A System-safety process for "by-wire" automotive systems

Steer-by-wire and other "by-wire" systems (as defined in this article) offer many passive and active safety advantages. To help ensure these advantages are achieved, a comprehensive system-safety process should be followed. Here we review standard elements of system safety processes that are widely applied in several industries and describe the main elements of our proposed analysis process for by-wire systems. The process steps include: 1) creating a program plan to act as a blueprint for the process, 2) performing a variety of hazard analysis and risk assessment tasks as specified in the program plan, 3) designing and verifying a set of hazard controls that help mitigate risk, and 4) summarizing the findings. Vehicle manufacturers and suppliers need to work together to create and follow such a process. A distinguishing feature of the process is the explicit linking of hazard controls to the hazards they cover, permitting coverage-based risk assessment.

by ***Sanket Amberkar***, ***Barbara J. Czerny***, ***Joseph D'Ambrosio***, *and* ***Brian Murray*** *of Delphi Automotive Systems; and* ***Joseph Wysocki*** *of HRL Laboratories.*

Recent advances in dependable embedded system technology, as well as continuing demand for improved handling and passive and active safety improvements, have led vehicle manufacturers and suppliers to actively pursue development programs in computer-controlled, by-wire subsystems. These subsystems include steer- and brake-by-wire, and are composed of mechanically decoupled sets of actuators and controllers connected through multiplexed, in-vehicle computer networks. There is no mechanical link to the driver. Steer- and brake-by-wire provide a number of packaging and assembly advantages over conventional subsystems. For instance, electromechanical brake-by-wire subsystems require no hydraulic fluid to store or load at the assembly plant and permit more modular assembly, thus reducing the number of parts to be handled during production. Steer-by-wire systems have no steering column and may also eliminate cross-car steering assemblies such as racks.

Both steer- and brake-by-wire also enable many new driver interface and performance enhancements such as stability enhancement and corrections for cross wind. Overall, by-wire systems offer wide flexibility in the tuning of vehicle handling via software. Moreover, steer-by-wire provides the opportunity for significant passive safety benefits; the lack of steering column makes it possible to design better energy-absorbing structures. Finally, an important potential benefit of by-wire subsystems is active safety; a capability only fully realized when they are integrated into systems. Integrated by-wire systems, referred to as drive-by-wire or X-by-wire, permit the implementation of a full range of automated driving aids, from adaptive cruise control to collision avoidance. While by-wire technologies promise many benefits, they must be carefully analyzed and verified for safety because they are new and complex. 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 incident. A system is generally considered to be safe if the level of risk is reasonable [1]. This must be evaluated according to societal, legal, and corporate concerns [2].

Hazards are potential unsafe events or conditions that could lead to an incident. Faults are potential physical or logical defects in the design or implementation of a device. Under certain conditions, they lead to errors (*i.e.*, incorrect system states), which can induce failures (*i.e.*, a deviation from appropriate system behavior). The failure is a hazard when it leads to an incident.

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 [3].

Safety is not equivalent to reliability; a safe system may be unreliable, and uncovered hazards in ultra-reliable systems may be severe. Moreover, not all hazards are induced by faults in individual components. Many undesired incidents are caused by unanticipated sequences of interactions between system components and the environment. 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. System safety programs seek to identify hazards and eliminate or mitigate them.

A system-safety program for by-wire systems or any other type of system must be coordinated between vehicle manufacturers and suppliers. Usually the parties will agree on and follow the same process, and the results should be complete and consistent.

Generic steer-by-wire system description

A 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. As explained before, this allows flexibility in the packaging and modularity of the design. Since it removes the direct kinematic relationship between the steering and road wheels, it enables control algorithms to help enhance driver input.

Figure 1 shows a conceptual design for a steer-by-wire system. The system can be subdivided into three major parts: a controller, a steering wheel subsystem, and a road wheel subsystem. The steering wheel system contains sensors to provide information about driver steering input. This information is sent to the controller, which employs knowledge of the vehicle's current state to command desired road wheel angle. The road wheel system contains actuators to position the wheels.

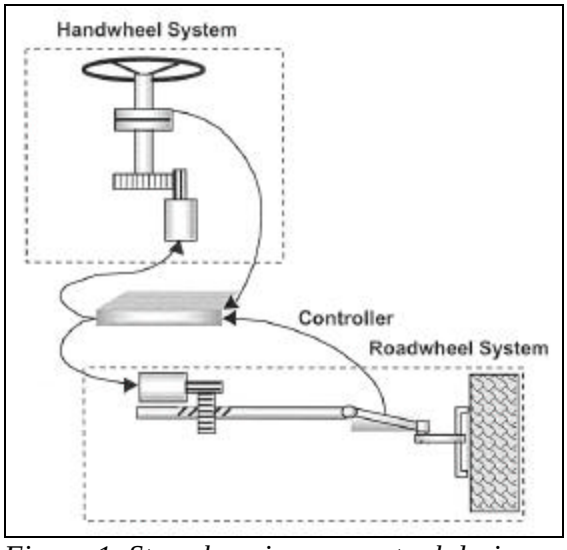

Figure 1. Steer-by-wire conceptual design.

An actuator in the steering wheel system provides road feedback to the driver. This also is commanded by the controller and is based on information provided by sensors in the road wheel system.

Although steer-by-wire applications do exist in aerospace, these systems provide only marginal guidance for automobile steer-by-wire systems because the design requirements are different. Thus different architectures and hazard control strategies might be appropriate. Such strategies exist for developing quantified hazard control requirements in automotive steering applications [4] and can be applied and expanded in by-wire applications.

The generic steer-by-wire system will be used as an example throughout the article to illustrate the process concepts and analysis.

Elements of a system safety process

Implementation of a system-safety program is an accepted excellent method for improving and documenting the safety of a product design [3]. The objectives of a system safety program include:

- Identify potential hazards and associated avoidance requirements
- Translate safety requirements into engineering requirements
- Provide design assessment and trade-off support to the ongoing design
- Assess relative compliance of design to requirements and document findings
- Direct and monitor specialized safety testing
- Monitor and review test and field issues for safety trends.

A major step towards achieving these objectives is to establish a system safety working group (SSWG) [1] for the product. An SSWG is comprised of senior design team members from the various disciplines involved in product design. Typically, an SSWG is responsible for providing for the design of safe products and conducting and/or monitoring any necessary safety tasks. SSWG meetings are held on a regular basis and serve as a forum for discussing the current status of safety-related activities and for discussing safety concerns.

While vehicle manufacturers have final responsibility for the entire vehicle, subsystem suppliers

are involved in the design process and responsible for their subsystems. An important issue for the SSWG and the overall safety program is the coordination of safety activities between a vehicle manufacturer and one or more suppliers. If a vehicle system works primarily in isolation, having little interaction with other vehicle systems, it may then be possible for the system supplier to establish the SSWG and safety program, and for the vehicle manufacturer to receive updates and approve actions. In this scenario, safety tasks may be primarily performed by the supplier, but the vehicle manufacturer has responsibility for identifying all possible interactions between the supplier's system and the rest of the vehicle and the overall vehicle performance. In addition, the vehicle manufacturer cannot view safety as solely the supplier's responsibility, and must take steps to ensure confidence in the suppliers ability to produce a safe system.

Another scenario is to establish a joint safety program, with a single SSWG having members from both the vehicle manufacturer and supplier. This approach is required when there is a high degree of interaction between the system provided by the supplier and other vehicle systems. Benefits of this approach include better understanding of system interactions, and fewer misunderstandings of system requirements and behavior. Capabilities of both partners can lead to synergy of effort at an early stage of product development. Potential disadvantages include the difficulties of coordinating activities among different organizations.

One last scenario to consider is when multiple suppliers are involved. In this case the vehicle manufacturer can establish an SSWG that includes representation from appropriate suppliers, and each can form their own SSWG. The vehicle manufacturer SSWG focuses on system interactions, while the supplier SSWG's focus is on component safety issues. Benefits of this approach include the ability of suppliers to protect better their intellectual property; disadvantages include possibly misunderstanding interactions between components provided by different suppliers.

Once the SSWG has been established, the group can initiate the execution of a system safety process to help achieve the safety program objectives. Figure 2 shows an example system safety process and how it relates to the overall design process. The top row of the figure show the primary design process steps, while the bottom row shows the corresponding system safety activities.

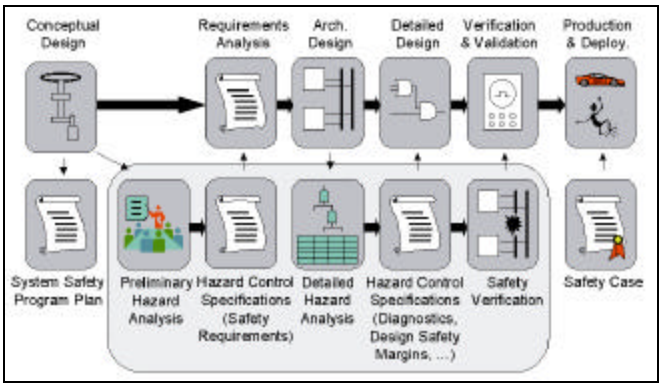

Figure 2. Example of safety system process.

At the start of the design process, a system safety program plan (SSPP) is usually written [5]. The program plan includes the relevant safety tasks to be performed, the safety organization that will be established to perform and monitor the tasks, and relevant documents such as applicable government regulations or standards. By writing a plan at the beginning of a product design, the organization establishes safety as a primary concern throughout the process and demonstrates a commitment to producing a safe product.

One of the first tasks in the SSPP is to perform a preliminary hazard analysis (PHA). The SSWG participates in one or more brainstorming exercises to construct a preliminary hazard list (PHL), which describes the potential hazards of the system. The potential safety risk associated with each hazard is then evaluated by assessing the likelihood and severity of incidents that could result from the hazard. For example, MIL-STD-882c [5] defines likelihood and severity categories as shown in Tables 1 and 2, and values for these categories can be combined to assess safety risk as shown in Table 3. This standard has been very influential in the system safety community; most other similar categories are based on MIL-STD-882c. By identifying the potential risk associated with each hazard, the PHA allows the SSWG to assess the safety of the proposed conceptual design and to focus engineering activities on eliminating or mitigating potential safety problems.

Once potential safety hazards have been identified, the SSWG must address them. There are

generally two methods of addressing potential hazards. The first is by means of safety requirements. These are specific design requirements added to the requirements and specification documents of a given project for safety reasons. They may address a range of potential hazards but are not linked to hazards as determined by analysis. For example, it is almost always a general requirement that a new system be at least as safe as any previous system it replaces. A more specific requirement might be that the system contains at least three independent sources of electric power.

Table 1. MIL-STD-882C Hazard Severity Categories

Description	Category	Definition
Catastrophic	I	Fatality, system loss, or severe environmental damage
Critical	II	Severe injury, severe occupational illness, major system or environmental damage
Marginal	III	Minor injury, minor occupational illness, minor system or environmental damage
Negligible	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage

The second method of addressing hazards is to define hazard controls. Hazard controls are any measure taken to address specific potential hazards or classes of hazards. They are linked to the potential hazards they are intended to mitigate. For example, suppose that potential hazard, H-SBW-255, is "loss of position sensor" in the steering wheel system, leading to a loss of steering. A hazard control for H-SBW-255 could be to add a second position sensor.

Hazards, hazard controls, and safety requirements must be translated into engineering requirements, quantifying acceptable levels of performance. These translated engineering requirements are integrated with other engineering requirements, and form the specification for the architectural design of the system (Figure 2).

Table 2 MIL-STD-882C Hazard Probability Levels

Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in the life of an item	Will occur frequently
Occasional	C	Likely to occur some time in the life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

Table 3 Example Risk Assessment Matrix

Frequency Severity	A	B	C	D	E
I	Critical	Critical	Critical	High	Mod.
II	Critical	Critical	High	High	Mod.
III	Critical	High	High	Mod.	Low
IV	Mod.	Mod.	Mod.	Low	Low

The preliminary activities of safety analysis, including the PHA, and a failure analysis of the main functional subsystems, permit the specification of a preliminary system architecture that satisfies safety as well as functional requirements. At this point, a more detailed hazard analysis is initiated. The goal of detailed hazard analysis is to identify and justify necessary hazard controls. Detailed hazard analysis provides a better understanding of the potential failure modes of the system, how they lead to hazards, and how proposed

hazard controls can best be combined to eliminate or mitigate potential hazards. A wide variety of hazard analysis techniques exist, and an appropriate subset must be selected. Figure 3 shows a list of possible techniques that can be applied, many of which are detailed in the System Safety Analysis Handbook [7]. The SSWG combines the results of the applied techniques to generate hazard control requirements that are achieved during the detailed design of the system (Figure 2).

Once detailed design is complete, including implementation of necessary hazard controls, the SSWG verifies that potential hazards of the conceptual design have indeed been eliminated or mitigated. Fault injection testing can be performed on software models, bench fixtures, or engineering vehicles to verify that hazard controls operate as intended. All hazard controls must be verified before the SSWG can sign-off on the reasonableness of the system.

Finally, the SSWG typically writes a safety case document for the system, justifying its belief that the system is reasonably safe. In this document, the SSWG summarizes the results of analyses performed and the steps taken to reduce potential risk, identifies the residual potential risk remaining in the system, describes why this level of risk is acceptable, and justifies the SSWG's belief that their assessment is accurate. The safety case is used to determine whether to accept the system's approach to safety.

Generic steer-by-wire example

When establishing a SSWG for a steer-by-wire system, expertise in the following areas is required: systems engineering, controllers, algorithms, motors and mechanical actuators, system safety, and electrical and mechanical reliability.

Once the SSWG is formed, its first task is to write the SSPP. As described above, the SSPP should state how the safety program relates to applicable standards if any. Examples of existing standards include MIL-STD-882C and IEC61508. Note that in North America, there are no MVSS standards that directly relate to steering. The SSPP defines the safety organization and specifies a set of safety tasks that will be performed. A list for steer-by-wire could include:

- Preliminary Hazard Analysis
- Modeling and Simulation
- Fault Tree Analysis (FTA)
- Failure Modes And Effects Analysis (FMEA)
- Software Verification
- Fault Injection Testing: Simulation, Bench, In-Vehicle
- Safety Case

1. Cause-Consequence Analysis
2. Common Cause Analysis
3. Electromagnetic Compatibility (EMC) Analysis and Testing
4. Event Tree Analysis (ETA)
5. Failure Modes And Effects Analysis (FMEA)
6. Failure Modes, Effects, and Criticality Analysis (FMECA)
7. Fault Tree Analysis (FTA)
8. Hazard and Operability Study (HAZOP) Hardware/Software Safety Analysis
9. Modeling
10. Root Cause Analysis
11. Safety Review
12. Sneak-Circuit Analysis
13. Software Failure Modes and Effects Analysis (SFMEA)
14. Software Fault Tree Analysis
15. Software Hazard Analysis
16. Software Sneak Circuit Analysis (SSCA)

Figure 3. Hazard Analysis Techniques

Once the plan is in place, the SSWG begins the preliminary hazard analysis. Typical hazards identified at this level include potential loss of steering—*i.e.*, a loss of ability to change the vehicle direction, which could be due to an electrical or mechanical failure. Other potential hazards include unwanted and erratic steering.

Potential hazards at this level are subdivided into causes at the functional subsystem level and interactions between the subsystems and between the subsystems and the driver and road conditions. As the hazard analysis progresses, the steering wheel, road wheel, and controller subsystems are further structurally divided into architectural components and finally into actual components of the fully defined system. At the same time, the potential hazards are translated into engineering values, such as degrees of deviation from commanded position [4]. Much of this analysis can be done by simulation, but fault injection into instrumented benchtop models and test vehicles is usually helpful.

One method for subdividing hazards to the functional and structural subsystems is by means of a fault-tree analysis tool. Fault tree analysis is a top down approach to study which individual faults or combination of faults could result in the top event hazard. This, in conjunction with the preliminary hazard analysis (PHA), can be used to evaluate design concepts and system configurations, or to guide in the development of hazard controls.

Figure 4 shows a simple fault tree for the potential loss of steering hazard. It includes potential failure modes for the controller, sensors, and actuators that are linked together with an OR gate to create the potential loss of steering hazard.

There are lower-level potential failure modes for the controller, sensors, and actuators that might lead to loss of steering. These potential failure modes would be identified and detailed under one of the three gates shown in Figure 4. The fault tree model can contain non-failure hazards to be avoided as well. Even without the benefit of automated analysis, the notational clarity of hierarchical structure makes fault trees an important hazard analysis tool. The importance of hierarchical hazard analysis was also noted by Bertram et al. [6].

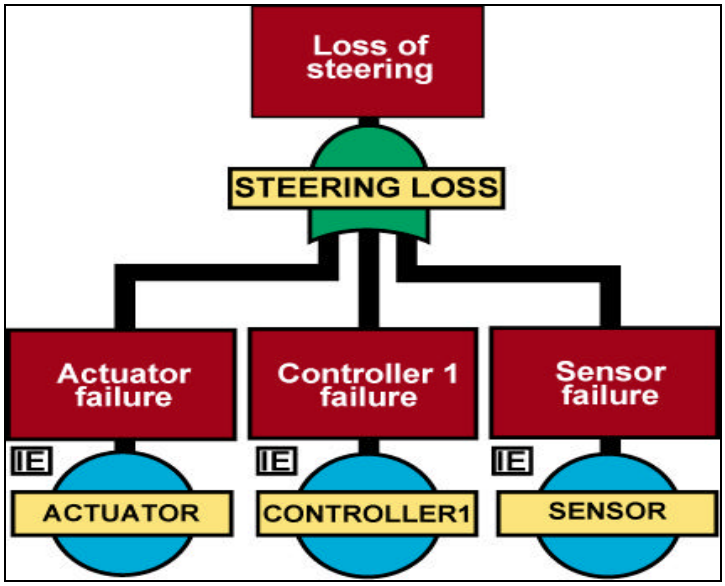

Figure 4. Fault tree for the conceptual design.

As noted, there are many ways of implementing hazard controls.

Of particular interest to complex embedded systems such as steer-by-wire are software-implemented hazard controls. These tasks monitor system states for signs of hazards and take action as required. Some potential hazards in systems such as steer-by-wire, may require fault tolerance because of inherent system limitations. This implies that some

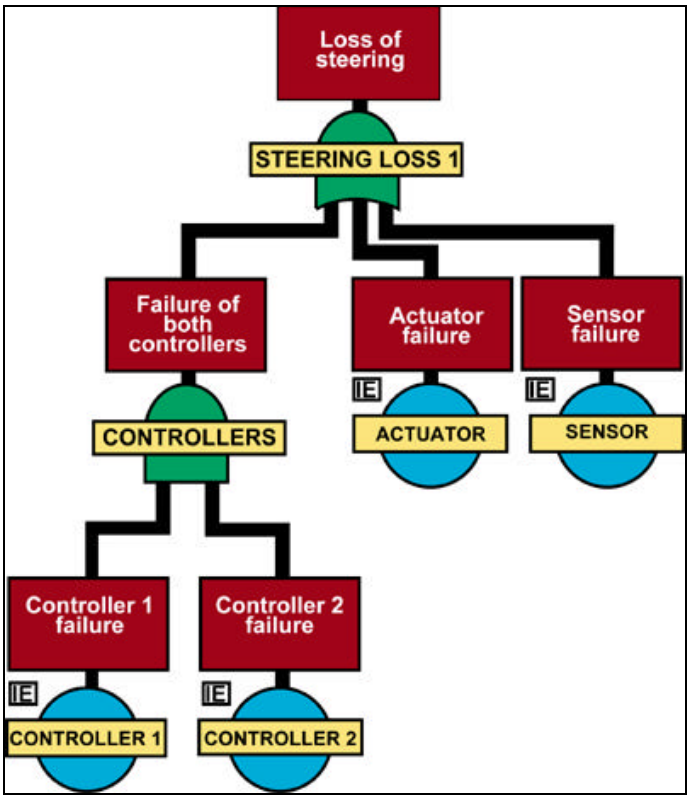

Figure 5. Modified fault tree.

redundancy may be needed in wiring, and/or controllers, and/or actuators, etc.

Next, we show how hazard controls can be linked to the potential hazards they mitigate, to show coverage. This approach also employs a fault tree analysis tool. Starting with the simple fault tree of Figure 4, but introducing the impact of hazard controls for reducing the risk, it is now possible to demonstrate improvements in the safety of the system.

The same likelihood of occurrence is assumed for each event in the fault tree. By introducing hazard controls into the fault tree, the likelihood that certain branches of the tree lead to the top event can be reduced, thus reducing the risk of the hazard. For example, if a redundant controller is added, it can take over for the primary controller if it fails. The addition of the controller reduces the likelihood that the system will fail due to a controller failure (Figure 5), since Controller 1 and Controller 2 must now both fail. From a design perspective, it is important to know how this additional hazard control should be added to the system

so that it can take over when necessary, *e.g.*, warm standby, system voting, etc.

Since hazard controls can be added at a high level, as just illustrated, or at lower sub-system or component levels, the fault tree can be useful in illustrating which of the hazard controls are being implemented, where they are being implemented, and how many exist.

Verification of compliance with the system level safety requirement during a failure can be performed on a test fixture designed to duplicate key vehicle operating conditions. While vehicle tests can be performed on some system samples, a fixture provides a repeatable design verification process by eliminating non-system sources of variation. Due to the correlation between the fixture and the vehicle, a system that complies with the requirements on the fixture would do so when installed in the vehicle.

The last task in the safety program is to prepare the safety case for the system. As explained before, this involves identifying the residual risk remaining in the system, describing why this level of risk is acceptable, and justifying the SSWG's belief that their assessment is accurate. For example, the SSWG must justify that the steer-by-wire design eliminates or mitigates risks associated with the loss of steering hazard.

Summary

A system safety process for by-wire automotive systems has been presented. The main elements include: creating a system safety program plan, performing a variety of hazard analysis and risk assessment tasks as specified in the program plan, designing and verifying a set of hazard controls that mitigate risk, and summarizing the findings. Some details of these tasks were presented and illustrated by applying them to a generic steer-by-wire example.

Contact

Brian T. Murray, Delphi Automotive Systems, 3900 Holland Rd., Saginaw, MI,
brian.t.murray@delphiauto.com

References:

1. N. J. Bahr, *System Safety Engineering and Risk Assessment: A Practical Approach*, Taylor and Francis, Wash. DC, 1997.

2. 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.

3. 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.

4. S. Amberkar, K. Eschtruth, Y. Ding, F. Bolourchi, "Failure Mode Management for an Electric Power Steering System" , ISATA 99AE002, 1999.

5. System Safety Program Requirements, MIL-STD-882C, 1993.
T. Bertram, P. Dominke, and B. Mueller, "The Safety Related Aspect of CARTRONIC", SAE International Congress, paper 1999-01-0488, 1999.

6. System Safety Analysis Handbook, 2nd Ed., System Safety Society, 1997.