modes. The data rate fully supports the control loop update needs.

Cellular

Cellular telephone operating in the 900 Mhz band is becoming more widespread, causing concern for spectrum saturation. Two alternative approaches to increasing the existing capacity of wireless telephony using digital transmission technology are currently in development in the United States. Large-scale commercial deployment is imminent for both schemes, following experimental field testing and development of detailed standards for each approach. The methodologies used are TDMA and code-division multiple access (CDMA).

TDMA relies on assigning each user a unique time slot for communication with a given base, which can be analogous to the lead vehicle in a platoon. The individual users are considered to be time-orthogonal since transmissions by different vehicles in disjoint time intervals have no effect on one another. The ideal capacity of TDMA is affected by the mobile environment, which is characterized by interference by other cell users in adjacent platoons, and multipath propagation which can result in deep fades. Users in different cells sufficiently separated from the transmitting cell can be assigned the same frequency band as that cell to increase capacity, with the risk of potential degradation in signal-to-interference ratio. Slotted multiple access schemes are also susceptible to self-interference resulting from multipath. Transmissions which propagate over two or more paths and arrive at the receiver separated in time can cause phase cancellation of the desired signal.

Wideband, non-orthogonal multiple access can mitigate the effects of limited capacity and multipath degradation. Spread spectrum multiple access techniques employ a waveform which appears random to anyone but the intended receiver of the signal. One advantage of CDMA is universal frequency reusage, which means that all transmitters communicating with a single base can use the same frequency because the waveform is inherently robust to interference. The spreading process causes competing users' signals to appear as band limited thermal noise, which is relatively benign. CDMA requires dynamic power control to prevent users closest to the receiver from being received at much higher power levels and swamping out more distant transmitters. Spread spectrum signals can be constructively combined if multiple paths are separated by more than 1 µsec for a 1Mhz bandwidth waveform, allowing all of the received energy to be utilized.

Personal Communication Services

Operating in the 1500–1700 MHz band, global personal communication services (PCS) extends the reach of terrestrial PCS islands by overlaying satellite services. Regional low earth orbit (LEO) satellite systems such as IRIDIUM support low-power operation of individual terminals, avoiding large power supply requirements necessary to transmit to more distant satellites. PCS transceivers will be designed to transmit or receive high quality voice as well as data and geolocation signals.

Land mobile satellite systems must also contend with the problems of variation in signal strength due to shadowing in urban areas as well as multipath fading. Studies have shown that severe fades are possible on urban streets, with durations on the highway somewhat shorter. The success rate of data transfers can be improved significantly in urban environments by employing automatic repeat request (ARQ) schemes to recover data lost during fades. Satisfactory results have been achieved in the majority of urban test beds, indicating that the overall communication performance of land mobile satellite systems will not be adversely affected.

Vehicle-Roadside Communications

In RSC 1 the control information which determines vehicle-vehicle spacing within the platoon is transmitted across the vehicle-roadside communications path.

220 MHz

The NTIA recently assigned new frequencies in the FM band for highway advisory messaging. The 220 MHz system automatically informs motorists of emergency situations through interruption of their vehicle radios. The 220 MHz receiver can be installed by plugging into the existing vehicle radio auxiliary input. The 220 MHz transmission is capable of initiating the action to turn on the vehicle radio or switch the audio from the driver selection to the emergency message. The characteristics of the 220 MHz transmission permits different messages to be programmed for both directions of traffic. The 220 MHz system may serve as an auxiliary source of information for a vehicle traveling on an automated highway. The system requires installation of 220 MHz transmitters every one to eight kilometers in areas of coverage.

Satellite

Low earth orbit (LEO) and medium earth orbit (MEO) satellite communications are another option available for roadside-to-vehicle auxiliary communications. The LEO approach is a proven, low risk, low cost approach to data relay via satellite. Existing LEO satellite systems are designed for use with low power transmitters compatible with roadside deployment, with excess capacity readily available for data message relay.

Several commercial LEO systems are currently being deployed, including IRIDIUM and ORBCOMM. The ORBCOMM network is online at the current time with an initial deployment of two satellites, with earth stations also in operation. The main deployment consists of 24 satellites, scheduled for completion in 1994. Availability requires that one of the satellites have simultaneous sight of the roadside uplink transmitter and the vehicle receiver. The placement of roadside uplinks can be specified to provide the level of communications availability required to ensure AHS safety.

Developing AHS Hardware

Microprocessors, digital hardware, analog hardware, communications hardware, wiring harnesses, connectors, radar equipment, and possibly fiber optics will occupy the interior, underbody, and engine compartment areas of AHS cars and trucks. Systems engineering has been developed as a means of dealing with this complexity, by providing a conceptual and organizational framework for managing the design, development, manufacture, marketing, servicing, and ultimate disposal of a system. It also guides the development of the infrastructure in which the system operates.[9]

Functional analysis defines a baseline of functions and function performance requirements which must be met in order to adequately accomplish the job.[10] Decomposing functions into subfunctions will make identification more manageable. Functional flow block diagrams may be used to indicate the sequential relationship of all functions that must be accomplished by a system. They depict the time sequence of functional events. A potentially large problem can be partitioned into several smaller but manageable ones. Once the functional analysis is complete the process of generating requirements, parameters and constraints can begin. Once a first cut at the requirements is in place different technical approaches are proposed and traded off against each other.

AHS Vehicle Subsystems

In the simplest terms the AHS vehicle will have automated steering, throttle, and braking functions that are normally executed by the human operator. The manner in which these functions are executed becomes the issue at hand for the systems design. A design can be optimized for very specific constraints or be versatile to accommodate expansion or a wider variety of options. An optimized design would be more cost effective and contain the minimum number of parts. It would contain only the amount of I/O and computational power necessary to meet it’s designed needs.

The approach to developing a system architecture to accomplish automated vehicle control will be reliant on some of the key design drivers. The primary drivers will be, the RSC in which the vehicle will operate, the state of actuation technology, the cost requirements, ranging scheme, and fail safe requirements.

Task 3. Reliability

The automotive industry constantly strives to find new and more economical ways to manufacture products that are high in quality and reliability. Reliability is important in today's automobiles. Reliability in an AHS vehicle will be at least as important. Crossing the evolutionary threshold from manual to automated vehicle control will bring with it many issues, probably the most important being the reliable and safe operation of AHS vehicles.

The electrical content of automobiles increases every year. AHS vehicles will require more electronic control systems than today's automobiles. These systems will require more powerful computers, more signals to be processed from sensors, and more signals to be output to control actuators. This added complexity in the vehicle architecture will require increased cooperation between component suppliers.

New methodologies and processes will be necessary to insure top quality and reliability in AHS. Traditionally the automotive industry has been reluctant to share component and system designs.[11] This proprietary behavior causes delays and additional cost in manufacturing and assembly.

Automobile manufacturers spend billions of dollars annually on warranty and liability claims. Traditional automotive manufacturer liability concerns may be small compared to those associated with an AHS vehicle, especially in terms of human causalities and property damage if a vehicle malfunction occurs. Many company liability issues surrounding AHS will need to be addressed.

GM's Saturn Corporation uses a specific, very effective methodology (Robust Engineering) in the design of their automobiles. By looking at the design up front and looking at how each component or system works with each other both from a design and assembly view point, the overall system benefited from higher reliability. Saturn's automatic and manual transmission development yielded about 30 new patents. Warranty costs have been negligible, manufacturing costs have been reduced, and development time is less.

The Robust Engineering methodology used at Saturn is one of many new developments found at the domestic automotive companies. Ford intends to substantially improve the 160,000 km maintenance schedule on the new Mercury Mystique and Ford Contour. Ford's longer term goal is to design for 240,000 km durability. Robust Engineering is a methodology that has no specific definition. It does involve solid interaction between individuals involved with development, manufacturing, costing, quality, and reliability. The goal of Robust Engineering is to make systems that are insensitive to manufacturing variations and to create designs that will last a long time in the field and have good reliability, durability, and quality.

Automotive manufacturers are delegating more and more of the engineering and manufacturing responsibilities to their suppliers. Suppliers will be required to submit detailed information on their products based on robust engineering methodologies, and suppliers will also be liable for warranty and liability cost sharing. Working closely with each other will be a necessity, robust engineering methodologies will flow down to the supplier levels.

Nissan Motor Co. Ltd., using robust methodologies, was able to reduce the heat treating time for parts used in some of their steering and powertrain assemblies from 10 hours to one minute. In Europe, Ford and Pirelli SpA used robust methodologies to resolve a timing belt failure problem. They were able to lower audible noise levels and double belt life and money was saved because the supplier could use less expensive materials.

Robust Engineering includes such methodologies as the following: quality function deployment (QFD), statistical process control (SPC), design for manufacturing (DFM), voice of the customer (VOC), total quality management (TQM), design for manufacturing (DFM), and simultaneous engineering (SE).

AHS Equipment

The addition of a large amount of electronic equipment raises reliability and maintainability issues which can affect the safety of AHS as well as the ability of a vehicle to qualify for entry onto the AHS highway. Reliability of modern electronics is determined primarily by system complexity and manufacturing techniques. Maintainability issues include repair/replacement decisions, self test capabilities, fault detection, and fault isolation.

AHS vehicle electronics can be compared in complexity to existing electronics such as video camcorders, cellular phones, and car radios. Like these, AHS vehicle electronics may not be well suited for do-it-yourself repair. The equipment may work flawlessly for years, only to fail without warning. Repair costs can be quite high, approaching 50 percent or more of the cost of the equipment. Using existing consumer electronics as a guide, the design of AHS equipment should include self test in order to predict impending failure and prevent sudden loss of operation. The equipment should be placed in the vehicle in such a way as to allow straightforward or modular removal and installation.

Backup systems are valuable as a method of compensating for the failure of safety critical electronics. Currently, braking systems are designed as two independent systems with a mechanical backup, in spite of the fact that a sudden failure of the braking system may be a statistically insignificant occurrence. In AHS, the controllers/actuators for the brakes and steering could require two completely independent systems, regardless of the reliability of the controllers and actuators.

Using existing equipment reliability trends as a guide, it is expected that the electronics equipment for AHS will be extremely reliable, and may last the lifetime of the vehicle. The equipment will likely contain a self test function which will effectively predict failures. Maintenance of failed equipment will probably involve replacement of the equipment rather than component repair, and could be quite expensive.

The following table lists typical equipment being analyzed for AHS and an estimate of the equipment reliability and maintainability.

Table 5. AHS Electronic Equipment Reliability And Maintainability

Equipment	Reliability	Maintainability	Comments
Video Sensors/Processors	Low	Low	Very complex device which requires significant computing power
Transceivers	Medium	High	Transmitter less reliable than receiver, but self-test is easy
Radar	Medium	Medium	Complicated device with exposed antenna
Processors/Controllers	High	High	Very reliable, even in vehicles
Ladar (Infrared Radar)	Medium	Medium	Exposed antenna
Infrared Communications	Medium	Medium	Fairly simple devices, with some self-test capability
Magnetic Field Sensors	Medium	High	Simple devices, but must be mounted in a partially exposed position
GPS Receivers	High	Medium	Complicated device with limited self-test capability

Modern Electronics Reliability

Modern electronic devices are extremely reliable, especially when compared to similar devices of older vintage. This trend is due to the fact that there are fewer internal components, with more functionality provided by each component. The most common failure in electronics is in the connections (wires, solder joints) between components. Assembly techniques are critical to the reliability of connections. This combination of reducing the number of components while improving the methods of interconnecting the components is expected to continue. Assembly and handling also affect the reliability of the components since damage due to electrostatic discharge can cause latent failures.

The mean time between failure (MTBF) can be used to measure reliability. MTBF values in the tens of thousands hours are common, with some devices reaching over one hundred thousand hours. A relative estimate of the reliability of candidate AHS equipment is included in the table. The values of low, medium, and high reflect current state of the art of the equipment types based on complexity of similar equipment.

Maintainability

In order to properly maintain electronics equipment, faults must first be detected, then isolated to a unit or component level which is replaceable, and finally replaced with a working unit. Replacement can be done at the component level, the board level, or the unit level. With the component count dropping and the training and test equipment required for fault isolation, replacement at the unit level seems reasonable. Self-test capability should be included in the units to aid in fault isolation.

The maintenance of equipment may measured by the mean time to repair (MTTR). MTTR includes the time to isolate the problem to the unit level, remove the unit, repair it, and reinstall it. The combination of self-test and unit level replacement will minimize the time to repair. Accessibility of the equipment is also a factor, since it impacts the removal/installation time.

Availability

Availability is a measure of the fraction of time that a device is available for use. The mathematical definition of availability is:

$$\text{Availability} = \frac{(\text{MTBF} - \text{MTTR})}{\text{MTBF}} \qquad (1)$$

Availability is an interesting measure to consider, since it shows that a short repair time is as important as a long MTBF. Both measures must be considered in evaluating acceptability of a unit for AHS implementation.

Video Sensors/Processors

Video equipment can be used for lateral control and obstacle detection. In either case, each video image must be analyzed pixel by pixel, which leads to a requirement for a video processor as well as the sensor (camera). If a stereo image is used, the cameras may require alignment, which adds to the maintenance. In addition, the video lenses must be pointed in the direction of vehicle movement, which subjects them to damage by objects thrown from the road and to reduced or blurred images from rain, mud, and dirt. For these reasons, both the reliability and maintainability are low.

Transceivers

Transceivers are becoming fairly reliable devices. Antennas are made of metal and can be installed with limited or no exposure to the outside elements, which increases relative reliability. The hardware circuitry is becoming more highly integrated, with an associated drop in component count. Reliability is rated medium based on comparisons to existing transceivers. Maintainability is estimated high since effective fault detection and isolation techniques for transceivers are well known.

Radar

As with other electronic devices, the radar processor is becoming smaller and more reliable as the level of hardware integration increases and the number of components decreases. An array antenna is more complex than a dipole antenna because it contains a large number of radiating elements often with electronically controlled phase shifters for beam steering. In addition, the radar antenna will be exposed to weather and thrown objects since it must be pointed in the direction of travel. Maintainability is judged medium due to the complexity, and reliability is judged medium due to the exposed antenna.

Processors/Controllers

Today's processors and controllers are highly integrated devices. They are produced in massive quantities, and are extremely reliable. Processor designs have advanced to the point where they can be placed in the high vibration and high temperature environment of a vehicle without loss of reliability. Reliability is judged high. Built-in-test techniques for the detection and isolation of faults are mature, yielding a maintainability rating of high.

Ladar

Laser radar devices, referred to as ladar, work on the same principle as RF radars, but operate in the optical band, typically in the IR range. They are not yet widely used, but they can be built simply and inexpensively. The transmitting and receiving lenses must be pointed in the direction of travel, which exposes them to debris and weather. The reliability is judged medium because of the exposed antenna. The maintainability is judged high because of the simplicity of the device.

Infrared Communications

These devices are similar to ladars and can be built simply and reliably. The transmitting and receiving lenses are exposed to debris and adverse weather conditions. Like ladars, they are judged to have medium reliability and high maintainability.

Magnetic Field Sensors

These sensors are used to follow a series of magnets spaced along the middle of the roadway. Typically, two sensors are mounted on the front corners of the vehicle and are aimed down at the roadway. This position shields the sensors from weather and most debris which can be thrown by the preceding vehicle. The sensors may require calibration since any error in a sensor reading will cause the vehicle to shift off of the center of the roadway. Magnetic field sensors are judged to have medium reliability because of their partially exposed mounting location and since they are used in pairs and may require periodic testing. Maintainability is judged high because the sensors are passive and fault detection and isolation are relatively simple.

GPS Receivers

These devices are fairly complicated, but the trend is to smaller units with higher levels of integration. The antenna is metal and can be protected from the environment. GPS receivers with built-in-test capability and fault isolation logic are becoming available, and should be used in AHS vehicles. The reliability is judged high because the GPS receiver is similar to a standard car radio in complexity, and the maintainability is judged medium because unit is likely to require modular replacement and depot repair.

Task 4. Achievement Of Fail-Soft Reduction In Functionality

Fault detection and fault mitigation are the two parts of fail soft reduction in functionality. An AHS control system like all others must first diagnose problems and then decide on what to do about the problem. This task will address both of these key areas.

Fail-Soft Design Approaches

In this task elements of vehicle and vehicle hardware design that are redundant or in some manner protect the system from failures of the sensors, controllers, communications, and actuators will be discussed. Items such as redundant circuits, alternate actuators, preferred failure modes, and special component designs and costs will be included.

The use of high quality components and a careful system design will not result in zero system failures. A fault tolerant computer system can yield satisfactory results even in the presence of faults. The basic idea behind building a fault tolerant capability is to provide the system with extra (redundant) resources, beyond the minimum required. Carrying spares for every possible contingency is impractical, however, and no system design can ever provide fault coverage for every conceivable failure scenario.

The desired level of dependability is achieved by building in protection against the most likely failures. Usually fault tolerant systems provide protection against failure in any single component or module, since the probability of multiple simultaneous failures is very small. The vast majority of computer system failures are transient or intermittent component failures. Such failures can be corrected by restoring the correct state without replacing the failing component.

Software fault tolerance is currently not as well developed as hardware redundancy methodology. At least one Apollo and one Space Shuttle mission were aborted due to software failures. Software reliability is achieved mainly through fault avoidance. Software faults are design errors rather than the faults experienced by hardware that can wear out.

Faults, Errors, And Failures

A fault is a physical defect, imperfection or flaw which occurs within hardware or software. Examples of faults are physical damage, short circuits, open circuits, and endless software loops. Faults may also result from design errors or external environmental conditions, such as temperature, electromagnetic interference, ionizing radiation, or system misuse.

An error is a manifestation of a fault, in which the logical state of an element differs from its intended value. An error in a system is the result of a fault but not all faults cause errors. A fault is termed latent if it has not yet caused an error to occur.

A failure is the nonperformance of some expected action. Failures (figure 2) are caused by errors which results in the system performing one of its functions incorrectly.

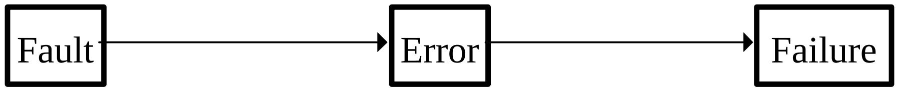

Figure 2. Failures Are Caused By Errors Which Are Caused By Faults

A fault can be characterized by its duration, nature, and extent. Fault duration can be transient, intermittent, or permanent. Transient faults are often due to external disturbances and are non-recurring. Intermittent faults cause a system to oscillate between normal and faulty operation, resulting in marginal or unstable operation. Permanent faults result from component failures, over stress, or design errors. Transient and intermittent faults occur more frequently than permanent faults but are harder to detect since they disappear.

The nature of a fault can be described as logical or indeterminate. Logical faults, such as a gate input stuck at logical zero, are easily modeled using statistical methods. Indeterminate faults do not have logical equivalents and are difficult to model.

Local faults affect single components. Global faults affect multiple parts. Multiple faults become more likely as system size grows, and require more extensive fault modeling.

Hardware Redundancy

Static (or passive) hardware redundancy uses the concept of fault masking to hide the occurrence of faults and prevent the fault from causing errors. Passive techniques do not require any action on the part of the system or operator. Passive systems use majority voting mechanisms to mask faults.

In an active (or dynamic) redundant system faulty components are detected, diagnosed, and removed from the system. Active techniques require that the system be reconfigured to tolerate faults. Dynamic redundancy involves the switching of modules or rerouting communications as faults occur.

Hybrid redundancy combines fault masking and fault detection, location, and recovery using spare components. Hybrid redundancy is used in long tern ultra-reliable applications when the probability of multiple faults is high.

Modular Redundancy And Voting

Modular redundancy and voting consists of using at least three identical modules having the same inputs and nominally expected to have the same outputs. A specific output for system use is obtained by choosing the output value obtained by a majority of the modules. A diagram is presented in figure 3.

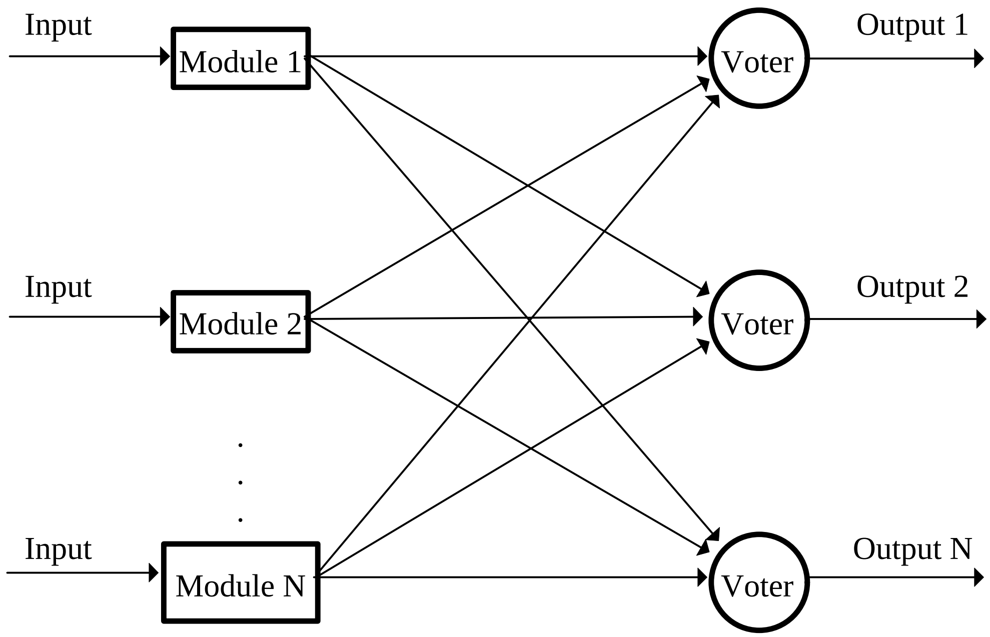

Figure 3. Modular Redundancy And Voting

Duplication With Comparison

An active redundant duplication with comparison uses two identical pieces of hardware running identical software. If the outputs of the two modules are different a fault is signaled. There is no way to determine which of two modules is defective in the basic scheme.

In figure 4, a duplicated microprocessor system is used to implement the comparison process in software. Each processor does identical calculations and places one copy of the results in local memory and a second copy in shared 2 port memory. Each processor compares its own calculated value with the other processor result obtained from two port memory. If the values do not match either processor can disable the control output using one of two series switches in the output signal line. Both processors must agree that results are identical before an output is available. A failure in one of the processors or in two port memory will also disable control output.

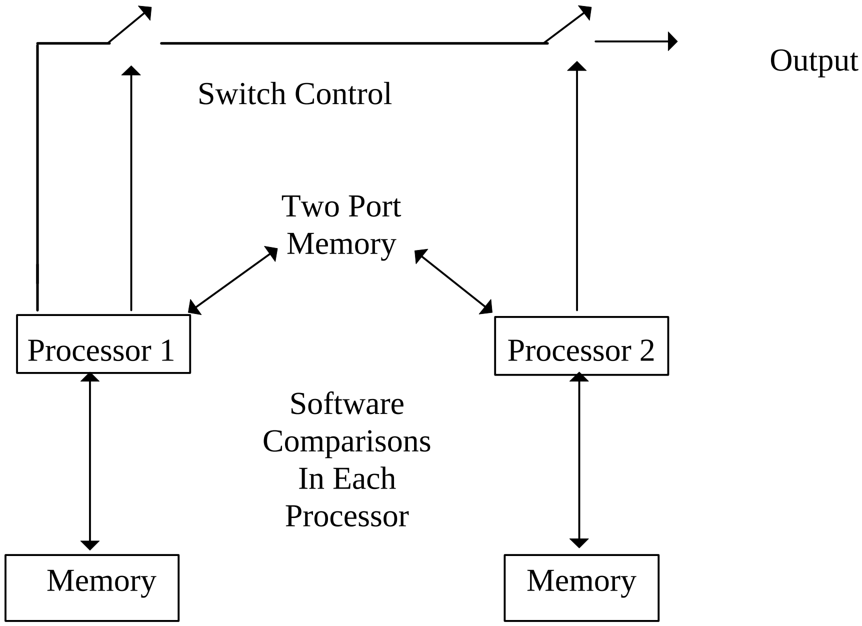

Figure 4. Duplicate And Compare System Configuration

Standby Sparing

In standby sparing configuration (figure 5) one module is operational and one or more modules serve as stand by or spare units. When a module's error detection circuitry detects a fault a new module is selected as the operational module. A control circuit monitors the fault output from each module to determine which module output to use.

An advantage of standby sparing occurs when a system uses a large number of identical modules. In this case redundancy can be achieved without having to duplicate every module.

One possible method for error correction circuitry is to combine two modules in a duplication with comparison configuration. The two modules are operated in parallel and their results are compared for error detection circuitry. When a module fails, a standby module pair is selected.

Alternating Logic

A circuit has the property of self duality when the output of itself is the logical compliment of itself when the input is complimented. Alternating logic uses this concept to detect a stuck at one or stuck at zero fault. If a self dual circuit single output is low it should go high when the complimented input is applied.

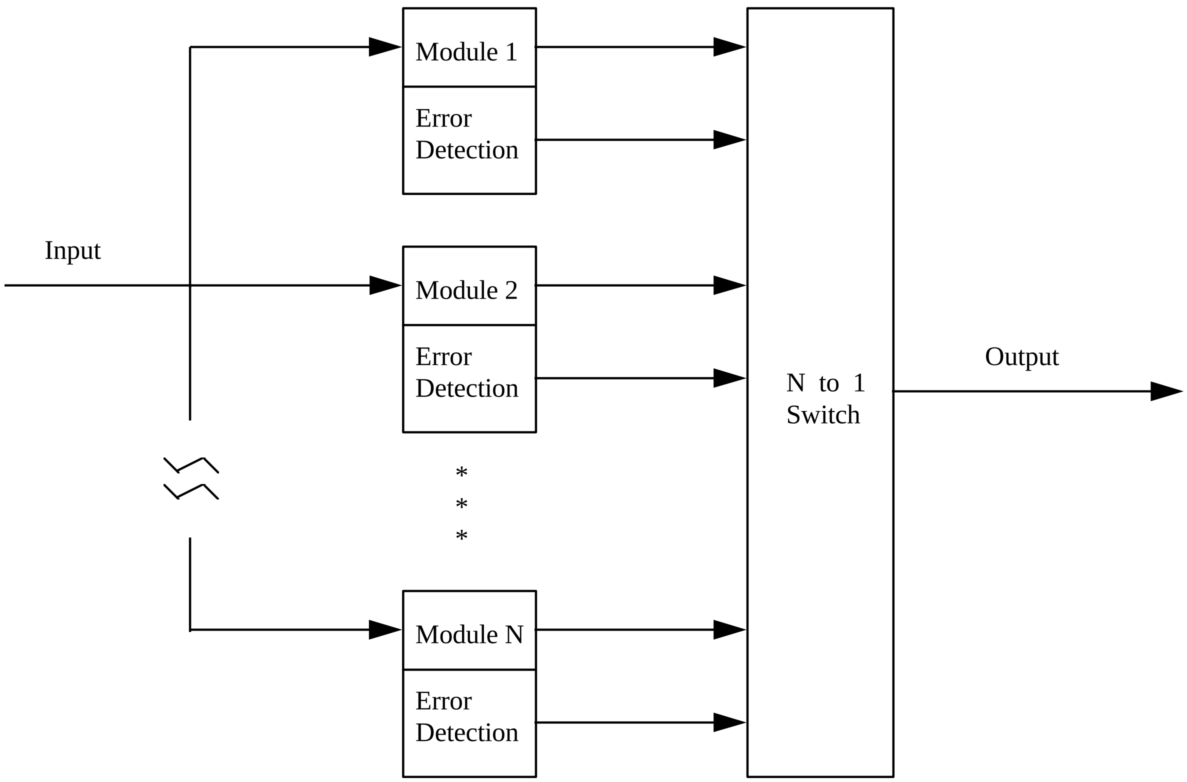

Figure 5. In Standby Sparing Configuration

Watchdog Timer

A watchdog timer is an extremely useful active hardware redundancy method. The timer must be reset periodically. If the time interval expires without a periodic timer reset, the timer can either reset or shut down the processor.

The frequency of timer reset is dependent on system requirements. If a system must detect a fault within 100 milliseconds then the timer should be reset at intervals less than 100 milliseconds.

The watchdog timer is good at detecting certain types of faults. If a processor stops or enters an endless loop the watchdog timer will detect the lack of response. In a heavily overloaded system, software may begin to take longer than expected to execute and the timer will reset the system.

N - Modular Redundancy with Spares

Most approaches to hybrid redundancy are based on the concept of N-Modular redundancy (NMR) with spares, as illustrated in figure 6. NMR with spares uses a basic core of N identical modules in a voting configuration. Spare modules are provided to replace failed units in the NMR core. The full voting configuration can be restored after one module fault. If a second fault occurs the fault can be masked providing tolerance of two faults. For a passive N-Modular approach to tolerate two faults , five identical modules would be required. The hybrid approach accomplishes the same results with four modules and additional fault detection, location, and recovery circuitry.

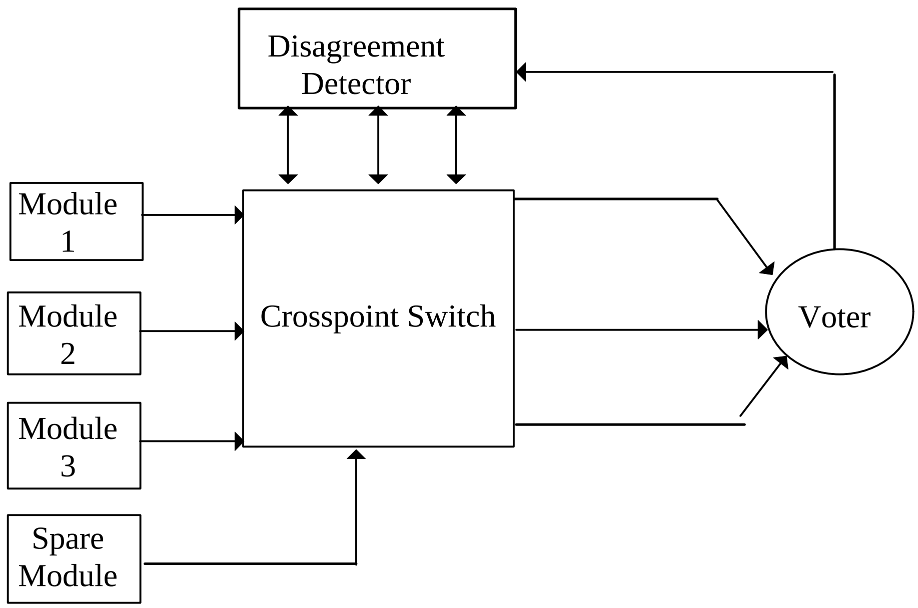

Figure 6. Four Module Redundant System With Spares

NMR with spares compares the output of each module with voter output. If a disagreement occurs, the module is labeled faulty and a spare module is switched in. Voting is always occurring between the active core modules.

Software Redundancy

Fault detection and fault tolerance can be done in software. Redundant software can occur in many forms; complete programs do not have to be replicated to have redundant software. Software redundancy can consist of a small memory test routine or a few lines of code to test the polarity and limits of an input.

Consistency Checking

Consistency checking uses advance knowledge of expected data values to verify correctness. If the tested data value lies outside the expected range, an error of some type has occurred. This approach can be used to verify operation of physical sensor inputs.

Hardware can be used to detect invalid instruction codes in computers. Each instruction code is checked to verify it is a legal instruction. If an invalid instruction is detected the computer can be halted to prevent erroneous instructions from being executed. This method is particularly useful in detecting a “run-away” processor that is trying to execute data instead of instructions.

Capability Checks

Capability checks verify that the system has expected capabilities. A simple memory test can read and write scattered memory locations to verify proper memory operation. Usually it is not necessary to read a large number of memory locations to obtain reasonable fault coverage.

Periodically the processor executes specific instructions on specific data and compares the results with data stored in read only memory (ROM). This test checks both the arithmatic logic unit (ALU) and memory where the results are stored.

Another capability check is the multiprocessor communications test in which all processors in a system verify they can communicate with each other. The processors periodically pass specific information to one another. Shared memory can be used as a communications medium if available.

N-Version Programming

N-version programming consists of designing the software N times and comparing the N results produced by these modules. Each of N modules are programmed by a separate group of programmers. Each group designs from the same set of specifications so each module has the same functionality. Theoretically by developing N versions of software independently, the same mistakes will not be made by all software engineers. When a software fault occurs it does not occur in all modules or occurs differently in each module so that the results generated by the modules will differ.

N-version software has two weaknesses. First, programmers tend to make similar types of mistakes so there are no guarantees that different versions of software will not have identical faults. Second, an error or omission from the common specification would be present in all versions of software.

Fault avoidance during software development can be used to avoid the problems with N-version software. Software designers use rigid design rules and methods to attempt to keep faults from occurring. If the software is designed correctly in the first place, fault tolerant software techniques such as N-version programming will not be required.

Information Redundancy

Information redundancy is the addition of information to data to allow fault detection, fault masking, or fault tolerance. An error detecting code allows errors introduced into a data word to be detected. Additional bits are introduced into a data word creating a new longer data word. Only a portion of the new words are valid. Occurrence of an invalid word signifies an error.

An error correcting code contains a scheme which allows data errors to be both detected and corrected. Real time correction allows a system to continue operation uninterrupted. Within a single word, the number of errors detectable or correctable is related to the minimum separation or Hamming distance between words of the code space. If two words have a Hamming distance of one, only one bit difference exists between data words. A single error transforms the word into another valid data word. If the distance is two then a single bit error creates a non-data code word, at least two bit errors would be required to change the original data word into a new valid data word. When data words with a Hamming distance of three change into a non-data word created by a single bit error, the distance from the original word is one and at least two words from any other data word, allowing the original word to be uniquely identified.

Larger Hamming distances allow detection and correction of greater numbers of bit errors. The cost of increased error coverage is larger words and increased algorithm complexity. Inexpensive integrated circuits are available for use in encoding and decoding errors in RAM storage. These memory support chips can typically correct single and double bit errors.

Parity Code

Single bit parity codes require the addition of an extra bit to an existing word so that the resulting word has an even or odd number of one bits. If the extra bit results in the total number of bits being odd, the resulting code is referred to as odd parity. If the total number of bits is even, the code is called even parity. Single bit parity has a Hamming distance of 2 allowing single bit errors to be detected but not corrected.

The two most common applications of parity are memory arrays and serial communications links. In a memory system additional hardware is added to handle the extra parity bit. A parity generator sets the parity bit to the proper state when a data word is stored in memory. A parity checker tests the data when read from memory and signals a fault when the stored and calculated values mismatch.

The biggest problem with single bit parity codes is the inability to detect some common multiple bit errors. Multiple parity bits can be used to increase multiple bit error detection.

Checksums

Checksums are used when blocks of data must be transferred from one location to another. The checksum is basically a sum of the original data. A checksum is calculated for the data being transmitted. The receiving data recalculates the checksum on incoming data and compares the result with the received checksum. Checksums can locate errors but not correct them. The complete data block in which a checksum was calculated must be corrected.

Checksums are also used to verify the integrity of system read only memory devices. A checksum is calculated when the read only memories are first programmed and stored in the ROM along with data. During system initialization time system ROM checksum is recalculated and compared with the stored value.

Hamming Error-Correcting Codes

Up to 60 or 70 percent of the faults in a system can be caused by memory errors. Transient faults are becoming more prevalent as memory density increases. Inexpensive memory error correction chips using Hamming code are readily available.

Hamming code is formed by partitioning data into multiple parity groups and specifying a parity bit for each group. Parity groups are overlapped in such a way to uniquely identify a faulty bit. Hamming code bits are generated during a memory write cycle and stored along with the original data. During a memory read the Hamming code is regenerated from the stored data and compared with the stored code value. The digital word resulting from the comparisons is defined as the syndrome. Non-zero bits in the syndrome correspond to changed bits in the stored data word or stored check bits. Using a controlled complementation unit the error can be corrected.

Fault Tolerant System Design Process

Both hardware and information redundancy can require large amounts of redundant hardware to implement. Time redundancy uses repetitions of calculations in ways that allow faults to be detected. If an error occurs, the calculation can be repeated to see if the disagreement remains or disappears. Time redundancy can't be used in all systems because of the additional time required.

Time redundancy can be used to detect whether a fault is transient or permanent. If after repeated calculations, the result is still erroneous, faulty portions of the system can be disabled. If the error goes away, no corrective action is required.

Fault tolerance must be coupled with other design techniques to be successful. Figure 7 shows a top level view of the design process. System design includes both fault tolerance and fault avoidance techniques. System evaluation must be done concurrently to ensure a successful fault tolerant design. System evaluation can help uncover problems early in the design phase when they are easier to correct. Evaluation methods include Markov reliability models, system repair models, combinatorial reliability models, and maintainability models. Evaluation techniques are used to locate failure prone circuit areas.

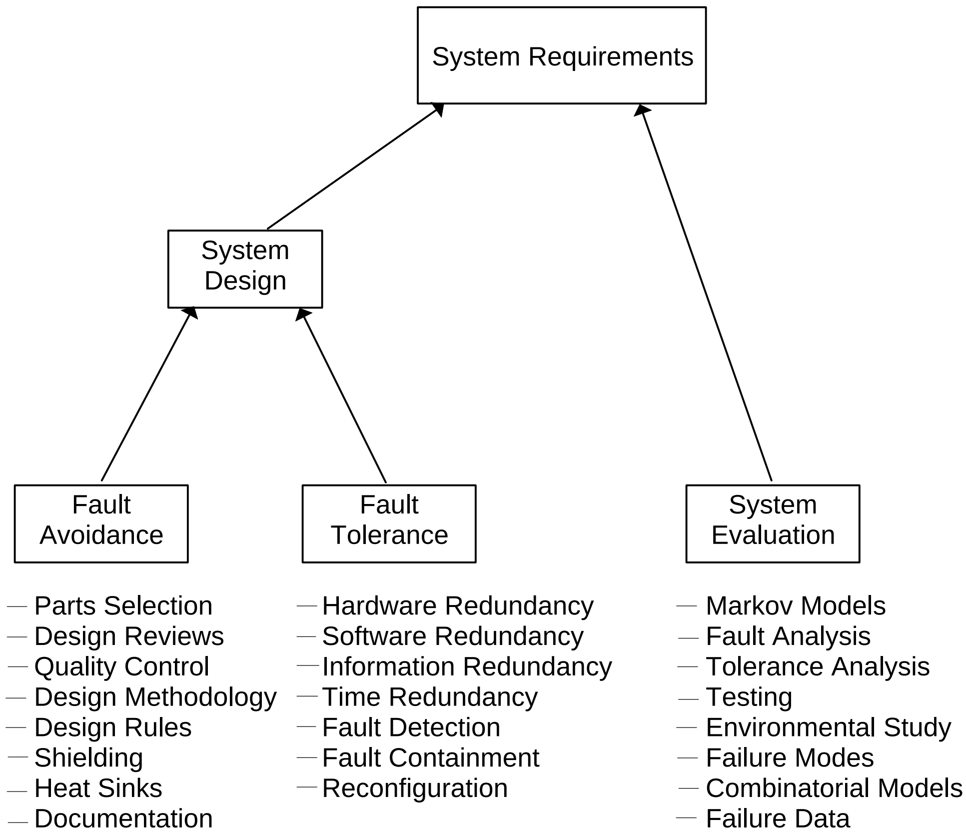

Figure 7. Top Level View Of The System Design Process

The design process consists of five major phases:

- Requirements.
- Conceptual.
- Specification.
- Design.
- Test.

The design process is iterative as tradeoff studies suggest design changes.

The requirements phase begins with a clear problem definition. A written description helps clearly define the problem to be solved. A set of requirements is extracted from this problem definition. The requirements should be verifiable using either analytical or experimental methods. The system is partitioned into manageable subprograms based on reliability requirements.

The conceptual phase begins with creation of several candidate designs. Using several designs will highlight the design strengths and weaknesses of each approach. The list of candidate designs is evaluated with a high level analysis of cost, reliability, weight, and other design parameters. The high level analysis should reduce the number of candidates to one or two.

During the specification phase a detailed plan to meet system requirements and produce a practical design is created. A system that is designed incorrectly will never perform as desired. Specification mistakes are a common pitfall in complex designs.

The candidate selected from high level analysis is carried through a complete hardware and software design phase including making prototypes. In most cases hardware and software can be developed in parallel. It is important to continue analysis of the system requirements (reliability, maintainability, and cost) to ensure that design decisions don't compromise the system. As hardware is developed more information will become available for failure rate estimation and fault coverage calculations.

The testing phase involves searching for faults of all types including design defects, implementation errors, and component defects. The test process is used to uncover architectural or algorithmic problems.

Future Directions of Fault Tolerant Designs

Previous fault tolerance work focused on gate level fault models. Modeling failures has dealt with localized rather than system wide faults. Active research in probabilistic reliability modeling will improve reliability estimation accuracy.

Future software language may provide syntax and run time support for fault tolerance. Built in fault tolerance mechanisms will increase software reliability and reduce software development time. Currently, fault tolerant software requires approximately 2.5 times longer for development than a non fault tolerant version.

Semiconductor manufacturers have produced chips such as memory controllers with built in error correction circuitry and processors with duplication and match circuitry. Fault tolerant techniques are now routinely appearing in general purpose computing systems. Fault tolerant component costs will continue to drop as they become more commonly used.

Fail-Soft Capabilities For AHS Vehicle Systems

The Automated Highway System (AHS) will be designed to reduce travel times, increase highway safety, reduce congestion, decrease the economic and psychological costs associated with accidents, lessen the negative environmental impact of highway vehicles, and increase lane capacity. In short, it is designed to improve highway capacity and safety. These two goals are interrelated since an unsafe system would not only cause significant safety problems but may also reduce highway capacity. Although, AHS, by definition, an automatic system, should be able to eliminate or reduce the human operating error by employing automatic vehicle control systems or hazard warning devices, it will still have to withstand all the physical environments which the human driver system encounters. Moreover, with additional system complexity, both hardware and software, the potential system failures which can cause safety problems may increase. These system failures can be generated by failed component(s), physical disturbances from the environment, operating errors, errors in the design, or production variations. Therefore, there is a need for system safety studies on AHS to determine what level of safety an AHS should provide, and how to accomplished this level of safety.

Researchers should work with policy makers to establish the safety level of the AHS system. To achieve the required level of safety, two steps are involved: failure analysis and failure mitigation. Failure analysis involves identifying hazards and performing hazard reduction analysis on both system and subsystem levels. Failure mitigation consists of failure detection and failure control strategy. They function under the assumption that a failure has occurred. This section focuses on the issues of failure mitigation at the vehicle level.

Fail-Soft Capabilities For AHS Vehicle Systems Overview

Definition

Fail-soft capabilities for AHS vehicle system are defined as vehicle capabilities employing sensing, computing, and control devices either on board vehicle or on the roadside such that the AHS can be self-adjusted to operate at a minimum safety level (fail-soft/fail-safe state) when failure (abnormal/hazard state) occurs. Such a minimum safety level may involve stopping the vehicle or even the entire highway system if it is deemed to be the appropriate safety level with respect to the particular failure situation.

Unique Feature

The unique feature of AHS fail-soft capabilities compared with those of conventional manual controlled highway system is support for vehicle coordination so that the impact of a failure (both on the severity of a possible accident, or on the reduction of traffic flow) may be minimized. That is, AHS vehicles will have the ability to react, in a coordinated fashion, to vehicle failures.

Failure Source

AHS failures can be generated by failed components, physical disturbances (wind, snow, or fallen object on the roadway, for instance), operating or design errors, and manufacturing variations. As far as vehicle-level fail-soft capabilities are concerned, the focus is on the component failures. Because of the large introduction of new components into the highway system, component failures may become a dominant factor that influences the safety of the AHS system. Structurally, the AHS contains the following component subsystems:

- Vehicle Systems – May contain communication components, information acquisition or sensing components, information display or warning components, control components, actuating components, existing vehicle mechanisms, and human/machine interfaces.

- Roadway or Roadside Systems – May contain communication components, information acquisition or sensing components, control components, local traffic management components.

- Central Control System – May contain communication components, network traffic management components, and human/machine interfaces.

The vehicle level fail-soft capabilities will address the failures attributed to both vehicle and roadside components.

Failure State

AHS may be operated when there are component failures. In terms of the safety of the system, there would be, according to the pre-defined safety criterion, two kinds of states to which the system will be directed as the result of failures. They are:

- Fail-Safe state – A state which ensures that safety is within the criterion as a result of the failure(s).

- Fail-Hazard state – A state which can not ensure the safety within the criterion as a result of the failure(s).

The fail-soft capabilities are to be designed to transform a fail-hazard state into some fail-safe state when failures occur.

Design Guideline

The following are some design guidelines for achieving an effective vehicle fail-soft system:

- Robust and Reliable Base Design – The more environmental/manufacturing/component variations the base vehicle design can tolerate, the fewer the situations and the lower the frequency of failures the fail-soft system needs to be designed to respond to.

- Identify Minimum Safety-Critical Components – The minimum safety-critical components of a AHS control function should be identified. Those critical components are the minimum components to ensure the existence of a fail-safe state in any AHS control function. The system can consist of other components to improve performance and robustness, but the loss of them will not degrade the system to a fail-hazard state. For example, the lateral control function can be accomplished alone by the lateral deviation measurement and the steering actuator with degraded performance. Therefore, the lateral controller should be able to switch to a fail-safe algorithm when yaw rate or lateral acceleration sensors fails. However, the failure of an automatic steering actuator or lateral deviation sensing device will certainly result in a hazardous situation. Such safety-critical components as automatic steering actuator and lateral deviation sensing device should be identified and designed with either high reliability or with redundant components. In fact, these two components are the most safety-critical components of the automatic control systems in terms of a single component failure.

- Design Automatic System so that It Fails to Its Manual State or Off Position – When an AHS automatic control system fails, it may be preferable to design the mechanical system to fail to its manual counterpart. This option may be necessary should human intervention be considered during some failure situations. However, this may not be feasible with certain mechanical designs. Yet even when failing to manual state is not feasible, the automatic control actuators should still fail to their "off" positions, i.e., no-throttle, and no-steering (the brake state is more complex) should be the automatic control fail modes.

- Implement Fail-Soft Design – Because of the introduction of new components and stringent performance requirements, the AHS system failure rate could be higher than that of the existing manual driving highway system. However, the coordination nature of the AHS structure and the extra sensing and control devices may present themselves as an opportunity to improve safety. To take advantage of this situation, fail-soft control strategies need to be designed and implemented.

Failure Mitigation

Failure mitigation is the process of reducing the impact of any failure should it occur. Fail-soft design is an effective way of failure mitigation. Fail-soft property can be interpreted as the ability of allowing a system to enter into a fail-safe state in the event that the system deviates from the normal operating mode. Because the fail-safe states are defined in accordance with the particular failure modes of the components, a system that is designed based on the fail-safe principle will lead a system into a corresponding fail-safe state, including maintaining the system operation or some levels functional degradation (e.g., reduce vehicle speed or increase vehicle spacing). Nevertheless, "fail-stop" sometimes is the one and final degradation state of the fail-safe state when any other functional degradation states are not enough to prevent the system from unacceptable hazards.

Fail-soft design can be achieved by a specially designed protection system which can detect system failures in the early stages and then lead the system into previously defined fail-safe states. It therefore consists of both failure detection and failure control. These two functions are interrelated and their effects are interdependent. They will be discussed in the next two sections.

Failure Detection

Failure detection/diagnosis is an essential function required for any fail-soft design. Based on the timely detecting results, failure control function can be performed to mitigate failure impact on the AHS. A failure detection system may include a number of supervising devices, each responsible for monitoring a pre-defined component(s). These devices can be integrated into the design of the functional system or components. The failure detection system may also be part of the vehicle diagnosis/check in/check out system. In the AHS environment, some failure detection responsibilities can be shared by roadside or platoon members as well.

Failure Detection Requirements

Since the failure detection system is responsible for detecting system/component failures, the requirements for the detection devices are very strict. These requirements are listed below:

- A failure detection system must be capable of detecting a critical state of the AHS vehicle system which may lead to a safety hazard.
- A failure detection system must be able to effectively detect failures and/or isolate failed component within a given time interval so that the failure control system can promptly respond to the conditions induced by the failures in order to mitigate the impact of the failure to AHS.
- A failure detection system is required to perform normally and continuously along with the observed AHS system/components. Therefore, it must be highly reliable.
- A failure detection system must itself be fail-safe, which specifies that the failure detection system should be capable of performing self-diagnosis and inform the AHS vehicle system of the detection system failure conditions.

Failure Detection Techniques

One unique technique, which can be implemented in the AHS vehicle level failure detection process, is to use the performance index of a specific AHS vehicle control function (via both model and signal processing approaches) as a continuous failure index variable. In addition, non-aggressive failure control strategy can be designed to work with such variable to modify some performance characteristics (e.g., to increase headway of such a vehicle when the performance index is low). Philosophically speaking, the basic control strategy of vehicle control in the AHS environment is to regard the vehicle system as a servo system. That is, to command the vehicle to perform some specific functions (e.g., lane following, headway regulation), and the vehicle accomplishes them. Therefore, anytime the vehicle does not perform as commanded, the possibility of some failure in the vehicle system (or impending failures) increases. By utilizing the communication capability of the AHS vehicles, a poll of the neighboring vehicles' normalized performance indexes can be gathered to further diagnose the possible failure in progress. Although this may not provide the exact location of a failure, it indicates the possibility of an impending failure and its nature (e.g., steering, braking) especially at an earlier stage.

Some other conventional failure detection/diagnosis techniques which can be used in the AHS environment are as follows:

- Strategically install sensing devices to directly observe the input/output of the targeted component.

- Applying process model, estimation technique, and decision method to monitor the non-measurable variables.

- Hardware or software self diagnosis can be incorporated in the design of a system or component.

- Duplicated (redundant) hardware items can be connected together to conduct comparison in order to determine the operating status.

The appropriate technique(s) should be chosen to detect the failures in the AHS vehicle environment. These failures consists of failures in the control units, sensing devices, communication links, interface elements, and actuation devices.

Failure Control Strategy

Once a failure is detected and identified in an AHS operation condition, failure control strategies then take place. There could be three different controls involved in an AHS failure control strategy. They are: single-vehicle failure control, coordinate failure control, and human assist/intervention failure control. They generally start in sequence but do not necessarily end in sequence. It is also not necessary for a failure control scenario to involve all three control phases. It depends on the nature of the failure and the corresponding fail-safe state. It is also worthwhile noticing that there may not be clear boundaries between those failure controls. It is merely a convenience of helping to discuss failure control strategies. The goal of these control strategies is to “lead” the AHS system (both the failed vehicle and the highway system) into a corresponding fail-safe state according to the particular failure on hand. Although it is always preferable to maintain the AHS system as close to its normal operational condition as possible, some functional degradation (e.g., reduce vehicle speed or increase vehicle spacing) is usually necessary to ensure certain system safety level. Even “fail-stop”, employed only when no other functional degradation states can prevent the system from unacceptable hazards, sometimes fails to guide the system into a fail-safe state when one or more inadvertent events occur. Nevertheless, the failure controller will still try to shut down the system in an orderly fashion with as little hazard as possible in a fail-hazard situation.

Emergency maneuvers often associate with failure controls, they can respond to road failures and other vehicle’s failures. However, there is a distinction between them. Failure control employ emergency maneuvers only when they are necessary. Some failures, if detected earlier, may not need emergency maneuvers at all. Failure controller decides which maneuver/action to take in what manner to achieve the minimum system performance impact with acceptable safety level in response to the detected failure. Whereas emergency control performs some predetermined actions when an emergency situation occurs.

Single-Vehicle Failure Control

Single-vehicle failure control is an individual vehicle failure control. It deals with vehicle’s own failure scenarios and does not involve any other vehicles. The control usually takes place right after a failure situation is detected (although there may not always be a clear distinction between detection and control). The purposes of such control are first to lead the failed vehicle into a fail-safe states and then to prepare for the coordinate failure control to become effective. There are two types of single-vehicle failure controls: transitional single-vehicle failure control and degraded single-vehicle failure control. They can be both applied for a single failure if applicable.

Transitional Single-Vehicle Failure Control

There are some types of failure which in general the AHS vehicles have the ability to control except during certain periods of failure (usually at the beginning of the failure). During such periods, the vehicle may become unstable or uncontrollable. Allowing it to happen, a fail-hazard situation may follow. Therefore, it is necessary for AHS fail-soft system to suppress these unstable or uncontrollable modes in the vehicle when those failures occur. Due to the instantaneous nature of such events, it may be advisable to install special sensors for such action.

A good example of the transitional single vehicle failure control is the tire burst controller. Tire burst is one of the common mechanical failures on the highway. Any fail-soft AHS vehicle control system needs to take care of this problem. It should be noted that the performance of run-flat tires is continually being improved and may be the best overall solution to the tire burst problem. However, it still represents one of the most easily understood examples of a transitional single-vehicle failure.

Since a burst tire would not provide more force than a good tire, it is a principle that automatic controlled normal vehicles should have the ability to control themselves in such a situation. Unfortunately, the unbalanced forces during the tire burst transient may result in an uncontrollable failed vehicle and create a hazard. In particular for the AHS scenario, the lane tracking ability may be lost even when there is no loss of total stability of the failed vehicle. Consequently, there is a need to develop some controlled maneuvers (possibly both open and closed loop controls) and the subsequent controlled speed reduction. Such a control mode falls into the category of transitional single-vehicle failure control.

Degraded Single-Vehicle Failure Control

There are other types of failure which may not involve safety critical components and do not have the immediate safe-hazard potential. For example, the loss of lateral acceleration sensor or lead vehicle velocity signals may not create an unsafe AHS immediately. However, appropriate actions have to be taken as soon as possible before the system degrades below safety level. Those immediate actions may consist of no increasing of speed, changing of controller’s gains (usually less aggressive), or switching to another control algorithm. Furthermore, it is usually preferable to perform those changes smoothly if possible. These actions are determined by the degraded single-vehicle failure controller, and the AHS performance may suffer degradation due to such actions. For example, larger jerk or larger spacing errors may be traded off with better safety. However, since the degraded single-vehicle failure control will eventually work with the coordinate failure control, such tradeoff would be continuously modified. In addition, the situation such as switching/gain-scheduling control algorithm after the tire burst controller accomplishes its task is also part of the function of degraded single-vehicle controller.

A typical single-vehicle failure control may involve the following actions:

- Failed vehicle prepares for emergency maneuvers and performs them if necessary.
- Failed vehicle broadcasts (if possible) about failure assessment.
- Failed vehicle performs transitional single-vehicle failure control when appropriate.
- Failed vehicle performs degraded single-vehicle failure control. The degraded single-vehicle failure controller can do self-adjustment based on the outcome from the coordinate failure control.
- Failed vehicle waits for instruction from roadside/central.

Coordinate Failure Control

The advantages of the AHS vehicle systems with respect to fail-soft capabilities is that the vehicle systems have additional sensing, computation and communication abilities, making the coordinate failure control possible. The key concept of “coordinate failure control” is to “isolate” the failed vehicle so that the rest of the system can be operated with safety (which also increases the safety of the failed vehicle since the possibility of a collision to other vehicle reduces). The basic maneuver is to direct the normal vehicles to yield to and to make room for the failed vehicle since the normal vehicles have more control ability than that of the failed vehicle. Upon detecting the existence of a failed vehicle(s) (through broadcasting from roadside or failed vehicle, or detecting by itself), the following actions may take place:

- Vehicles/platoons in the immediate area surrounding the failed vehicle prepare for emergency maneuvers and perform them if necessary.

- Roadside/platoon leader/surrounding vehicles identify the nature of the failure(s) through either broadcast information or detection schemes.

- Roadside/platoon leader/surrounding vehicles perform preventive maneuvers based on the identified nature of the failure. For example, no vehicle should be parallel to a failed vehicle with steering-related problem unless there is a safe barrier between them.

- Roadside/platoon leader suspends all non-essential and non-safe maneuvers based on the nature of the failure. The prohibited maneuvers may involve roadway entry and exit, platoon merging, separation, passing, and lane changes.

- Roadside/platoon leader starts platoon separation with respect to the failed vehicle to create safe spacing and safe speed. For example, the new leading platoon may increase speed slightly and the new trailing platoon has to reduce speed (even to a stop if necessary).

- Roadside/Traffic Central determines appropriate actions for vehicles away from the failed vehicle.

- Roadside/Traffic Central determines what other failure control action to be taken to resolve the failure problem. For example, to remove the failed vehicle from roadway, or to initiate a human assist failure control.

The coordinate failure control will continue function until the failure situation disappears.

Human Assist/Intervention Failure Control

Human intervention in an AHS environment is always controversial. However, let's take the automatic brake failure as an example. Let us assume that the automatic brake system failed to its manual system and the manual brake function is serviceable. Further let us assume that both the lateral control and engine control systems are functional. Under these situations, once a safe distance and a safe speed (for human driver, for example) are established, there is no reason not to let the driver assist the failure control system to "drive" the failed vehicle (actually only to monitor the brake function since there is high chance the brake will never be used) to the nearest exit or some buffer area. The alternative is to stop the traffic or to pull the vehicle away from highway (which may also involves shutting down, at least partially, the highway).

There are four key criteria to satisfied before human assist failure control can be granted:

- The appropriate manual system is serviceable.
- Safe operating environment is established for the human driver.
- Human driver acknowledge and acceptance of the manual failure control function.
- The AHS maintains the ability of monitoring the human assist vehicle.

A safe but degraded AHS operating mode can be established with human assist failure control when the four criteria are satisfied. A typical human assist failure control may involve the following steps:

- Failed vehicle reports the appropriate manual system is serviceable.
- Safe manual operating condition (appropriate spacing and velocity) is achieved through coordinate failure control system.
- Roadside signals failed vehicle/driver of manual assist function pending.
- Driver acknowledges of accepting manual assist control.
- Roadside renders particular assist function to the human driver.
- Roadside/failed vehicle monitors driver assist function.
- Failed vehicle leaves AHS roadway.

<u>Vehicle Fail-Soft Strategy Examples</u>

The following are examples of some components' fail-soft strategies based on automatic control functions. Note that failure of a sensor or actuator may imply the loss of the corresponding communication if it applies (i.e., when the controller (actuator) receives measurement (command, respectively) from the communication link either roadside to vehicle or vehicle to vehicle). They are by no means inclusive.

Lateral Control Function

- Automatic Steering Actuator: safety-critical component; no fail-safe state; difficult to perform human assist function; need very reliable or redundant component.

- Lateral Deviation Sensor – Safety-critical component; may not have fail-safe state; need to investigate the possibility of developing a transitional single-vehicle failure control by employing other sensors and neighboring vehicle information to perform fail-stop function; redundant sensor is a good idea; standard coordinate failure control may be applied; emergency control is a possibility; limited human assist may be feasible for certain situations (yet it still need transitional failure control).

- Yaw Rate, Lateral Acceleration Sensors – Non safety-critical components; has fail-safe state; need to design degraded single-vehicle failure controller; standard coordinate failure control; no need for human assist failure control.

- Steering Angle – Non safety-critical component; has fail-safe state; may need to design transitional single-vehicle failure control (depends on the nature of control strategy employed); need to design degraded single-vehicle failure controller; standard coordinate failure control; no need for human assist failure control.

- Tire – Non safety-critical components (low tire pressure or tire burst); need both transitional and degraded single-vehicle failure controls; standard coordinate failure control; no need for human assist failure control.

- Control Unit – Safety-critical component; no fail-safe state; no single-vehicle failure control ability; standard coordinate failure control may apply; need very reliable or redundant component; human assist function may be applicable in some very limited situation.

Longitudinal Control Function

- Automatic Throttle Actuator – Non safety-critical component; has fail-safe state (fail-safe equals to fail-stop when there is no human intervention); standard coordinate failure control; human assist failure control has great help.

- Automatic Brake Actuator – Non safety-critical component; has fail-safe state; no ability for emergency stop function (except for human intervention); standard coordinate failure control; human assist failure control has great help.

- Throttle Angle, Engine Speed, Brake Pressure Sensors – Non safety-critical component; has fail-safe state; may need to design transitional single-vehicle failure control (depends on the nature of control strategy employed); need to design degraded single-vehicle failure controller; standard coordinate failure control; no need for human assist failure control.

- Range/Range Rate Sensor – Non safety-critical component; has fail-safe state (fail-safe equals to fail-stop when there is no human intervention); may need transitional single-vehicle failure control; need degraded single-vehicle failure control; standard coordinate failure control; human assist failure control will help.

- Longitudinal Velocity and Acceleration Sensors – Non safety-critical components; has fail-safe state; need to design degraded single-vehicle failure controller; standard coordinate failure control; no need for human assist failure control.

- Lead Vehicles' Information – Non safety-critical component; has fail-safe; may need transitional single-vehicle failure control; need degraded single-vehicle failure control; standard coordinate failure control; no need for human assist failure control.

- Control Unit – Safety-critical component; no fail-safe state; no single-vehicle failure control ability; standard coordinate failure control may apply; need very reliable or redundant component; human assist function may be applicable in some situation.

Task 5. Retrofit Analysis

Introduction

AHS will be faced with retrofit issues soon after AHS vehicles are deployed. These issues are retrofitting existing AHS vehicles with updated equipment and retrofitting non-AHS vehicles with AHS equipment. Aftermarket suppliers of AHS equipment need to be technically knowledgeable about AHS vehicles and aware of AHS regulations and standards.

Retrofitting Existing AHS Vehicles

When AHS vehicles are first deployed into the marketplace customer feedback will heavily influence changes and modifications to the vehicles and their subsystems. Vehicle manufactures and aftermarket suppliers will need to coordinate various aspects of product development such as product electrical interface and specifications, mechanical packaging and mounting, and environmental requirements such as temperature, shock, and vibration.

Electronic Product Integration

When a new product such as a controller is developed to replace an older controller, the new version will have added inputs and outputs for greater capability. For example, an updated controller could have the ability to drive twice as many actuators as the older controller. Added functionality requires that additional wiring be installed. This in turn requires a new or modified wire harness and wire connector(s). The product integration activity must consider, in the development phase, all of the potential implications and impacts that an updated piece of equipment has on the vehicle system. Problems such as data bus contention, radiated emissions, and overdriven circuits must be avoided.

Mechanical Packaging Of Electrical Components

Sometimes products are redesigned in order to take up less space, weigh less, or to be more rugged. One of the most significant problems that currently affects the vehicle owner is car theft.[12] Typically cities such as New York and Los Angeles are thought of as major hot spots for theft, but cars are disappearing from the streets of Berlin, Paris, and London at alarming rates. Some insurance companies in Europe have dropped their coverage to 90 percent of the vehicles worth unless it is equipped with an anti-theft device. But these systems create difficulties for audio suppliers because anti-theft electronics takes up space previously allotted for music systems. Now the space must be shared with other systems such as air bags, antilock brakes, and the steel beams installed for safety.

Integration of several controllers into one will save money, increase reliability, and conserve space. Conserving space will be heavily emphasized by vehicle makers in the future. In order to fit all of the necessary electronics into the envelope of the vehicle, new and innovative packaging solutions will be sought out by the vehicle makers and by after market suppliers, in order to insure a place for their products. The marketing and sales division of Bose Corporation feel that they need to make their products smaller and more packageable. It may mean partitioning their audio systems differently and placing the radio electronics in the trunk.

Environmental

The automotive controller is subject to a wide range of temperatures, vibration, and shock. Mounting this component in the passenger compartment of a vehicle has cramped the available space in that area. As a result, engine controllers, transmission controllers, and antilock brake controllers have been developed for under-hood mounting. These controllers are mounted in the engine compartment where they must stand up to a much harsher environment than if they were mounted in the passenger compartment. The development of such equipment changes the manufacturing approach to product development.

Retrofitting Non-AHS Vehicles

Adding AHS equipment to non-AHS vehicles without any prior design for retrofit could prove to be quite difficult. If the vehicle is provided with space to accept AHS equipment the retrofit process would be more feasible. In manufacturing vehicles with the intent that some day they will be retrofitted with AHS equipment, the manufactures will need to consider the proper hooks (provisions) for the equipment.

A current example of retrofitting vehicles without any prior design support from vehicle manufacturers is the aftermarket addition of hand controls for disabled drivers. Suppliers are challenged with installing their equipment into vehicles that are not set up in advance to accept this retrofit. As a result these aftermarket suppliers must acquire vehicles and design the controls around the geometry and space constraints of the vehicle driver's compartment with very little dialogue with the vehicle manufacturer.[13] These designs are work-around and are not optimized. Some companies have experienced law suits as a result of accidents caused by failure of this equipment.

Space Requirements For Hardware

To develop a non-AHS vehicle for AHS retrofit in the future the vehicle manufacture will consider space requests for actuators, controllers, wire harnesses, hydraulic lines and hoses, and a variety of other hardware. The vehicle manufacturer could make the future AHS retrofit installation easier if space is allotted for such hardware as controllers in order to insure their presence when needed. Real estate inside of the vehicle will be a premium. If there is no space left in the passenger compartment, the trunk or engine compartment become the next alternative areas. Wiring harnesses should have spare leads for future addition of AHS controllers, sensors, data lines, power lines, and various controlled and discrete outputs.

Systems And Software Considerations

In the design of a vehicle's electrical architecture often there are provisions put in to allow for growth. Control modules are designed with more capability than they need for their application at the time, anticipating future growth and added functionality in the future. Software is often written to contain the necessary hooks for future needs. For example, software could be written to command an actuator that may be installed in the vehicle in the future. This software hook or provision could be disabled until it was needed.

Conclusion

Retrofitting existing AHS vehicles with updated equipment is concluded to be possible. Modular component design could allow straightforward replacement with next generation equipment. Some retrofits could be as simple as replacement of existing microprocessor program memory chips with replacements incorporating additional functionality. Some upgrades however may require additional wiring. Such retrofits would be much easier if early designs incorporate spare capacity for anticipated input/output and wiring requirements. For best integration of systems into the vehicle all power and interface requirements should be addressed at the time of initial vehicle design. This requires that interface specifications and standards for stages of an evolving AHS be fully determined long before the specific hardware and software is produced for a given stage. The concept of a multiplexed data bus is one solution which may support increased input/output capacity without compromising the reliability of interconnects.

The retrofitting of AHS capability to non-AHS vehicles is concluded to be very difficult unless the vehicle is built as an “AHS-ready” vehicle. An “AHS-ready” vehicle should include at a minimum all required actuation capability and have sufficient space available to install AHS-specific vehicle equipment. Wiring, power, sensors, and mounting provision can likely be retrofitted, but would also be a desirable feature for an “AHS-ready” vehicle. The inclusion of all actuators may not be a severe requirement considering the present trends towards throttle-by-wire, brake-by-wire, and steer-by-wire.

Task 6. AHS Vehicle Technologies Applied To Non-AHS Roadways

The AHS is the most technology-intensive component of ITS. The likelihood of AHS deployment success may be greatly increased if the component technologies could be deployed gradually and ahead of actual AHS deployment to provide valuable and self-sustained pre-AHS user services. Since not all roadways will be instrumented to support automated driving, the likelihood of success may also be improved if the component technologies can also provide valuable user services on non-AHS roadways.

Several of the capabilities provided by the AHS technologies, especially the communications systems, may be compatible with operation on non-AHS or pre-AHS roadways. It is expected that certain key building blocks of the AHS system will become available to the general driving population as part of the evolution of ITS, allowing a transition to full AHS functionality over a period of time. This will permit user familiarity and acceptance of AHS functions to occur in a gradual manner as increasing levels of technology are introduced into the vehicle.

This task identifies possible pre-AHS or non-AHS user services that can be provided by using equipment installed on an automation-equipped vehicle designed for use on an AHS. The user service perspective in the ITS program is taken in identifying pre-AHS or non-AHS applications of AHS technologies. The identified user services are put in two general categories, driving-facilitating user services and non-driving user services. AHS technologies can facilitate the provision of many of the 28 user services (in six general areas) that the US ITS Architecture is required to support.[14] To distinguish these services from others, they will be referred to in the text with initials capitalized, e.g. the user service of Safety Readiness in the general area of Advanced Vehicle Safety Systems.

This task will concentrate on the services provided to the users of the automation-equipped vehicles and will not address how automation-equipped vehicles may help achieve the goals of traffic management, including incident management, travel demand control, and traffic control. For example, an automation-equipped automobile can serve as a probe vehicle, collecting important traffic information. Although such a service to traffic management centers could be provided in exchange for free traffic information from the traffic management center, the analysis will concentrate on the perspectives of vehicle owners and fleet operators.

AHS technologies include vehicle technologies (including sensing, vehicle-roadside communication, vehicle-to-vehicle communication, computerized decision-making for vehicle control, and actuation), roadway support, and roadside intelligence. Sensing and computerized decision making can provide warnings to the driver on non-AHS roadways. Together with the actuators, they can enable partially automated normal driving and emergency maneuvering for collision avoidance (beyond warnings). The communication equipment can provide a means to access data as well as provide information for various driving and non-driving purposes.

Driving Services

Continuous Vehicle Condition Monitoring

Automated vehicles, including automobiles, transit vehicles and commercial vehicles, are likely to possess the capability of continuous self-monitoring. Exact contents of the capability depends on the actual deployed technologies. Possible features include the abilities of the vehicles to detect imminent vehicle failures and suggest safe driver reactions. Such imminent failures include tire burst, brake failure and many other possible failures. This service is a major component of the user service of “Safety Readiness” under the general area of “Advanced Vehicle Safety Systems”. In the general area of Commercial Vehicle Operations, it is the user service of On-Board Safety Monitoring.

Vehicle Position Location

Automatic Vehicle Location (AVL) and Automatic Vehicle Identification (AVI) systems are currently being implemented for such applications as tracking commercial vehicle fleets, locating stolen vehicles, or in-transit fee collection. Position location systems similar to those possible on an automated highway may also be integrated with map-matching functions to assist drivers in navigation and route planning. The instrumentation required to perform vehicle position location can be independent of the roadway in a vehicle-centered technology such as GPS. The tag-beacon approach relies on beacons installed at regular intervals along the highway.

Driver Monitoring

An important AHS design issue is how to ensure the safety of resumption of manual vehicle control after a long period of automated driving. Driver monitoring functions can be used to verify, at least partially, the readiness and fitness of the driver for manual driving. Note that this function applies to all drivers, including those of commercial vehicles. This help achieve the ultimate goals of the user service of Automated Roadside Safety Inspection in the general area of Commercial Vehicle Operations.

Roadway Condition Monitoring

For those AHS operating scenarios where the vehicles themselves are responsible for the identification of roadway driving conditions, the vehicles’ roadway condition monitoring capability can be used on non-AHS roadways.

Headway Maintenance

The applicability of longitudinal control technology to non-AHS roadways depends on the implementation selected. Vehicle spacing can be maintained using a variety of radar techniques to provide inputs to the control loop, or by means of radio communication between vehicles. Adaptive Cruise Control (ACC) based on vehicle-centered sensing may be widely available prior to full AHS deployment and is a good candidate for parallel use on non-AHS highways.

Lane Keeping

Lateral control of the vehicle can be accomplished using vehicle-centered techniques, such as video imaging and radar, or infrastructure intensive approaches, including magnetic markers, buried wire, and tag-beacon communications. Video imaging is the most compatible system for use on non-AHS roadways since the lane lines are the primary source for lane sensing. The performance of video imaging in adverse weather and lighting conditions may restrict its use on non-AHS highways where a secondary lateral control methodology is not available. Radar technology deploys the ranging element in the vehicle, but may require a physical barrier at the lane boundaries with lane demarcation configurations compatible with electromagnetic sensing. Both magnetic markers and buried wire are infrastructure intensive, and will be limited to use on instrumented sections only. The tag-beacon technology relies on infrastructure electronics, and can be exploited only on highways which are instrumented.

Obstacle Detection

The technology of blind spot obstacle detection exists and is currently deployed on school buses and some trucks to prevent accidents. This technology is a good candidate for widespread use prior to introduction of fully automated lanes. The instrumentation required is vehicle-based and can be exploited on surface streets as well as non-AHS highways. An advantage to evolutionary introduction of AHS-related capabilities is the ability to familiarize the user with automated tools in a gradual process. Obstacle detection is a good candidate for this role due to its early availability and low complexity of the user interface.

Collision Avoidance: Longitudinal, Lateral, And Merging

Collision avoidance is likely a crucial capability of any automation-equipped vehicle, including automobiles, transit vehicles, and commercial vehicles. There exist three major groups of possible collision avoidance capabilities: longitudinal, lateral, and merging. Longitudinal and lateral collision avoidance are two separate user services in the general area of “Advanced Vehicle Safety Systems”. A major difference between the two user services and the collision avoidance capability of an automation-equipped vehicle is that the former provides only warnings while the latter could also provide vehicle control for emergency maneuvering. A merging collision avoidance system warns the driver of the danger at a traffic merging location and/or reacts automatically to avoid any collision at the merging location. This could be treated as lateral collision avoidance. Since AHS is assumed to operate only on freeway-type roadways and there are no intersections on freeways, the user service of “Intersection Collision Avoidance” in the general area of “Advanced Vehicle Safety Systems” may not be supported by automation-equipped vehicles.

Vision Enhancement For Crash Avoidance

If the automation technologies include some form of vision-based or image-processing technologies, then the user service of "Vision Enhancement for Crash Avoidance" can be provided readily for non-AHS roadways.

Pre-Crash Restraint Deployment

Since a key feature of any automated highway system is short average spacing, pre-crash tensioning of restraint systems such as seat belts can increase safety as well as perceived safety of AHS. This could be a required feature of any automation-equipped automobile, in which case it can provide the user service of Pre-Crash Restraint Deployment in the general area of Advanced Vehicle Safety Systems. Present air bag restraint systems require precise timing which only begins after a crash is occurring so thus are not candidates for pre-crash deployment. See Activity G – Comparable Systems Analysis for a discussion of automobile air bag systems.

Emergency Notification And Personal Security

The communication capability of the automated vehicles allows the vehicle users to initiate distress signals for incidents like mechanical breakdown, car-jacking, etc. The sensors on board automated vehicles can sense the occurrence of a collision and automatically send information about the location and severity measure to emergency personnel. These two capabilities form the user service of "Emergency Notification and Personal Security" in the general area of Emergency management.

Electronic Payment

Individual automated vehicles would have to identify themselves to the automated highway systems and perhaps nearby vehicles through communication for various reasons, e.g. checking if vehicle is equipped for automated driving, checking vehicle inspection and maintenance record, routing, maneuver negotiation etc. This capability can easily accommodate the user service of Electronic Payment.

On-Route Driver Information

With the communication capability of an automation-equipped vehicle, driver advisories, which are similar to pre-trip planning information, convey traffic conditions and other related information.

Route Guidance

Through the communication devices on the automation-equipped vehicles, the user can request route guidance. The guidance can be based on dynamic traffic condition reflecting real-time information about the transportation system. Directions can consist of simple instructions on turns or on upcoming maneuvers. This is the user service of Route Guidance in the general area of Travel and Traffic Management.

Other Services

In addition to the driving services, the US ITS Architecture provides additional services which are not related to AHS functionality. They may be grouped into non-driving and commercial vehicle services. The non-driving services are:

- Vehicle self-diagnostics.
- Accessing pre-trip travel information.
- Communication medium for ride matching and reservation.
- Accessing en-route transit information.
- Facilitating public transportation management.
- Facilitating personalized public transit.
- Enhancing public travel security.

The commercial vehicle services are:

- Facilitating commercial vehicle electronic clearance.
- Facilitating commercial vehicle administration process.
- Facilitating commercial fleet management.
- Enabling hazard materials and incident notification.

CONCLUSIONS

Vehicle operational issues were identified and discussed as they relate to the development, operation, and deployment of AHS vehicles. The issues concerning the development of AHS vehicle functionality include the state of existing vehicle instrumentation, impending equipment developments, degree of integration of components, subsystem reliability, impact to vehicle cost, and production considerations. The factors associated with the successful operation of AHS-equipped vehicles include the compatibility with non-AHS roadways, manual control options for emergency maneuvers, fault tolerance, fail-safety, and maintainability. Deployment aspects regarding AHS vehicles include the ability to retrofit non-AHS vehicles with AHS instrumentation, compatibility of early AHS equipment with future upgrades, maintaining optimum capability as technology advances, and consumer acceptance of automated vehicle features.

AHS will be reliant on dependable communications between vehicles and between the infrastructure and vehicles. A high degree of research and development must be dedicated to RF communications and it's role in AHS vehicles. Interference, power consumption, transmitting power limits, FCC regulations, RF congestion, frequency allocation, and communication protocol are some areas that should be researched.

Automotive electronics shows the same trends as those for home electronics and PC equipment. The cost of specific capabilities decrease as vehicle companies demand cost reductions from their suppliers. However, at the same time, additional vehicle functions and features are controlled by electronics and the level of functionality of existing features is expanded. Thus, the total cost of electronic content continues to rise.

AHS-specific items on vehicles will likely be more expensive because the initial quantity produced will be small. Furthermore, AHS electronics will need to incorporate more sophisticated components capable of operating at faster speeds than what is normally needed on non-AHS vehicles. In the past, new electronic technology has not driven the automotive electronics market, but Federal mandates may, and profit always motivates the market. Automotive manufactures will not install more expensive or sophisticated electronics in their products unless they have to or have financial incentive to. Therefore, the general trend of cheaper electronics in the future may not affect AHS, especially in the beginning phase.

The software development and systems development efforts will be substantially more complex than for present systems. In order to make the AHS vehicle affordable to the public, automotive manufacturers and or the infrastructure stakeholders must be willing to spend funding to initially deploy AHS. In general, the type of electronics equipment required for AHS is highly reliable, tending to operate flawlessly for years, but typically fails without the warnings associated with degraded performance common to traditional vehicle subsystems such as engines or brakes. It is recommended that AHS-specific subsystems include built-in-test capability to predict impending failure and prevent sudden loss of functionality. Safety-critical subsystems may require multiple redundancy or back-up systems to ensure error free operation.

The most cost effective approach to ensuring reliable system operation is to increase the MTBF of subsystem elements. System MTBF is a function of the total number of components. High levels of integration reduce the overall complexity, minimizing interconnects and eliminating sources of error in manufacturing and assemble and reducing potential points of failure. The current trend in vehicle engine controllers toward integrating functionality may establish the best approach for achieving highly reliable AHS equipment.

Unit self-test capability is recommended to enhance efficient diagnostics of AHS-specific equipment. The installation of vehicle equipment will also affect the maintainability of the equipment. Modular design of electronics equipment is one method of minimizing mean-time-to-repair. This approach allows repair of failed units at the factory, while malfunctioning units are merely unplugged and replaced at service stations. This may provide economies of scale required to reduce maintenance costs of complex subsystems, reducing the need for trained technicians to the factory level only.

System engineering methodologies and concurrent design processes are recommended to ensure AHS quality and reliability, and subsequent safe performance. Robust Engineering practices have been implemented within the automobile industry and are well suited for AHS development programs. Structured engineering methodologies will provide assurance that reliability, durability, and quality requirements are coordinated closely. The level of complexity of the AHS will require a high degree of attention to this aspect of design, development, and manufacturing throughout the system life cycle.

The fail-soft analysis determined that the lateral position control and longitudinal position control functions are critical to safe operation. Several safety critical aspects of the lateral control function are lacking fail-safe states, including the steering actuator, deviation sensor, and processing unit. The longitudinal processing unit also lacks a fail-safe operating state. Failures in this type of component will cause immediate interruption of a safety-critical function. Extremely reliable components or redundant elements are required in these instances to prevent failures. An alternate solution is to introduce the driver as a back-up source of control, however this solution has serious safety considerations, especially in close vehicle following modes.

The retrofit analysis concludes that retrofitting existing AHS vehicles with updated equipment is possible. Modular component design could allow straightforward replacement with next generation equipment. Some retrofits could be as simple as replacement of existing microprocessor program memory chips with replacements incorporating additional functionality. Some upgrades however may require additional wiring. Such retrofits would be much easier if early designs incorporate spare capacity for anticipated input/output and wiring requirements. For best integration of systems into the vehicle all power and interface requirements should be addressed at the time of initial vehicle design. This requires that interface specifications and standards for stages of an evolving AHS be fully determined long before the specific hardware and software is produced for a given stage. The concept of a multiplexed data bus is one solution which may support increased input/output capacity without compromising the reliability of interconnects.

The retrofitting of AHS capability to non-AHS vehicles is concluded to be very difficult unless the vehicle is built as an “AHS-ready” vehicle. An “AHS-ready” vehicle should include at a minimum all required actuation capability and have sufficient space available to install AHS-specific vehicle equipment. Wiring, power, sensors, and mounting provision can likely be retrofitted, but would also be a desirable feature for an “AHS-ready” vehicle. The inclusion of all actuators may not be a severe requirement considering the present trends towards throttle-by-wire, brake-by-wire, and steer-by-wire.

The analysis of the application of AHS technologies to non-AHS roadways concluded that several capabilities may be available and that this is one of the benefits of an evolutionary deployment. Transition to full AHS functionality over a period of time will permit user familiarity and acceptance of AHS functions as increasing levels of technology are introduced into the vehicle. Pre-AHS functions which are compatible with evolutionary deployment as well as operation on non-AHS roadways include automated headway maintenance and obstacle detection. Control of vehicle spacing using radar sensor inputs is referred to as adaptive cruise control and is a good candidate for use on non-AHS highways. The instrumentation required to implement obstacle detection is vehicle-based and can be exploited on arterials as well as non-AHS highways since no infrastructure modification is required.

The U.S. ITS Architecture provides many additional services such as traffic flow management, travel planning, enhancements to vehicle navigation, and vehicle identification for commercial vehicle operations which are not directly related to AHS functionality.

REFERENCES

1. Cambridge Systematics, Inc., Incident Management, October, 1990.

2. D. J. Holt, “Editorial - Electronics”, Automotive Engineering, September, 1994.

3. General Motors, Public Interest Report, 1994.

4. S. E. Underwood, Delphi Forecast and Analysis of Intelligent Vehicle-Highway Systems Through 1991, University of Michigan, July, 1992.

5. S. S. James, “The Allison HD Transmission,” SAE Technical Paper 932998, 1993.

6. J. Keebler, “TRW’s Electric Power Steering Ready For The Road,” Automotive News, March 14, 1994.

7. Autofacts, “World Airbag Market,” As reported in The Hansen Report on Automotive Electronics, March, 1994.

8. D. Ferris, “No Company Has A Lock On ABS, Traction Control”, Wards Auto World, May, 1994.

9. W. M. Spurgeon, “System Engineering and Quality,” Automotive Engineering, June, 1994.

10. Defense Systems Management College, Systems Engineering Management Guide.

11. D. C. Smith and J. Lowell, “Robust Engineering”, Wards Auto World, March, 1994.

12. M. Sorge, “Have it your way in tomorrow’s cars”, WARD’S Auto World, June, 1994.

13. P. Hillcoff, Automobility Manufacturing Corporation, Telephone conversation, August 10, 1994.

14. U.S. Department of Transportation and ITS America, “ITS Architecture Development Program - Phase 1 Summary Report,” November, 1994.

BIBLIOGRAPHY

ENTERPRISE Program The, Evaluating New Technologies for Roads Program Initiatives in Safety and Efficiency, Castle Rock Consultants, October, 1990.

Johnson, B. W., Design and Analysis of Fault Tolerant Digital Systems, Addison Wesley, Reading, Massachusetts, 1989.

Pradhan, D. K., Fault Tolerant Computing, Prentice Hall, Englewood Cliffs, New Jersey, 1986.

Stockner A. R., M. A. Flinn, and F. A. Camplin, "Development of the HEUI Fuel System-Integration of Design, Simulation, Test, and Manufacturing", SAE Technical Paper 930271, 1993.