

System Safety Applied To Vehicle Design

Peter L. Goddard

P.L. Goddard and Associates, Inc.

Copyright © 2008 SAE International

ABSTRACT

The development of a modern transportation product requires that the safety of the product be considered at every stage of its life, from initial design to ultimate product disposal. Virtually all of the decisions that can positively effect product safety are made during the product design stage with most of the critical decisions being made early in the process. As a result, early incorporation of system safety into the design process has been shown repeatedly to result in safer products.

Incorporation of formal system safety programs into ground transportation vehicle design programs is comparatively recent. Historically, in both the automotive and the heavy goods vehicle industry, product safety has been provided through consistent over design of evolutionary system elements to ensure correct functioning under repeated exposure to worst case stresses. The degree of over design has been confirmed through a combination of experience with previous generation products, testing, and where warranted, through stress analysis techniques such as finite element

analysis. As advanced technology, particularly computer control of an increasing number of on board systems, has been incorporated into new vehicle designs, traditional approaches to ensuring product safety are no longer adequate for all elements of vehicle design.

This paper discusses system safety as an applied methodology that, when incorporated into the design effort for vehicle components, feeds back to the design team an ongoing assessment of the relative risks of potential design alternatives. A discussion of the relationship of system safety to the overall safety surrounding vehicle use is provided. Specific discussions of some of the design approaches driven by the integration of electronic systems into vehicle design are given, as is a top level discussion of the way that system safety must be incorporated into the design team effort to be effective. Specific analysis techniques are presented and discussed at a summary level to impart an understanding of how the output of these analyses can be used to measure the risk of a specific design implementation and allow it to be controlled.

Chapter 1 INTRODUCTION

VEHICLE DESIGN SAFETY

Safety as it applies to the transportation of goods and persons on the nation's and the world's highways is a large, diverse topic. Only some of the elements of the transportation system provided by the roadway systems can be influenced by the vehicle designer to provide enhanced safety. As shown in Figure 1-1, the roadway transportation system consists of many elements. Some of these elements, for example climatic conditions, are not capable of being controlled. Others, such as development of regulations, signs applied to the roadway environment, licensing of vehicle operators, emergency services, and enforcement of regulations are properly the domain of governmental agencies. The elements of the transportation system which are subject to being influenced by the design engineering applied to them include both roadway design, and vehicle designs. Roadway design to promote safety in use is a well developed discipline, with national standards agreed to by the states under the auspices of the American Association of State Highway Transportation Officials (AASHTO). AASHTO publishes a wide range of roadway design related technical materials that are used world wide in the design of roads. Readers with an interest in this area should consult Reference 1. Roadway design issues will not be further discussed in this paper, which focuses on vehicle design issue and specifically on embedded processing applications.

In addition to the other elements of the transportation system, the designs applied to both passenger and commercial vehicles using the roadway impact the relative safety of users of the roadway systems. Vehicle designs can influence safety through a combination of reduction of accident severity, using both active and passive design features, and by providing the driver with assistance in maintaining control of the vehicle within the environment in which it is being used. Design of a vehicle to allow occupants to survive collision events, including single vehicle loss of control events, includes vehicle features such as collapsible steering, energy absorbing crush zones, and provided occupant restraint equipment, both passive and active. Seat belts are proven to limit the severity of injury and help prevent fatalities. However, although they are passive devices, seat belts require an active participation by the vehicle occupant in his or her decision to use the provided safety equipment. Legal penalties have been and continue to be effective in causing drivers and passengers to use seat belts. Unfortunately, use of seat belts is still not universal. Seat belt use has been accepted by the passenger car driver as a necessity, but less so for commercial vehicle drivers. In addition to seat belts, vehicle designs now include a variety of active devices, the use of which is passive with respect to the driver. These devices are only apparent to the

driver through the labeling provided on the vehicle and upon occurrence of a collision. These devices include air bags at knee, thorax, head, and side. Seat belt pretensioners are increasingly being deployed with air bag systems. Additionally, active deployment of roll bars and active steering wheel collapse is available on some vehicles. The use of active devices, while increasing survival rates in collisions, presents a new and unexpected potential hazard to the vehicle occupants. Air bags and roll bars must be deployed with considerable force to allow the device to be in place quickly and to absorb sufficient energy to provide needed protection. As a result, air bags and in some cases roll bars which deploy inappropriately have the potential to present a hazard to the vehicle occupants.

While collisions are the result of a complex interaction of events and actions, review of the collision data collected by NHTSA provides some insight into contributing causes of collisions, thus potential safety improvements. Figure 1-2, below, shows the relative frequency of some contributing collision causes, taken from Reference 2. While somewhat dated, significant changes in the underlying contributing causes of collisions is considered unlikely. As shown in the table, in depth investigation of causes identified the vehicle design or defects as a contributing cause in only 4.5% of the collisions studied, while environment could be shown as a contributing cause in 12.4% of collisions and human factors in 70.7% of collisions.

Since environmental conditions are not subject to control by vehicle designers, improvements in vehicle mishap rates through vehicle design must focus on either prevention of vehicle defects or providing additional aids to the driver to reduce human factors causes. An examination of the underlying causes of vehicle failure related mishaps (see Reference 2, Table 2-1) leads to the conclusion that improvements in vehicle reliability could reduce or eliminate as much as 50% of the vehicle failure causes. Approximately half of all equipment related vehicle mishap causes are not subject to improvement through more robust vehicle designs. Many of these, for example tire under inflation, require contributory vehicle owner neglect. Although some tire pressure monitoring systems are now standard on passenger vehicles, owners must respond to the warnings given. As a practical matter, only about 2.25% of collisions might be eliminated by more robust designs. The practicality of the needed increases in reliability or of additional equipment is limited in part by cost considerations.

Improvement of the human factor designs for automobiles is a more fertile ground for safety improvement through improvement in existing designs and the introduction of new design features. With over 70% and possibly greater than 90% of all collisions being

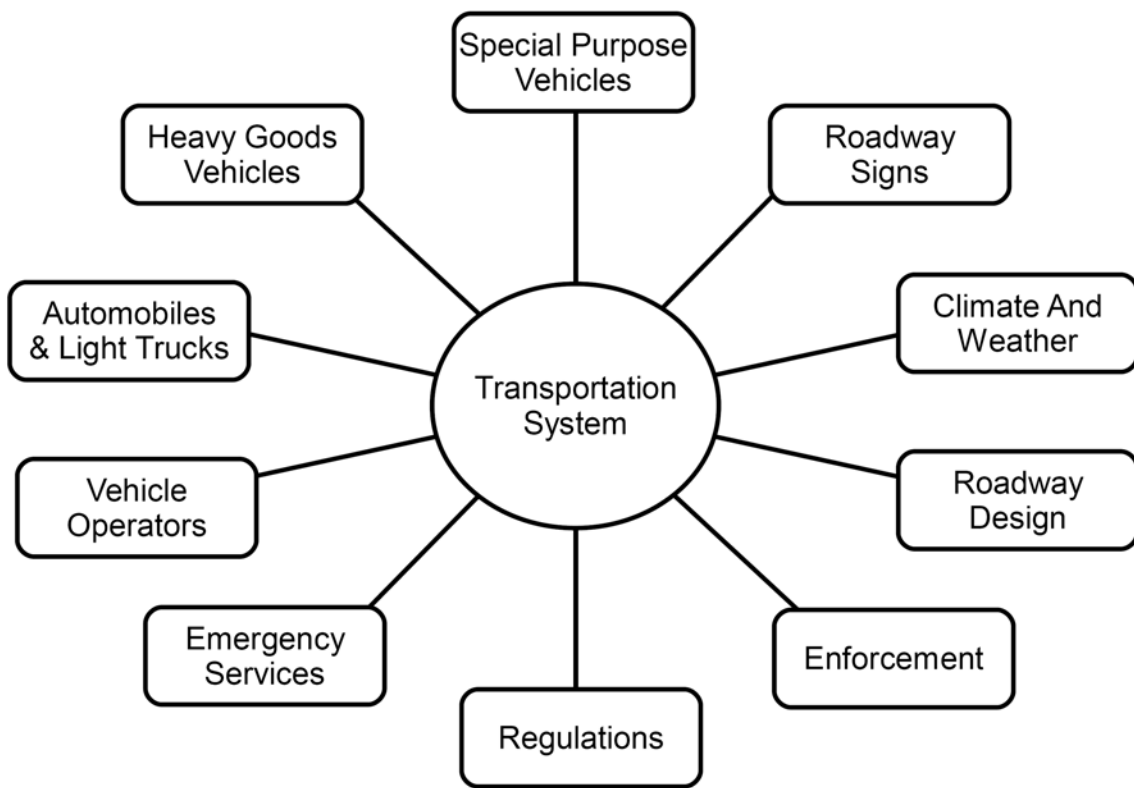


Figure 1-1. Roadway Transportation System Elements

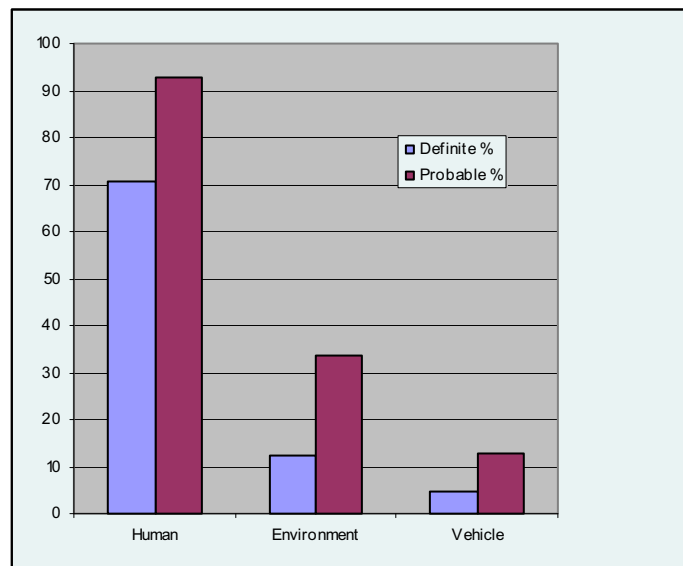


Figure 1-2. Causes Of Vehicle Mishaps

related to human factors, introduction of driver aids has the potential to provide significant benefits. The introduction of such aids must not introduce an unacceptable level of new hazards. Figure 1-3, below, shows the relative rate at which the human based errors contribute to vehicle mishaps. All of these causes are subject to reduction through careful introduction of driver aids. Prior to introducing such devices, it is necessary to demonstrate that any device which is introduced to provide the driver with improved vehicle control capability is safe for introduction onto the public roadways.

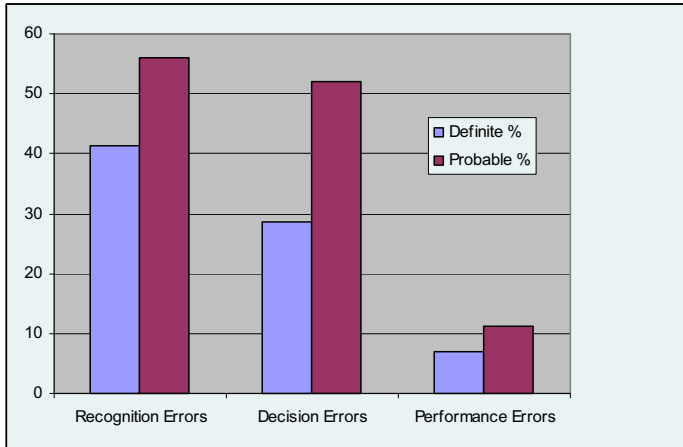


Figure 1-3. Driver Errors Contributing To Mishaps

DRIVER ASSISTANCE SYSTEMS

With the introduction of driver assist systems that require the driver to sacrifice vehicle control to an automated system under some conditions, a potential risk of incorrect behavior is introduced. Table 1, below, provides a brief overview of some of the associated risks. The introduction of this risk is comparatively new to the automotive environment. Mechanical products wear and eventually fail, almost always providing advance notice through noise, vibration, or excess tolerance felt by the driver prior to actual failure. Electronic devices provide no warning of impending failure. Failures tend to be sudden and unpredictable with the expectation that the driver will be able to either handle the sudden change in performance introduced by the failure, or that the severity of effect at the vehicle level and frequency of occurrence are acceptable.

The safety of mechanical elements of a vehicle are ensured by a combination of deliberate over-design, stress and life testing, and evolutionary development. Mechanical elements of vehicles are deliberately oversized to ensure that a lack of exact understanding of the stress environment which a vehicle might encounter cannot result in a safety critical failure. Mechanical elements are then subjected to multiple life times of expected worst case applied stress and examined following exposure to these worst case conditions. Any wear which indicates a potential for in service failure results in changes to the product to preclude the failure. Mechanical elements of vehicle designs feature

extensive re-use and evolutionary product change. As a result, failure of mechanical safety critical vehicle elements is quite rare. Electrical and electronic designs can be subjected to similar testing, but the testing cannot produce substantial confidence in those designs.

For an electronic system to provide assistance to a driver, the automated system must be given the authority to remove some or all direct control of the vehicle from the driver. This shift in control must be limited to those cases where it is reasonable to assume that the automated system with its quicker response times and accurate sensing of vehicle motions can provide responses that are either too rapid for human capability or involve control methods not available to the driver^(a). With the introduction of vehicle control capability which considers the driver's intent in performing control actions, but may perform outside that intent when necessary to maintain vehicle stability, a set of potential vehicle movements are introduced that cannot sensibly be considered within the capability of a driver to control. Thus, ensuring that the control systems which have been introduced have at most an extremely remote potential for inducing unwanted and/or uncontrollable vehicle movement is crucial. Ensuring that these control systems cannot cause unwanted vehicle movement requires a combination of analysis and testing prior to field exposure. As a minimum, the producer of the control system must be able to self 'certify' that no credible single fault could result in unwanted vehicle movement for a time sufficient to cause a loss of vehicle control by the driver. Assisting system designers in providing such assurance is the function of system safety engineering and of the safety approach discussed in this paper.

The risk issues introduced by the addition of control electronics are not new. The aerospace industry has used a variety of safety critical embedded control systems in aircraft, in military specialty vehicles (e.g. Tanks), and in weapons systems for many decades. In many cases, these embedded control systems have advanced to a control by wire design where the operator has no direct control over the system. All control is filtered by and provided through the electronic control system which is free to override the operators command if it senses that such override is appropriate. This has allowed the development of aircraft that are inherently unstable and require continuous computer aided adjustment of control surfaces to maintain safe flight. The advantage associated with such a system is one of an improved performance envelope. Similar advances have occurred throughout aerospace and military systems over the past several decades. As a result

(a) A slip control system (SCS) has authority over the braking force at each of the four wheels in a passenger car. It also has limited authority over throttle and steering. Thus, if a front engine, rear drive, passenger car were to take a curve at excessive speed with a resulting slip of the rear end of the vehicle, the SCS may choose to apply brakes to the rear brake on the inside of the curvature while closing the throttle slightly and optionally moving the steering to compensate. This would result in the vehicle immediately regaining stability. Single wheel braking capability has never been available in the

Control System Type	Span Of Control	Advantage Provided	Risk Introduced (partial list)
Electronic Power Steering	Steering assist level	Tunable steering feel Can be commanded by other vehicle systems (e.g. SCS)	Application of steering assist when not commanded Erratic steering assist Reversed steering assist
ABS	Brakes on each wheel	Improved braking on low mu surfaces	Brakes not applied when commanded. Extended stopping distance
Slip Control (SCS)	Brakes on each wheel Steering (limited) Throttle (limited)	Improved vehicle control, particularly on low mu surfaces	Brake applied to one or more wheels unexpectedly Incorrect slip control causing increased slip Unexpected release of one or more brakes
Crash Sensing	Air bag deployment Pretensioner activation Fuel cut off Battery disconnect Roll Bar deployment Soft hood deployment	Allows application of passive safety devices – air bags, pretensioners, soft hood pedestrian protection. Allows active crash safety improvement through extra roll bars, battery and fuel cut off during collision	Unexpected/Improper air bag deployment Other risks are primarily annoyance and financial
Auto Cruise Control	Brake application (limited) Throttle (limited)	Automatic adjustment of speed to surrounding traffic	Failure to brake when expected Unexpected/Improper throttle application.
Smart Key Systems	Door locks Window operation Engine start Engine operation	Improved theft security	Entrapment of individuals with injury due to excess heat – particularly small children
Electronic Throttle	Throttle application	Improved air pollution Improved gas mileage	Sudden unexpected application of throttle Unexpected failure to apply throttle in critical situation
Brake By Wire	Brake application	Ability to use all electrical brakes on hybrid or electric vehicles	Unexpected brake application Failure to apply braking when commanded
Lane Departure Warning	Steering (limited)	Steering angle (low force applied, can be overcome)	Unexpected/Improper application of steering torque

Table 1-1. Driver Assist Systems And Associated Risks

many, if not most, of the safety assessment techniques needed to evaluate the risk associated with such systems have been created and verified for effectiveness as a part of the design and development of aerospace and military products. These programs are rigidly monitored and evaluated by the various government agencies. The analysis techniques needed to evaluate the risk of erroneous embedded control system performance exist and can be applied to passenger and heavy goods vehicle designs which include safety critical embedded control systems. Because of early adoption of safety critical system control provided by embedded control systems, a set of design solutions, appropriate to aerospace systems, which ensure the safety of the system under control have been developed, deployed, and are field verified.

Many of these solutions, such as redundant elements, can be problematic when introduced in passenger and heavy goods vehicle designs, which are recurring cost sensitive. A major difference between aerospace and highway transportation vehicles is in production volume. Many of the aerospace products which have been developed using safety critical embedded control systems are of limited volume. As a result, the ratio between recurring and non-recurring cost favors solutions which minimize non-recurring costs at the expense of raising recurring costs. Actual ratios between recurring and non-recurring costs are product and contract dependent, however, ratios of 90% non-recurring and 10% recurring would not be considered unusual in many aerospace related products. The passenger vehicle design is typically high to extremely

high volume, with recurring costs of 80 to 90 percent of product costs for an embedded control system not being unusual. As a general rule, in aerospace low volume products, adding hardware to help minimize analysis and test requirements is a cost effective approach. In automotive, using additional testing and analysis to help minimize recurring hardware costs is the cost effective approach. The result of this difference is that aerospace design solutions to the problems introduced by the use of safety critical embedded control systems cannot always be applied. If extensive analysis and testing allows the hardware required to be minimized, then such an approach has merit in the automotive industry. Similarly, the analysis techniques used in and which have grown out of low volume products have needed to be adapted to the automotive environment. Heavy goods vehicles occupy the area between the two types of approaches. Volumes are modest by automotive standards, but much larger than many aerospace products. Recurring costs are important, but not as critical as they are for automotive products.

Due to the comparatively new application of safety critical control systems to automotive applications and the unique cost environment of the automotive and heavy goods vehicle industries, the passenger car and light truck vehicle manufacturers and tier 1 suppliers

have recognized a need to apply formal safety programs to their control system product designs. The primary international standard which has been mandated on automotive and some heavy goods vehicle designs is IEC-61508. This international standard, released in December of 1998 (volumes 1, 3, 4, and 5) and in the first two quarters of calendar year 2000 (volumes 2, 6, 7), entitled "Functional Safety Of Electrical/Electronic/Programmable Electronic Safety-Related Systems", consists of seven volumes of information (**Reference 3**). Requirements for safety, for system design, for hardware design, and for software design are imposed. The intent of this international standard has been to be a 'master' standard that could be directly imposed on product development programs while an industry specific standard is developed from IEC-61508 and imposed. For the automotive industry IEC working draft 26262 is expected to result in the industry specific standard. It is expected that WD-26262 will also be imposed on safety critical control system product developments for heavy goods vehicles once the standard is completed and approved. The safety approaches discussed later in this paper present an approach that fulfills the requirements of these standards, albeit with some adaptation to later versions of these standards, particularly WD-26262.

Chapter 2: Safety and Risk

INTRODUCTORY CONCEPTS

A system is considered 'safe' whenever the risk of use of the system is 'acceptable' to the individual that will use the system and to society at large. These are easy terms to use in the abstract. Almost everyone has an internal concept of what is safe enough for his or her comfort. Unfortunately, almost everyone's concept of adequately safe is different, varying by the type of system, the personality of the user, and the individual's tolerance for risk. Finding a definition for 'safe' enough for use in a public domain is difficult, although some guidance is available.

The concept of a system being safe requires consideration of two related issues: potential severity of harm, and the rate at which such harm might occur. A system may be acceptable even though its use includes a potential for fatal outcomes if the likelihood of such outcomes is sufficiently remote. Acceptability of risk as a function of both potential severity of injury and frequency of occurrence is illustrated in Figure 2-1, below.

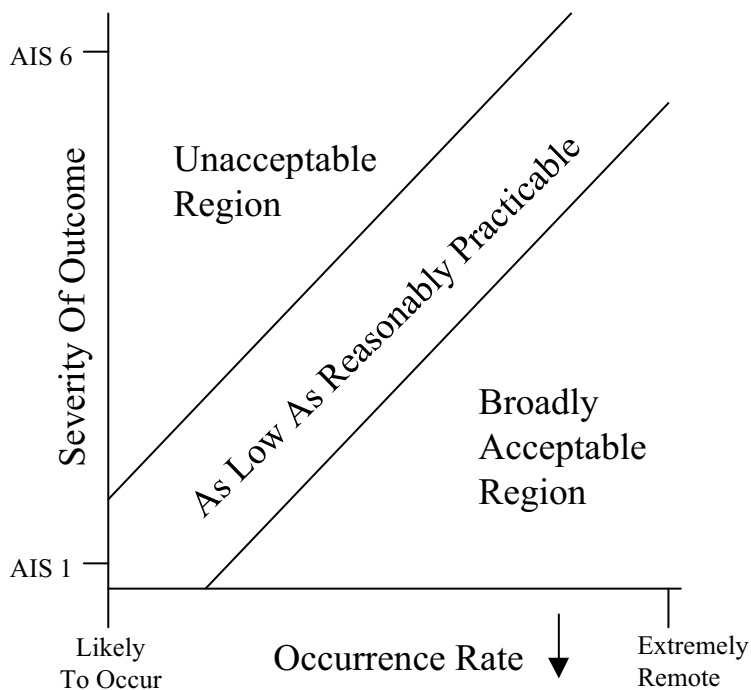


Figure 2-1. Risk Acceptability

As shown diagrammatically in Figure 2-1 as injury severity and/or frequency of exposure to injury increases, the risk of a system's use move from broadly

acceptable to tolerable (perhaps) to unacceptable. The concept

used in judging acceptability of a system is that of achieving a risk that is as low as reasonably practicable as a minimum. The concept of as low as reasonably practicable allows for systems that are inherently dangerous so long as all reasonable measures have been taken to reduce the likelihood of occurrence and the system's use has a defined benefit that exceeds the overall cost of use. For example, a loaded heavy goods vehicle traveling down a roadway at a speed of 60 Mph is inherently dangerous. The kinetic energy contained in the vehicle assures that any loss of control has the potential to result in severe injury and possibly fatality. Society has found that the risk of allowing such a vehicle on the roadways is acceptable so long as the frequency of occurrence of any loss of control is sufficiently remote. As a result, drivers of such vehicles must be trained and licensed more carefully than passenger vehicles, the vehicles are subject to inspection, and restrictions on weight and speed are often imposed. All of these measures are intended to minimize the frequency of occurrence of unwanted events making the risk as low as reasonably practical for the benefit provided.

The approach to system safety that is required for the development of systems follows a multiple step approach that is deliberately designed to reduce the overall risk associated with the use of a system Figure 2-2, below provides an overview of the standard, prioritized, approach to minimizing the risk associated with a system or product.

As shown in the figure, for each risk which is able to be identified for a system, the designer should first attempt to eliminate the risk through alternative design approaches. When it is either not practical or not possible to completely eliminate an identified risk, design measures should be taken to minimize the likelihood of the risk occurring. If complete elimination of the identified risk is not possible and the design measures taken to reduce risk result in a level of residual risk that is unacceptable, measures must be taken to separate the user and any bystanders from the energy release that may occur. If unacceptable levels of risk exposure exist after attempts to eliminate and minimize the risk, and separation of the user from any energy release is not practical, the user may be able to be trained to identify the onset of the risk event, allowing minimization of the severity of any likely outcome. As a last choice, warning the user and any others exposed to the risk may help minimize the severity of the worst case potential outcome.

Elimination of identified risks through design change is sometimes possible. For example, replacement of

flammable materials with non-flammable materials can result in elimination of fire risks. For electronic devices, which are inherently flammable, packaging in sealed metal covers can result in automatic smothering of any potential fire. Similarly, changes in materials can result in elimination of risks associated with corrosion and/or environmental risks. Elimination of identified risks through design is always the most desirable approach.

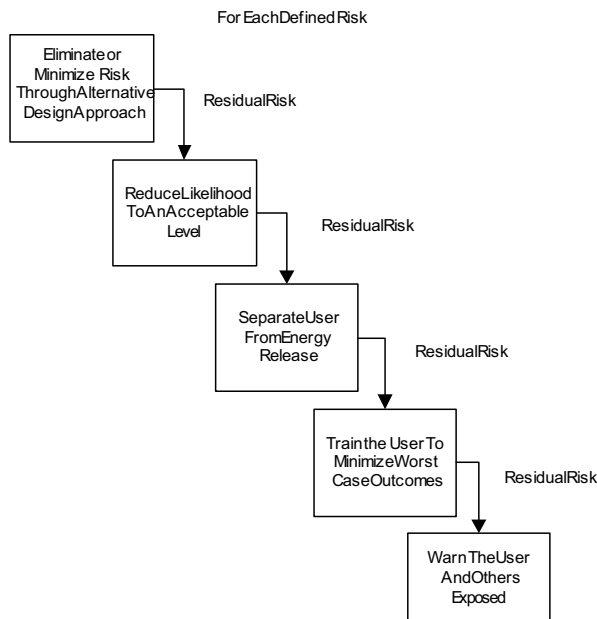


Figure 2-2. Prioritized Approach To Risk Reduction

Reduction of identified risks to an acceptable level is the next most desirable approach to achieving system safety. It is often possible to reduce the risk imposed by a product on its user and any others to levels broadly acceptable to society. This approach typically requires the use of components that are more robust than the minimum required, selection and use of high reliability components within the system design, application of redundancy, or design techniques which ensure that the system or product transitions to a safe state for any foreseeable fault or failure.

Separation of the user from the energy release associated with the identified risk may be an acceptable approach for some products if design elimination and design risk reduction do not result in an acceptable level of residual risk. Separation of the user from energy release often requires shields or barriers, including barriers that absorb some or all of the energy release to minimize the likely energy impact to the user and any others. Shields over belts are an example of minimizing risk through separation. Air bags in passenger vehicles are an example of energy absorbing barriers. The user (driver, passengers) of the vehicle has his or her kinetic energy absorbed over a longer distance than would occur with the vehicle occupant striking an interior vehicle component such as a dashboard. The air bag

thus reduces the energy per unit time imposed upon the occupant, reducing the severity of outcome of a collision.

The final two approaches shown in the diagram are inherently weak choices, but sometimes are the only viable approaches to minimizing the risk associated with a product. User training can help prevent risks associated with operator errors and can help provide some mitigation of risk if the operator can intervene in the product's unwanted behavior. Training of heavy goods vehicle drivers is a good example of this approach. The cause of the majority of vehicle collisions has been attributed to driver errors, both of the heavy goods vehicle and of surrounding traffic. As a result having drivers trained to be able to recognize the start of an unwanted event and capable of providing as much outcome mitigation as the vehicle's performance envelope allows can be effective in some cases. Failures of the heavy goods vehicle itself can result in unexpected vehicle path deviation. Given the relatively slow change in direction that occurs in large vehicles, a trained driver can often minimize the worst case outcome of the failure.

The final and least desirable choice in minimizing risk is to provide warning labels. Warning labels are widely used, but tend to be of minimum effectiveness when intended to minimize risk to a user. For many products, the main purpose of warning labels for the user is to minimize manufacturer liability risk for foreseeable misuse of the product. However, warning labels on potentially dangerous items, when intended to remind trained technicians of proper procedures, can be very effective.

Elimination of identifiable risk should always proceed in a measured, prioritized, fashion, designed to result in minimum overall risk to the user and to others not directly involved in a product's use. Whenever possible, elimination of safety risk through design is the preferred approach, with reduction in the likelihood of risk to an acceptable level being a close second. Other, less effective, approaches may be required, but should be reserved for those cases where design based solutions cannot be employed.

IDENTIFYING PRODUCT RISKS

As a part of identifying the risks that may exist for a system or product, the safety engineer must carefully examine the full range of possible sources of risk which may involve the product. Potential interactions between a product being developed and the larger system of which it is part must be considered during normal operation, during and following maintenance, under conditions of failure, and under conditions of foreseeable misuse.

Introduction of a product to a vehicle must include consideration of the behavior of the product itself and also its impact on the vehicle as a system component.

of a new or a changed product can result in unintended interactions between vehicle elements and between the driver and the vehicle. In identifying potential risks, the safety engineer must consider the full range of potential interactions. For example, installation of an electric park brake (EPB) into passenger vehicles, as is now becoming common in the EU market, has required careful design to preclude unexpected interactions between the service brakes and the park brake. Driver deployment at speed of an EPB can result in vehicle instability if some form of moderation is not used. This has generally required that the slip control system for the vehicle be aware of and respond to EPB commands when the vehicle is at speed. Interactions with drivers must also be considered when identifying system and product risks. During the early years of ABS penetration of the automotive market, the city of Buena Park, California experienced an unexpected number of police vehicle loss of control events during high speed pursuits.

The root cause was identified as being an interaction between the ABS and the police officers driving the vehicles. The police officers, highly trained in high speed pursuit, automatically pumped the brakes in making quick speed reduction to ensure continued steering control during hard braking. This had been the appropriate response to maximize vehicle performance prior to ABS penetrating the market. For a vehicle with ABS, the result was a significant and unexpected reduction in braking. This interaction had not been fully considered and conveyed to the cities purchasing the ABS equipped police cruisers prior to this time

In addition to system interactions during operation, the safety analyst must consider the risks associated with a complete or partial loss of functionality. As drivers become increasingly dependent on electronic systems, consideration of the sudden loss of function becomes increasingly important. Mechanical systems often provide warning of impending loss of function through performance changes which can be sensed by the driver. Drivers can sense increased looseness in mechanical elements which are often the precursor of complete failures of linkages and connections. Similarly, mechanical gearing and bearings will often make noticeable amounts of noise prior to failure, allowing the driver to have the vehicle serviced prior to any failure event. Electronic systems are seldom capable of providing advance warning of failure. Thus, complete and unanticipated loss of function can occur. When assessing the overall risk of total loss of function, the safety analyst must include the effect of the driver behaving incorrectly.

The introduction of electronics and of processing elements has introduced a new set of risks that must be considered by the safety analyst identifying potential system risks. Electronic systems with processing elements are capable of unexpected and incorrect behavior in ways that were not issues with earlier mechanical systems. If an electronic system has authority over a function, it has the potential to

incorrectly perform that function unless specifically designed to preclude such behavior. The improper behavior that must be considered in establishing potential product risks includes not only loss of function, but also partial functioning (e.g. brakes only one wheel), unexpected application of the function (e.g. brakes without warning), and reversal of function (steering assist in direction opposing the driver). Unless and until it can be shown in the final design of the product that such behavior has been precluded, including under conditions of failure, the safety analyst must assume that unexpected and unwarranted behavior may occur due to errors in the processing function. Both hardware and software product design may have the potential to cause unexpected behavior.

In establishing the potential risks of a product, operation under worst case conditions, including those of driver error and driver foreseeable misuse must be considered. If an electronic park brake is provided, one or more drivers will push the EPB activate button at high speed. This may be the result of driver error, curiosity, or deliberate misuse. Similarly, the impact of the entire vehicle operational envelope should be considered in establishing potential system hazards. Vehicles are driven in many weather conditions and across a wide variety of roadway surfaces, including dirt, gravel, snow, and ice.

In establishing potential system risks, maintenance related risks, including those associated with product disposal need to be examined. Unexpected activation of the electronic system may be possible resulting in entrapment of, or other direct injury to the technician. The technician may take (or fail to take) one or more maintenance actions that result in the electronic product behaving incorrectly as the result of service errors. An additional risk for electronic systems is that of incorrect reuse. Electronic systems which are identical (or nearly so) from a hardware system may be dependent on a downloaded set of data which causes the unit to be adapted to the specifics of the vehicle in which it is installed. As a result, installation of a product which is correct from a hardware standpoint while incorrect from a software standpoint is within the envelope of potential system risks. Installation of similar, but incorrect product by an amateur repair technician (often the owner) late in the product life due to selection of the replacement parts from salvage yards is also a potential source of risk. For example, the programming and response of a slip control system for any two cars may be markedly different, resulting in an unexpected and improper system intervention if an incorrect unit is installed

Those risks associated with disposal of the product are also to be included in the set of risks associated with a product. Existence of environmentally sensitive materials may result in special handling being needed during disposal of the product. Any parts of the product or system that might have the potential to cause injury

must be considered. High pressure accumulators for hydraulic systems are an example of such product based risks that need to be understood and correctly handled during disposal.

TYPES OF RISK TO BE CONSIDERED

Engineers evaluating the potential risks associated with a product must consider both direct and consequential risks associated with use of the product. In a vehicle environment, consequential risks tend to be the more severe of the two categories of risk exposure. Direct risks of product use are usually considered to include three types of risk. The product may provide a direct risk to a vehicle occupant, may pose a risk of direct damage to the environment, or may damage other vehicle components. Consequential risks are those that are caused indirectly by the behavior of the product being considered. Changes in vehicle behavior due to product operation or under conditions of failure, are consequential risks which may or may not be able to be controlled by the driver.

DIRECT RISKS - An automotive product's potential to create a direct risk to vehicle occupants and or maintenance technicians is often limited. Direct injury due to cuts and abrasions, contact with high voltage, burns due to thermal contact, or due to exposure to high current potential tend to be minor, rarely exceeding abbreviated injury scale (AIS) rankings of 1 (Reference 5). Standard practices for protective covers, radius of edges and corners, thermal exposure, and protective padding exist for most vehicle interior products which might have the potential to directly injure a vehicle occupant. Direct risks to vehicle occupants which are potentially caused by passive action, while important, are easily avoided. Active passenger protective devices, such as air bags, have the potential to directly injure vehicle occupants that are out of normal positions, should they become activated. The risks associated with inadvertent activation of these products is control system related and can result in injuries of any AIS level, depending on the specifics of the unwarranted activation. The direct injury risks associated with a product are considered to be a part of product safety.

Some automotive products have the potential to cause minor environmental damage if toxic products used in their operation are released into the environment. Vehicles use some products which, if released in sufficient quantity, might harm the environment. Oil based products, including gasoline, lubricating fluids, and power steering and brake fluids have the potential to damage the environment if released, particularly if released in large quantity. Most vehicle use involves quantities of fluids that could, at worst, result in minor environmental damage if released due to failure of a seal or similar causes. As with most minor direct risks, protection against the minor environmental risk being imposed, is handled by following standard industry practices for the robustness of seals and retaining

devices. Risks associated with environmental damage are a part of environmental safety concerns.

In addition to directly harming vehicle occupants, or the environment, some vehicle systems have the potential to damage other systems under conditions of failure. This is primarily a risk associated with electronic systems which may be connected to other, physically remote, electronic systems through wiring. Any failure of one unit which might place an unexpected high voltage on the interconnecting wiring has the potential to cause damage to other units. In some cases application of a ground potential to interconnecting wiring may damage a connected unit. Because grounded wiring is a well known failure event in vehicle wiring, most electronic units are designed to be self protecting against application of a chassis potential to any wiring element. This type of risk, referred to as equipment safety, tends to be minor in modern vehicle designs.

INDIRECT OR CONSEQUENTIAL RISKS - In addition to the risks of a product injuring a vehicle occupant or a maintenance technician, damaging the environment, or damaging other vehicle systems, indirect risks which are the consequence of incorrect product behavior exist. These risks, treated under the concept of system safety, are based on the effect on vehicle and/or driver of incorrect product behavior. The product itself does not cause the injury. Instead, the product causes unacceptable changes in vehicle (the system) performance which may lead to collisions or single vehicle loss of control events. These system safety risks tend to be the most important risks to protect against as they may cause consequential injury ranging from property damage to AIS 5 or AIS 6 level injuries.

Product induced risks, both direct and consequential, must be protected against as a part of good design practices. Most direct injury risks can be effectively avoided through the use of time proven vehicle design practices. Safety practitioners that are called upon to evaluate the safety of on-board vehicle systems may be able to avoid extensive analysis efforts if effective design controls are imposed on the design team by company practice and are enforced by an effective quality assurance organization. An exception is direct injury caused by improper deployment of passenger protective devices. Indirect risks, particularly those related to embedded electronic processing devices are comparatively new and require extensive care in design and supporting analyses to validate the acceptability of these designs.

ACCEPTABLE LEVELS OF RISK.

While complete elimination of risk is desirable, it is seldom practical to accomplish. All of life provides some exposure to risk. Keeping risk within acceptable bounds is the purpose of design safety. A product is considered 'safe' when it achieves a level of risk low enough to be acceptable to society, is at least as risk free as existing

similar products, and is consistent with user expectation. Achieving this level of risk reduction requires that the design team understand the user's expectation, the history of similar products that are in use, and the level of risk that is considered generally acceptable within society at the time of product introduction. Additionally, any product is expected to ensure the risk to the user and the public is "As low as reasonably practicable".

It is a core tenant of system safety that no product should be introduced that is not at least as safe for use as the product it replaces. This is a consistent statement that any designer and/or manufacturer is obligated to ensure that the product offered for sale does not degrade overall safety through its introduction. For example, a tea pot would not be allowed to be sold if the likelihood of the handle unexpectedly failing in use, potentially severely scalding the user, was greater than that of the average tea pot of the same price and quality. There are generally two exceptions to this rule. If a product provides clear and unambiguous indication of imminent failure in a time frame that allows a user to take reasonable precautions prior to the failure, the concept of risk no greater than existing products may be violated. Many mechanical products provide early warning of wear and subsequent likelihood of failure through their in-service behavior for a lengthy period prior to actual failure. As a result, although the product may have a greater potential to fail than existing products, it is reasonable to expect most users to seek repair prior to actual failure. For example, mechanical mechanisms in steering systems will develop 'play' in the steering control which will progressively increase over time. Actual failure is only likely after a long period of marginal performance, allowing the driver to have the vehicle serviced at a convenient point well in advance of any substantial risk of failure.

Another exception to the rule of 'risk no greater than existing products' is made for products which provide an offsetting advantage that makes the increased risk acceptable. This exception is only reasonable when there is broad societal agreement with the proposed trade off of risk. For example, installation of air bags in automobiles caused a significant increase in the risk of severe injury or fatality for undersized front seat occupants. Some small adults, children and babies in car seats were placed at high risk with the introduction of these devices. However, NHTSA found that the potential life saving effect of air bags on unbelted front seat passengers was sufficiently great as to make air bag installation attractive. Most of the risk was then mitigated through mandating placement of children and infants into rear seats of vehicles. Some small adults remained at risk of injury, but the size of the population at risk was sufficiently smaller than the lives potentially saved by air bags to allow their introduction (1).

Determination of the acceptability of products which provide a tradeoff between risks and rewards is most properly the role of governmental agencies. Due to

liability considerations, it is seldom in the best interest of a product design and manufacturing organization to attempt to place a product for sale that has such a trade off implicit in its design without prior studies and formal trade off and commentary by government agencies.

(1) Modern, advanced air bag designs have largely eliminated the problems with air bag injuries through the use of multiple stages and sensing of seat positions along with more refined sensing of the power needed

In most cases, if a product passes the "safe as existing products" test, it will be consistent with user expectations. Newer products must either behave in ways that are intuitive to the user or must provide sufficient warning of any risk to make users aware prior to being exposed to unexpected levels of risk. Warnings of user behavior that result in an unexpected increase in risk may either be behavioral changes that feed back to the operator (e.g. aircraft controls that vibrate to warn of impending stall), warning lights and messages, or other direct feedback to the operator of the product (or system of which the product is part). Warning labels should be used when needed to warn users of potential risks, but should not be considered a substitute for more direct dynamic warning to the driver. Warning notes which are included in user's manuals or similar instructions or guides should be provided, but should not be expected to serve as the primary method of warning users if other methods are able to be provided.

Throughout the discussions of safety provided thus far, an assumption has been made that there is an understanding of what 'safe' means in practical terms. In fact, one of the most difficult concepts in system safety is how to determine when a product is acceptably safe for public use. There are very few studies and documents which even make an effort to discuss the concept of acceptable risk, and fewer still that approach quantification of acceptable levels of risk. Even so, many products do have risk associated with their use. Among the problems in determining acceptable risk are issues of an individual's perceived control over the risk and the ability to perceive a high risk situation in advance of its occurrence, allowing mitigating actions to be taken. Users will accept a higher risk if they perceive that they have control over the outcome. Acceptance of higher risk when control is perceived seems to be independent of whether or not the control perception is correct in practical terms. As the potential severity of injury rises, the likelihood of occurrence must be increasingly remote (see Figure 2-1). This guidance is fine, in principal, but difficult to apply without quantification. However, some limited numeric guidance is provided by U.S. government practices and the U.K. HSE.

The U.S. military requires acceptance of product safety based on the level of program management signature required to accept identified product risks. [Since many military products, such as ordinance, must be inherently unsafe under some conditions, procedures to accept products with significant potential to cause severe injury or death are necessary.] The signature levels required

are described in Mil-Std-882D (Reference 6). That document uses four categories of hazard severity, with catastrophic being the highest severity – potentially leading to severe injury or death. Catastrophic hazards can be signed for by the Program Manager – the lowest signature level allowed – so long as the rate of exposure does not exceed 1 in 10^6 for a lifetime of usage of the product. This translates to an hourly rate of $\sim 2 \times 10^{-10}$ per hour of use for automotive use and approximately an order of magnitude smaller for heavy goods vehicles. Products with catastrophic hazards with higher rates of exposure require sign off by more senior acquisition managers.

The U.S. FAA, which is charged with certifying transport aircraft for use and which uses certification standards that are recognized world wide, provides some limited indication of the level of acceptable risk for the most severe outcomes in their certification requirements. The Code of Federal Regulations, Title 14, section 25.1309 requires that for electronic systems installed in transport aircraft, “....The airplane systems and associated components, considered separately and in relation to other systems must be designed so that (1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable”. This is then defined by Advisory Circular 25.1309 to be equal to 1×10^{-9} per flight hour. Since such a failure occurrence does not correspond to a 1:1 risk of aircraft accident, this is relatively consistent with the requirements of Mil-Std-882D.

The most definitive statement of what level of risk may be considered broadly acceptable for public use occurs in the U.K. Health and Safety Executive document “Reducing risks, protecting people” (Reference 4). The U.K. HSE considers a risk broadly acceptable for potentially fatal outcomes so long as the yearly risk is equal to or less than 10^{-6} . This equates to a rate of approximately 2×10^{-9} per hour of operation for automotive equipment.

A designer attempting to determine whether or not a specific design is considered broadly acceptable would reasonably be expected to compare the risk caused by his product for severe injury with potential for fatality to the above rates which appear to be generally acceptable within the U.S. and the U.K. It should be considered that these rates apply both to large populations of a product and equally to production batches of a product. Table 2-1 below shows the comparative level of exposure for some commonly accepted risks.

OPPORTUNITY FOR RISK REDUCTION

Vehicle system design engineers and vehicle subsystem developers have a limited ability to reduce the risk associated with roadway use. As discussed earlier in the paper, most collision causes include errors by the human controlling the vehicle. Over seventy percent of

all collisions, both multiple vehicle and single vehicle have one or more driver errors as at least a partial cause. Figure 2-3, below, which has been developed from the data provided in Reference 7, shows the relative frequency of the most prominent human based contribution to causes for collisions. Some of these causes cannot reasonably be attacked by the equipment design community. Others, such as lane keeping, drowsy and oversteering all are potentially subject to improvement through the development and deployment of various driver warning devices and driver aids.

The development of effective driver warning devices and aids requires that the devices be acceptable to the user, sensible for the full range of use environments common to vehicles, and demonstrated as being incapable of imposing new and unacceptable risks to the user and to surrounding roadway traffic. Warning device implementations in hardware and software must be effective enough to ensure that warnings can be depended on to be given when needed yet forgiving enough not to be an annoyance to the driver when engaged in levels of error in behavior that do not represent a substantive risk. For example, it is normal for a vehicle to wander somewhat in lane and to vary speed in response to changes in the roadway incline and curvature. Drivers of automobiles instinctively position themselves as far away as possible without violating lane boundaries when passing larger commercial vehicles. Lane departure warning systems and/or lane guidance systems must allow for such behavior and be designed not to ‘nag’ the driver unnecessarily. Slip control systems must be effective, but must not overreact to minor roadway condition changes that the driver does not expect assistance for. At the same time, these systems must provide warning or assistance before the vehicle is placed into a hazardous situation. An additional constraint placed on the designer of driver warning devices and driver aids is that the devices must be part of a self contained system. Locating all of the sensors and processing for a vehicle on board the vehicle may not be optimum for crowded urban areas where infrastructure support could be developed. Supporting infrastructure is seldom sensible for rural areas. A final constraint on any device intended to reduce collision rates is that it must be shown to be safe enough for use on public roadways.

The amount of improvement which may occur as a result of a new system cannot always be known with precision. Accident investigation is imprecise at best. The data is dirty and cannot always be made otherwise through investigation and/or follow up. For example, at least some of the oversteering and the swerving shown in Figure 3-2 will have been a response to actions by other drivers or to roadway debris. Neither of these causes are able to be influenced by the equipment designer. In addition, some drivers may adapt their driving hazards to take more chances since they are aware that the system is helping them be ‘safe’. As a result, it is crucial that a new system be shown to be adequately safe for public

use prior to deployment. Since the degree of improvement may not be known with accuracy for a considerable period of time, the amount of risk that can be allowed to be introduced by a new system is minimal.

Two major risks occur with respect to the implementation of driver aids that deserve some discussion. Drivers may develop a dependency on the aid which has been provided. Also, the system which is assisting the driver may behave in unexpected or unplanned ways, introducing risk to the vehicle containing the system and to other roadway users.

The introduction of driver warning devices and particularly driver aids into automobiles tends to occur over several years. For automotive systems, devices are initially introduced in high priced luxury automobiles. Over succeeding years, the devices migrate to less expensive automobiles and, once proven over time, into the least expensive vehicles. Heavy goods vehicle safety systems are deployed without this cost sensitivity. During initial installation and use, driver's aids should be designed and tuned to recognize the existing skill set of the driving public. Limited driver skill is not a significant issue for professional drivers of commercial vehicles. As the device penetrates the market and begins to interact with drivers that are familiar with the expected behavior of the system, different 'tuning' to improve device performance may become practical. Over time, and with complete market penetration, drivers may become dependent on the device. As an example, a slip control system provides correction for unwarranted vehicle slip through its ability to develop and control brake pressure at each wheel independently. This is a capability not given to a driver and results in the slip control system being able to maintain positive vehicle control through curves at speeds which are higher than those which can be safely attained by most drivers. If the slip control system is tuned to enhance the driving experience, it is relatively easy for drivers to become dependent upon the device and to incorporate the additional speed margin provided by the device into their normal driving. As a result, if the device goes out of service, the ability of the driver to maintain control of the vehicle under what appears to be normal conditions to the driver may be compromised. This is particularly true for young drivers

that may never have driven without such a device installed. As a result, single thread system design architectures that were appropriate and safe at the time of introduction of a driver aid may become problematic over time.

Driver assist systems (as compared to driver warning systems), of necessity, require that the system be capable of taking control of the vehicle when the system determines that taking control from the driver is appropriate. The reactions required are much faster than those possible for a driver. This results in an opportunity for incorrect control of a vehicle resulting in a collision. If a processor can take control of a vehicle element, such as a brake, or the steering angle, it has the potential to do so improperly, resulting in the driver's aid system becoming a collision cause. It is to this issue that the introduction of a formal safety case is addressed. Well proven solutions to most of the risks are known, but are legacy from aerospace industry. In that industry, using increased recurring costs to minimize non-recurring engineering costs is traditional and cost effective. That approach can be problematic for automotive applications. Thus, a major limitation on the vehicle and vehicle subsystem designer for improving the current collision rates is that a new system must be shown to be adequately safe while meeting the aggressive cost demands of the automotive and heavy goods vehicle marketplaces. A formal safety program, similar to that used for many decades on aerospace and military programs is crucial to minimize the risk of inadvertent deployment of a system with the potential for hazardous behavior.

Activity or Risk Element	Likelihood
Broadly Acceptable Level - FAA - U.S. DOD - U.K. HSE	1*10 ⁻⁹ per flight hour 2* 10 ⁻¹⁰ /hr (Automotive equivalent level) 2* 10 ⁻⁹ /hr (Automotive equivalent level)
Gas Incident (fire, explosion, fatal)	1 in 1,510,000 annual risk
Fatal Road Accident	14.6 in 100,000 annual fatality risk
Rail Travel Accident (fatal)	1 in 1,533,000 passenger journeys
Aircraft Accident	1 in 125,000,000 passenger journeys
Fatal lightning strike	1 in 10,000,000 annual risk in the U.S.
Fatality to Employee On Job	1 in 125,000 annual risk
Canoeing fatality	1 in 750,000 outings
All Types Of Fatal Accidents	1 in 4064 annual risk

Table 2-1. Some Comparative Risks

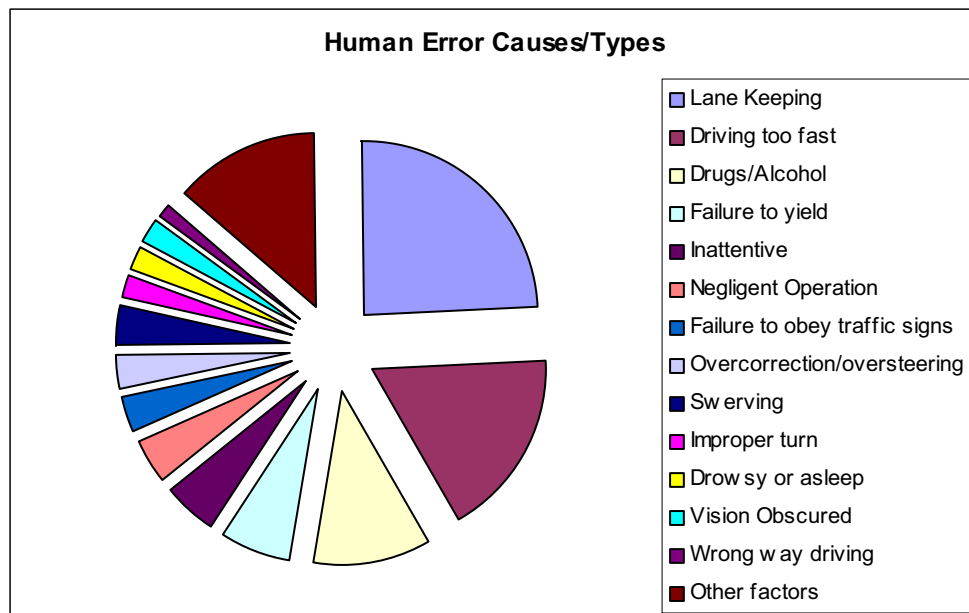


Figure 2-3. Human Error Contribution To Collision Causes

Chapter 3: Design For Safety

Product safety starts with the design process. The design which is developed for a product is, of necessity, driven by the function of the product and by its safety criticality. Vehicle design, particularly for high volume automotive products, requires that a product be adequate for its intended function, safe in normal use, safe under conditions of failure, and cost effective to produce. Having a competitive product for use in vehicles requires that the design minimize recurring costs for the product to the extent possible while still maintaining adequate safety and reliability. The results of the tradeoff between cost and safety drive the safety analyses needed to support the design program.

TRADITIONAL SAFETY APPROACH

Historically, most safety critical vehicle products have been either mechanical or hydraulic. Electronics for basic vehicle functions such as engine control entered vehicle design in the 1970's. Microprocessor based control systems did not become assigned to safety critical systems until the 1990's. As a result, there are traditional and time proven approaches to achieving high reliability and safety from both mechanical and hydraulic products. The design approaches to achieve robustness and ensure safety for electronic products, particularly processing based products, are not as well proven due to complexity and continuously evolving technology. Achieving needed safety with processing based systems requires a careful, measured approach to the design which includes detailed safety analysis. While electronics and processing systems have been used in safety critical applications in aircraft for many decades, the solutions used in those industries are not generally usable for vehicle based products due to recurring cost restrictions.

MECHANICAL PRODUCTS - Mechanical designs tend to fail due to wear. Well designed mechanical products can withstand many times the worst case stress which the product is likely to be exposed to. As a result, sudden failure of mechanical parts during normal service life is unusual and reflects either a lack of understanding of the in-service stress environment during design (design faults), or production errors in the manufacture of the product (production quality faults). Failure of mechanical parts due to wear out is well known. These failures tend to occur late in the product life cycle and often 'telegraph' the potential for failure to the driver well in advance of any physical failure. The basic approach to mechanical products that are critical has always been to design the part so that it can withstand many times the worst case expected stress, precluding sudden failure of the part. As wear in a safety critical part occurs, the vehicle experiences a change in behavior, warning the driver of impending failure. Mechanical elements that are beginning to enter their end of life tend to have

mechanical movement where none should occur, make noise, and sometimes vibrate. This behavior helps make the driver aware of an increased likelihood of failure.

Redundancy of mechanical systems is rare, but not unknown. Federal Motor Vehicle Safety Standards (FMVSS) requires redundancy of some systems. For example, multiple automatic return mechanisms must be a part of a throttle system to meet FMVSS 124 requirements. However, mechanical redundancy, except in response to regulatory requirements is rare. The more common approach to ensuring mechanical system adequacy has been to design for high reliability of individual components.

HYDRAULIC PRODUCTS - Hydraulic designs for safety critical products have used approaches which are similar to those used for mechanical products. Design elements are sized to ensure survival at many times any expected worst case stress. Seals are more robust than minimum requirements to help assure survival in service. Seals are sometimes provided in redundant pairs, ensuring that two seal failures must occur prior to any leakage.

Driver's are depended upon to help prevent safety critical failures due to hydraulic product problems. Changes in behavior may be evident to the driver, resulting in an unscheduled maintenance event. Fluid levels in reservoirs may be reduced, which can be noticed during routine, scheduled, maintenance. Fluid leakage, the most common precursor of major failure of a hydraulic system, may cause noticeable fluid spots on driveways or under the vehicle in which the product has been installed. Most hydraulic fluid has a distinctive smell which can be detected by drivers if leakage is occurring in the engine compartment. As a result, most hydraulic failures can be detected and managed prior to having a safety critical effect.

As with mechanical single thread designs, safety of the design for most hydraulic products can be addressed with carefully performed FMEAs and design verification tests. A formal safety program with a large suite of analyses to evaluate the design is not needed.

NON PROCESSING ELECTRONIC PRODUCTS - Prior to the 1990's electronic designs were employed in functions that allow abrupt failure of the product to occur without resulting in a safety critical outcome. A significant percentage of the electronic products in vehicles is used in entertainment, security, comfort and convenience systems. Some electronic designs, although used in vehicle critical functions such as engine and pollution control, cannot cause an immediate safety critical effect upon failure. For those non processing based electronic systems employed in safety critical systems, a mechanical or hydraulic system remains in place that can provide continued, albeit reduced

capability, service in case of unexpected electronic failure. In addition to alternate technology backup systems for those non processing based electronic systems which have safety critical functions, high reliability is attained through electrical and thermal stress reduction. However, unlike mechanical and hydraulic systems, electronic products seldom fail gracefully. As a result, advanced warning to the driver of impending failure is difficult or impossible.

Similar to mechanical and hydraulic product designs, safety engineering can adequately support single thread electronic product designs using FMEAs and extensive design verification tests. In addition to the traditional life and environmental tests, the abrupt nature of failures in electronic components mandates the addition of fault insertion testing to validate that failures cannot result in unsafe vehicle behavior. However, the use of processing based electronic systems results in the introduction of unexpected risks. Processing systems invoke active control that is based on sensed conditions of use. As a result, these systems can have the potential to introduce active failures that mechanical, hydraulic, and non-processing based electronics could not cause.

EFFECTIVENESS

Both mechanical and hydraulic products are proven to provide adequate safety characteristics in vehicle products. The combination of gradual failure based on wear and changes in behavior of the vehicle prior to any safety critical event have been effective. Driver's are warned in advance of most safety critical failures and are able to inspect the vehicle and to have the vehicle maintained prior to a safety incident occurring. In part, this is because the causes of mechanical and hydraulic failures are well understood. Also, because failures tend to be gradual, drivers have sufficient time and skills to mitigate undesirable behavior. Maintenance of vehicles, although problematic, is not a significant cause of safety critical behavior even when performed by marginally skilled individuals. Incorrect replacement parts, which are physically identical or nearly so and also fit the mounting locations for the original part, are unlikely even when obtained through salvage facilities.

The effectiveness of traditional approaches to mechanical and hydraulic design for safety critical products is reflected in their contribution to collision rates. National highway statistics and previous studies of accidents indicate that mechanical failures, including hydraulic systems, are responsible for less than five percent of all collisions (see references 2 and 7). Many of those failures may be at least partially caused by vehicle owners not performing required servicing or ignoring evidence of imminent failure. Use of electronic products in safety critical functions, particularly the use of processing systems, introduces new failure modes and abrupt failures which may have the potential to raise the overall contribution of vehicle hardware based collisions to the national statistics.

PROCESSING BASED CONTROL SYSTEMS

The introduction of processing based control system electronics into vehicles has resulted in improvements in vehicle performance, handling, and capability, while supporting the driver and helping maintain vehicle control under difficult conditions. The introduction of these systems also introduces some new and potentially significant safety issues. Helping design teams ensure that the newly introduced risks of these systems do not outweigh the benefits should be the primary goal of an effective safety program.

The introduction of processing electronics to vehicle designs has allowed improved monitoring of some mechanical and hydraulic systems, for example brake fluid levels are routinely monitored and a low level signaled to the driver well in advance of any possible loss of braking capability. Processing systems also allow compensation of mechanical system wear. Electronic ignitions routinely maintain correct engine timing and performance although the distributor, the gear drive to the distributor, and the timing chain undergo wear and increased tolerance over time. When compared to vehicles prior to the introduction of electronic ignition, the decrease in needed vehicle maintenance is substantial.

The most important contribution of processing based electronics has been in the area of improving driver control capability. Driver capability and control is a major issue in vehicle and traffic safety. A driver directly or indirectly contributes to the cause of greater than 70% and possibly over 90% of all traffic collisions (reference 2). As a result, improving driver control capability has more potential for reducing the number of collisions than any other collision cause. Control systems for braking now provide ABS on most vehicles sold, improving the ability of many drivers to control vehicles on low traction surfaces. Slip control systems, now widely available and soon mandatory on all new automotive vehicles, help a driver maintain vehicle control under conditions where a substantial number of drivers would not be capable of regaining vehicle control. Steering assist systems, lane departure warning systems, and vision systems to help detect animals and pedestrians under adverse lighting conditions, systems that monitor behind a vehicle for cyclists, pedestrians, and objects, and collision avoidance systems are currently available on some vehicles and are extending driver capability, potentially reducing collision rates.

Processing systems, to be effective at their assigned functionality of improving driver performance, must be given control authority over safety critical vehicle systems. To be effective in applying slip control, the assigned processor must have full authority over the vehicle's braking at each wheel. As a result, a potential hazard of braking one or more wheels unexpectedly is introduced. Similar risks are introduced with other processing systems in safety critical functions.

The risk of these products to behave under failure conditions in ways that result in a vehicle hazard is a function of the design approach taken. Assuring that a product cannot exercise control incorrectly when failures occur requires that additional complexity be added to the design. The intent of the increased complexity is to provide assurance of safe behavior. Figures 3-1 through 3-6, below present a set of potential conceptual approaches to processing system design. These figures represent a small subset of the possible variations in processing design that are possible. Below each of the figures is a brief presentation of where the technique would be appropriately used, the costs associated with the approach, the effectiveness of the approach at assuring safety, the impact on the driver, and the impact on the safety program of the approach. As the complexity of the design approach increases, the sophistication of the safety analyses that are used to evaluate the design must also increase. The safety program, and in particular the safety design analyses discussed in this paper are appropriate for the approaches shown as Figures 3-2 through 3-5. True redundancy, with its requirements for coordination between processors and the detailed interchange of information required to assure real-time switchover requires additional safety analysis measures. At the time of preparation of this paper, redundancy with real time recovery has not been introduced into production vehicles. However, once steer by wire and brake by wire systems begin to be deployed, redundancy with real time recovery will be necessary.

The figures outline the fault detection, protection, and recovery approaches for the processing element only. Self testing and or replication of sensors and of actuators may be needed depending on the system being designed. Fault handling approaches for sensors and actuators are not shown in the figures.

SINGLE PROCESSOR WITHOUT DIAGNOSTICS - Figure 3-1 shows the approach of using a single processor (or multiple processors, each with unique and non-overlapping functions) to provide control of one or more actuators. The processor(s) takes its input from the sensors, processes that information and drives one or more actuators to a desired state or position. Diagnostics are either not present or are minimum. In most cases of failure, the driver notices that the services being provided are inoperative. If incorrect behavior is driven by the single thread processing, the driver is expected to compensate for that behavior.

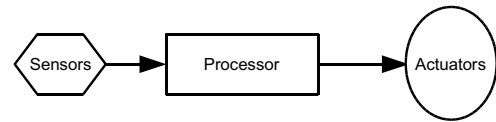


Figure 3-1. Single Processor Without Diagnostics

Use - This type of approach is used for applications where erroneous behavior of the actuators either causes no safety related effect or the effect is so mild as to ensure that almost all drivers can easily provide any needed corrections.

Cost - The cost of this approach is very low. No replication of processing hardware is needed. No additional hardware is needed for diagnostic functionality. Very little, if any, processing throughput and memory are used by diagnostics and any other non-function related code.

Effectiveness - The effectiveness of this approach in providing safety assurance is very limited. This type of processing approach should be reserved for functions that are not safety critical.

Impact On Driver - The driver is the primary detection mechanism for failures in this approach, although limited warning through the driver information system may be available due to loss of signal. Loss of service resulting in changes in vehicle performance are expected to be apparent to the driver.

Example Systems - Entertainment electronics and climate control.

Impact On Safety Program - The safety design analysis needed to support this type of system is minimal, usually limited to FMEAs and possibly fault insertion tests.

SINGLE PROCESSOR WITH SELF DIAGNOSIS - Figure 3-2 shows the approach of using a single processor (or multiple processors, each with unique and non-overlapping functions) to provide control of one or more actuators. Unlike the approach shown in Figure 3-1, the processor(s) have extensive diagnostic routines that identify processing failures and both attempt to shut the processor off directly and through an independent shut down path. As with the approach of Figure 3-1, the processor(s) takes its input from the sensors, processes that information and drives one or more actuators to a desired state or position. Diagnostics are also being run with a periodicity that precludes unsafe vehicle level behavior under conditions of product failure. The intent of this type of system is to ensure that the system achieves loss of service in all failure cases.

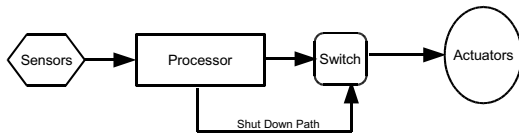


Figure C.2. Single Processor With Self Diagnosis

Use - This type of approach is used for applications where errors in service cause unacceptable safety risks, but loss of service can occur without significant safety implications. For those failures which do not immediately cause loss of service, the system is designed to detect the faults and allow the system to revert to its safe, non-operational state. The service being provided by the system must allow sufficient latency between the occurrence of any fault and erroneous vehicle level behavior to allow detection and shut down without unacceptable false alarm rates.

Cost - The cost of this approach is low to moderate. Extensive self checking can use a considerable amount of processing throughput and memory capacity, mandating a larger processor size than required by the approach of Figure 3-1. Throughput costs as high as 40% are not unheard of. There will also be increase testing costs for this approach. Each and every diagnostic path will need to be verified through extensive fault insertion testing.

Effectiveness - The effectiveness of this approach in providing safety assurance is a function of the effectiveness of the diagnostic set. This approach can achieve very high fault detection percentages, given enough of the processor throughput for diagnostics. This type of processing approach should be reserved for functions that can have complete loss of processing function without causing a safety incident.

Impact On Driver - The driver is usually notified via the driver information system for all failures. That warning may or may not be sufficient to allow the driver to continue to use the vehicle. However, the approach should only be applied to systems where the driver remains in control after system shut down.

Example Systems - ABS systems. slip control systems. steering assist systems. lane departure warning systems.

Impact On Safety Program - The safety design analysis needed to support this type of system is substantial. The safety program and the related analysis discussed in the remainder of this paper are appropriate.

SMART EXTERNAL WATCH DOG - Figure 3-3 shows a processing approach which includes both internal processor diagnostics and an intelligent external watchdog that trades information with the processor. The watch dog is used to lower the amount of processor

throughput which must be sacrificed to run adequate diagnostics on a single processor, safety critical, system. The intelligent watch dog may be a custom ASIC or another small processor. The main processor continuously feeds the results of a complex, continuously changing, calculation to the smart watch dog, validating the ability of the processor to accurately produce results. In case of errors, either the processor or the intelligent watch dog can shut down the circuit using independent shut down mechanisms.

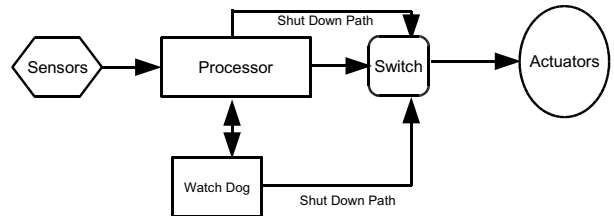


Figure 3-3. Single Processor With Smart External Watch Dog

Use - As is true of the single processor with extensive self testing, this type of approach is used for applications where errors in service cause unacceptable safety risks, but loss of service can occur without significant safety implications. For those failures which do not immediately cause loss of service, the system is designed to detect the faults and allow the system to revert to its safe, non-operational state. With the inclusion of a smart watch dog circuit, often implemented as a custom ASIC, the processor throughput demands can be significantly reduced. Also, since the processor is no longer depending on being able to shut down erroneous service using a failed device (itself), confidence in the ability of the system to achieve shut down is increased. The service being provided by the system must allow sufficient latency between the occurrence of any fault and erroneous vehicle level behavior to allow detection and shut down without unacceptable false alarm rates.

Cost - The intelligent watch dog is often implemented as an ASIC which raises hardware recurring cost. In some cases, the size of the processor required is reduced when compared to the approach shown in Figure 3-2, but still larger than that of the approach of Figure 3-1. Complexity of the processor self test can be somewhat simplified when compared to approaches which depend entirely on the processor to check itself, marginally reducing non-recurring software development costs. The shut down circuit, shown in Figure 3-3 as a switch will need to be independent from the processor, potentially adding recurring hardware costs.

Effectiveness - The effectiveness of this approach is dependent on the care with which the diagnostic approach is designed. This type of system is based on a combination of processor self diagnosis and the effectiveness of the watch dog circuit in confirming processor accuracy. Done correctly, this approach can

achieve safety in-service that is adequate for critical circuitry.

Impact On Driver - The driver is usually notified via the driver information system for all failures. That warning may or may not be sufficient to allow the driver to continue to use the vehicle. However, the approach should only be applied to systems where the driver remains in control after system shut down.

Example Systems - Electronic power steering systems, slip control systems.

Impact On Safety Program - The safety design analysis needed to support this type of system is substantial. The safety program and the related analysis discussed in the remainder of this paper are appropriate.

SAFETY BAG PROCESSOR - Figure 3-4 shows a processing approach which includes both primary processing path and a second processor, generally of smaller capability, that independently reads from the sensors and calculates an approximation of the appropriate control parameters. This calculation is then used to check the calculations by the primary processing path. If the results are sufficiently similar (allowing for latencies from independent sensor input), then the switch remains enabled and the output of the primary processing controls the actuator(s). Either the primary or the safety 'bag' processor can shut down the processing output, resulting in loss of service. This helps ensure that errors anywhere in the primary processing path are detected and erroneous output precluded.

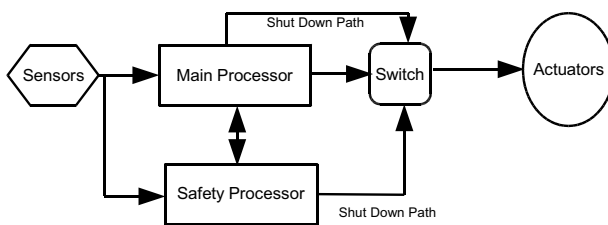


Figure 3-4. Single Processor With Safety Bag Processor

Use - As is true of the single processor with extensive self testing and the intelligent watch dog approaches, this type of processing implementation is used for applications where errors in service cause unacceptable safety risks, but loss of service can occur without significant safety implications. For those failures which do not immediately cause loss of service, the system is designed to detect the faults and allow the system to revert to its safe, non-operational state. With the inclusion of the safety processor, an improvement in diagnostic capability over a smart watch dog circuit, can be realized. The service being provided by the system must allow sufficient time between the occurrence of any

fault and erroneous vehicle level behavior to allow detection and shut down without unacceptable false alarm rates.

Cost - The hardware recurring cost of this approach is greater than with a single, self checking, processor. However, the non-recurring engineering costs are less. Using two processors allows much of the diagnostic resource demand to be provided by the comparison process. This eliminates the need for extensive diagnostic software that must run in the primary processor, reducing the costs of software development and testing. The hardware recurring costs of this approach may or may not be higher than with an ASIC based intelligent watch dog circuit. The difference in cost is often dependent on the production volume expected. As very high volumes are produced, the costs associated with using an ASIC tend to be reduced. The cost is also sensitive to the size of the safety processor necessary to implant the independent processing check path.

Effectiveness - This approach can be extremely effective in ensuring the health of the processor is accurately known and that shut down can be effectively achieved. Achieving the potential effectiveness of this approach is dependent on careful design of the processing checks between the two processors.

Impact On Driver - The driver is usually notified via the driver information system for all failures. That warning may or may not be sufficient to allow the driver to continue to use the vehicle. However, the approach should only be applied to systems where the driver remains in control after system shut down.

Example Systems - Electronic power steering, slip control systems, lane keeping systems,

Impact On Safety Program The safety design analysis needed to support this type of system is substantial. The safety program and the related analysis discussed in the remainder of this paper are appropriate.

REPLICATED PROCESSING - Figure 3-5 shows a processing approach which includes both primary processing path and a duplicate secondary processing path. Both processors read the sensors independently and calculate the appropriate control parameters. If latency is allowed for in the comparison process, then the comparison is successful if the two calculated values are within a predetermined tolerance of each other. When latency is not allowed, the processing is clocked using a common (or coordinated) source and the outputs are expected to be identical for comparison to be successful. Either processor can independently shut down the processing output. The comparator stops any output that fails comparison.

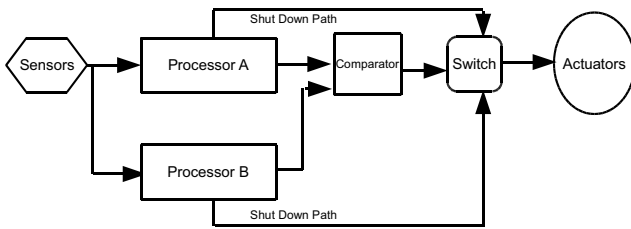


Figure 3-5 Replicated Processing

Use - Replicated processing with both processors completely calculating the processing and comparison of results being the criteria for allowing control is a way of ensuring that there is no possibility of erroneous control being exercised for any period of time. Most automotive processing that allows for loss of function has some allowable latent time during which erroneous control can be permitted. Such systems do not need a real time, lock step, comparison process. However, if no erroneous latency is permissible, for example in an passenger protection system deploying air bags, this type of processing can be effective.

Cost - The recurring hardware cost of this approach is high, with a two same size processors being demanded. However, the non-recurring cost of developing extensive diagnostics is significantly reduced. There is also a cost for this approach in false alarm rates.

Effectiveness - This approach is extremely effective in ensuring against erroneous control outputs, particularly when the fault detection time that can be allowed is at or near zero.

Impact On Driver - The driver is usually notified via the driver information system for all failures. That warning may or may not be sufficient to allow the driver to continue to use the vehicle. However, the approach should only be applied to systems where the driver remains in control after system shut down.

Impact On Safety Program - The safety design analysis needed to support this type of system is substantial. The safety program and the related analysis discussed in the remainder of this paper are appropriate.

REDUNDANT NON-STOP PROCESSING - Figure 3-6 shows a processing approach which includes multiple processing paths. In practice, this type of approach is intended for situations that require non-stop processing. The processors execute in lock step, with a comparison of the outputs. If a processor failure occurs, the remaining processors should agree with each other and be divergent from the defective processor. The comparator then blocks the output of that processor and sends it into a reset and extensive self test. If the erroneous processor fails its self test, it is declared defective, and appropriate warnings sent. If the erroneous processor successfully completes its self test,

it is allowed to resynchronize and attempt to rejoin the processing. After a predetermined number of failed attempts to rejoin the processing, it is permanently marked defective. Only outputs which successfully complete the comparison process drive the actuator(s).

Use - This type of approach is reserved for cases where a loss of function is unacceptable.

Cost - Cost is very high due to multiple replicated processors. Three processors is a minimum to allow conflict between the processors to be resolved.

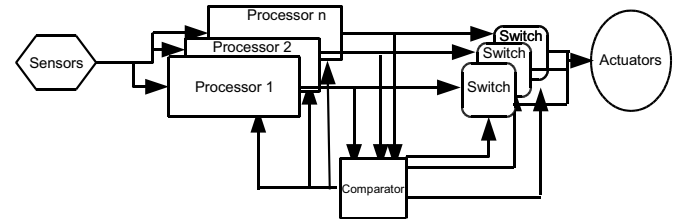


Figure 3-6. Redundant Non-Stop Processing

However, for specific low volume applications (as are commonly found in Aerospace), the savings in non-recurring engineering are sufficiently great to justify using the approach. There is sometimes vulnerability to transient faults if care is not used in implementing this approach.

Effectiveness - This approach is effective at eliminating any possibility of erroneous control while ensuring against loss of service.

Impact On Driver - The driver never sees a change in vehicle level performance under conditions of failure. Illumination of a warning lamp or message may be the only way the driver knows that system service is needed..

Example Systems - Steer by wire, brake by wire

Impact On Safety Program - This approach can have a major impact on the safety program. An expansion on the safety analyses discussed in this paper is advisable. In particular, full sneak circuit analysis, detailed modeling, and extensive fault injection testing may be appropriate. Extensive environmental testing to ensure behavior beyond specified environmental limits – temperature, EMI, water immersion, etc will also be needed.

SAFETY PROGRAM SCOPE

The processing design for an embedded processing system must be carefully considered when designing a safety program to support product development. For products that will have minimal safety impact in service, simple processing designs and safety programs may be adequate. As the potential safety impact of a product increases, the processing approach must become more complex along with the safety program to support

development of the product. The discussion of safety program and the various parts of a safety program provided in the remainder of this paper focus on designs using the approaches shown in Figures 3-2 through 3-5. A replicated processing with real-time recovery as shown in Figure 3-6, while used in some safety critical applications, has not yet appeared in the

vehicle design arena. As control by wire techniques advance, this type of processing approach will allow removal of considerable mechanical and/or hydraulic hardware, providing savings in cost and in weight. The safety program to support such systems will need to be an extension of those elements discussed in this paper.

Chapter 4: Safety Program Overview

Ensuring the design of safety critical products, particularly those including processing elements and software, requires that a formal approach to safety be adopted. The formal approach which has been used previously in aerospace and medical products has been adapted to automotive needs and is becoming widely accepted. Safety programs to support development of driver's aids for heavy goods vehicles are less common. However, formal verification of safety prior to deployment on heavy goods vehicles is more important than for automobiles due to the larger vehicle sizes and the greater kinetic energy.

Automotive and heavy goods vehicles have always included many elements that are safety critical. Wheels must stay attached, tires must survive poorly maintained roadways, steering must survive under a high stress and shock environment. Other safety critical vehicle elements must survive equally well under a harsh environment. Most of the safety critical products that make up a vehicle are mechanical and/or hydraulic. The engineering principles behind these devices are well known and proven. Design methods to ensure against failure under worst case stress are known and have been used in vehicle designs for many decades. As a result, safety is ensured by judicious over design to preclude failure of these devices. The approach that is taken is one of evolutionary design, proceeding from current designs to next generation designs as a series of small, verifiable changes. A formal safety program is not needed to ensure the safety of the various mechanical and hydraulic elements making up a vehicle so long as reasonable care is used in the design process.

Electronic devices in general and processing devices in particular are not well proven and cannot be subjected to evolutionary development. New components and technology enter the electronics marketplace on a continuous basis. Older components and technologies are declared obsolete and are no longer available. Additionally, each new processing device mandates changes to any existing software to adapt the software to the specifics of the new device. Some software reuse occurs, but not always with the certainty of performance needed for safety critical elements. Much of the software in each new, safety critical, processing element is newly developed. Additionally, reused software is exposed to an environment unique to the specifics of the vehicle, making it vulnerable to unexpected errors in performance. The introduction of any safety critical electronic and/or processing device or software should include a formal safety approach that seeks to identify the risks inherent in the design, the protection against those risks provided by the design approach taken, and the residual risks of the design. Without such a formal approach, it is virtually impossible to determine whether or not a product is appropriate for its intended use.

Testing to show that the given design meets the needed safety critical event avoidance is not practical as the time required would delay product introduction by many years due to the small probabilities being verified.

A formal safety program consists of a series of well defined steps – planning, hazard identification, safety requirements derivation, design analysis, validation, and documentation of the results of the safety program in a formal safety case document. The purpose of the safety program and resultant safety case can be stated as.

“A safety case consists of the performance of, and documentation of, a set of analyses and tests designed to identify potential hazards, establish requirements for their avoidance, verify that the design of the product prevents the occurrence of the identified hazards or limits their occurrence to an acceptable likelihood, and documents evidence that the product is appropriate for its intended use.”

The first step in the safety program is the development of a tailored plan that seeks to focus safety engineering and design engineering resources on a set of analyses that is appropriate to the design in question and is likely to produce value added assessment of the design. Generally, a safety program is common to the product types and culture of the company doing the design, allowing a basic plan to form the basis for tailored planning for specific product(s). Tailoring of the executed safety case to the criticality of the product and the specifics of the product type is then accomplished by additions to and exceptions to the published basic plan. Figure 4-1, below shows the basic flow of a formal safety program with documentation of the safety case itself as the final output of the safety program.

Beginning with the master plan, the size and scope of each of the steps in the safety case development is tailored to the product specifics. Following establishment of the program, the initial activity is determining what hazards might be possible given the product being developed. Once the hazards have been identified and quantified, the required risk avoidance for each potential hazard is determined. Safety requirements, consistent with the needed avoidance of the identified hazards, are then developed and imposed on the design. These initial activities need to occur very early in a design program, ideally during early conceptual design. Early identification of the hazards, the hazard avoidance required, and the appropriate requirements to support such hazard avoidance allows safety to be incorporated into the design of the product. This also ensures that any needed changes to candidate designs are able to be accomplished with minimum cost and schedule impact. Performance of these early safety program tasks once there is an existing product design leads to the

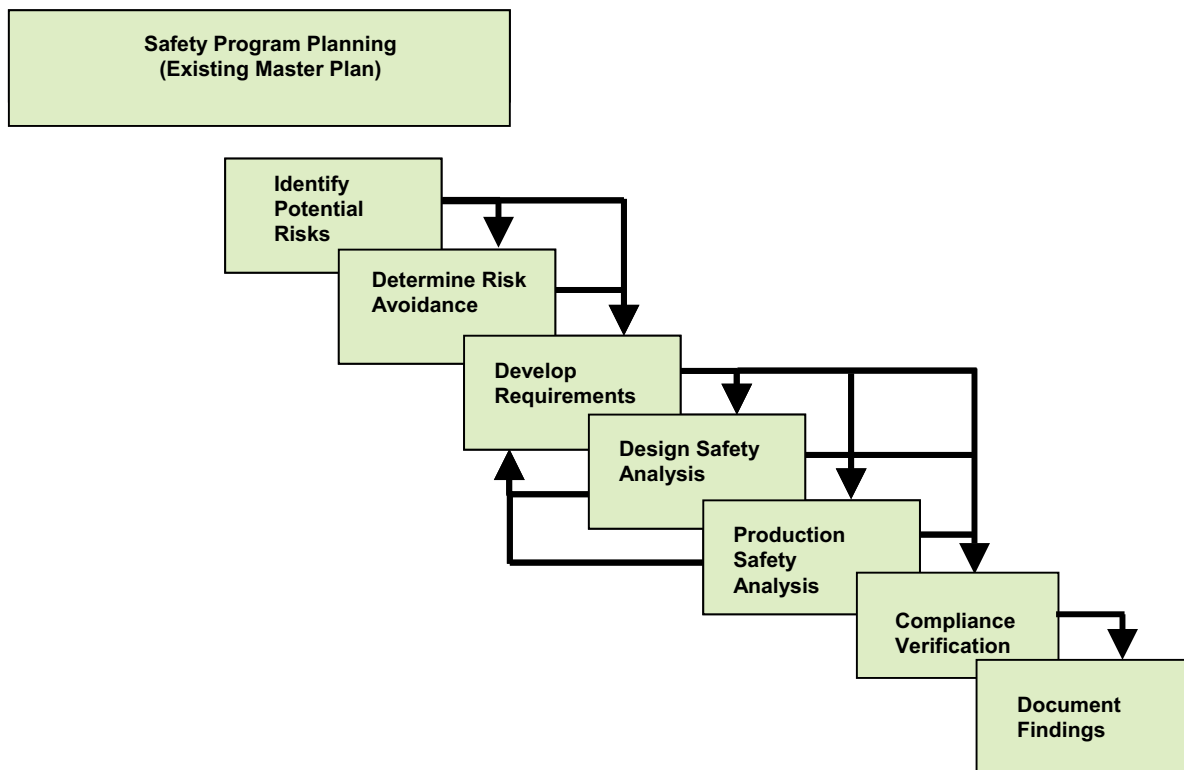


Figure 4-1. Safety Program Flow

problematic. If discrepancies between the needed hazard avoidance and the actual design are identified, changes tend to be expensive and resistance to change by the design team may be an issue.

Once the early safety program tasks have been completed and safety requirements are available to the product design team, analysis of the various candidate product designs can be undertaken. Safety analysts should be involved in the various trade-offs required to establish an effective system design, helping drive the design toward compliance with the required hazard avoidance. Once the system design is established, analysis of the detailed implementation of that design is undertaken. As with the system analyses, the intent of detailed design analyses should be to ensure that the design fully supports the needed safety characteristics as it develops. This helps minimize the cost of achieving the desired safety characteristics.

Once design analysis has shown that the product, as designed, is capable of achieving the required hazard avoidance, the safety analysts need to review the production planning and process to help identify any production actions which might compromise the designed in safety of the product. It is a crucial step in the process of achieving adequate product safety to review the production process. There may be critical items that have been identified for careful production inspection, handling, or control. The safety engineer should review each drawing and production process step to ensure that any mandated controls have, in fact, been recognized and integrated into the production process. In addition to review of the drawing set and the production process, a process FMEA should be performed by the product's manufacturing engineering staff. Safety specialists should review the results of the process FMEA for any potential compromise of designed in product safety. Where potential safety product issues arise in the production process, specific steps to correct such issues should be documented by the assigned safety engineer and followed up with manufacturing engineering.

Once all of the necessary analysis has been completed, the results of the safety effort should be documented and the results, including any residual risk associated with the product, should be presented to the design team and to senior management at the company developing the product. Documentation of analysis results in a formal safety case has several advantages, among them are partial reuse of analysis products on similar equipment to minimize cost, a basis for any required residual risk discussions with the customer for the product, a means of communicating product risk to company senior management, and as a documented set of analyses which may be used to legally defend the design, should such a defense become necessary. Two types of documentation are produced at this late stage of a safety program. The first of these is a cross reference between the safety requirements imposed on the design early in the safety and design programs and the documentation (analyses, tests, etc) which provide evidence that the design either meets the stated safety requirements or provides the rationale for why such compliance is inappropriate. The second document is the safety case document. The safety case document should provide full discussion of the findings of the safety program and any residual safety risk for the product. It is a common

practice to require that the safety case document be signed by one or more senior managers, documenting that they have been made aware of the findings of the safety program.

Each of the various safety case steps has specific requirements and produces documentation. The specific documentation produced is discussed in the sections which follow, along with the content of the documentation. It is good practice to make the documented analyses attachments to or appendices of the safety case document, ensuring that the analyses upon which the safety case is based are retrievable when needed.

Chapter 5: Establishing System Hazards

The first analysis task required in an effective safety program is to identify all of the potential hazards for the system. Identification of these hazards allows the remainder of the safety program to work on establishing requirements to avoid the hazards and ensuring that those requirements are achieved. Identification of hazards is not based on the product's design and should be done prior to the beginning of or concurrent with the development of the design concepts to be used for the product. The hazards identified for the product should be based on a combination of hazardous behavior exhibited by similar existing systems, standard lists of product hazards and risks, and careful and methodical examination of the potential for hazard created by the product's functions and span of control. The design of the product itself must not be used as the basis for establishing the hazards. To do so risks embedding assumptions in the hazard list which may not be valid later, possibly resulting in omission of a hazard.

HAZARDS FROM PREVIOUS SYSTEMS

An initial step in identifying potential hazards is to research available data to determine what hazardous behavior may have been exhibited by previous products that are the same or similar to the product being designed. The review of data should include, but not be limited to, publicly available sources. There may be data which is kept within the company developing the product on field returns, recalls, and warranty claims for previous generations of the product or on similar products previously developed by the company. Access to this type of data, if it exists, is crucial. Actual field deployment of a product exposes the design to environments and use conditions that are difficult, if not impossible, to recognize during the development phase. A thorough examination of the company's available field data, including corrective design actions which may have been caused by knowledge gained from use, is appropriate.

An additional benefit of accessing existing company field data is that knowledge of previous history can allow the safety program to be tailored to place emphasis on those areas where design errors have occurred previously. For products intended for use on-board vehicles, errors in the designs which result in safety related events in service can result in product recalls. Recalls are time consuming, inordinately expensive, and harmful to the company's reputation. Focusing the safety program in ways that help minimize the likelihood of a recall event is an excellent way to garner senior management support for the safety effort.

Along with the company data, publicly available data should be reviewed. Data bases on recalls and on complaints are collected and made available over the

internet by the National Highway Transportation Safety Administration (NHTSA). It is possible to access these data bases without cost as well as data bases on traffic statistics, summaries of those statistics, and numerous U.S. Department of Transportation reports which provide analysis of the statistics and research of interest. Anyone who is involved in or interested in the safety of vehicles and vehicle based products would be well served by spending a substantial amount of time reviewing the information available on and through the DOT and NHTSA web sites.

In addition to company and publicly available data sources, the literature on safety related to transportation should be reviewed regularly. Sometimes, researchers have access to data that is not generally available and provide some of that data in technical papers. These papers are published in symposia proceedings, technical journals, reports issued by DOT, and by the various universities which do transportation related research. University of California and University of Michigan have particularly large transportation research communities. Many of their published research findings are available through their web sites.

An additional source of potential hazards is available as standardized lists of hazards which have been published in the literature and in various texts on safety. These hazards are generally limited to physical hazards such as cuts, burns, high voltage, and similar concerns. These hazards apply to almost every electronic product whether or not the product is safety critical in its operation.

Table 5-1, below provides a partial listing of some of the more prominent data sources for identifying hazardous behavior that may have occurred with previous generation or with similar products to the one being designed.

In addition to the hazards identified through research of company data bases, the span of control of, and the functions provided by, the product being considered must be assessed for potential hazards. The approach to identifying hazards based on span of control is that if a system has authority (full or limited) over a part of the vehicle, it can exercise that control in an unexpected and potentially unsafe manner. For example, if a system has authority over the steering position, it could unexpectedly steer the vehicle. The same system might also incorrectly follow commands and erroneously position the steering, reverse the steering applied, perform erratically, or be difficult for a driver to control.

The intent of identifying hazards is not to identify hazards which do exist as a function of the product design. Instead, an assumption of malicious behavior is

Data Source	Data	Contents
U.S. NHTSA	Recall Data Bases Traffic Facts by Year General Estimates System Fatal Accident Reporting System DOT Studies On Accident Causes Special Crash Investigation Data	Hazards Caused By Fielded Products Summarized accident causes All outcome accident data Fatal accident data Assessment by researchers of accident causes Information on new technology performance
U.K. Department For Transport	Traffic Statistics	Similar to NHTSA data, but less complete
U.S. NTIS	Study reports on traffic statistics, accident causes, human factors (older studies, modest cost to access)	Varies by study. Many of the older studies include assessment of information that may not be otherwise available.
University Research Centers	Studies and research into traffic accident causes by automobiles and heavy goods vehicles	Varies by university focus and by the study and researcher. Some of the most valuable research into underlying accident causes and human response are in the university studies.
Company Internal Data Bases	Actual field performance of earlier generation products and/or similar products.	Can be the most valuable of all of the data bases as it reflects the experience of the manufacturer with a focus often on the exact product type of interest.

Table 5-1 Hazard Identification Data Resources

made. It is assumed that if some version of the product could be designed that might have the ability to behave erroneously, then a potential hazard exists. The intent of requirements and then to show that the design has managed to avoid any substantive risk of the potential hazard.

One of the common errors made by those that are new to system safety is to use the product's design or design concept in deciding what hazards to place on the hazard list. What is needed is a listing of potential hazards that may or may not be precluded by the design approach and implementation that results. The hazard list that is used to drive all remaining safety activity must be complete to ensure that no potential hazard is overlooked. It is very easy to make the mistake of looking at the existing design and deciding that a specific hazard cannot occur for that design. Later, when sufficient changes have occurred in the design, the hazard is not a part of the hazard listing resulting in protection against the hazard's occurrence not being provided.

IDENTIFYING FUNCTIONAL BASED HAZARDS

The most common approach to determination of the span of control and of the function based hazards is to perform a Hazard and Operability Analysis (HAZOP) on the system and its functions. To perform a HAZOP, a standard series of steps is taken to arrive at a formal assessment of the possible hazards.

the remainder of the safety program is to ensure against each hazard by imposing necessary and sufficient

1. The system to be subjected to the HAZOP is defined. This should be done on the basis of the top level specification for the product, *not* the actual product design. Identification of the boundaries (input, output, span of control) to be considered is necessary before the beginning of any analysis.
2. Complete any planning needed for the analysis, including how the analysis will be subdivided for larger systems and exactly what will be considered. The data needed to support performing the HAZOP should be collected as a part of the planning.
3. Decide on the team needed to perform the analysis. As with FMEAs, a HAZOP is best performed using a team of engineers. This helps ensure that potential hazards are not missed. For some relatively simple systems, the analysis can be successfully performed by a single analyst with review by other design team members to help assure completeness.
4. Perform the HAZOP by assessing the impact on each function and/or function set and control element of a set of guide words – no, more, less, reverse, ...
5. Document the HAZOP in a set of HAZOP sheets (see Figure 5-1, below).
6. Extract a list of hazards from the analysis for use as potential hazards for the products.