Engineering Design Concept for Intelligent Vehicle-Highway System Safety

WEI-BIN ZHANG

The development of an intelligent vehicle-highway system (IVHS) will require methodologies for predicting and controlling system safety. An introductory examination of safety-related issues for IVHS design is presented. Safety problems that may be encountered with the application of IVHS technologies are assessed, and methodologies for safety analysis, system specification, and hazard reduction are examined.

The goals of the intelligent vehicle-highway system (IVHS) and IVHS devices are to improve highway capacity and safety. These two goals are closely interrelated, because an unsafe system or devices would not only cause significant safety problems (liability, societal, or politically oriented) but also dramatically reduce the capacity of the system. Therefore, there is a need for safety studies on the overall suggested IVHS to determine (a) the potential level of safety of the IVHS or IVHS devices and (b) how to accomplish this level of performance.

As explained by Hitchcock in a paper in this Record, studies have been conducted to investigate the safety benefits of the IVHS and IVHS devices by analyzing the frequency and consequences of accidents on the existing highway system and by comparing these incidents with the predictions applied to the IVHS and IVHS devices. The aim of these studies, which support IVHS goals, is to estimate the extent to which the suitably applied advanced technologies will eliminate or reduce human errors in the decision-making and maneuvering process, thereby reducing the occurrence of accidents. These studies are based on assumptions that the system or devices would satisfy predefined safety requirements. IVHS policy makers have described these safety requirements as the prevention of new safety hazards (*1*). A hazard is defined as a condition in which an accident may occur and no action by the control system can prevent it.

To reduce current safety hazards and to eliminate possible new ones, IVHS researchers must conduct an intensive hazard analysis, in which all possible hazards are identified and evaluated. Hazard analysis is the heart of the system safety efforts and can be conducted at multiple levels (or stages), as follows:

- At the system analysis level, major safety hazards are addressed by using preliminary hazard analysis (PHA) and fault tree analysis (FTA). Through these analyses the system configuration can be assessed, and the requirement specifications of the system can be initially defined. The hazards identified are subject to further evaluation and perhaps control in the follow-up studies.
- At the subsystem design level, the preliminary design of components that will perform a specified function of the system is conducted. Detail system hazards are investigated. The cause-consequence sequence of failures and hazard properties is analyzed.

The analyses at the different levels interact in a close-loop form. After a specific safety hazard is identified, hazard reduction analysis must be conducted, including an investigation of the countermeasures for eliminating (or reducing) the hazard in the subsystem design level and improvements (or modifications) to the system configuration and requirement specification in the system analysis level.

The objective of the following paragraphs is to address issues that should be considered in the system safety design. The cause-consequence relationship of system failures is investigated, and the various methodologies for reducing system failures and providing fail-safe features are assessed.

IVHS

An IVHS can be defined as a system that involves the application of sensing, information, communication, and control technologies to observe, guide, and control the movement of vehicles in a traffic system (or to assist in the performance of those functions) (*2*) on existing roadway infrastructures. According to the subfunctions of the system, an IVHS can be grouped into the following four functional subsystems:

1. Advanced traffic management system,
2. Advanced traveler information system,
3. Advanced vehicle control system, and
4. Commercial vehicle operations system.

Structurally, an IVHS possesses component subsystems. Disregarding specific functions, the component subsystems may consist of the following:

- A vehicle system, which may contain communication components, information acquisition or sensing components, information display or warning component, control compo-

Program on Advanced Technology for the Highway, Institute of Transportation Studies, University of California (Berkeley), 1301 South 46th Street, Building 452, Richmond, Calif. 94804.

nent, actuating component, existing vehicle mechanisms, and human-machine interface;

- A roadway or roadside system, which may contain information components, communication components, vehicle presence detection components, and local traffic management components; and
- A central control system, which may contain communication components, network traffic management components, and human-machine interface.

The component subsystems usually interact. Each component subsystem may serve as several functional subsystems, and a group of component subsystems can constitute a functional subsystem. By either classification (functional or constitutional), and IVHS would be hybrid in the sense that the entity contains more than one functional or component subsystem. Figure 1 shows the IVHS component subsystems and their interactions.

There will also be IVHS devices that represent one or more entire or partial component subsystems and perform a single function of an IVHS functional subsystem. IVHS devices will be applied individually before a fully automated IVHS or IVHS subsystem is developed.

DEFINITIONS

In defining IVHS safety, the terms *hazard* and *risk* are used. A hazard in the highway traffic system implies a potential for introducing accidents, which may take the form of a vehicle collision or other undesired events resulting in damage to life or property. Risk is associated with the likelihood or possibility of harm. It is related to the probability that the frequency, intensity, and duration of the stimulus will be sufficient to transfer the hazard from a potential state to a loss (*3*).

According to a generic interpretation, safety can mean hazard free or no risk, as come dictionaries define the term. However, few systems can actually perform at a hazard-free level. Technically, safety can be described using an inverse function of risk (*4*). Hence, a low-risk system will have high safety. In many safety analyses, the degree of safety is measured by using statistics of accidents. Indeed, hazard should be a main factor measured in evaluating safety because it creates the possibility for an accident.

Safety of an IVHS primarily relies on preventing collisions between vehicles because people are the direct users, and because vehicles are actuating components in the system. A vehicle that possesses inherent failures may represent a hazard. It is possible to envisage an accident in which a vehicle collides with a neighboring vehicle or in which an unsafe condition exists that endangers the driver and passengers or others in the vicinity of the vehicle. The unsafe condition refers to the possibility of loss of life or property damage, or both. Therefore, safety of an IVHS or IVHS devices involves ensuring that the vehicles will operate within the designed environments without resulting in an unacceptable risk. Unacceptable risk means that both the frequency and magnitude of the hazards are not publicly (societally or economically) acceptable. There is an arbitrary division between acceptable and unacceptable known as the safety criterion (sometimes defined as safety factor or safety margin). The establishment of a safety criterion for engineering safety has been intensively assessed in risk analysis techniques. The safety criterion can be defined for an IVHS by fatality or property damage and by the influence of the accident on the efficiency of the overall highway system.

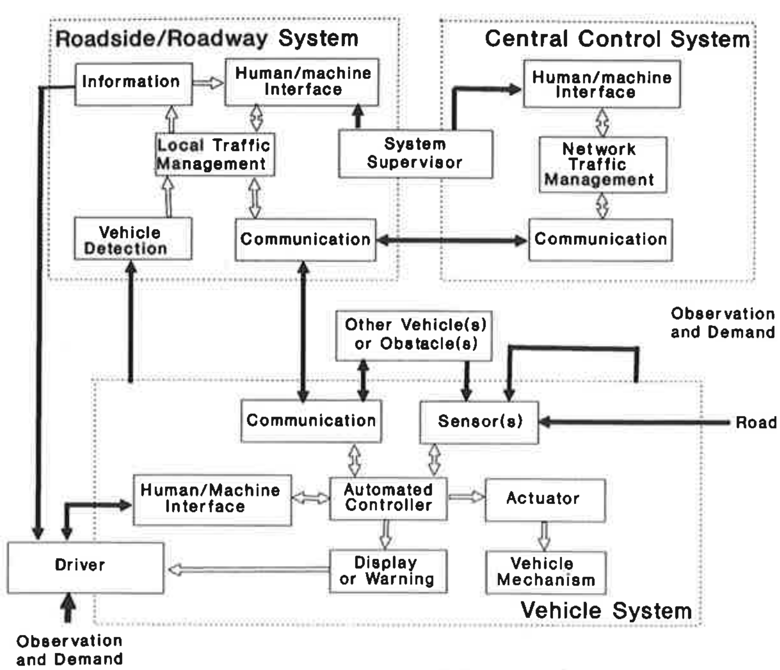

FIGURE 1 IVHS component subsystems.

SAFETY FOR TODAY'S DRIVER-VEHICLE-ROAD SYSTEM

Because it is likely that the IVHS would operate on the existing road infrastructure and in a similar physical environment, it is useful to review the safety problems of the existing highway system.

Drivers, vehicles, and the road have already constituted a system called the driver-vehicle-road (DVR) system. However, whether or not the DVR system is a controllable system is debatable. In the existing DVR system, the driver is the key control component (or subsystem), and the remainder of the system—the vehicle and the road—are, in their present forms, relatively simple components. With regard to the traffic management of the DVR system, the system is sometimes considered as being under control. However, the control functions are effective only at limited locations and only if the drivers obey the traffic regulations and management instructions.

The driver possesses multifunctional sensing and adaptive capabilities; however, these abilities can be restricted by some environmental and human factors. Human sensing abilities are affected by weather or road conditions. In addition, such human factors as alertness, fatigue, and motivation can significantly influence the sensing and decision-making process in vehicle control and may cause operation errors. A driver may be willing to disregard traffic regulations or instructions and may operate the vehicle accordingly. Statistics indicate that driver errors contribute to over 75 percent of all accidents (*5*). Hence, the driver is not considered a controllable operator. Further, it can be concluded that the current DVR system cannot be regarded as a system that is under control in an engineering sense (*6*).

There have been many efforts made toward enhancing safety features for the DVR system, including efforts to design safer cars and improvements to roads and traffic management systems. Clearly, each of these efforts can have, at most, a finite effect, and most of the benefits have already been enjoyed. Improved vehicle and road designs in particular have had positive effects on improving driver performance and reducing human errors; however, these improvements can only lead to limited enhancements against human factor contributions. More advanced traffic management systems may also enhance safety to a limited extent. Hence, substantial efforts have been conducted to provide a means of protection against accidents. The technologies developed for pursuit of this protection are called life-saving (L–S) technologies and largely consist of crush or impact protection designs (*7*). As a result of applying L–S technologies, the structure of the vehicle has been designed to absorb the greatest portion of the energy from most front or rear collisions. Energy-absorbing materials have also been applied for side-impact or roof-crush protection. Safety devices have been developed, including the safety seat belt, supplemental inflatable restraints or air bags, and a self-aligning steering wheel. All of these protective designs have been effective to various extents.

IVHS SAFETY PROBLEMS

IVHS technologies are expected to enhance the safety of the traffic system and to improve the overall system capacity in a number of ways (*8*). By definition, this system should be able to eliminate or reduce human operating error by employing automatic vehicle control systems or hazard warning devices. However, because the IVHS or IVHS devices will be applied on the existing infrastructure, the system or devices must be able to withstand the physical environments that the existing DVR system encounters. Furthermore, the system will also have to confront the operational environments that are developed through the application of the IVHS or IVHS devices, as well as additional influence by human factors.

Safety hazards are considered to be dominated by system failures. Failures may create errors in the operation, and hence, a safety hazard may be introduced. A system failure can be generated by failed components, physical disturbances from the environment, operating errors, errors in the design, or production variations. These sources of system failures should all be considered in the system safety analysis and design. The factors that are considered as stimulus of system failures include component failures, physical disturbances, new operating environments, design errors, and human interference.

Component Failures

As one of the common sources of system failures, component failures may become a dominant factor influencing the safety of the IVHS. Because of the introduction of new components, the system failure rate could be higher than that in the existing DVR system. The electronic, mechanical, and hydraulic components that are introduced in the IVHS must suffer a wide range of environmental conditions. Many of these environmental factors can contribute to component failures, which, in turn, may cause degradation of the functions of the system. The environmental factors may include temperature, humidity, rain, shock, vibration, and so on.

Physical Disturbances

Environmental factors, such as wind (which can create significant external force) and snow (which changes the vehicle-road interaction), will also generate difficulties in the operation of the system.

New Operating Environments

An IVHS or a system with IVHS devices may function in different operational environments than the existing DVR system. For instance, the new system may be designed in such a way to allow the vehicles to operate closer together both laterally and longitudinally, thus improving the capacity of the system. However, if an error that is mainly caused by system failure occurs, and if this error is larger than the designed system tolerance, a hazard will occur. Because the system tolerance of an IVHS would be different from that of the existing DVR system, the specification of hazards suitable for various forms will be different. A similar example can be demonstrated in a system equipped with IVHS devices. If a vehicle has been equipped with a collision warning device, for instance, it is likely that a driver's driving style will change after the driver becomes familiar with the device. By relying on the device, the driver then becomes more aggressive or pays less attention to upcoming objects. If the warning range of the device is set for effective usage on the highway, and if the system then fails to alert the driver in a situation in which a warning should be given, the chance of collision will be greater in an equipped vehicle than in an unequipped vehicle when both are under the same conditions.

Design Errors

Preventing specification or design errors is an important issue in the system design. Many examples have demonstrated, unfortunately, that safety hazards were created by specification or design errors. Design errors often cause safety hazards that are excited by multiple failures or simultaneous failures.

Human Interference

Humans can affect safety in many ways often difficult to foresee: in system production, maintenance, handling, and operation. For example, people sometimes use controls in wrong sequences, do not follow operating instructions, or do not maintain their equipment properly. Therefore, humans may create many difficulties for the system designer and may cause safety problems in the overall system operation.

These factors are fundamentally achieved by combining the stimulus of system failures with enhancement of system hazards. Because these factors exist, it is necessary to specify and design the IVHS or IVHS devices to withstand the environments or to ensure that no (or minimal) undesired events will occur as the result of the interference of the environments.

HAZARD ANALYSIS

Hazard analysis is crucial in designing the IVHS or IVHS devices, because the system configuration and functions can be affected by system hazards. For example, assume a vehicle moving in a platoon undergoes a steering system failure, and the failed steering system turns the vehicle 90 degrees. This situation represents a critical or catastrophic hazard, and the hazard will no doubt lead to an accident. According to this assumption, a system configuration should be designed either to avoid the hazard, which may lead to an accident, or to reduce the collision impact. However, there must be a hazard analysis to investigate under what conditions this particular hazard can occur in the real world. Moveover, the hazard analysis (FTA, in this case) must be used to determine what type of failure would initiate the hazard, whether the failure that causes the hazard would be detectable, and if the hazard would be preventable.

Hazard analysis should be performed in the early stages of safety studies and at the system level. Because the IVHS or IVHS devices contain many unknown factors, it is necessary to make some technical assumptions by defining the system configuration, the environments in which the system works, and so on. The assumptions should also include the component subsystems that will function in the suggested IVHS. Configuring the system is considered a primary step for conducting hazard analysis. At this level, PHA and FTA are usually applied.

When studies on safety hazards are conducted at the component subsystem level, a standard analysis method known as failure mode effects and criticality analysis (FMECA) has to be applied in evaluating the design, method of operation, and environment in which the system works. The cause-consequence relationships leading to system failures must also be identified at this point. Once the component subsystems are defined, major assemblies, subassemblies, or even parts of each component and their functions are then identified. Detailed studies on failure mechanisms of each component (that is, failures, failure modes, and their consequences) then can be examined. FMECA must be followed by FTA to develop the relationship between the occurrence and the sequence of hazard events and finally to evaluate possible failures. FMECA is an essential step in the understanding of the system, without it, FTA cannot be performed.

Systematic safety analysis should be conducted in a closed-loop form. The steps and analytical methods are shown in Figure 2.

ELEMENTS IN SYSTEM SPECIFICATION FOR IVHS SAFETY

Conventional system design usually follows a procedure that includes defining the functional requirements of the system, establishing system specifications, and then designing the system that will accomplish the specified functions. In the system specification the engineers are confronted with an optimization in which capacity and safety are both required. The following elements should be taken into account in the system specification.

Safety Criteria

Safety hazards can be classified as catastrophic, critical, marginal, or negligible (or other classes, if desired), depending on the severity of their consequences. In the system specification, a delineation or safety criterion should be given to define which hazard levels are unacceptable. The safety criterion should take the form of a marginal line on a frequency-consequence diagram, which stipulates the acceptability or unacceptability of the type of hazards on the basis of their consequence and the probability of occurrence.

The establishment of safety criteria must be based on risk assessment at the system analysis level. It requires a systematic consideration of system safety and efficiency, as well as societal acceptability of hazards. A variety of safety criteria for defining the level of acceptability of risks have been proposed for several different applications (*9*). For IVHS, the safety criteria should give, in a quantitative form (e.g., the number of fatalities, severity of injury, or property damages), a description of the types of hazard that are acceptable even if they lead to accidents and the indication of the hazards that are unacceptable. The safety criteria have to be obtained by

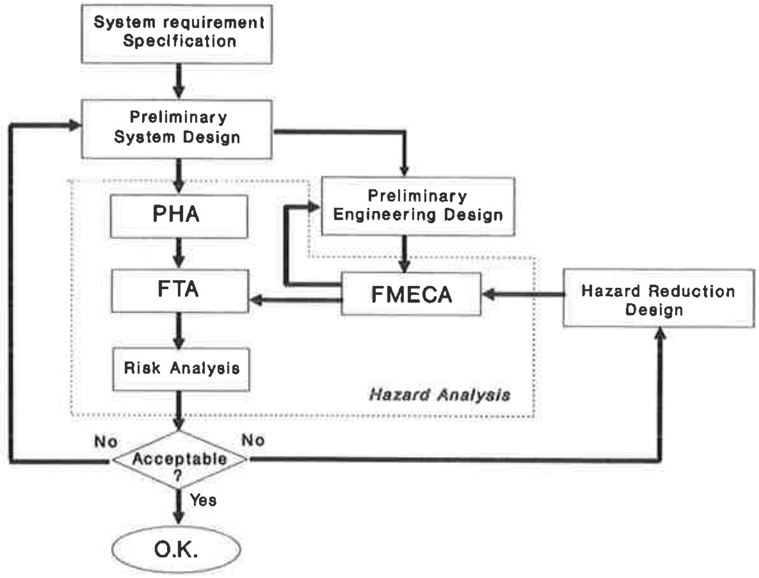

FIGURE 2 Systematic safety analysis.

risk analysis (e.g., the probability risk assessment) in which the impact of all possible accidents within the system is assessed by determining both the likelihood and the consequences of the accidents. Through the analysis, a frequency-consequence relationship can be developed that will first be used in assessing the acceptability of a system and will then serve as a criterion for the system specifications.

Safety States

A system can operate either in normal mode or in failure mode. In the normal operating mode, the system functions as intended in a given condition or situation. (The intended tasks do not include those being wrongly specified, because specification errors have been included in the system failures.) It seems reasonable to suggest that a system is under safe condition if it is in a normal operating mode, because an unsafe condition arises only when a safety-critical component fails to control the vehicle as its design intended. Therefore, in the safety design of a system, attention is usually given to the failure modes of the system.

A failure of a safety-critical component may or may not lead a system into hazards. There would be, according to the predefined safety criterion, only two kinds of states to which the system will be directed as the result of failures:

1. *Fail-Safe (F–S) State.* A state that ensures that no hazard exceeding the safety criterion occurs as a result of system failure; and
2. *Fail-Hazard (F–H) State.* A state in which a hazard exceeding the safety criterion occurs as a result of system failure.

It is the goal of the IVHS researchers to design the system or devices so that it is possible to transfer to an F–S state when hazardous failures occur in the system. Therefore, there is a need to predefine the F–S states according to the discovered failures. Because the severity of a hazard resulting from a particular failure is time or environment dependent, or both, there could be more than one F–S state for a safety-critical component. These F–S states may include graceful degradation, degradation and stop, or emergency stop.

For example, a video collision-detection device may suffer a complete failure of the illumination components. This failure may not affect the system's operation when there is sufficient illumination (natural light or any other kind of illumination). The failure may affect, to a certain extent, the system safety when there is not enough illumination. It will endanger the safety of operation when there is no illumination. Therefore, the F–S states for these three conditions can be normal operation, low speed operation (here, the consideration is concentrating on safety but not on the traffic laws), and stopping the vehicle.

Safety-Critical Components

An IVHS will possess a variety of components at different functional levels. Some components are inherently such that their failures can induce hazards; other are not so. Further, the hazards caused by failures of different components may or may not exceed the predefined safety criterion. While investigating the effects of failures within a particular component or their effects on particular functions, the term *safety-critical* is often used. The safety-critical nature is inherent in the definition of system functions and is incorporated with predefined system functions. Safety-critical functions are those that can induce, cause, or allow a hazardous system state. A safety-critical component is a component or device that performs safety-critical functions. The identification of the safety-critical components must be based on the hazard analysis. To enumerate the safety-critical components, it is necessary to investigate all the possible inherent failures of each component and to examine whether these failures can lead the system into an unacceptable hazard. The safety-critical components should be clearly defined at a very low functional level.

In an IVHS, system safety is defined by the safety of the vehicle, as explained previously. Safety-critical components, therefore, are included among the limited set of components or devices that is directly related to the vehicle-maneuvering functions and the information function. Failures in these functions can introduce system hazards.

Hazard Reduction Principle

In the system specification safety should be incorporated in the definition of the system's physical and operational conditions or environments, as well as hazard control strategies.

In defining the environments attention has to be given to allow the vehicle to operate both in normal and in emergency situations, as well as in situations in which accidents are unavoidable. For example, proper longitudinal spacing between vehicles should be chosen (a) to use the highway effectively, (b) to allow the vehicles to respond correctly to the emergency situation, and (c) to reduce the impacts of the collision if accidents occur.

The system functional requirements should detail the identified hazards, the causes of hazards, and their corresponding F–S states. The system specification also provides a principle for hazard reduction, in which various approaches for transferring a system from a hazard to an F–S state are given. The hazard reduction principle usually follows the system safety precedence, that is, to eliminate hazards, to reduce hazards, to provide safety devices, to provide warning devices, or to provide special procedures.

DESIGN FOR SYSTEM SAFETY

Safety design is essential for providing countermeasures to ensure that both the frequency and the magnitude of accidents do not exceed the acceptable level. To conduct the safety studies, the designer must not only understand and take into account the usual design features, such as operability, quality, and efficiency, but must also fully appreciate the range of environmental conditions throughout the life of the IVHS devices, the range of production methods that will be used in manufacture, and, most important, failures that may occur at any time in the system or within the devices under the predefined conditions.

Many techniques have been developed for providing system safety. In particular, the application of various safety or safety-oriented reliability techniques in transportation engineering, such as techniques applied in railway transportation and air transportation, will have considerable value as exemplars. The safety or reliability techniques are not assessed in detail here; however, several safety design methodologies are discussed.

Design for Robustness

An IVHS or IVHS devices will be applied in a wide range of environments. The components of the system or devices will be produced by different manufacturers, and distinct design and quality control rules will be applied. Therefore, the system or devices will be subject to variations, including allowable production lapses, environmental changes, parameter drift in time, and other factors that can affect the output parameter values in service. Thus, the performance specifications of the system or devices must be met over a large range of input tolerances.

The robust design concept combines elements of control theory and statistical design to optimize product design in relation to its ability to tolerate the expected variations in the environment and production variations. Hence, adaptation of components or the overall system against parameter and process changes is provided. With robust design application, production and maintenance can be relative easy and less expensive.

Design for Reliability

The reliability design concept is applied to ensure that the system continues operation under given conditions for its expected life. Through reliability design, a component should possess sufficient ensurance against progressive weakening to withstand fatigue, corrosion, wear, and so on, thus reducing its failure frequency.

By applying appropriate reliability techniques, it would be possible to design a system with a low failure rate according to the strictly defined specifications. However, whether an IVHS or any IVHS devices can be constructed to meet and be maintained at specific engineering requirements is doubtful. It is well known that the failure rate of any system may be substantially higher than expected in the original design according to the so-called burn-in and wear-out phenomena (which correpond to the initial failure rate and aging failure rate in the "bathtub" curve). In reality, it is obviously not economically practical to design and produce a huge number of vehicles that will always be inherently failure free in all environments. In addition, there is always the possibility of having errors in the design. The practical considerations of cost might also limit the extent to which total reliability can be ensured. For these reasons, reliability design will be applied as one of the design methodologies for system safety, but not the primary methodology.

F–S Design

Fail-safe, as the term suggests, should indicate the ability of a system to ensure that it can be handled safely (i.e., to avoid a hazardous condition) should it reach conditions outside specified tolerances.

As a design principle, F–S has sometimes been interpreted as fail-stop; therefore, this approach has been considered to be inefficient. In fact, this interpretation involves distortions. By using the definitions of system states, the F–S property can be redefined as the ability of allowing a system to enter into an F–S state in the event that the system deviates from the normal operating mode. Because the F–S states are defined in accordance with the particular failure modes of the components, a system that is designed on the basis of the F–S principle will lead a system into a corresponding F–S state, including maintaining the system operation or one-level functional degradation (e.g., reduce the vehicle speed). It is true that fail-stop will be applied, because stop is the single, final degradation state of the F–S states; however, it is applied only when other functional degradation states would not be enough to prevent the system from unacceptable hazards.

F–S design can be accomplished by a specially designed protection system that can detect system failures in the early stages and then lead the system into previously defined F–S states. The key issue in F–S design is the assurance that the protection system will be fail-safe. Two types of failures are addressed in designing the F–S protection system: (a) F–H failures (where the protection system fails to guide the system into an F–S state when one or more inadvertent events occur and (b) F–S failure (the protection device forces the system to enter into an F–S state when no inadvertent event exists). It is crucial that the protection system be designed fail-safe, that is, to avoid F–H failures, although F–S failures also need to be reduced.

Other Safety Design Approaches

Other safety approaches should also be considered in the safety design to reduce the severity of impacts if vehicles in the IVHS are involved in accidents. Many L–S technologies that have been employed in the existing DVR system can be applied to protect people from fatality, injury, or property damage.

CONCLUSIONS

Designing for minimal acceptable hazard in an IVHS or IVHS devices means that a complete identification of system hazards will have to be accomplished from the hazard analysis. Then, alternatives for eliminating or controlling the specific hazard will have to be evaluated so that an acceptable control method for hazard reduction can be chosen.

To identify the safety hazards completely, preliminary design of components of the system or devices is required to understand in depth the failure mechanisms of the system. Thereafter, FMECA and FTA can be conducted. Safety criteria should be given in the system specification and design; thus, the safety-critical components and safety states of the IVHS or IVHS devices can be defined. The strategies that will lead the vehicles to safety as the result of system failures should be designed for those components that are defined as safety critical.

Important issues for designing a safe IVHS or IVHS device have been investigated, and some preliminary definitions have been given. Technological concerns in the specification and design of the IVHS or IVHS devices have been discussed. The design methodologies for providing system safety have been assessed to provide a basis for evaluating technologies applied for reliability and safety design. Further work will be reported later.

ACKNOWLEDGMENTS

The research reported here is part of the Program on Advanced Technology for the Highway, prepared under the sponsorship of the State of California Business Transportation and Housing Agency, Department of Transportation. The author also wishes to thank Anna Bozzini, Anthony Hitchcock, and Steven Shladover for their contributions, technical or otherwise, that helped to shape the final form of this paper.

REFERENCES

1. *Final Report of the Working Group on Advanced Vehicle Control System (AVCS).* Mobility 2000, Dallas, Tex., March 1990.
2. S. Shladover. Roadway Automation Technology—Research Needs. Presented at 68th Annual Meeting of the Transportation Research Board, Washington, D.C., 1989.
3. H. Roland. *System Safety Engineering and Management.* Wiley, New York, 1983.
4. P. O'Connor. *Reliability Engineering.* Hemisphere Publishing Co., Washington, D.C., 1988.
5. I. Treat et al. *Tri-Level Study of the Causes of Traffic Accidents—Executive Summary.* Report DOT-HS-805-099. U.S. Department of Transportation, May 1979.
6. J. F. M. Bryant. Is the Motor Vehicle and Its Drive Part of a System? Human Factors in Transportation. *Proc., 10th Annual Conference, Ergonomics Society of Australia and New Zealand.* Adelaide, S. Australia, 1973.
7. R. Stempel. Where Auto Safety Stands Today. In *Media Update on Passive Restraints*, Warren, Mich., July 1989.
8. E. Deakin. *Opportunities and Constraints for Advanced Highway Technologies: A Speculative Analysis.* Research Report UCB-ITS-PRR-89-7. Institute of Transportation Studies, University of California at Berkeley, Richmond, Oct. 1989.
9. J. Thomson. *Engineering Safety Assessment: An Introduction.* Longman Scientific and Technical, 1987.

Publication of this paper sponsored by Committee on Vehicle User Characteristics.