SAE TECHNICAL PAPER SERIES

2001-01-0674

A Comprehensive Hazard Analysis Technique for Safety-Critical Automotive Systems

Sanket Amberkar, Barbara J. Czerny, Joseph G. D'Ambrosio,
Jon D. Demerly and Brian T. Murray
Delphi Automotive Systems

The Engineering Society For Advancing Mobility Land Sea Air and Space®
INTERNATIONAL

SAE 2001 World Congress
Detroit, Michigan
March 5-8, 2001

400 Commonwealth Drive, Warrendale, PA 15096-0001 U.S.A. Tel: (724) 776-4841 Fax: (724) 776-5760

ISSN 0148-7191

Printed in USA

2001-01-0674

A Comprehensive Hazard Analysis Technique for Safety-Critical Automotive Systems

Sanket Amberkar, Barbara J. Czerny, Joseph G. D'Ambrosio, Jon D. Demerly and Brian T. Murray
Delphi Automotive Systems

ABSTRACT

Hazard analysis plays an important role in the development of safety-critical systems. Hazard analysis techniques have been used in the development of conventional automotive systems. However, as future automotive systems become more sophisticated in functionality, design, and applied technology, the need for a more comprehensive hazard analysis approach has arisen.

In this paper, we describe a comprehensive hazard analysis approach for system safety programs. This comprehensive approach involves applying a number of hazard analysis techniques and then integrating their results. This comprehensive approach attempts to overcome the narrower scope of individual techniques while obtaining the benefits of all of them.

INTRODUCTION

Rapid advances in automotive electronics have fueled an ever-increasing number of new features within vehicles. In many cases, these are new entertainment or driver information features [1], in other cases, advanced control systems for powertrain or chassis. In addition to new features, there is a trend toward the integration of the functions, systems, and technologies that implement them. These new systems will permit unprecedented increases in driver and passenger safety as well as comfort and convenience, however, their complexity is higher than previous systems and they will control essential vehicle functions. Such systems have the capacity for damage when not operating properly, and are commonly called safety-critical systems [3].

Safety-critical systems are designed and analyzed carefully in order to verify not only that they operate as they were intended, but also to prevent them from operating in any way that is not desired. A system safety process facilitates this design process [2]. In this paper, we describe a comprehensive hazard analysis approach for system safety programs. The comprehensive approach involves applying a number of hazard analysis techniques and then integrating their results. This comprehensive approach attempts to overcome the narrower scope of each individual technique while obtaining the benefits of all of them.

Safety is intimately connected to the notion of risk, and popularly means a relatively high degree of freedom from harm. Risk is a combination of the likelihood and the severity of an unplanned, undesirable event. A system is generally considered to be safe if the level of risk is reasonable [4]. Reasonable risk must be evaluated according to societal, legal, and corporate concerns [5].

Hazards are potential unsafe events or conditions that could lead to undesired consequences or events. A hierarchy or interaction of undesired causes typically combine to result in a hazard. Faults are potential physical or logical defects in the design or implementation of a device or system. Under certain conditions, they can lead to errors, that is, incorrect system states. Errors may induce failures, that is, deviations from appropriate system behavior. Failures are hazards if they can lead to undesired, safety-related consequences. Note that not all hazards are the result of faults. Hazards can also be caused by unanticipated sequences of interactions between components or subsystems.

System safety engineering is the application of engineering and management principles, criteria, and technology to provide a reasonable and achievable level of safety together with other system design constraints throughout all phases of the system lifecycle [6].

Reliability, $R(t)$, is the probability that a system has not failed by some time t. The popular notion of a reliable system is that it is trouble-free for a long time. Safety is not equivalent to reliability; a safe system may be unreliable, and uncovered hazards in ultrareliable systems may be severe. Moreover, as noted above, not all hazards are induced by faults in individual components. Each component may work correctly and the system itself may be operating according to specification, however, the specification may not account for all operating conditions, and as noted above, unanticipated component and subsystem interactions can also lead to hazards. System safety programs seek to identify hazards and eliminate or mitigate them. Two commonly used standards documents are used as the basis for implementing many system safety programs: MIL-STD-882D [7] and IEC 61508 [8]. A typical system safety program is illustrated in Figure 1.

The goal of a system reliability program is to predict the trouble-free lifetime of a system and to determine ways to extend it. Reliability prediction employs rigorous mathematical techniques based on probability theory to determine overall system reliability from failure data about components. Some tools have been developed to aid this task, for instance, Reliability Block Diagrams (RBDs). In addition to prediction, a reliability program typically involves detailed analysis of the potential failures of a system and its components. A variety of tools have been developed for this latter task, including Failure Mode, and Effects, Analysis (FMEA), and Fault Tree Analysis (FTA). Reliability analysis tools are also frequently used in system safety analysis as detailed in the rest of this paper.

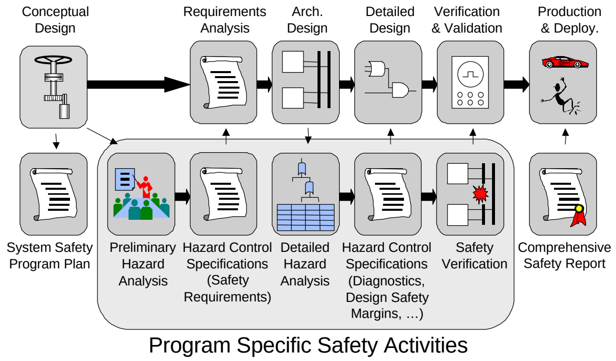
Conceptual Design
Requirements Analysis
Arch. Design
Detailed Design
Verification & Validation
Production & Deploy.
System Safety Program Plan
Preliminary Hazard Analysis
Hazard Control Specifications (Safety Requirements)
Detailed Hazard Analysis
Hazard Control Specifications (Diagnostics, Design Safety Margins, …)
Safety Verification
Comprehensive Safety Report
Program Specific Safety Activities

Figure 1: Example System Safety Process

The risk of hazards due to failures can be further reduced by shrinking the probability that they will occur. One approach to safety analysis is to quantify the probability of system failures that can cause hazards. If this probability is minimized, safety is considered to be maximized. However, establishing consensus on acceptable failure probabilities is difficult, and extremely low probabilities are difficult to verify. Moreover, the entire approach does not include hazards caused by unanticipated interactions of components or subsystems.

An alternative approach is to focus on identifying and mitigating hazards, alone, or in groups. Risk is reduced when adequate mitigating controls are in place for all hazards. There are four basic approaches to mitigating hazards, and priority is placed on them in the following order:

1. Eliminate the hazard by “designing it out”
2. Control the hazard by fault-tolerant or fail safe devices, diagnostics and control algorithms, etc.
3. Prevent the hazard from causing undesired consequences, e.g., by warning the driver or others
4. Reduce the consequences of undesired events

This approach is generally accepted by most industries within the U.S.

Another fundamental difference of approach relates to the scope of an analysis. Using the approach outlined in MIL-STD-882D, hazards are analyzed and mitigated in the entire system under consideration. IEC 61508 focuses on the design and implementation of safety functions that monitor a system and take safety-related corrective actions when failures occur.. In this paper we assume a program based on MIL-STD-882D.

A fundamental element of most safety programs is hazard analysis, that is, the systematic identification and cataloging of hazards and the specification of mitigating controls. In this paper, we review a set of common hazard analysis techniques and describe how they work together in a safety program. There are hundreds of hazard analysis techniques in practice today, so this list is far from exhaustive. However, most analysis techniques are variations on the set proposed here. Hazard analysis techniques can be broadly categorized as deductive (top-down) or inductive (bottom-up). Deductive techniques focus on systematically identifying causes of undesirable effects, while inductive techniques focus on predicting effects of a priori known problems such as faults.

In this paper, we will focus on design analysis techniques and will not consider specification analysis. A separate set of analysis techniques are appropriate to determine the completeness and consistency of specifications [13], a key element of determining that the system always does what is expected and does not do anything unexpected. Modifications to any technique may be required for a specific situation.

In the next section, we describe the motivation for a comprehensive hazard analysis approach. We review some existing automotive systems that are forerunners to X-by-wire systems, and introduce X-by-wire as a case study to be used throughout the paper. Finally, we detail the proposed set of hazard analysis techniques in the following section, describing how the techniques can play together to form a comprehensive hazard analysis program.

SAFETY CRITICAL AUTOMOTIVE APPLICATIONS

Hazard analysis techniques are currently used in the development of conventional systems. However, as future systems become more sophisticated in functionality, design, and applied technology, the need for a comprehensive hazard analysis approach becomes more apparent.

Some of the motivations for this are the following:

- New technologies, while enablers of enhanced functionality, may have additional or new failure modes that need to be studied.
- New technologies generally lack the extensive operational history of conventional systems.
- As the functional capability and domain of operation of new systems increases, it is necessary to understand how they may behave under a failed condition.
- Technologies such as ‘by-wire’ that do not rely on mechanical linkages for backup, must be analyzed so that an adequate level of redundancy is designed into the system, and that other appropriate hazard controls are satisfied.
- In addition, as systems are integrated over distributed networks and share information, the integrity of both the networks and the information communicated needs to be verified.

X-by-wire involves the electronic integration of a number of automotive component functions (e.g., steering and braking). In this section, we review several new electronic products that represent the first steps down the path to creating X-by-wire systems. In particular, two current steering system products are presented, along with a steer-by-wire system. A similar progression of technology could also be shown for brake systems. All of these systems involve electronic control of motor-driven actuators, which is a fundamental feature of X-by-wire systems. As this progression in technology occurs, the need for an enhanced, more comprehensive hazard analysis approach increases.

ELECTRONIC POWER STEERING

The E•STEER™ system (Figure 2) is an Electronic Power Steering (EPS) system developed by Delphi Automotive Systems. It incorporates a steering gear, assist mechanism, and electronic controller to provide responsive steering assist, and eliminates the need for a power steering pump, hoses, hydraulic fluids, and a drive belt and pulley on the engine. Sensors measure two primary inputs — driver torque (or effort) on the steering shaft and hand-wheel position. These two primary inputs along with the vehicle speed signal and other system variables are continuously fed into an electronic control module which performs two main functions:

- It ascertains the integrity of the signals and inputs
- It determines the direction and amount of steering assist

This is the first major step in the introduction of electronics into the steering system. Since this system replaces the assist provided by the previous hydraulic system with assist provided by an electric motor, while maintaining the mechanical link, appropriate deactivation of active components is sufficient in most cases to maintain safe operation when errors are detected. This is accomplished through the many integrity features built into E•STEER™. The system continuously runs detailed self-checks and diagnostics to ensure proper operation and turns the system off if discrepancies are found. One significant difference between EPS and conventional power steering, is that EPS obviously has different potential failure modes that had to be comprehended in the hazard analysis.

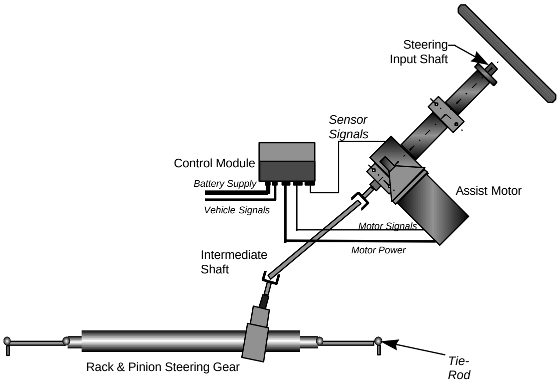

Figure 2: The E•STEER™ System

FOUR WHEEL STEER

The QUADRASTEER™ system, also developed by Delphi Automotive Systems, provides four-wheel steering capabilities in order to provide enhanced directional control of the vehicle over conventional two-wheel steering systems. The rear steering angle is governed by the driver’s steering wheel angle input and other vehicle dynamic quantities, such as vehicle speed. The rear steering sub-system in QUADRASTEER™ is a steer-by-wire system; there is no mechanical linkage between the driver and the rear subsystem. However, the front steering subsystem is conventional. QUADRASTEER™ consists of the following main components:

- The four-wheel steer electronic control module
- A rear steer actuator and steerable rear axle assembly
- System controls, including servo loop controls, position sensors, serial communication equipment, and controller hardware

QUADRASTEER™ is an intermediate step between E•STEER™ and full steer-by-wire. As with E•STEER™, appropriate deactivation of active components is sufficient in most cases to maintain safe operation when errors are detected since the front wheels can still be steered.

STEER-BY-WIRE

A front steer-by-wire system replaces the traditional mechanical linkage between the steering wheel and the road-wheel actuator (e.g., a rack and pinion steering system) with an electronic connection. This allows flexibility in the packaging and modularity of the design. Since it removes the direct mechanical kinematic relationship between the steering wheel and the road wheel, it enables control algorithms that enhance driver input.

Figure 3 shows a conceptual design for a steer-by-wire system. The system can be subdivided into two major parts: a hand-wheel subsystem, and a road-wheel subsystem. The hand-wheel system contains sensors to provide information about driver steering input. This information is sent to a controller, which incorporates knowledge of the vehicle's current state to command desired road-wheel angle. The road-wheel system contains actuators to position the wheels.

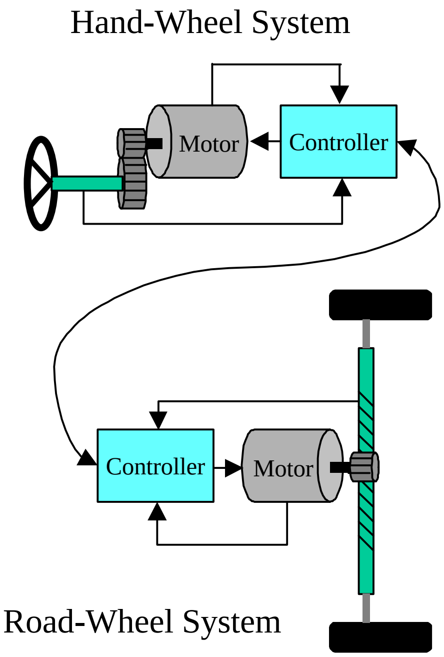

Figure 3: Steer-By-Wire Conceptual Design

An actuator in the hand-wheel system provides road feedback to the driver, via the hand-wheel controller. The hand-wheel controller provides feedback based on information provided by sensors in the road-wheel system.

Although by-wire applications do exist in aviation and aerospace, these systems provide only partial guidance for automotive steer-by-wire systems because the original design requirements and constraints were different. Thus, new architectures and hazard control strategies might be appropriate.

Hazard analysis strategies have been previously applied in steering systems [9]. However, steer-by-wire incorporates many new technologies and eliminates other components of conventional steering systems. Therefore, steer-by-wire strongly motivates the development of a more comprehensive hazard analysis approach.

Hazard analysis begins with a conceptual design such as the one shown in Figure 3. This system will be used as an example for the rest of the paper.

COMPREHENSIVE HAZARD ANALYSIS

A comprehensive hazard analysis of a system involves analyzing different views of the system over the entire product-design cycle and integrating the results so that a consistent and complete representation of the system's hazards, failure modes, faults, and hazard controls is constructed. By analyzing different views, failures that may be difficult to identify in one view may be identified more easily when analyzing another view.

In this section, we describe a set of hazard analysis techniques that can provide this useful multi-view analysis. These techniques are:

- Preliminary Hazard Analysis (PHA)
- Reliability Block Diagrams (RBD)
- Fault Tree Analysis (FTA)
- Failure Modes Effects Analysis (FMEA) and Failure Modes Effects and Criticality Analysis (FMECA)
- Common Cause Analysis (CCA)

Each technique examines a specific view of the system, and as a result, has an associated set of strengths and weaknesses. Through the use of a hypothetical road-wheel system design for a steer-by-wire vehicle, we examine the strengths and weaknesses of the analysis approaches, and describe how these techniques can be combined to provide a comprehensive hazard analysis that capitalizes on the strengths of the analyses while overcoming their weaknesses.

PHA

The goal of PHA is to identify high-level system hazards and to determine the criticality of potential mishaps that may arise. PHA is performed in the early life cycle stages of system development so that safety requirements for controlling the identified hazards can be determined and incorporated into the early design development. The PHA tends to quickly focus the design team's attention on the true safety issues of a product concept. The basic steps for performing a PHA are:

1. Perform brainstorming or review existing potential hazard lists to identify potential hazards associated with the system .

2. Provide a description of the hazard, and potential mishap scenarios associated with the hazard.
3. Identify potential causes of the hazard.
4. Determine the risk of the hazard and mishap scenarios.
5. Determine whether controls can be added to the system to eliminate or mitigate the risks. At this stage, only a hazard control feasibility study and system requirements to control the hazards are needed.

The PHA typically relies on a tabular format that may contain headings for hazard name, hazard description, potential causes of the hazard, mishap scenario, hazard severity, hazard likelihood, risk, hazard controls, severity with hazard controls, likelihood with hazard controls, and risk with hazard controls.

Figure 4 shows a conceptual design for a hypothetical steer-by-wire, road-wheel system. To bound the scope of this example, many signals, e.g. hand-wheel torque, are omitted. In the design concept, a controller receives a road-wheel position command describing a desired road-wheel angle (i.e., RW Position Command). By reading the actual road-wheel position (i.e., RW Position Measured) of the road-wheel actuator, the controller attempts to minimize the difference between the desired position and the actual position. PHA is an appropriate technique to apply to the road-wheel system conceptual design, because with minimal effort it may be possible to identify needed architectural/system safety requirements that would otherwise require a great deal of effort to implement in the later stages of the product-design process.

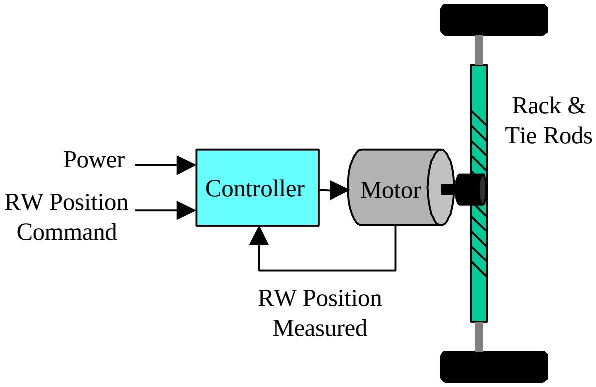

Figure 4: Road-wheel System Conceptual Design

Table 1 shows a portion of the preliminary hazard analysis for the road-wheel system. Some of the potential hazards identified, such as "loss of steering," will have a high risk. Appropriate hazard controls are identified to either eliminate or mitigate this risk: hazard controls should be added until the risk is reduced to an acceptable level (e.g., Low).

In this example, redundant controllers and motors are suggested to provide fault tolerance for the "Loss of steering" hazard (see Figure 5). For the rack and tie rods, highly reliable mechanical components similar to conventional steering systems are suggested to avoid faults leading to "Loss of steering."

Table 1: Preliminary Hazard Analysis

Potential Hazard	Effect	Risk	Control
Loss of steering	Severe collision	Critical	Fault tolerant controller & motor system; Fault avoidance for rack & tie rods
Excessive noise	Dissatisfied customer	Low	

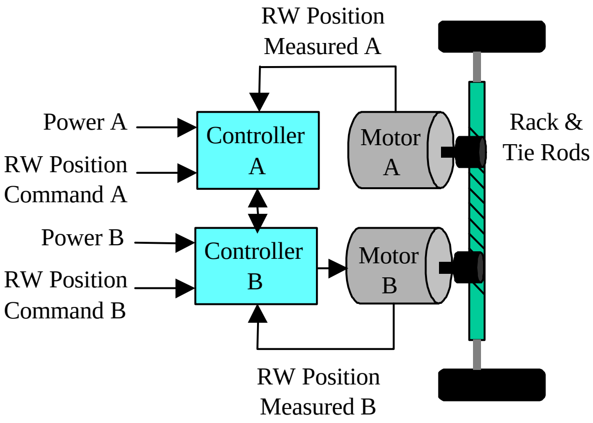

Figure 5: Road-wheel System Architecture

RBD

An RBD can be thought of as a flow diagram from the input of the system at the left-hand side of the diagram, to the output of the system at the right. Each block in the reliability diagram represents a component, element, or subsystem of the system. For a series system, the blocks are placed in series to indicate that a path from the input to the output is broken if any one of the components fails. For a parallel system, the blocks are placed in parallel to indicate that the path from the input to the output is broken only if at least one component along each parallel path fails. Most systems are combinations of series and parallel systems. The flow from input to output along at least one path in the diagram must be preserved if the system is to maintain its operation [12]. Common cause failures can be identified in RBD's by identifying blocks that repeat in all paths of the diagram.

The basic steps for creating an RBD for a specific hazard are:

1. Determine the input starting point for the system and the flow of the system from the input to the output.
2. Starting from the input and working toward the output, identify system components that could contribute to the specific hazard if they failed.
3. For each component, create a block in the RBD and place it in a position relative to its position in the input to output flow of the system.

Once the RBD has been constructed, the conditions for failure can be computed. A sum-of-products Boolean Algebra expression can be written directly from the diagram; every product term in the expression is a potential combination of component/subsystem failures that can lead to system failure. These product terms are called cut sets. Clearly, the overall expression should be minimized for the cut sets to be most useful.

Figure 6 shows the RBD for "Loss of steering" for the road-wheel system. The inputs to the system (e.g., RW Pos Mea, RW Pos Cmd, and Power) are on the left, the output component is on the right. Two parallel paths exist, one for each controller & motor combination. Thus, the RBD indicates that acceptable steering performance is produced with only one of these paths operating. However, since only one in-series block exists for the Rack / Tie rods, these components must be functioning if "Loss of steering" is to be avoided.

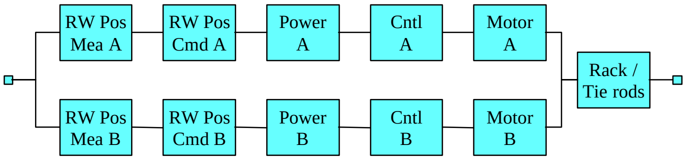

Figure 6: Road-wheel System RBD for Loss of Steering

Typically, a separate RBD would have to be created for each potential hazard to provide full coverage. However, if a comprehensive hazard analysis approach is taken, it is possible to focus RBD efforts on the most serious potential hazards, and let other analysis techniques address the less serious ones. This has the benefit that it is possible to implement a limited set of RBDs quickly without consuming a great deal of resources, such that RBDs can be implemented for several proposed architectures to compare their potential safety benefits or disadvantages.

Table 2 shows some of the cut sets generated from the "Loss of steering" RBD. These cut sets fall into two categories: single point failures, and one failure in each of the two redundant paths. Although for this simple system, the results may be obvious, for complex systems, RBD cut sets can often identify common cause and other failures that might not have otherwise been identified.

Once the RBD cut sets have been identified, they must be reviewed to determine if any pose a significant risk. One possible method to assess cut set risk is to determine the severity for each cut set from the severity of the hazards that the cut set can lead to, and then develop a risk prioritization number (RPN) for each cut set based on the severity and the likelihood of the cut set itself. Those cut sets with higher RPNs are actively tracked (as shown in Table 3), and the hazard risk assessment is revised as needed based on the information provided by this critical RBD list. If the risk associated with a hazard must be reduced, then the RPN of the failures that lead to the hazard can help identify which failures should be addressed. In addition, to improve reliability and customer satisfaction, the design team may choose to lower the RPN of some failures even though they do not lead to any potential safety risks.

Table 2: Example RBD Cut Sets

Rack / Tie Rods	Motor A & RW Pos Mea B
Motor A & Motor B	Cntl A & Motor B
Motor A & Cntl B	Cntl A & Cntl B
Motor A & Power B	Cntl A & Power B
Motor A & RW Pos Cmd B	Cntl A & RW Pos Cmd B

Table 3: Critical RBD Cut Sets

Failures	Cause	Hazard	RPN
Rack / Tie Rods	Mech. stress	Loss of Steering	20
Cntl. A & Cntl. B	Common software	Loss of Steering	30
Power A & Power B	Common charging system	Loss of Steering	20
RW Pos Mea A & RW Pos Mea B	Common mode sensor failure	Loss of Steering	15

FTA

Fault Tree Analysis (FTA) is used to analyze the causes of hazards, rather than to identify hazards. The top event in a fault tree is a known system hazard, such as loss of steering. The goal of FTA is to work downward from this top event to determine the credible ways in which the undesired top-level event could occur, given the system operating characteristics and environment. The fault tree is a graphical model of the parallel and sequential combinations of faults that could result in the occurrence of the top-level hazard. The faults can be events associated with component hardware failures, human errors, such as requirements' errors, design errors and software bugs.

Similar to RBDs, FTA uses Boolean logic (AND and OR gates) to depict the combinations of individual faults that can lead to the top-level hazard. In this case, the expression is explicitly represented in the diagram. At each level in the tree, the more basic events that may lead to the problem shown in the previous level are listed. The gates at each level permit or inhibit the passage of fault logic up the tree. A higher level event is the output of a gate, while the inputs to the gate are the lower level events. The type of gate chosen depicts the relationship between the input events that is required for the output event to occur. An AND gate means that all of the events input to the AND gate must occur for the output of the AND gate to occur. An OR gate means that only one of the events input into the OR must occur for the output of the OR to occur.

Once the fault tree is completed to sufficient detail, a Boolean expression of the tree can be written to show the specific combinations of identified basic events that are sufficient to cause the top-level hazard. As in RBDs, the product terms of this expression are called cut sets. If the analysis is limited to reviewing cut sets, FTA is a qualitative analysis method, however, if individual probabilities are known for all of the basic events, the probability of the top-level event can be quantified.

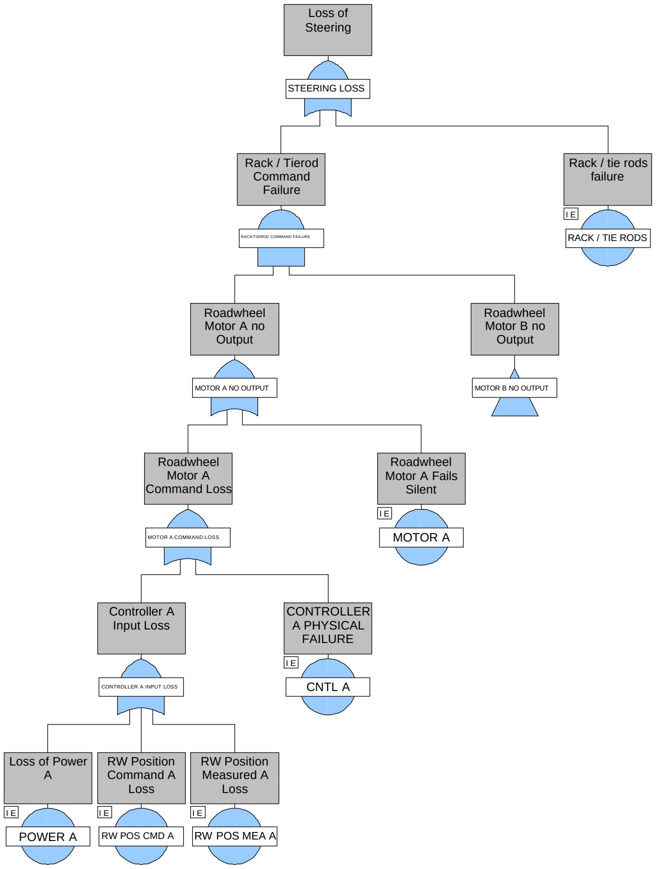
Loss of Steering
STEERING LOSS
Rack / Tierod Command Failure
Rack / tie rods failure
I E
RACK/TIEROD COMMAND FAILURE
RACK / TIE RODS
Roadwheel Motor A no Output
Roadwheel Motor B no Output
MOTOR A NO OUTPUT
MOTOR B NO OUTPUT
Roadwheel Motor A Command Loss
Roadwheel Motor A Fails Silent
I E
MOTOR A COMMAND LOSS
MOTOR A
Controller A Input Loss
CONTROLLER A PHYSICAL FAILURE
I E
CONTROLLER A INPUT LOSS
CNTL A
Loss of Power A
RW Position Command A Loss
RW Position Measured A Loss
I E
I E
I E
POWER A
RW POS CMD A
RW POS MEA A

Figure 7: Loss of Steering System-Level Fault Tree

The basic steps for performing a FTA [10] are:

1. Determine a top-level event to analyze.
2. At each level, and for each intermediate event or component, consider command path faults (signal flow), secondary faults (environmental or external), and primary failures (inherent or internal).
3. Continue with this until basic events are reached or it is determined that the tree has been sufficiently expanded.
4. Generate a Boolean expression of the tree to determine the combinations of basic events that can lead to the top-level hazard of the tree.

Figure 7 shows a system-level fault tree for “Loss of steering” of the road-wheel system. Starting at the output component (i.e., Rack and Tie rods) of the system, the fault tree was systematically constructed by identifying the primary and command failures of the component that lead to “Loss of steering.” For this system-level fault tree, a single “primary” basic event (e.g., Rack/Tie Rod failure) has been included for each of the main components (e.g., Rack and Tie Rods) to represent the internal failure of the component. To limit the scope of the analysis in this example, wiring components and secondary events (e.g., external failures due to EMI), have not been considered. For the Rack and Tie Rod component, a command failure occurs when both motor inputs are lost. Thus, an AND gate is applied to capture this relationship. Once primary and command failures are identified for a given component, the process is repeated for the next set of components that provide a command to the given component.

The example fault tree in Figure 7 captures the same logical relationships among components as the RBD in Figure 6. As a result, the cut sets produced from the fault tree are identical to those generated from the system RBD. Here are some of our observations on the uses and relative benefits of RBDs and FTA:

1. For “total loss of functionality hazards” (e.g., “Loss of steering”), RBDs are easier to construct than fault trees because of the close correlation between the RBD and the mechanization diagram of a system.
2. For “total loss of functionality hazards,” RBDs provide a graphical view of system redundancies, and provide a good mechanism for visually communicating this information.
3. Fault trees provide a hierarchical decomposition of hazards that permits dependencies between faults, errors, failures and hazards to be readily observed and tracked.
4. For engineers and managers that do not have detailed experience with either technique, the graphical representation of how combinations of faults lead to top-level events provided by the fault tree AND and OR gates is easier to understand than the series and parallel combinations of blocks in an RBD.
5. Construction and maintenance of either detailed fault trees or RBDs can require significant effort.

Based on these observations, we typically perform RBD analysis to evaluate the ability of proposed architectures to provide some functionality (e.g., steering), and then implement detailed fault trees to evaluate the highest risk hazards.

FMEA AND FMECA

FMEA and FMECA are traditionally considered inductive techniques that [11]:

- Identify and evaluate potential failure modes of a product design and their effects
- Determine actions or controls which eliminate or reduce the risk of the potential failure
- Document the process.

FMEAs are widely used in the automotive industry [11], where they have served as a general purpose tool for enhancing reliability, trouble-shooting product and process issues, and as a standalone tool for hazard analysis. Here we consider their use when integrated into a comprehensive hazard analysis approach.

The basic steps to perform a FMEA or FMECA are:

1. Identify and list individual components, the function they provide, and their failure modes. Consider all possible operating modes.
2. For each failure mode, determine the effects of the failure on all other system components and on the overall system.
3. Determine the severity of the failure, the potential causes of the failure, and the likelihood that a potential cause will occur.
4. Identify the current design controls that will assure the design adequacy for the failure controls. Determine the ability of the proposed design controls to detect a potential cause, or the ability of the proposed controls to detect the subsequent failure mode before the component is released for production.
5. Determine the RPN based on the severity, occurrence, and detection rankings.
6. For the highest ranking RPN's, recommend actions to take that will reduce the severity, occurrence, and/or detection rankings.
7. Re-evaluate the RPN based on the new estimates of the severity, occurrence, and detection rankings.

The results of the FMEA or FMECA are documented in a table with column headings such as item, potential failure mode, potential effects of the failure, severity of the failure, potential causes of the failure, the likelihood that a potential cause will occur, current design controls, risk priority number, and recommended actions [11]. The primary difference between FMEA and FMECA is that the latter explicitly includes criticality analysis for both the original design and the final design, while not all references to FMEA include this.

Table 4: System Design FMEA

Item	Failure Mode	Effect	Cause	RPN
Motor A	Bound output	Motor A position locked; Loss of steering	Rotor bound	80
	No output	Motor A no output; Degraded steering	Winding short	10
	Low efficiency	Degraded steering	Contamination	10

Table 4 shows a portion of the system design FMEA for the road-wheel system. Each major component in Figure 5 has been examined for failure modes, effects, causes, and RPNs have been identified (only Motor A is shown in Table 4). The effect of each failure mode lists both the effect on the function provided by the component and the subsequent hazard effect.

In this example, we attempt to illustrate how important failure modes missed in one type of analysis may be identified in another. In addition to "No output," an additional failure mode, "Bound output," has been identified as contributing to the "Loss of steering." hazard The "Bound output" failure mode was not comprehended in the command failures for the Rack and Tie Rods, and since for this failure "Loss of steering" occurs even if only one of the motors exhibits this failure mode, the RBD and fault tree analysis must be revised. Specifically for the fault tree, an OR gate is required to capture this relationship. By performing a comprehensive hazard analysis involving multiple techniques, the likelihood of missing failure modes is reduced.

As in typical automotive system analysis, a comprehensive hazard analysis involves performing FMEAs for components as well as for the system. Table 5 shows a motor component FMEA. The motor FMEA identifies the causes of "Rotor bound" so that the risk associated with this failure can be reduced. In this case, contamination is identified as the primary cause, and both design and manufacturing controls can be specified to reduce the risk of this failure.

To maintain consistency among the FMEAs, the causes in the system FMEA are the failure modes in the component FMEA, and the failure modes in the system FMEA are the effects in the component FMEA. Maintaining consistency among analyses reduces oversights and misunderstandings because a failure mode has only one name and is appropriately accounted for in every analysis.

Table 5: Motor Design FMEA

Item	Failure Mode	Effect	Cause	RPN
Gear	Gear bound	Bound output; Loss of steering	Fractured tooth due to fatigue	80
Windings	Winding short	No output; Degraded steering	Overheating	10
Rotor	Rotor fracture	No output; Degraded steering	Fatigue	10
	Rotor bound	Bound output; Loss of steering	Contamination	80

An FMEA may identify additional failures not found during fault tree analysis, so it is important to maintain consistency among fault tree and FMEA results. Figure 8 shows fault trees developed for the motor that are consistent with the motor FMEA. Two trees exist, one for “No output” and one for “Bound output.” By maintaining consistency among the FMEAs and fault trees, failures identified by one are always guaranteed to be included in the other.

Figure 9 shows a revised fault tree that includes the component fault trees along with the needed revision identified by the system FMEA. This fault tree not only identifies how all failures lead to the “Loss of steering” hazard, it also provides a comprehensive view of all identified failure modes.

A FMEA typically attempts to identify all of the ways a component may fail, and how these failures impact a system. However, it does not necessarily identify problems related to bad inputs or external influences. By considering command inputs and secondary inputs, fault tree analysis attempts to address hazards that do not explicitly arise from component failures. Thus, fault tree analysis may identify needed hazard controls to prevent system accidents [13] that may occur even though no component has failed. In addition, the focused, deductive nature of fault tree analysis may identify failures that might be missed by the broader, inductive FMEA. Conversely, the broad coverage provided by FMEA may identify relevant failures that are outside the scope of a narrowly focused fault tree analysis.

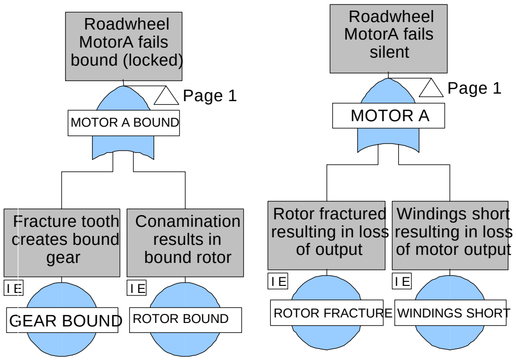
Roadwheel MotorA fails bound (locked)
Page 1
MOTOR A BOUND
Fracture tooth creates bound gear
I E
GEAR BOUND
Conamination results in bound rotor
I E
ROTOR BOUND
Roadwheel MotorA fails silent
Page 1
MOTOR A
Rotor fractured resulting in loss of output
I E
ROTOR FRACTURE
Windings short resulting in loss of motor output
I E
WINDINGS SHORT

Figure 8: Motor Fault Trees

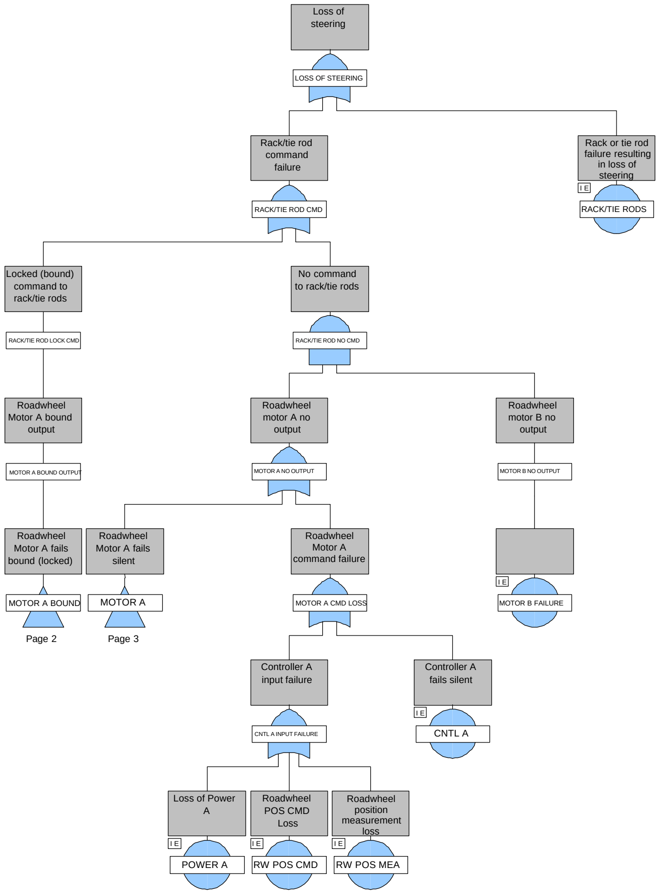
Loss of steering
LOSS OF STEERING
Rack/tie rod command failure
RACK/TIE ROD CMD
Rack or tie rod failure resulting in loss of steering
I E
RACK/TIE RODS
Locked (bound) command to rack/tie rods
RACK/TIE ROD LOCK CMD
No command to rack/tie rods
RACK/TIE ROD NO CMD
Roadwheel Motor A bound output
MOTOR A BOUND OUTPUT
Roadwheel motor A no output
MOTOR A NO OUTPUT
Roadwheel motor B no output
MOTOR B NO OUTPUT
Roadwheel Motor A fails bound (locked)
MOTOR A BOUND
Page 2
Roadwheel Motor A fails silent
MOTOR A
Page 3
Roadwheel Motor A command failure
MOTOR A CMD LOSS
I E
MOTOR B FAILURE
Controller A input failure
CNTL A INPUT FAILURE
Controller A fails silent
I E
CNTL A
Loss of Power A
I E
POWER A
Roadwheel POS CMD Loss
I E
RW POS CMD
Roadwheel position measurement loss
I E
RW POS MEA

Figure 9: Revised System Fault Tree

COMMON-CAUSE ANALYSIS

Common cause analysis [14] is used to identify mishap sequences where two or more events can occur due to a single common event or causative mechanism. The single common event may itself be caused by a common process or manufacturing defect, a common human operator error, a common external event, or a specification error that leads to problems throughout a design. Common cause analysis may also be used in accident reconstruction. The basic steps to common cause analysis are:

1. Identify and group the critical components to be evaluated. These components and their relationships can be identified using other analysis techniques, such as FMEA's and FTA.
2. Within the groups, check for commonalities such as physical location and manufacturing characteristics, common manufacturers, a common design process that could introduce a generic design defect, etc.
3. Within each identified commonality, check for credible failure modes such as, electrical shorts or opens, maintenance errors, etc.
4. Identify generic causes or trigger events that could lead to the credible failure modes, such as, corrosion, overheating, fire, flood, etc.
5. Based on the above, draw conclusions and make recommendations for corrective action. Corrective actions include requirements redesign, invoking emergency procedures, and function degradation.

The critical cut sets identified in Table 3 include several common cause groups. For example, the position sensors are identical components, and both are located on or near the Rack. Given their close proximity, these two sensors could possibly fail at the same or nearly the same time due to influences from the external environment. Since common cause analysis identifies potential multi-point failures all resulting from the same cause, it can identify failures missed by a FMEA. In addition, it may identify failures missed by FTA and RBDs due to the large number of cut sets that may need to be examined and since the analysis is entirely focused on only identifying common cause failures.

SUMMARY AND CONCLUSIONS

Hazard analysis plays an important role in the development of safety-critical systems. Hazard analysis techniques such as FMEAs have been used in the development of conventional systems. However, as future systems become more sophisticated in functionality, design, and applied technology, the need for a more comprehensive hazard analysis approach becomes apparent.

In this paper, we have described a comprehensive hazard analysis approach based on the following analysis techniques:

- PHA
- RBD
- FTA
- FMEA
- CCA

We have shown that combinations of these techniques can lead to a more thorough hazard analysis since each considers the analysis problem from a different point of view. Each technique tends to lead more quickly to results that are closely linked to the particular strength of that technique. The use of multiple techniques increases the rigor of a safety analysis program and increases the resources that must be applied. However, if properly managed, combinations of hazard analysis techniques can work together to make each more efficient than if applied independently. For example, FTA can help inform, structure, and accelerate FMEA analysis, which is typically performed anyway for automotive systems.

These techniques have been widely applied in the military, aerospace, and nuclear industries, and the automotive industry should consider the guidelines and precedents that have been set in these other industries. Both from a supplier and a manufacturer's perspective, it will be important to establish a relatively common approach to comprehensive hazard analysis.

REFERENCES

1. S. Buckley and K. Johnson, “Concepts Designed to Enhance the Customer's Driving Experience”, *Proceedings, SAE International Congress on Transportation Electronics*, 2000-01-C031, Oct. 16-18, 2000.
2. S. Amberkar et. al., “A System Safety Process for By-Wire Automotive Systems”, *in Design and Technologies for Automotive Safety-Critical Systems* SP-1507, Society of Automotive Engineers, Inc., 2000, pp. 69-74.
3. P. J. Perrone and B. W. Johnson, “Distributed Safety-Critical Systems,” in *Fault-Tolerant and Distributed Systems* (ed. D. R. Avresky and D. R. Kaeli), Kluwer Academic Publishers, pp. 173-194, 1998.
4. N. J. Bahr, *System Safety Engineering and Risk Assessment: A Practical Approach*, Taylor and Francis, Wash. DC, 1997.
5. P. L. Goddard, "Automotive Embedded Computing: The Current Non-Fault-Tolerant Baseline for Embedded Systems", in *Proc. 1998 Workshopon Embedded Fault-Tolerant System*s, pp. 76-80, May 1998.
6. M. Allocco, G. McIntyre, and S. Smith, "The Application of System Safety Tools, Processes, and Methodologies within the FAA to Meet Future Aviation Challenges", in *Proc. 17th International System Safety Conference*, pp. 1-9, 1999.
7. DOD Standard Practice for System Safety, MIL-STD-882D, February 10, 2000.
8. *Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems – Parts 1-7*, IEC 61508-1-7.

9. S. Amberkar, K. Eschtruth, Y. Ding, F. Bolourchi, “Failure Mode Management for an Electric Power Steering System” , ISATA 99AE002, 1999.
10. US Nuclear Regulatory Commission, *Fault Tree Handbook*, NUREG-0492, January 1981.
11. Society of Automotive Engineering, *Potential Failure Modes and Effects Analysis Reference Manual SAE J1739.*
12. Barry W. Johnson, *Design and Analysis of Fault Tolerant Digital Systems*, Addison-Wesley Publishing Company, Inc., 1989.
13. Nancy G. Leveson, *SAFEWARE, System Safety and Computers*, Addison-Wesley Publishing Company, Inc., 1995.
14. US Nuclear Regulatory Commission, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies,* NUREG/CR-4780, Vol. 1, January 1988.

CONTACT

Joseph G. D’Ambrosio, Delphi Automotive Systems, joseph.g.d.ambrosio@delphiauto.com