FUNCTIONAL SAFETY CONSIDERATIONS FOR FOUNDATIONAL STEERING SYSTEMS

Christopher Becker
John Brewer
Wassim Najm
Larry Yount
U.S. Department of Transportation, Volpe National Transportation Systems Center
United States of America

Paul Rau
U.S. Department of Transportation, National Highway Traffic Safety Administration
United States of America

Paper Number 17-0267

ABSTRACT

As part of its mission to save lives, prevent injuries, and reduce economic costs due to road traffic crashes, the National Highway Traffic Safety Administration (NHTSA) researches methods to ensure the safety and reliability of emerging safety-critical electronic control systems in motor vehicles. As advanced driver assistance systems and other emerging technologies are introduced into new motor vehicles, the overall safety of these advanced electronic systems relies in part on the safety of the underlying foundational systems, such as steering systems.

This study applies the Concept Phase (Part 3) of the ISO 26262 industry standard to two generic representations of foundational steering systems – electric power steering (EPS) and steer-by-wire (SbW). The generic EPS and SbW system architectures were developed based on interviews with industry subject matter experts and through literature describing existing EPS and SbW system designs. The paper outlines one approach to performing a Hazard Analysis and Risk Assessment (HARA) and developing a Functional Safety Concept. The approach incorporates several analysis methods, including Hazard and Operability study, Functional Failure Modes and Effects Analysis, and Systems-Theoretic Process Analysis. This approach is then applied to the EPS and SbW systems to identify vehicle-level hazards, and derive safety goals and functional safety requirements.

The paper presents the vehicle-level hazards and safety goals derived from the analysis and includes a discussion of "fail-safe" and "fail-operational" needs, which may inform the derivation of functional safety requirements. The results of this study may serve as an example for how different analytical methods could be applied to develop a functional safety concept. This study is primarily illustrative of the methods and is not intended to reflect a minimum set of safety requirements for existing or future foundational steering systems. Therefore, this paper does not provide any functional safety requirements.

INTRODUCTION

The mission of the National Highway Traffic Safety Administration (NHTSA) is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes. NHTSA's regulatory authority is largely established around new vehicles. Recognizing the increasing prevalence of electronics in today's motor vehicles, NHTSA established the electronics reliability research area to study the body of methodologies, processes, best practices, and industry standards that are applied to ensure the safe operation and resilience of safety-critical automotive electronic systems.

Two categories of automotive electronic systems – advanced driver assistance systems (ADAS) and highly automated vehicles (HAVs) – are revolutionizing the automotive industry. As these electronics-based advanced vehicle technologies are introduced into new motor vehicles, the overall safety of these advanced electronic systems relies in part on the safety of the underlying foundational systems. While emerging technologies may be designed in accordance with the International Organization for

Standardization (ISO) 26262 functional safety standard.

This paper describes research by the Volpe National Transportation Systems Center (Volpe), in conjunction with NHTSA, to develop an example functional safety concept for generic representations of two such foundational systems – an electric power steering (EPS) system and a steer-by-wire (SbW) system.

Electric Power Steering System

The market share for EPS systems is expected to increase over the next decade. Some estimates predict EPS systems could be installed in over 70 percent of North American vehicles by 2021 [1] [2].

The EPS system is a power-assisted steering system that combines the steering input from the driver with torque from a power-assist motor. The combined steering forces are mechanically transmitted to the road wheels [3]. Depending on the EPS system architecture, the power-assist motor may be located at the steering column or at the rack and pinion. A key element of the EPS system architecture is the persistent mechanical connection between the driver and the road wheels via the steering column.

Figure 1 shows the layout of a generic column assist EPS system architecture.

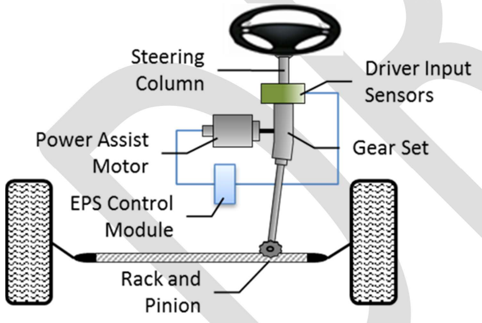

Figure 1. Depiction of a generic column assist EPS system.

In addition to providing power-assist to the driver's steering input, the generic EPS system analyzed in this research includes two additional features: active steering and four-wheel steering (4WS). While these additional features are not ubiquitous in EPS systems, they present unique safety considerations and are illustrative of the advanced functionality that may be introduced through electronics.

The active steering feature enables the EPS to adjust the steering ratio[1] as a function of vehicle speed [3]. For example, with the active steering feature, the EPS control module may decrease the steering ratio at low vehicle speeds to make the vehicle more responsive to the driver's steering command. To provide more stability at higher vehicle speeds, the EPS control module may increase the steering ratio by operating the power-assist motor in the opposite direction of the driver's steering command. The active steering feature also enables steering independent of the driver's input (*e.g.*, crosswind compensation) [4] [5].

The 4WS feature controls the rear-wheel heading based on the driver's steering input and vehicle speed [6]. The rear wheels may turn "in-phase"[2] at higher vehicle speeds to provide more stability (*e.g.*, during lane change maneuvers) or in "reverse-phase"[3] at lower vehicle speeds to provide more maneuverability. In some 4WS configurations, the rear wheels may "toe-in," or point inward, to provide greater directional stability (*e.g.*, during heavy braking).

Steer-by-Wire System

Although several manufacturers and Tier-1 suppliers have performed research on SbW systems, only one production vehicle currently offers SbW as a feature.

The SbW system measures the torque and angle of the driver's steering input and electronically transmits the driver's steering input to the steering actuator assembly (*e.g.,* a steering motor). The steering actuator assembly is responsible for providing all steering forces required to adjust the heading of the road wheels [7] [8] [9]. During normal operation of a SbW system, none of the driver's steering inputs are mechanically transmitted to the road wheels. Since there is no mechanical connection between the steering wheel and the road wheels, the SbW system also simulates all feedback to the driver via a separate feedback motor.

Figure 2 depicts a generic SbW system and its key components.

[1] The steering ratio defines the relationship between how much the heading of the road wheels changes in response to the driver's rotation of the steering wheel.

[2] In-phase means the rear wheels turn in the same direction as the front wheels.

[3] Reverse-phase means the rear wheels turn in the opposite direction of the front wheels.

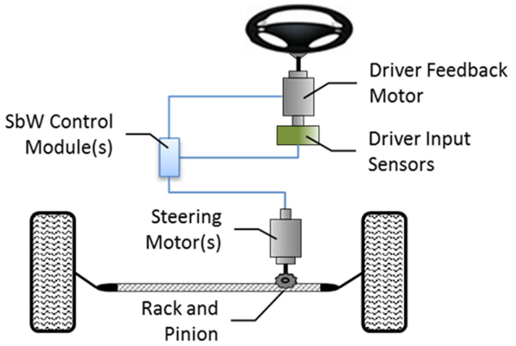

Figure 2. Depiction of a generic SbW system.

This study categorizes SbW systems based on whether they retain vestiges of the mechanical connection between the steering wheel and road wheels. A full SbW system does not include a steering column or other mechanisms for mechanically transmitting the driver's steering input to the wheels. In particular, a full SbW system does not include a mechanical backup subsystem. In contrast, an intermediate SbW system retains the steering column as a mechanical backup subsystem in the event of a failure of the electronic portion of the SbW system [10].

The generic SbW system considered in this research also includes the active steering and 4WS features described previously.

Steering in the Context of Automated Vehicles

The vehicle's steering system, along with the propulsion and braking systems, comprise the foundational actuating systems that enable certain ADAS and HAV technologies. For example, automated lane centering (ALC) systems may rely on the foundational steering system as the primary actuator to steer the vehicle along the desired trajectory.

The SAE International (SAE) document J3016 describes the five levels of automation and the allocation of the steering and acceleration/ deceleration tasks between the driver and the vehicle at each level [11].[4] While other factors further differentiate the five levels of automation, the relevant factors for this paper are described below.

Level 0: No Automation – The human driver is responsible for all steering and acceleration/ deceleration tasks.

Level 1: Driver Assistance – Depending on which features are activated, either the steering or acceleration/deceleration task is executed by the vehicle, but not both. Since the driver retains control over either the steering or acceleration/deceleration task, it can be expected that the driver is fully engaged in the driving task.

Level 2: Partial Automation – The steering and acceleration/deceleration tasks are executed by the vehicle, but the human driver is responsible for monitoring the driving environment and resuming control of the vehicle immediately upon request from the vehicle system. Studies have documented the inherent difficultly for humans to remain engaged in a passive monitoring task with no activity [12] [13] [14]. This issue of whether the driver of a vehicle operating at Level 2 automation is engaged in the driving task is crucial for a proper functional safety analysis. This paper differentiates between scenarios where the driver is fully engaged in the driving task and able to immediately resume control of the vehicle ("Level 2 (Engaged)"), and scenarios where the driver may not be fully engaged in the driving task and is therefore unable to immediately and safely resume control of the vehicle ("Level 2 (Not Engaged)").

Level 3: Conditional Automation – The vehicle executes the steering and acceleration/deceleration tasks and is responsible for monitoring the driving environment. The human driver is responsible for resuming control of the vehicle following an appropriate transition time, during which the vehicle continues to perform the driving tasks.

Level 4: High Automation – The vehicle executes the steering and acceleration/deceleration tasks and is responsible for monitoring the driving environment. The vehicle is capable of reaching a minimum risk state in the event the driver does not resume control of the vehicle when requested. Level 4 automated systems may only operate in certain driving modes (*i.e.*, use cases).

Level 5: Full Automation – The vehicle executes the steering and acceleration/deceleration tasks and is responsible for monitoring the driving environment. The vehicle is capable of reaching a minimum risk state in the event the driver does not resume control of the vehicle when requested. Level 5 automated

[4] In the September 2016 Federal Automated Vehicles Policy, NHTSA adopted the SAE definitions for levels of automation [15].

vehicles operate in all driving modes, in contrast to the restricted set of use cases that define Level 4.

In this paper, the term HAV refers to vehicles operating at automation Levels 3 through 5 [15]. ADAS typically operate at lower levels of automation (Levels 1 and 2).[5]

FUNCTIONAL SAFETY METHOD AND APPROACH

The automotive industry developed ISO 26262 to address safety challenges stemming from the trend of increasing complexity, software content, and mechatronics implementation; and the risks associated with both systematic and random hardware failures [16]. Specifically, ISO 26262 focuses on mitigating risks resulting from malfunctions of electrical and electronic systems. This research identifies and analyzes potential hazards that could result from electrical or electronic failures which impact the functions of vehicular control systems. The study follows Part 3 of ISO 26262 to identify the integrity requirements of these functions at the concept level, independent of implementation variations.

This study also considers potential causes that could lead to such functional failures and documents the technical requirements the ISO 26262 process suggests with respect to the identified Automotive Safety Integrity Level (ASIL) of the item under consideration. While this study does not go into implementation strategies to achieve these ASILs, ISO 26262 provides a flexible framework and explicit guidance for manufacturers to pursue different methods and approaches to do so. Manufacturers employ a variety of techniques, such as ASIL decompositions, driver warnings, fault detection mechanisms, plausibility checks, redundancies, etc., to achieve the necessary ASILs that effectively mitigate the underlying safety risks.

Figure 3 illustrates the hazard analysis and safety requirements development process applied in this study, which is adopted from the Concept Phase (Part 3) of ISO 26262 [16].

Item Definition

The Functional Safety Concept process shown in Figure 3 begins with the item definition. The two hazard analysis techniques applied in this study, Hazard and Operability Study (HAZOP) and Systems-Theoretic Process Analysis (STPA) require different system representations. Therefore, the item definition for the EPS and SbW systems included enumerating the functions of each system to support HAZOP and modelling each system as a hierarchical control structure to support STPA.

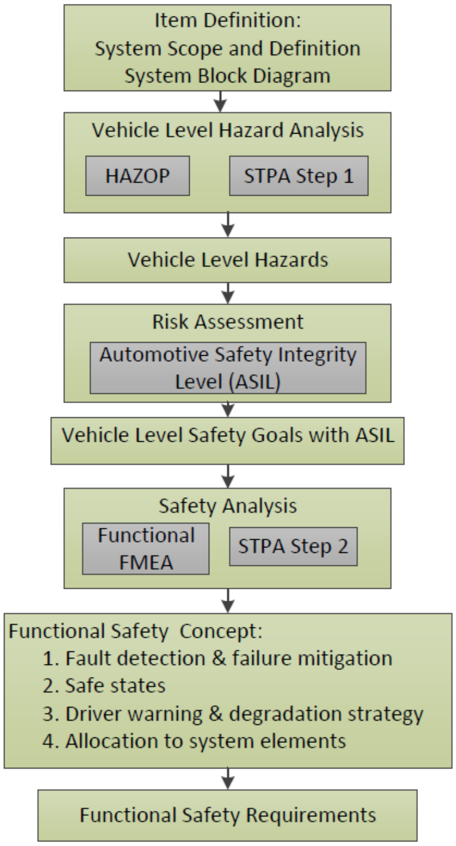
Item Definition:
System Scope and Definition
System Block Diagram
Vehicle Level Hazard Analysis
HAZOP
STPA Step 1
Vehicle Level Hazards
Risk Assessment
Automotive Safety Integrity Level (ASIL)
Vehicle Level Safety Goals with ASIL
Safety Analysis
Functional FMEA
STPA Step 2
Functional Safety Concept:
1. Fault detection & failure mitigation
2. Safe states
3. Driver warning & degradation strategy
4. Allocation to system elements
Functional Safety Requirements

Figure 3. Functional Safety Concept process applied in this study.

Hazard Analysis

This study independently applied two hazard analysis methods to identify the vehicle-level hazards. HAZOP begins with a list of system functions and postulates how deviations of those functions (*i.e.*, malfunctions) may result in one or more vehicle-level hazards [17]. STPA models the system as a hierarchical control structure, where proper controls and communications in the system ensure the desired outcome for emergent properties such as safety [18]. In the STPA framework, a system will not enter a hazardous state unless a controller issues an unsafe control action (UCA) or fails to issue a control action needed to maintain safety. The first part of STPA,

[5] Traffic jam assistant, which follows a lead vehicle while keeping the vehicle centered in the lane at low speeds, is one example of this type of ADAS system.

STPA Step 1, focuses on identifying these UCAs in an iterative process to determine the vehicle-level hazards.

These two hazard analysis methods consider the system operation through different frameworks – functions and control actions. Independently performing HAZOP and STPA Step 1 and synthesizing the resulting hazards, may help yield a more comprehensive analysis – either by one method identifying additional hazards or by the two methods independently confirming the same set of hazards.

Risk Assessment
This study applied the ASIL risk assessment process described in ISO 26262. In this risk assessment process, analysts assign an ASIL to each hazard by evaluating the dimensions of severity, exposure, and controllability for a set of operational situations [16]. ISO 26262 defines discrete values for each of the three dimensions used to determine the ASIL. For example, exposure values range from "E0" for operational scenarios with the lowest frequency to "E4" for operational scenarios with the highest frequency. The ASILs themselves range from "A," which is the least critical ASIL rating, to "D," which is the most critical ASIL rating. In addition to the four ASIL ratings, ISO 26262 specifies a quality management (QM) category for hazardous events that do not achieve the minimum level of ASIL A [16].

Safety Goals
Each identified hazard was assigned a safety goal, in accordance with ISO 26262. Safety goals are the top-level safety requirements on the system. The set of safety goals identified for a system should address all the identified vehicle-level hazards [16].

Safety Analysis
As with the hazard analysis step, this study independently applied two safety analysis methods to identify possible failures and causal factors that could potentially result in a vehicle-level hazard.

The Functional Failure Modes and Effects Analysis (FMEA) was adapted from SAE Standard J1739 [19]. The Functional FMEA focused on the identification of failure modes, potential effects, and potential failure causes or mechanisms based on the system's functional behavior. Since this study is implemented at the concept phase and is not based on a specific design, probability estimations for failures and detection of failures were not performed.

The second part of STPA, STPA Step 2, involves analyzing each component and interaction in the control structure representation of the system to determine if the component or the interaction may contribute to one of the UCAs identified in STPA Step 1. This generates a set of causal factors or scenarios that can support the development of functional safety requirements.

Functional Safety Concept and Requirements
This study developed an example functional safety concept and example functional safety requirements by following the remaining portions of Part 3 of ISO 26262. According to ISO 26262, elements considered as part of the functional safety concept include [16]:

- Fault detection and failure mitigation;
- Transitioning to a safe state;
- Fault tolerance mechanisms;
- Fault detection and driver warning; and
- Arbitration logic.

The functional safety concept and requirements developed in this study are intended to illustrate the ISO 26262 process and are not intended to reflect a minimum set of safety requirements for existing or future foundational steering systems. Therefore, this paper does not include any functional safety requirements.

RESULTS

Hazard Analysis
Examples of the HAZOP and STPA Step 1 analyses are provided in Table 1 and Table 2, respectively.

Table 1.
Example HAZOP analysis

Potential Hazard	Unintended vehicle lateral motion/ unintended yaw
Malfunction (Incorrect direction)	Measures torque in the opposite direction.
Function	Detects steering torque input from the driver.

Table 2.
Example STPA Step 1 analysis

Potential Hazard	Unintended vehicle lateral motion/ unintended yaw
Unsafe Control Action	The steering control module commands the rear-wheels to turn in reverse-phase when: • steering is not commanded by the driver or other vehicle systems.
Control Action	Commands the rear wheels to turn in reverse-phase

The HAZOP and STPA analyses identified four potential vehicle-level hazards that may apply to a generic EPS system and six potential vehicle-level hazards that may apply to a generic SbW system. Three potential hazards were common to both the EPS and SbW systems, while the remaining potential hazards applied only to one system. Table 3 presents the potential vehicle level-hazards identified in this study along with the applicable foundational steering system. Each potential hazard is described in more detail in the remainder of this subsection.

Table 3.
Identified potential vehicle-level hazards

Potential Vehicle Level Hazard	**System**	
	EPS	**SbW**
Unintended vehicle lateral motion/ unintended yaw	●	●
Insufficient vehicle lateral motion/ unintended yaw	●	●
Unintended loss of steering assist	●	
Loss of vehicle lateral motion control		●
Reduced responsiveness to the driver's commands due to increased rear-wheel drag	●	●
Incorrect feedback resulting in an incorrect driver reaction		●
Intermittent response to steering control input		●

Since this study only considers generic representations of the EPS and SbW systems, the potential hazards presented in Table 3 may differ or may not apply to specific steering system designs.

Unintended vehicle lateral motion/unintended yaw describes situations where the vehicle moves laterally more than, at a faster rate than, or in the opposite direction of the steering commanded by the driver or another vehicle system controller. This hazard also covers situations where the driver's steering command overrides an active safety system, resulting in more steering than is necessary to maintain the safety of the vehicle.

Insufficient vehicle lateral motion/unintended yaw describes situations where the vehicle moves laterally, but less than or at a slower rate than the steering commanded by the driver or another vehicle system controller. This hazard also covers situations where the driver's steering command overrides an active safety system, resulting in less steering than is necessary to maintain the safety of the vehicle.

Unintended loss of steering assist describes situations where the EPS system becomes unavailable in an uncontrolled manner (*e.g.*, the loss of assist is sudden and the driver is not notified). However, mechanical steering is still available. Since the scope of ISO 26262 is limited to electric and electronic systems, this study did not consider the loss of mechanical steering in EPS systems.

Loss of vehicle lateral motion control is specific to the SbW system, where all steering requests are transmitted electronically. This hazard describes situations where the SbW system does not respond to steering inputs from the driver or other vehicle systems.

Reduced responsiveness to the driver's commands due to increased rear-wheel drag only applies to vehicles equipped with the 4WS feature. This hazard describes an incorrect rear-wheel position that causes an increased drag effect, slowing the vehicle, but not at a level that results in significant vehicle deceleration. This drag effect may also affect the vehicle's response to driver inputs, for instance if the driver is trying to steer.

Since SbW systems simulate all feedback to the driver, *incorrect feedback resulting in incorrect driver reaction* describes situations where the feedback provided at the steering wheel is incorrect and sufficiently misleading that it causes the driver to incorrectly steer the vehicle. Examples of incorrect feedback to the driver may include delayed, missing, or counterintuitive feedback.

Intermittent response to steering control input describes situations where the SbW system does not provide a smooth or consistent response to steering inputs. Examples of this hazard may include a jerky response to steering inputs or a delayed steering response.

Safety Goals and ASILs

Details of the ASIL classification exercise and the establishment of safety goals will be published in a separate report.

Example Fault Tolerant Architectures

This study considered example fault tolerant architectures for the EPS and SbW systems as part of the functional safety concept. These fault tolerant architectures were identified based on the results of the safety analysis and the set safety goals, and provided a framework for the derivation of the more detailed functional safety requirements.

Considerations for fault tolerant architectures are particularly important for SbW systems, since SbW systems do not have a direct mechanical connection between the driver and the front-wheels during normal operation; a key component of the functional safety concept is ensuring that the driver retains a minimum level of steering capability following an electronic fault in the SbW system. This study provided examples of two architectural strategies that could achieve this requirement: “Fail Safe” and “Fail Operational.”

Fail-safe – An electronic system is “Fail-Safe” if the system transitions to a safe state to ensure safety of the system following one (or several) failure(s) [20]. An intermediate SbW system is an example of a fail-safe architecture, where the system transitions to a safe state, such as engaging the mechanical backup, following detection of an electronic fault in the SbW system. Similarly, a fail-safe EPS system architecture would transition to a safe state, such as reverting to purely mechanical steering, following the detection of an electronic fault in the EPS system. For fail-safe architectures, it is important to ensure that the system does not violate any of the safety goals when transitioning to a safe state. In addition, the driver should receive the appropriate notification as the system transitions to a safe state.

Fail-safe systems may incorporate redundancy such that no single electronic fault is capable of resulting in a critical hazard. However, a fail-safe architecture may not require the same level of redundancy as a fail-operational architecture, since the system is designed to transition to a safe state immediately following detection of a fault. For example, a fail-safe architecture may only include two redundant controllers. If there is a disagreement due to an internal electronic fault in either of the controllers, the system transitions to a safe state. Fault effect independence must be validated through a method such as Common Mode Analysis (CMA).

Figure 4 shows examples of key fail-safe concepts as applied to a SbW system.

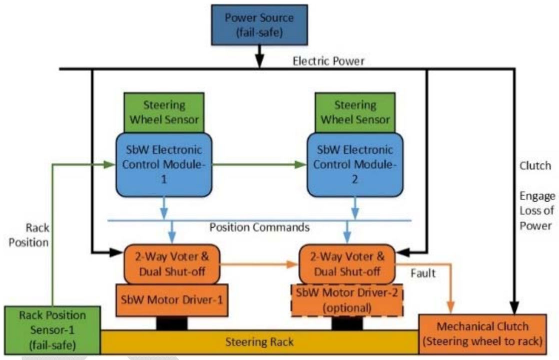
Power Source
(fail-safe)
Electric Power
Steering Wheel Sensor
Steering Wheel Sensor
SbW Electronic Control Module-1
SbW Electronic Control Module-2
Clutch
Engage on Loss of Power
Rack Position
Position Commands
2-Way Voter & Dual Shut-off
2-Way Voter & Dual Shut-off
Fault
SbW Motor Driver-1
SbW Motor Driver-2 (optional)
Rack Position Sensor-1 (fail-safe)
Steering Rack
Mechanical Clutch (Steering wheel to rack)

Figure 4. Example fail-safe concepts as applied to a generic SbW system.

Fail operational – An electronic system is “Fail Operational” if any first electronic fault is detected and does not result in a loss of any primary electronic system functionality that is essential to the safety of the system [20]. In the case of a full SbW system, this means ensuring that the SbW system continues to provide steering in response to the driver’s steering commands without violating any of the system’s safety goals. A fail-operational EPS system would be capable of providing full electronic steering assistance to the driver following any first electronic fault.

Following any first electronic fault, if the degraded system is no longer fail-operational to any subsequent fault, the system may then only qualify as fail-safe. Essentially, the system can safely sustain a minimum of two fully independent electronic faults prior to loss of primary system functionality, at which point the system would need to transition to an associated safe state. As with the fail-safe architecture, independence of the effects of these faults can be validated using techniques such as CMA.

Redundancy is commonly used to ensure a fail-operational architecture. Redundancy can be physical redundancy, such as multiple fully redundant computing elements that “vote” their outputs. Thus, when one element is “out-voted,” a fault is presumed and the faulted element is blocked from asserting control on the system. Alternatively, “analytical redundancy” may be used. By using independent data streams, encoding methods, and evaluation algorithms, fault effects associated with data corruption could be identified and mitigated.

Common fail-operational architectures include “triplex,” which employs a three-way voting scheme, and “dual fail-safe,” which employs two fail-safe or fail-silent[6] elements. In the dual fail-safe architecture, if either element detects a failure, that element is blocked from asserting control on the system. Fail-operational architectures may also be extended to provide additional levels of fault tolerance (*e.g.*, capable of sustaining three independent faults before losing primary system functionality) [20].

Figure 5 shows examples of key fail-operational concepts as applied to a SbW system, by depicting a triplex architecture with a three-way voting scheme for the controllers and a dual fail-safe architecture for the power supply.

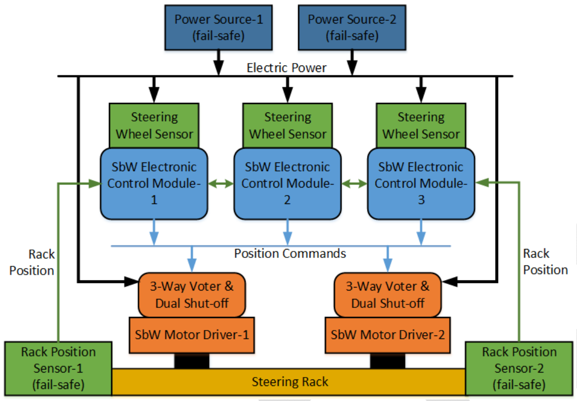
Power Source-1 (fail-safe)
Power Source-2 (fail-safe)
Electric Power
Steering Wheel Sensor
Steering Wheel Sensor
Steering Wheel Sensor
SbW Electronic Control Module-1
SbW Electronic Control Module-2
SbW Electronic Control Module-3
Position Commands
Rack Position
Rack Position
3-Way Voter & Dual Shut-off
3-Way Voter & Dual Shut-off
SbW Motor Driver-1
SbW Motor Driver-2
Rack Position Sensor-1 (fail-safe)
Steering Rack
Rack Position Sensor-2 (fail-safe)

Figure 5. Example fail-operational concepts as applied to a generic SbW system.

In the fail-operational schematic shown in Figure 5, there is no mechanical backup for the primary steering function. Instead, the configuration of controllers, sensors, power supplies, and actuators is sufficiently redundant to provide full steering capability following any single electronic failure. In addition to redundancy, detection and mitigation of electronic faults in each subsystem is another key element of the fail-operational schematic shown in Figure 5.

The switch to the redundant system (or removal of defective control path from contributing to the actual steering control of the vehicle) needs to happen with sufficient speed to avoid inducing driver errors or violating any of the safety goals. In addition, the driver should receive the appropriate notification of the error and indication that the vehicle requires service since the designed level of redundancy no longer exists.

Example Safe States

The functional safety concept also includes consideration of safe states. ISO 26262 defines a safe state as an operating mode of the item without an unreasonable risk [16]. A safe state may be the intended operating mode, a degraded operating mode, or a switched off mode. The developer of the functional safety concept attempts to maximize the availability of the item while ensuring the safety of the vehicle operation. Therefore, a careful consideration is given to selecting the safe states in relation to the potential failure modes.

Table 4 presents example safe states for the generic EPS system analyzed in this study. For all the example safe states presented in Table 4, the system would also provide appropriate notification to the driver.

Table 4.
Example safe states for a generic EPS system

	Example Safe State
1	Disable steering assist at high speeds (restrict steering assist to low speeds)
2	Disable rear-wheel steering assist and return rear wheels to straight-ahead position
3	Disable all steering assist

The first two safe states describe operating modes of the EPS system with reduced functionality. Specifically, each of these safe states disables certain advanced steering functions while leaving the core EPS system intact. In the third safe state, the EPS system is disabled completely and the foundational steering system reverts to purely mechanical steering. Mechanical steering does not provide power steering assist and would not support advanced features such as active steering or 4WS. Transition to the mechanical backup system would generally be combined with appropriate notification to the driver.

Table 5 presents example safe states for a generic SbW system. Table 5 indicates which safe states apply to full SbW systems and which apply to intermediate SbW systems. For all the example safe states presented in Table 5, the system would also provide appropriate notification to the driver.

[6] A fail-silent element may shut off or enter another state that does not provide any outputs to the remainder of the system after one (or several) failure(s) [20].

Table 5.
Example safe states for a generic SbW system

Example Safe State		Full SbW	Inter. SbW
1	Issue a driver notification, but retain full steering availability	●	●
2	Restrict propulsion (*e.g.*, limp-home mode)	●	
3	Gradually reduce propulsion until vehicle stops	●	
4	Engage mechanical back-up system		●
5	Disable feedback motor	●	●
6	Disable rear-wheel steering assist and return rear wheels to straight-ahead position	●	●

For the first safe state, the driver is notified of the presence of a fault, but the SbW can continue to operate with full steering availability – if the system architecture can safely allow for full operation following the fault (*i.e.*, the system is fail-operational). If an intermediate SbW system is designed to be fail-operational, this first safe state may apply. However, if an intermediate SbW system is only designed to the level of fail-safe, then the SbW system may not support this safe state.

In full SbW systems where the system can no longer ensure safe operation – for example, following failure of multiple redundant elements – the safe states may include gradual reduction of the vehicle speed, as described by the second and third safe states [9].

In intermediate SbW systems, the system may engage the mechanical back-up system to maximize the availability of the vehicle systems in lieu of other approaches, such as reducing vehicle speed. The mechanical backup steering subsystem may have reduced functionality. For example, the mechanical backup may not respond to the driver's steering inputs with the same steering profile as the normally-operating SbW system (*e.g.*, no power steering). Furthermore, the mechanical backup may not support advanced features such as active steering or 4WS. Transition to the mechanical backup system would generally be combined with appropriate notification to the driver.

The fifth and sixth safe states describe disabling certain features of the SbW system, but these safe states retain the primary functionality (*i.e.*, steering).

DISCUSSION

Foundational Steering Systems in the Context of ADAS and HAVs

The example functional safety concepts presented in this study were based on generic EPS and SbW systems, such as those that may be found in Level 0, Level 1, and Level 2 (Engaged)[7] automated vehicles. However HAVs and Level 2 (Not Engaged)[8] automated vehicles may impose additional requirements on the foundational steering systems that might not be apparent during an initial analysis. These additional requirements arise when considering the interface between the ADAS or HAV system and the foundational steering system. These interfaces might not be fully apparent until the ADAS or HAV system design is sufficiently mature.

In particular, the example functional safety concepts for the generic EPS and intermediate SbW system specify a fail-safe architecture. The safe states for these systems include immediately reverting to manual control – either by disabling the system electronics, as in the EPS system, or by engaging a separate mechanical backup, as in the intermediate SbW system. However, HAVs must provide the driver with sufficient notification before reverting to manual control. In the event of a failure in a fail-safe EPS or SbW system, immediately reverting to manual control would not support the HAV requirement to continue operating until the driver resumes control of the vehicle. While not a HAV, ADAS operating at Level 2 (Not Engaged) may encounter similar challenges since the driver may not be sufficiently engaged to resume steering immediately.

Two possible approaches for implementing foundational steering systems that support the full range of ADAS and HAV systems include:

[7] Level 2 (Engaged) describes a subset of Level 2 automated vehicles where the automated system is capable of ensuring the driver remains fully engaged in the driving task. Since the driver is fully engaged in the driving task, it is more likely that the Level 2 assumption that the driver can immediately assume control of the vehicle is valid.

[8] Level 2 (Not Engaged) describes a subset of Level 2 automated vehicles where the automated system cannot ensure that the driver is fully engaged in the driving task, increasing the potential for the driver to misuse (*e.g.*, over-rely on) the system. In these instances, the Level 2 assumption that the driver can immediately assume control of the vehicle may not be valid.

- A single fully fail-operational foundational steering system, such as a fail-operational SbW system.
- Pairing a fail-safe foundational steering system with a second foundational system that provides redundant actuation of the ADAS and HAV system commands. For example, differential braking via the brake/stability control system may be able to execute ADAS or HAV system commands in the event of a failure that disables the electronic portion of the steering system [21].

As ADAS become more prevalent and HAVs are introduced, the foundational steering systems, along with other foundational vehicle systems, may need to be reassessed to determine if the introduction of ADAS and HAVs impose additional requirements on these systems. As these technologies continue to mature, additional solutions may also be developed that are capable of ensuring the foundational steering systems can meet the requirements imposed by ADAS and HAVs.

CONCLUSIONS

This study applied the Concept Phase of the ISO 26262 functional safety standard to two generic foundational steering systems – an EPS system and a SbW system. The functional safety process presented in Figure 1 incorporates multiple hazard and safety analysis methods, and in particular illustrates how a newer hazard analysis method – STPA – can be incorporated into the functional safety process. Although not required in ISO 26262, application of multiple hazard analysis processes may help ensure all relevant vehicle-level hazards are identified.

This study developed example functional safety concepts for the EPS and SbW system. As part of the functional safety concept, this study provided examples of fault tolerant architectures that may apply to foundational steering systems. However, the applicability of these fail-safe and fail-operational architectures to the foundational steering systems may be affected by requirements imposed by higher level ADAS or HAV systems.

Finally, this paper highlights challenges with the key assumption that drivers are always available to immediately resume control in vehicles with Level 2 automated systems. In particular, for systems that cannot ensure the driver is fully engaged in the driving task, Level 2 (Not Engaged), the driver may not be able to immediately resume control of the vehicle. This case may require special consideration in terms of the fault tolerant architecture of the foundational steering system. Additional research may be necessary to determine the conditions under which this assumption for Level 2 vehicles is not valid and to identify driver monitoring strategies that ensure the driver is fully engaged in the driving task.

REFERENCES

[1] Frost & Sullivan, "Active Safety and Fuel Economy Features Push the Use of Electric Power Steering in North American Cars," Frost & Sullivan, [Online]. Available: http://images.discover.frost.com/Web/FrostSullivan/NA_PR_JCarson_NEA5-18_15Dec14.pdf. [Accessed 22 September 2015].

[2] H. Greimel, "NSK: Electric Power Steering Saves Fuel," Automotive News, 4 August 2014. [Online]. Available: http://www.autonews.com/article/20140804/OEM10/308049987/nsk:-electric-power-steering-saves-fuel. [Accessed 22 September 2015].

[3] ZF Lenksysteme, "ZF Active Steering in the Steering Column," [Online]. Available: http://www.bosch-automotive-steering.com/fileadmin/_migrated/content_uploads/Aktivlenkung_Lenksaeule_0911_E.pdf. [Accessed 5 August 2015].

[4] B. Prope, "Ford's Electric Steering Enables Pull-Drift Technology," WardsAuto, 17 Mar 2009. [Online]. Available: http://wardsauto.com/news-analysis/ford-s-electric-steering-enables-pull-drift-technology. [Accessed 12 January 2017].

[5] K. Reif, Ed., Brakes, Brake Control and Driver Assistance Systems: Function, Regulation and Components (Bosch Professional Automotive Information), Springer Vieweg, 2014.

[6] American Honda Motor Co., Inc., "2015 Acura TLX: Chassis - Model Press Kit," Honda News, 4 August 2014. [Online]. Available: http://www.hondanews.com/channels/tlx-press-kit/releases/2015-acura-tlx-chassis. [Accessed 5 August 2015].

[7] J. R. Pimentel, "An Architecture for a Safety-Critical Steer-by-Wire System," in *SAE 2004 World Congress & Exhibition*, Detroit, 2004.

[8] H.-D. Heitzer, "Development of a Fault-Tolerant Steer-by-Wire Steering System," *Auto Technology,* pp. 56-60, 4 2003.

[9] D. Cesiel, M. C. Gaunt and B. Daugherty, "Development of a Steer-by-Wire System for the GM Sequel," in *2006 SAE World Congress*, Detroit, 2006.

[10] Nissan Motor Corporation, "Direct Adaptive Steering," Nissan, [Online]. Available: http://www.nissan-global.com/EN/TECHNOLOGY/OVERVIEW/direct_adaptive_steering.html. [Accessed 12 January 2017].

[11] SAE International, *J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems,* 2014.

[12] O. Carsten, F. Lai, A. Jamson and N. Merat, "Control task substitution in semiautomated driving: does it matter what aspects are automated?," *Human Factors,* vol. 54, no. 5, pp. 747-761, 2012.

[13] R. Llaneras, J. Salinger and C. Green, "Human factors issues associated with limited ability autonomous driving systems: Drivers' allocation of visual attention to the forward roadway," in *7th International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design*, 2013.

[14] C. Rudin-Brown and H. Parker, "Behavioural adaptation to adaptive cruise control (ACC); implications for preventive strategies," *Transportation Research Part F-Traffic Psychology and Behaviour,* vol. 7, no. 2, pp. 59-76, 2004.

[15] National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy,* 2016.

[16] *ISO 26262 Road Vehicles - Functional Safety, Final Draft (FDIS),* 2011.

[17] International Electrotechnical Commission, "IEC 61882: Hazard and Operability Studies (HAZOP Studies) - Application Guide," 2001-05, Edition 1.0.

[18] N. Leveson, Engineering a Safer World, Cambridge: MIT Press, 2012.

[19] Society of Automotive Engineers, "SAE J1739: Potential Failure Mode and Effects Analysis in Design and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes," 1994-07.

[20] R. Isermann, R. Schwarz and S. Stölzl, "Fault-Tolerant Drive-by-Wire Systems," *IEEE Control Systems Magazine,* pp. 64-81, October 2002.

[21] J.-w. Lee, N. K. Moshchuk and S.-K. Chen, "Lane Centering Fail-Safe Control Using Differential Braking". US Patent 20,120,283,907, 8 November 2012.

[22] S. Choi, F. Thalmayr, D. Wee and F. Weig, "Advanced driver-assistance systems: Challenges and opportunities ahead," Feburary 2016. [Online]. Available: http://www.mckinsey.com/industries/semiconductors/our-insights/advanced-driver-assistance-systems-challenges-and-opportunities-ahead.