U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

NHTSA

DOT HS 812 574

August 2018

Functional Safety Assessment of a Generic, Conventional, Hydraulic Braking System With Antilock Brakes, Traction Control, and Electronic Stability Control

Notice

This document is disseminated under the sponsorship of the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation or the National Highway Traffic Safety Administration. The U.S. Government assumes no liability for use of the information contained in this document.

This report does not constitute a standard, specification, or regulation.

If trade or manufacturers' names or products are mentioned, it is because they are considered essential to the object of the publications and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Suggested APA Format Citation:

Becker, C., Arthur, D., & Brewer, J. (2018, August). *Functional safety assessment of a generic, conventional, hydraulic braking system with antilock brakes, traction control, and electronic stability control* (Report No. DOT HS 812 574). Washington, DC: National Highway Traffic Safety Administration.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No.0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	August 2018	July 2015 – August 2016

4. TITLE AND SUBTITLE
Functional Safety Assessment of a Generic, Conventional, Hydraulic Braking System with Antilock Brakes, Traction Control, and Electronic Stability Control

5. FUNDING NUMBERS
Intra-Agency Agreement
DTNH22-15-V-00022
51HS6CA200

6. AUTHORS
Christopher Becker, David Arthur, and John Brewer

7. PERFORMING ORGANIZATION NAME AND ADDRESS
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-NHTSA-16-08

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
National Highway Traffic Safety Administration
1200 New Jersey Avenue SE
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
DOT HS 812 574

11. SUPPLEMENTARY NOTES
Paul Rau was Contracting Officer Representative for this project.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

12b. DISTRIBUTION CODE
This document is available to the public through the National Technical Information Service, www.ntis.gov.

13. ABSTRACT
This report describes the research effort to assess the functional safety of foundational braking systems, specifically focusing on conventional hydraulic braking systems that includes antilock brakes, traction control and electronic stability control, which are typically included in current generation vehicles. This study follows the concept phase process in the ISO 26262 standard and applies a hazard and operability study, functional failure mode effects analysis, and systems theoretic process analysis methods. In total, this study identifies eight vehicle-level safety goals and 198 CHB system functional safety requirements (an output of the ISO 26262 process). This study uses the results of the analysis to develop potential test scenarios and identify possible areas for diagnostic trouble code coverage.

14. SUBJECT TERMS
conventional hydraulic braking, antilock braking system, ABS, traction control system, TCS, electronic stability control, ESC, hazard and operability study, HAZOP, failure mode effects analysis, FMEA, systems theoretic process analysis, STPA, ISO 26262, hazard analysis, risk assessment, HARA, and functional safety requirements.

15. NUMBER OF PAGES
147

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	

Foreword

NHTSA's Automotive Electronics Reliability Research Program

The mission of the National Highway Traffic Safety Administration is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes. As part of this mission, NHTSA researches methods to ensure the safety and reliability of emerging safety-critical electronic control systems in motor vehicles. The electronics reliability research area focuses on the body of methodologies, processes, best practices, and industry standards that are applied to ensure the safe operation and resilience of vehicular systems. More specifically, this research area studies the mitigation and safe management of electronic control system failures and making operator response errors less likely.

NHTSA has established five research goals for the electronics reliability research program to ensure the safe operation of motor vehicles equipped with advanced electronic control systems. This program covers various safety-critical applications deployed on current generation vehicles, as well as those envisioned on future vehicles that may feature more advanced forms of automation and connectivity. These goals are:

1. Expand the knowledge base to establish comprehensive research plans for automotive electronics reliability and develop enabling tools for applied research in this area;
2. Strengthen and facilitate the implementation of safety-effective voluntary industry-based standards for automotive electronics reliability;
3. Foster the development of new system solutions for ensuring and improving automotive electronics reliability;
4. Research the feasibility of developing potential minimum vehicle safety requirements pertaining to the safe operation of automotive electronic control systems; and
5. Gather foundational research data and facts to inform potential future NHTSA policy and regulatory decision activities.

This Report

This publication is part of a series of reports that describe NHTSA's initial work in the automotive electronics reliability program. This research project specifically supports the first, second, fourth, and fifth goals of NHTSA's electronics reliability research program by gaining understanding on both the functional safety requirements for Automated lane centering control systems and related foundational systems, and how the industry standard may enhance safety.

Specifically, this report describes the research effort to assess the functional safety and derive safety requirements related to a generic conventional hydraulic brake (CHB) system that includes features such as antilock brakes, traction control, and electronic stability control. This supports the overall project objective of assessing the functional safety of ALC systems, and the

foundational steering and braking control systems upon which these ALC systems are based. The analysis described in this report follows the Concept Phase of the ISO 26262 standard.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

A/D	analog/digital
ABS	antilock braking System
ACC	adaptive cruise control
ACS/ETC	accelerator control system/electronic throttle control
AIS	Abbreviated Injury Scale
ALC	automated lane centering
ASIL	Automotive Safety Integrity Level
BPP	brake pedal position
BPPS	brake pedal position sensor
CAN	controller area network
CF	causal factor
CHB	conventional hydraulic braking
CIB	crash imminent braking
CPU	central processing unit
DTC	diagnostic trouble code
DVI	driver-vehicle interface
EEPROM	electronically erasable programmable read-only memory
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ESC	electronic stability control
ESD	electrostatic discharge
FARS	Fatality Analysis Reporting System
FMEA	failure mode effects analysis[1]
FMVSS	Federal Motor Vehicle Safety Standard
FTTI	fault tolerant time interval
GES	General Estimates System
HAZOP	Hazard and Operability Study
I/O	input/output
IC	integrated circuit
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization

[1] Editor's Note: The term "Failure Mode Effects Analysis," FMEA, was coined by the Department of Defense in 1949 in a military standard called MIL-P-1629, which later morphed into MIL-STD-1629 and its amended forms, cited in this report. Over the years, the term itself has changed, sometimes using "Modes," plural, instead of "Mode," and sometimes inserting the word "and," to Failure Mode *and* Effects Analysis. It is clear in the original that the term means the effects of a failure mode, not a failure mode or modes AND effects thereof. As such, the term must remain unitary as "failure mode effects," and the totality as an analysis of those effects. Thus, NHTSA prefers to use "failure mode effects analysis" as it preferred term in respect to father and son, MIL-P-1629 and MIL-STD-1629, without necessarily asserting that other forms of the term are "wrong." Variant terms are left as they are when quoting or citing a source, but is changed or "corrected" as well as lowercased (because it is a generic form of analysis) in text.

KAM	keep alive memory
MIL	malfunction indicator light
ms	millisecond
QM	quality management
RAM	random access memory
ROM	read-only memory
SAE	SAE International, formerly the Society of Automotive Engineers
SG	safety goal
SOH	state of health
STPA	system-theoretic process analysis
T_b	braking torque
TBD	to be determined
TCS	traction control system
T_e	propulsion/engine torque
T_r	road surface frictional torque
UCA	unsafe control action
UNECE	United Nations Economic Commission for Europe
V	velocity
Volpe	Volpe National Transportation Systems Center
VOQ	vehicle owner questionnaire
WSS	wheel speed sensor

EXECUTIVE SUMMARY

The National Highway Traffic Safety Administration established the electronics reliability research area to study the mitigation and safe management of electronic control system failures and operator response errors. This project supports NHTSA's electronics reliability research area by:

- Expanding the knowledge base for automated lane centering systems and the foundational steering and braking systems upon which ALC relies.
- Providing an example for implementing a portion of the voluntary, industry-based functional safety standard, the International Organization for Standardization's ISO 26262.
- Deriving example functional safety requirements.
- Providing research to inform potential future NHTSA policy and regulatory decision activities.

As advanced driver assistance systems and other automated technologies are introduced into the nation's fleet, the safety of these systems will depend in part on the safety of the underlying foundational vehicle systems. While emerging technologies may be designed in accordance with the ISO 26262 functional safety standard, many foundational systems currently deployed are legacy systems that predate ISO 26262.

This report describes research by the Volpe National Transportation Systems Center, supported by NHTSA, to derive functional safety requirements related to one such foundational system ─ the conventional hydraulic braking system. Foundational braking systems may be used in conjunction with foundational steering systems to form the basis for automated lateral control technologies, such as ALC.

The primary purpose of this work is to study and analyze the potential hazards that could result from cases of electrical or electronic failures impacting the functions of vehicular control systems. The study follows the ISO 26262 process 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 of the item under consideration. While this study does not go into implementation strategies to achieve these ASILs, the ISO 26262 process 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.

In order to assess the CHB system, this study applies a method for developing a Functional Safety Concept by following the Concept Phase (Part 3) of the ISO 26262 standard.[2] The following outlines the analysis approach used in this study along with key findings.

1. Defines the scope and functions of a generic CHB system. The CHB system uses hydraulic brake pressure to generate friction forces that are applied to the road wheels The CHB system considered in this study also includes three electronic features – antilock braking, electronic stability control, and traction control.[3]

2. Performs a vehicle-level hazard analysis using both the Hazard and Operability study and the system theoretic process analysis method. By integrating the hazards identified in both the HAZOP study and STPA, the process establishes nine vehicle-level hazards.

3. Applies the ASIL assessment[4] approach in the ISO 26262 standard to evaluate the risks associated with each of the identified hazards. The vehicle-level hazards identified for the CHB system ranged from QM to ASIL D; ASIL D is the most severe ASIL.

4. Performs a safety analysis using both the functional failure mode effects analysis and the STPA method.

5. Derives 198 functional safety requirements for the CHB system and components by combining the results of the two safety analyses[5] (functional FMEA and STPA) and following the Concept Phase in the ISO 26262 standard.[6]

6. Identifies 280 generic diagnostic trouble codes listed in the SAE International Recommended Practice, SAE J2012,[7] that are relevant to the CHB system.

7. Develops 11 examples of potential test scenarios that could be used to validate the safety goals and functional safety requirements. The example test scenarios provided in this

[2] The Concept Phase of the ISO 26262 standard is the initial stage of the development process and can be implemented before the specifics of the system design are known.

[3] Federal Motor Vehicle Safety Standard No. 126 mandates that ESC is included as a standard feature in all model year 2012 and later light vehicles. Although not mandated, the ABS and TCS functions are also included as standard features in most, if not all, current light vehicles.

[4] The ASIL is established by performing a risk analysis of a potential hazard that looks at the severity, exposure, and controllability of the vehicle operational situation.

[5] The HAZOP study is not used directly in deriving the functional safety requirements. The HAZOP study is used to identify the relevant vehicle-level hazards, which are then assigned ASILs that cascade down to the functional safety requirements.

[6] All requirements presented in this report are intended to illustrate aset of requirements that could be derived from the safety analysis results. These safety requirements are not intended to represent NHTSA's official position or requirements on the CHB system.

[7] SAE J2012 defines the standardized DTCs that on-board diagnostic systems in vehicles are required to report when malfunctions are detected.

report are a small fraction of the possible test scenarios that may be needed to validate the safety goals and functional safety requirements for the system.

The results of this report may be used to:

- Demonstrate how the Concept Phase of ISO 26262 may be implemented, including integration of multiple analysis methods.
- Establish a baseline functional safety concept for future development of CHB systems.
- Provide research data for future NHTSA activities with respect to CHB systems.
- Illustrate how the analysis results may be used to develop potential test scenarios to validate the safety goals and functional safety requirements.

1 INTRODUCTION

1.1 Research Objectives

In conjunction with NHTSA, Volpe is conducting a research project to assess the functional safety of automated lane centering systems in light vehicles.[8] These ALC systems are largely implemented through foundational braking and/or steering control systems. Therefore, the reliability of the ALC technology depends in part on the reliability of these foundational systems. The foundational systems are shared resources that may also be used to implement commands from other longitudinal and lateral control systems such as adaptive cruise control, forward collision avoidance, and emergency steer assist.

This project is part of NHTSA's electronics reliability research program for ensuring the safe operation of motor vehicles equipped with advanced electronic control systems. The objectives of this project are:

1. Identify and describe various ALC, foundational braking, and foundational steering system implementations, including system variations related to the five levels of automation defined in SAE J3016[9] [1].
2. Determine the hazards and their severity levels pertaining to the functional safety of ALC controls and related foundational systems, and identify functional safety requirements and constraints.
3. Assess diagnostic and prognostic needs.
4. Identify performance parameters and recommend functional safety test scenarios.
5. Review human factors considerations, including driver-vehicle interface requirements and the need for driver awareness and training resources.

[8] Light vehicles include passenger cars, vans, minivans, SUVs, and pickup trucks with gross vehicle weight ratings of 10,000 pounds or less.

[9] The five levels of automated driving systems include:

- Level 1 automation where the vehicle is controlled by the driver, but some driving assist features may be included in the vehicle that can assist the human driver with either steering or braking/accelerating, but not both simultaneously.
- Level 2 automation where the vehicle has combined automated functions, like speed control and steering simultaneously, but the driver must remain engaged with the driving task and monitor the environment at all times.
- Level 3 automation where an automated driving system on the vehicle can itself perform all aspects of the driving task under some circumstances. The driver is still a necessity, but is not required to monitor the environment when the system is engaged. The driver is expected to be takeover-ready to take control of the vehicle at all times with notice.
- Level 4 automation where the vehicle can perform all driving functions under certain conditions. A user may have the option to control the vehicle.
- Level 5 automation where the vehicle can perform all driving functions under all conditions. The human occupants never need to be involved in the driving task.

In addition to assessing the functional safety of ALC systems, this research project will study the functional safety of two foundational steering system variants — electric power steering and steer-by-wire — and a conventional hydraulic brake system with electronic stability control, traction control system, and an antilock brake system.

1.2 Conventional Hydraulic Braking

This report covers the study of the CHB system. The CHB system uses hydraulic brake pressure to generate friction forces that are applied to the road wheels. The friction generated by CHB system converts the kinetic energy of the vehicle to thermal energy,[10] which dissipates into the atmosphere [2]. As the rotation of the road wheel slows, braking forces are transferred to the road at the road-tire interface, ultimately stopping the vehicle.

In the CHB system, the driver's input is in the form of hydraulic brake pressure generated by brake pedal pressure and augmented with a brake booster. This results in a direct mechanical application of braking forces.[11] In addition to the mechanical application of brake forces, the CHB system includes electronic braking functions, such as ABS, TCS, and ESC, which can further adjust the driver's braking input or generate braking forces independent of the driver. These features are described in more detail in Section 3.4 of this report.

This study reviewed some of the current safety issues related to CHB systems. This study included a review of crash data in the General Estimates System and Fatality Analysis Reporting System to understand the crash types at least partially attributable to braking system related failures. NHTSA's recall and vehicle owner questionnaire databases were also reviewed to identify potential failure modes related to CHB systems. The findings from the review of current safety issues are included in Appendix A.

1.3 Report Outline

This report documents the approach and the findings of the analysis of the CHB system. In addition to this Introduction, the report contains the following sections.

- **Section Two**: Details the analysis approaches, including descriptions of the hazard and safety analysis methods used in this study.
- **Section Three**: Provides the description of a generic CHB system that includes features such as ABS, TCS, and ESC. It also defines the analysis scope and assumptions used in this study.
- **Section Four**: Details the vehicle-level hazard analysis approaches and results.
- **Section Five**: Documents the risk assessment of the identified vehicle-level hazards.

[10] Unlike CHB systems, regenerative braking systems recover a portion of the kinetic energy, which is stored as electrical energy in the rechargeable energy storage system. Regenerative braking is out of scope for this project.
[11] This is in contrast to brake-by-wire systems, which electrically transmit the driver's braking input to the system control module instead of a direct mechanical application of hydraulic pressure to generate brake forces. Brake-by-wire systems are out of scope for this project.

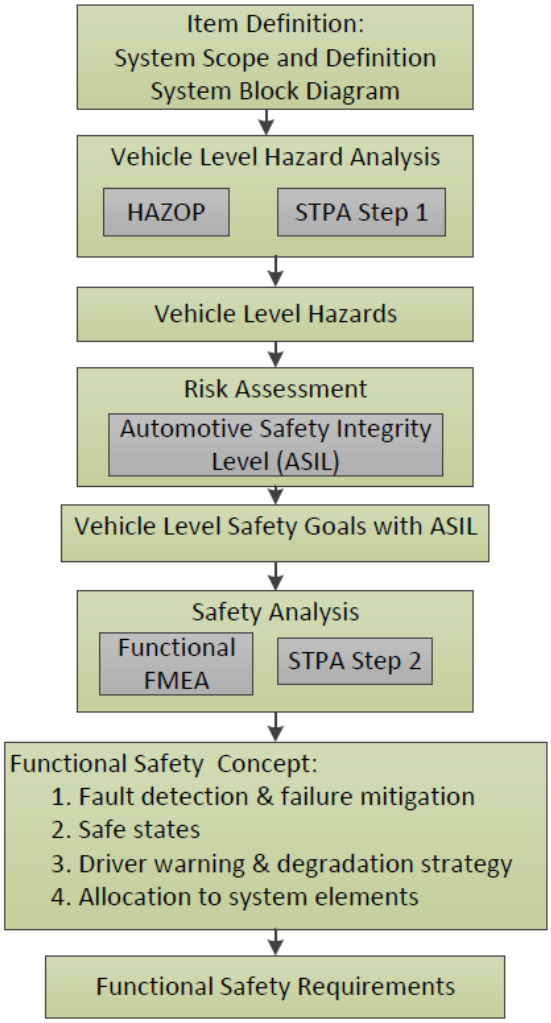
- **Section Six**: Summarizes the vehicle-level safety goals derived from the hazard analysis and risk assessment.
- **Section Seven**: Details the safety analysis that supports the functional safety concept and the safety requirements.
- **Section Eight**: Describes the functional safety concept.
- **Section Nine**: Lists the functional safety requirements.
- **Section Ten**: Identifies common diagnostic trouble codes covering the CHB system and discusses the need for additional diagnostics for the CHB system.
- **Section Eleven**: Provides examples of potential functional safety test scenarios based on the results of this study.

2 ANALYSIS APPROACH

The primary purpose of this work is to study and analyze the potential hazards that could result from cases of electrical or electronic failures impacting the functions of vehicular control systems. The study follows the ISO 26262 process to identify the integrity requirements of these functions at the concept level, independent of implementation variations. ISO 26262 is a functional safety process adapted from the International Electrotechnical Commission's standard, IEC 61508. It is intended for application to electrical and electronic systems in motor vehicles (Introduction in Part 1 of ISO 26262 [3]). Part 3 of ISO 26262 describes the steps for applying the industry standard during the concept phase of the system engineering process.

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 of the item under consideration. While this study does not go into implementation strategies to achieve these ASILs, the ISO 26262 process 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 1 illustrates the safety analysis and safety requirements development process in this project, which is adopted from the Concept Phase (Part 3) of ISO 26262.



HAZOP: Hazard and Operability study
STPA: Systems-Theoretic Process Analysis

- **STPA Step 1**: Identify Unsafe Control Actions
- **STPA Step 2**: Identify Causal Factors

FMEA: Failure Mode Effects Analysis

Note: ISO 26262 does not recommend or endorse a particular method for hazard and safety analyses. Other comparable and valid hazard and safety analysis methods may be used at the discretion of the analyst/engineer.

Figure 1. Safety Analysis and Requirements Development Process

2.1 Analysis Steps

As depicted in Figure 1, this project involves the following steps.

1. Define the system:
    a. Identify the system boundary. Clearly state what components and interactions are within the system boundary, and how the system interacts with other components and systems outside of the system boundary.
    b. Understand and document how the system functions.
    c. Develop system block diagrams to illustrate the above understandings and to assist the analysts in the rest of the process.
    d. Record any assumptions about the system operation or configuration made when defining the system.
2. Carry out the hazard analysis using both the HAZOP [4] and the STPA method [5]. The output of the hazard analysis step is a list of vehicle-level hazards. If the methods do not use a common list of hazards at the outset, an additional step may be necessary to synthesize the hazards identified using the HAZOP and STPA methods.
3. Apply the ISO 26262 risk assessment approach to the identified vehicle-level hazards, and assign an ASIL to each hazard as defined in ISO 26262.
4. Generate vehicle-level safety goals, which are vehicle-level safety requirements based on the identified vehicle-level hazards. The ASIL associated with each hazard is also transferred directly to the corresponding vehicle-level safety goal. If a safety goal satisfies more than one vehicle-level hazard, the more stringent ASIL is applied to the safety goal.
5. Perform safety analyses on the relevant system components and interactions as defined in the first step of this process. This project performs both a functional FMEA [6] and STPA to complete the safety analysis.
6. Follow the ISO 26262 process to develop the functional safety concept, including functional safety requirements at the system and component levels, based on results from the functional FMEA and STPA, ISO 26262 guidelines, and industry practice experiences.

Once the safety goals and functional safety requirements are derived, these are used along with the safety analysis results to develop potential test scenarios and performance parameters.

This report describes how the HAZOP study, functional FMEA, and STPA methods were applied to a generic CHB system that includes ABS, TCS, and ESC features.

2.2 Hazard and Safety Analysis Methods

This project uses multiple analysis methods to generate a list of hazard and safety analysis results.[12] These methods are described in this section.[13]

2.2.1 Hazard and Operability Study

This study uses the HAZOP study as one of the methods for identifying vehicle-level hazards. Figure 2 illustrates the analytical steps of the HAZOP study.

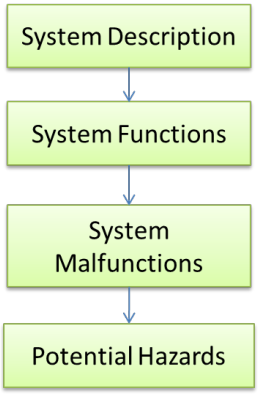


Figure 2. HAZOP Study Process

This study performs the HAZOP study steps in Figure 2 as follows:

1. Define the system of study and the scope of the analysis. Draw a block diagram to illustrate the system components, system boundary, and interfaces. This step is accomplished in the first step of the overall project (Figure 1).
2. List all of the functions that the system components are designed to perform. This step is also accomplished in the first step of the overall project (Figure 1).

[12] ISO 26262 does not recommend or endorse specific methods for hazard or safety analysis. Comparable and valid hazard and safety analysis methods may be used at the discretion of the analyst/engineer.
[13] This report provides more details on the STPA than other methods because the application of the STPA method to automotive electronic control systems is relatively new. Unlike HAZOP and Functional FMEA, a standard approach has not been defined and published for STPA. Therefore, this report provides more descriptions in order to better explain how the analysis is performed.

3. For each of the identified functions, apply a set of guidewords that describe the various ways in which the function may deviate from its design intent. IEC 61882[14] lists 11 suggested guidewords, but notes that the guidewords can be tailored to the particular system being analyzed [4]. The HAZOP study implemented in this project uses the following seven malfunction guidewords:
    - Loss of function
    - More than intended
    - Less than intended
    - Intermittent/wrong timing[15]
    - Incorrect direction
    - Not requested
    - Locked function

    The combination of a system function and guideword may have more than one interpretation. In these situations, the analyst may identify more than one malfunction.
4. Assess the effect of these functional deviations at the vehicle level. If a deviation from an intended function could potentially result in a vehicle-level hazard, the hazard is then documented.

2.2.2 Functional Failure Modes and Effects Analysis

The FMEA is a bottom-up reliability analysis method that relies on brainstorming to identify failure modes and determine their effects on higher levels of the system. There are several types of FMEAs, such as system or functional FMEAs, design FMEAs, and process FMEAs. This study uses a functional FMEA in the safety analysis to identify failure modes at the function level that could lead to the vehicle-level hazards. The failure modes identified by the functional FMEA are used to derive the safety requirements.

Standard J1739 by SAE provides guidance on applying the functional FMEA method [6]. The analysis includes the following steps:

1. List each function of the item on an FMEA worksheet.
2. Identify potential failure modes for each item and item function.
3. Describe potential effects of each specific failure mode and assign a severity to each effect.
4. Identify potential failure causes or mechanisms.
5. Assign a likelihood of occurrence to each failure cause or mechanism.

---

[14] IEC 61882:2001, *Hazard and operability studies (HAZOP studies) - Application guide*, provides a guide for HAZOP studies of systems utilizing the specific set of guide words defined in this standard; and also gives guidance on application of the technique and on the HAZOP study procedure, including definition, preparation, examination sessions, and resulting documentation.

[15] Timing is critical for certain CHB system functions (e.g., ABS, ESC). Therefore the "intermittent" guide word was extended to also consider an incorrect timing response.

6. Identify current design controls that detect or prevent the cause, mechanism, or mode of the failure.
7. Assign a likelihood of failure detection to the design control.

This study applies the first four steps listed above for the functional FMEA. Since this study is implemented at the concept phase and is not based on a specific design, the FMEA does not assume controls or mitigation measures are present; there is no data to support Steps 5 through 7. The completed functional FMEA worksheet is intended to be a living document that would be continually updated throughout the development process.

2.2.3 Systems-Theoretic Process Analysis

The STPA is a top-down systems engineering approach to system safety [5]. In STPA, the system is modelled as a dynamic control problem, where proper controls and communications in the system ensure the desired outcome for emergent properties such as safety. In the STPA framework, a system will not enter a hazardous state unless an unsafe control action is issued by a controller, or a control action needed to maintain safety is not issued. Figure 3 shows a process flow diagram for the STPA method.

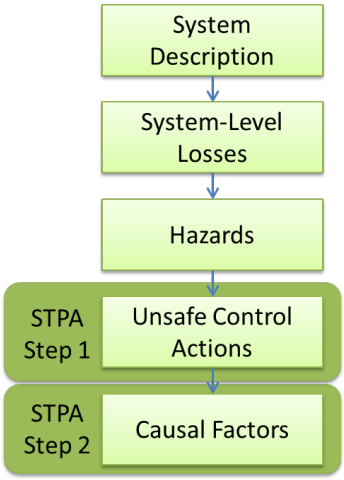


Figure 3. STPA Process

This project performs STPA following these steps:

1. Define the system of study and the scope of the analysis:
    a. Draw a hierarchical control structure of the system that captures the feedback control loops (controller, sensors, actuators, controlled process, and communications links). This control structure is a generic representation of the system, based on common implementation strategies.

b. Identify the system boundary and interfaces with other vehicle systems and the external environment.

This step is accomplished in the first step of the overall project (Figure 1).

2. Define the loss or losses at the system level that should be mitigated. STPA defines system-level losses as undesired and unplanned events that result in the loss of human life or injury, property damage, environmental pollution, etc. [5]. For this project, one loss was considered: occurrence of a vehicle crash.
3. Identify a preliminary list of vehicle-level hazards. STPA defines a hazard as a system state or set of conditions that, together with a particular set of adverse environmental conditions, will lead to a system-level loss [5]. In this project, a preliminary hazard list is generated based on engineering experience and a literature search. This list is refined during STPA Steps 1 and 2.
4. **STPA Step 1**: Identify potential UCAs issued by each of the system controllers that could lead to hazardous states for the system. Four sub-steps are involved:

    a. For each controller in the scope of the system, list all of the relevant control actions it can issue.

    b. For each control action, develop a set of context variables.[16] Context variables and their states describe the relevant external control inputs to the control system and the external environment that the control system operates in, which may have an impact on the safety of the control action of interest. The combinations of context variable states are enumerated to create an exhaustive list of possible states. This approach is based on a recent enhancement to the STPA method [7] that enumerates the process variable states during STPA Step 1. Process variables refer to variables that the control algorithm uses to model the physical system it controls. However, this study is not based on a specific design and a detailed process model algorithm is not available. Therefore, this study modifies this approach to focus on context variables instead of process variables.

    c. Apply the UCA guidewords to each control action. The original STPA literature includes four such guidewords [5]. This study uses a set of six guidewords for the identification of UCAs as illustrated in Figure 4.

[16] The context variables describe the context in which a controller issues a control action. For example, the control command "provide braking pressure" may operate in the context of the driver's braking command and braking commands from other vehicle systems.

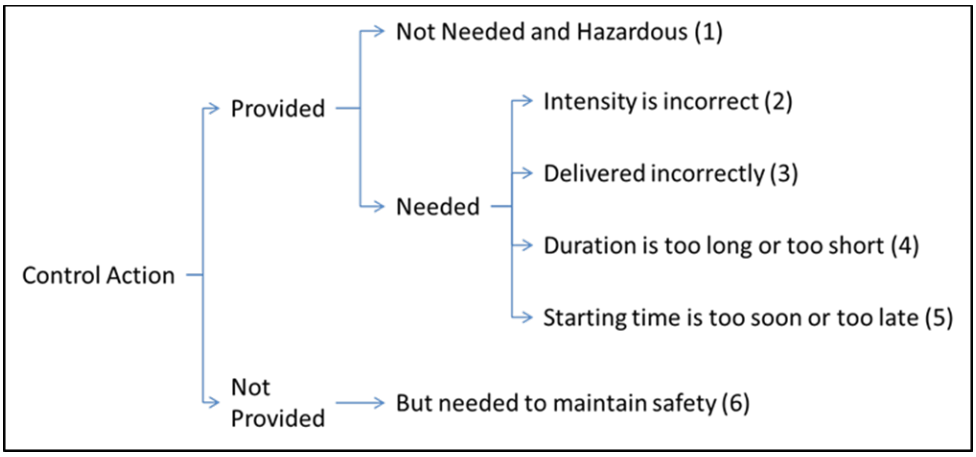


Figure 4. Guidewords for UCAs

For each control action, assess each of the six guidewords against each of the context variable combinations to determine if it could lead to any of the preliminary vehicle-level hazards. If this step identifies new hazards, add them to the vehicle-level hazard list initiated in the previous step.

d. Apply logical reduction to the resulting UCA matrix using the Quine-McCluskey minimization algorithm [8] in order to reduce the number of UCA statements.

STPA Step 1 produces a list of UCAs that can be used to derive safety requirements for software control logic and initiate the STPA Step 2 analysis.

5. **STPA Step 2:** Determine causal factors for each UCA identified in STPA Step 1.

   Analyze 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. STPA literature provides 17 guidewords to assist the analyst in identifying CFs [5]. This project uses an expanded list of 26 guidewords for identifying CFs. Appendix B provides the list of CF guidewords and detailed causes under each guideword that are used in this project.

As discussed above, there are two main analysis steps in STPA (Figure 3). This project applies STPA Step 1 in the hazard analysis stage of the study and STPA Step 2 as part of the safety analysis stage (Figure 1).

3 SYSTEM DEFINITION

3.1 System Analysis Scope

The scope of this analysis includes all components involved in transmission of forces from both the driver-operated control and electronic control system to the brake pads which apply forces to the road wheels. However, the scope of this study terminates at the transmission of braking forces to the road wheels. That is, transfer of forces from the road wheels to the road surface is out-of-scope for this study. This includes tire wear, wheel alignment, or other mechanical failures that may prevent the road wheels from transferring the appropriate forces to the road surface. However, sensors and associated algorithms within the CHB system that detect and react to the effects of adverse road conditions are considered in this study.

This analysis also considers incoming braking requests from other vehicle systems that may be implemented through the CHB. However, this analysis assumes that these other vehicle systems are operating correctly. Failures in other vehicle systems that could result in incorrect braking requests are out of scope for this study.

The following list identifies specific elements considered to be <u>in-scope</u> for this study:

1. All mechanical components leading from the driver-operated control to the brake pads, including the following.
    - Brake pedal
    - Brake booster
    - Master cylinder/hydraulic reservoir
    - Hydraulic lines and hoses
    - Brake pads or drums
2. All components in the electronic control system, including the following:
    - CHB control module, including the electronic functions of ABS, TCS, and ESC
    - Brake pedal position sensor
    - Brake pressure sensor
    - Wheel speed sensors
    - Yaw rate and lateral acceleration sensors
3. All connections between the components listed above, including:
    - Wired connections
    - Communication over the vehicle bus (e.g., controller area network)
4. Incoming braking requests from other vehicle systems
5. Interfacing sensor signals, including:
    - Roll rate and longitudinal acceleration data
6. Interface with the human operator of the vehicle

The following list identifies specific failures and hazards considered to be out-of-scope for this study.

- Failures in the road wheels (e.g., low tire pressure, tread wear, etc.) that affect transfer of forces to the road or affect feedback to the driver
- Hazards not directly caused by malfunctioning behavior specific to the electronic control system, such as fire hazards
- Failures in other vehicle systems (e.g., steering system, electronic parking brake) that may lead to lateral or longitudinal motion related hazards
- Failures in other vehicle systems that may result in incorrect braking requests
- Failures in the instrument panel display (considered an interfacing system) that prevent driver notifications from illuminating
- Failures due to improper maintenance over the lifetime of the vehicle (e.g., incorrect parts, failure to conduct scheduled inspections, etc.)

3.2 Analysis Assumptions

In addition to the system scope defined in Section 3.1, this analysis includes several assumptions regarding the operation of the CHB system. The following list identifies the key assumptions made in this study. Each assumption is addressed by explaining how the findings from this study may apply to cases where the assumption is no longer valid, or whether additional analysis is needed.

- The CHB system modelled in this report includes three features ─ ABS, TCS, and ESC. Many, if not all, model year 2012[17] and later light vehicles come equipped with these three features standard. This analysis does not assume any design limitations on the braking authority of these functions.
  - *Findings in this report relating to the ABS, TCS, and ESC (e.g., malfunctions, UCAs, faults, CFs, and safety requirements) may not apply to CHB systems that do not include these functions.*
- The ABS, TCS, and ESC functions are contained within the CHB system control module, along with other electronic CHB system functions. Other designs may house the ABS, TCS, and ESC functions in separate controllers.
  - *Functional safety requirements related to the ABS, TCS, and ESC functions apply regardless of whether these functions are housed in one control module or multiple control modules. For system architectures that include multiple control modules, additional requirements related to communication between the separate control modules.*

[17] FMVSS 126 mandates that ESC be included as a standard feature on all model year 2012 and later light vehicles. The ABS and TCS functions rely on similar hardware and manufacturers have also started including these as standard features.

- The TCS and ESC functions are capable of requesting modifications to the propulsion torque provided via the ACS/ETC system.
  - *The hazards, safety goals, and functional safety requirements related to propulsion torque would not apply to CHB systems where the TCS and ESC functions do not request modifications in the propulsion torque.*
- Electronic brake system features other than ABS, TCS, and ESC are only considered in the aggregate based on the potential effects a malfunction may have on the overall CHB system. For example, malfunctions in a panic brake assist feature or brake disc wiping feature may be both captured by causal factors related to applying the incorrect hydraulic pressure to the wheels.
  - *Detailed analysis of other electronic brake system features may be necessary to identify failure modes specific to these features.*
- Secondary brake systems, such as the emergency or parking brake, are not considered as part of the CHB system, although these systems may share components (e.g., brake calipers).
  - *A separate analysis would be required to assess faults related to the emergency or parking brake system, including electronic parking brake systems.*
- The CHB system is responsible for computing the vehicle speed based on individual wheel speed measurements. Other vehicle architectures may obtain the vehicle speed from other vehicle systems, such as the transmission system.
  - *Portions of this analysis related to computing the vehicle speed would not apply to CHB system architectures that are not responsible for determining the vehicle speed.*
- The tires are capable of transmitting the appropriate forces to the roadway. This analysis does not assess faults that may affect the ability of the tires to transmit forces (e.g., worn treads, low pressure, etc.).
  - *Additional analysis would be required to assess faults related to the tires.*
- The driver is physically capable of operating the vehicle (e.g., the driver is not impaired, distracted, etc.). The scope of this study is limited to how the DVI may lead the driver to issue an unsafe steering command.
  - *A separate human factors study would be required to evaluate driver-centric failures that affect their ability to operate the vehicle.*
- Vehicle automation systems are not considered in the analysis of the foundational CHB system. This includes potential mode confusion which may affect the driver's braking inputs.
  - *A later stage of this project will analyze the ALC system and will include DVI considerations related to mode confusion. The findings from the ALC system analysis will be published as a separate report.*
- Safety strategies, such as redundant sensors, are not considered in the hazard analysis or safety analysis stages. They are only considered as part of the functional safety concept and are reflected in the safety requirements.

- *Once specific design strategies have been adopted, additional hazard and safety analyses should be performed to determine if the safety measures are adequate and do not introduce additional hazards into the system.*

3.3 System Block Diagram

Figure 5 shows a block diagram representation of the generic CHB system considered in this study. Interfacing vehicle systems are shown in gray and are treated as black boxes with respect to the CHB system. As discussed in Section 3.1, this analysis assumes that these interfacing vehicle systems are functioning properly.

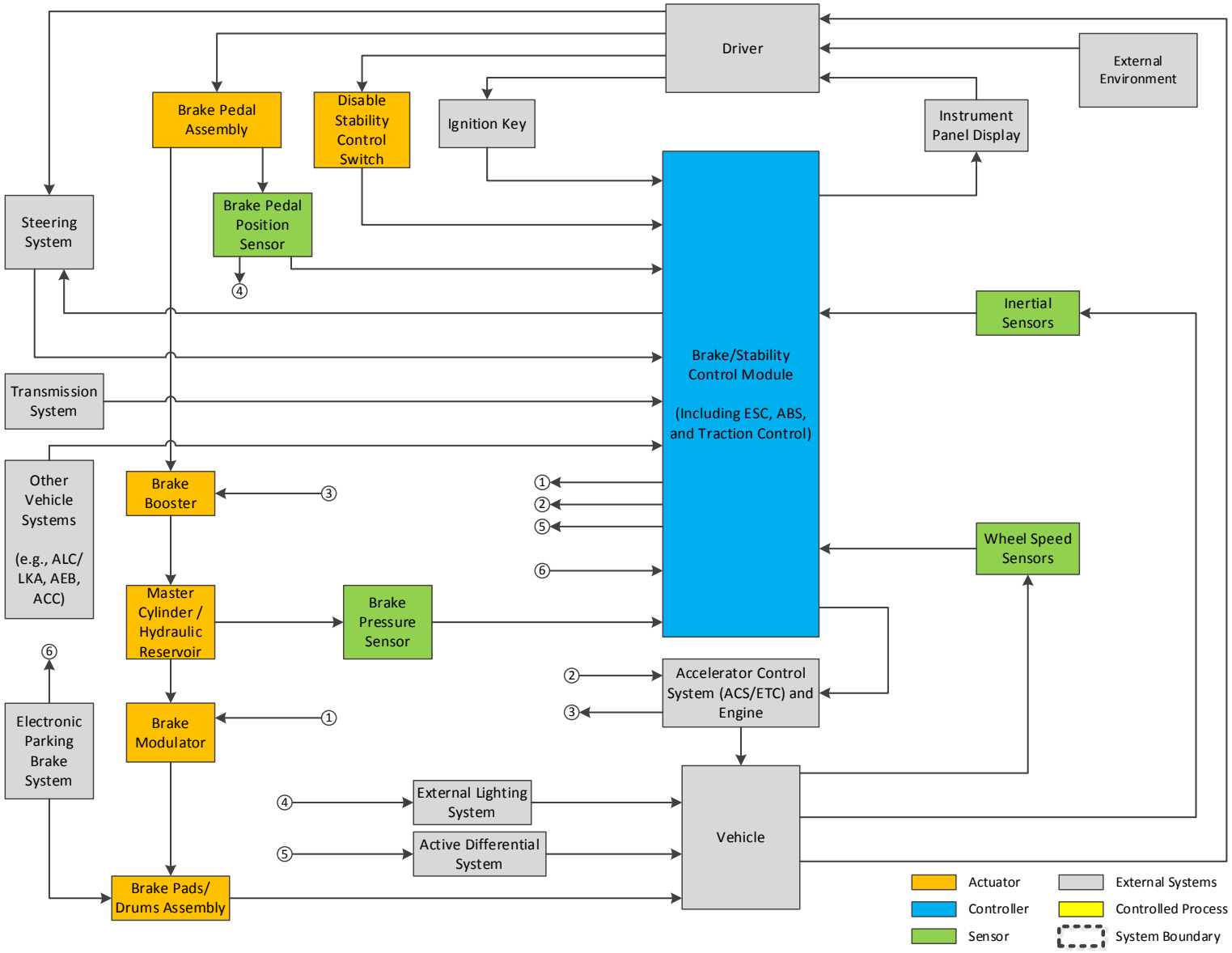


Figure 5. Block Diagram of a Generic CHB System with ABS, TCS, and ESC Features

3.4 System Description

The following descriptions of CHB components outline the functions of a CHB system. [9] [2] [10] [11]

3.4.1 Driver-Operated Control and Braking Requests From Other Vehicle Systems

The brake pedal is the driver's primary interface with the CHB system. As the driver presses the brake pedal, a push rod connected to the pedal moves a piston in the master cylinder, which increases the hydraulic pressure in the brake lines. In brake systems that have two separate brake circuits, the master cylinder may contain two chambers for generating hydraulic pressure.

The brake booster is a mechanical device located between the brake pedal and master cylinder that uses vacuum pressure to mechanically amplify the driver's action on the brake pedal. This reduces the amount of force the driver must apply to the brake pedal. The vacuum pressure may be provided from the engine intake manifold or from a separate vacuum pump.

The driver's command affects the braking system in two ways:

- The driver's application of the brake pedal transmits hydraulic pressure directly to the brake pads to slow the vehicle.
- The BPPS measures the driver's braking input. This measurement is transmitted to the CHB control module, which uses the brake pedal position (BPP) in algorithms to determine the driver's intent and the appropriate amount of pressure modulation the CHB system should provide.

In addition to responding to the driver's braking input, the CHB control module also receives and implements braking requests from other vehicle systems, such as the ALC system. The CHB control module arbitrates these braking requests with the driver's braking request and determines an appropriate brake pressure based on the vehicle's current operating state. These adjustments may be made independent of braking inputs from the driver.

3.4.2 Mechanical Transmission of Braking Forces

The mechanical portion of the braking system transmits brake pressure to the brake pads through hydraulic brake lines. Most light vehicles are equipped with a split service brake system, meaning two or more hydraulic subsystems are used to deliver hydraulic pressure to the brake pads. Failure of one of the hydraulic subsystems does not impair operation of the other hydraulic subsystems.

The hydraulic pressure is converted to a mechanical (friction) force by either the brake pads (calipers) or brake drum. The friction force converts the kinetic energy of the wheel to thermal energy (heat), which is dissipated to the atmosphere. As the rotation of the wheel slows, braking force is generated at the tire-road interface ultimately reducing the vehicle's longitudinal motion. The amount of braking force that can be transferred to the road is a function of the road adhesion

and the longitudinal slip[18] of the tires. The *mu-slip curve* illustrates this relationship; an example mu-slip curve is shown in Figure 6.[19]

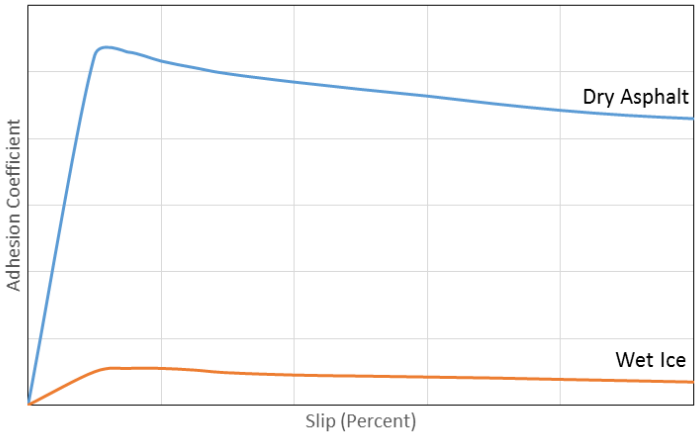


Figure 6. Example Mu-Xlip Curve

A key principle for the CHB system is that each tire can only provide a particular maximum (horizontal) friction force based on the normal (vertical) load between that wheel and the road and the instantaneous coefficient of friction. The CHB system cannot modify or create friction beyond what is available between the existing tires and the existing road surface. The horizontal force is a vector that can be resolved into longitudinal and lateral components. Assuming the brakes are being applied, the longitudinal force is used to decelerate the vehicle and minimize stopping distance. The lateral forces on the front wheels generally provide steering forces which are used to intentional change the vehicle direction. The lateral forces on the rear wheels typically provide directional stability (i.e., ensuring the orientation of the vehicle matches its path).

In the CHB system, the mechanical portion of the braking system is also responsible for providing feedback to the driver. For example:

- Mechanical failures in the steering system may cause changes in the braking feel.
- The brake pedal travel stops when the brake pedal reaches its maximum displacement.

In most braking scenarios, there is a direct relationship between the driver's brake pedal application and overall vehicle deceleration. However, in certain scenarios (e.g., emergency

[18] Longitudinal slip is the relative motion of the tire to the road surface (i.e., sliding) that occurs when the circumferential velocity of the wheel differs from the velocity of the vehicle. [9, p. 14]
[19] This example is intended to illustrate the relationship between percent slip and the adhesion coefficient. The diagram does not represent actual mu-slip curve data.

braking) the CHB control module may intervene and adjust the hydraulic brake pressure to enhance stability, steerability, stopping capability, and execution of driver intent.

3.4.3 CHB Control Module and Brake Modulator

The CHB control module receives the pedal displacement measurement from the BPPS as well as data from other sensors throughout the vehicle.

- Vehicle dynamic sensors measure the vehicle's motion, including yaw rate, roll rate, lateral acceleration, and longitudinal acceleration. Sometimes multiple vehicle dynamics sensors may be combined into a single sensor unit (e.g., multi-axis sensor).
- WSSs provide the CHB control module with information about the rotational speed of individual wheels.
- Brake pressure sensors measure the hydraulic pressure in the brake system.
- Steering wheel angle and torque sensors measure the driver's intended directional heading.

This sensor data allows the CHB control module to determine the vehicle's dynamic behavior, the driver's intent with respect to lateral and longitudinal control, and in some cases environmental and road surface conditions. The CHB control module uses these measurements to calculate the amount of assistance or intervention that the CHB system should provide to help the driver retain control of the vehicle.

The CHB control module implements braking assistance or intervention using the brake modulator, including implementing braking adjustment requests from other vehicle systems, such as a crash-imminent braking system or ALC system. The brake modulator contains a series of valves that allows the CHB control module to adjust the hydraulic pressure delivered to the brake pad/drums located at each wheel. In addition, the brake modulator contains a pump that allows the CHB system to increase the hydraulic pressure in the brake lines independent of the driver.

3.4.4 Antilock Brake System

Brake pressure that induces 100 percent wheel slip (i.e., wheel rotation stops and the wheels are "locked") will reduce the effective transfer of forces from the wheels to road surface (see Figure 6). Wheel lock-up reduces the effective stopping performance of the vehicle and can also reduce steerability by limiting the transfer of lateral forces to the road surface. ABS is a feature implemented by the CHB control module intended to prevent individual wheels from locking-up.

ABS activation is in the form of a cyclical series of pressure hold, pressure release, and pressure reapplication events. The ABS function controls the hydraulic pressure of the brakes to maintain the brake pressure within the "stable" region of the mu-slip curve (see Figure 7). The control module implements the hold-release-apply cycle in an attempt to remain near the peak friction. The ABS function typically does not generate additional braking independent of the driver.

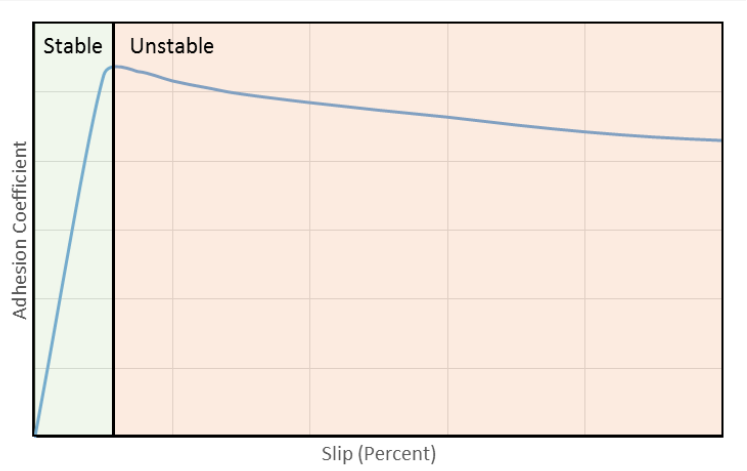


Figure 7. Stable and Unstable Regions of Mu-slip Curve

At a minimum, ABS evaluates the data from individual wheel speed measurements and the BPPS (e.g., applied versus unapplied) to assess whether intervention is necessary. Depending on the ABS algorithm design, additional vehicle dynamics data, such as longitudinal acceleration, may also be considered. Some ABS algorithms may also be designed to detect if the driver is trying to stop on a deformable surface (e.g., snow or sand). In these instances, the ABS function may not intervene and allow the wheels to lock, which could improve stopping performance.

3.4.5 Traction Control System

The TCS function has many characteristics in common with ABS, except that TCS is primarily implemented during acceleration rather than braking.[20] TCS uses similar sensors to ABS (e.g., brake application status, individual wheel speed data, etc.) to detect if wheel slip (also called "spin" in the case of acceleration) is entering the unstable region (see Figure 7). The algorithms do not use a cyclical control protocol, as with ABS. Instead, short intervention cycles are used and the CHB system continuously monitors wheel speed and surface conditions.

Through the TCS function, the CHB control module can modulate both the engine torque applied to the drivetrain as well as generate hydraulic brake pressure independent of the driver. To generate hydraulic brake pressure, the brake modulator in TCS-equipped CHB systems contains additional valves for isolation and priming, and a pump which can provide hydraulic brake pressure in the absence of brake pedal application. To reduce the engine torque delivered to the drivetrain, the CHB control module issues torque reduction requests to an accelerator control system equipped with electronic throttle control (ACS/ETC).

[20] This section only discusses implementation of the TCS function through the brake system. Other vehicle architectures may implement TCS in other ways, such as using torque converters, clutches, and differentials; or through torque vectoring.

3.4.6 Electronic Stability Control

In its April 2007 final rule for FMVSS 126, NHTSA defines ESC as *"systems that use computer control of individual wheel brakes to help the driver maintain control of the vehicle during extreme maneuvers by keeping the vehicle headed in the direction the driver is steering even when the vehicle nears or reaches the limits of road traction."* [10] FMVSS 126 mandates that ESC is included as a standard feature on all model year 2012 and later light vehicles.

ESC intervenes when the vehicle's actual course deviates from the driver's intended course. Typically this occurs when the vehicle nears the limits of road traction. Two common deviations are oversteer and understeer, as shown in Figure 8. Oversteer occurs when the rear wheels reach the limits of road traction before the front wheels, and the rear portion of the vehicle begins to spin out. This results in more yaw than the driver's intent. Understeer occurs when the front wheels reach the limits of road traction before the rear wheels, and the vehicle plows out. This results in less yaw than the driver's intent.

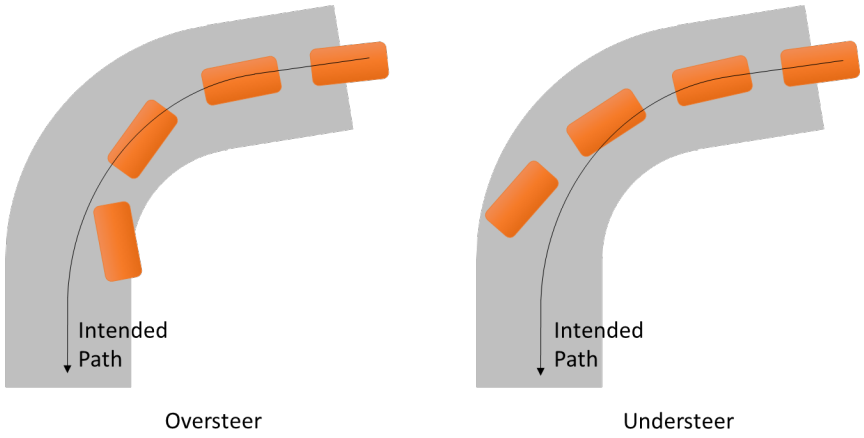


Figure 8. Depiction of Oversteer and Understeer Conditions

To correct the undesired vehicle yaw, ESC brakes individual wheels to create a differential braking force. This causes a corrective yaw moment for the vehicle. ESC continues through closed-loop control until the vehicle heading and the driver's intended heading are aligned. In addition to applying a differential braking force, ESC can also modulate the engine torque to assist in maintaining the vehicle's heading.

In addition to correcting oversteer and understeer conditions, ESC may also intervene to provide yaw rate stability in other situations. For example, ESC may apply differential braking to provide directional stability when the vehicle is on split-mu[21] surfaces. ESC may also intervene by

[21] Mu (μ) is the symbol typically used to represent the surface friction or adhesion coefficient. Split-mu surfaces are surfaces with significantly different friction coefficients at different wheels of the vehicle. For example, dry asphalt may be present on the left side of the vehicle and "black ice" may be present on the right side of the vehicle. The

temporarily increasing engine torque to prevent sudden engine braking from causing wheel lock-up (i.e., engine drag torque control).

3.4.7 Fault Detection

The CHB control module is responsible for monitoring the electronic braking system for potential faults. In the event the CHB control module detects a fault in the system, certain electronic braking functions may be suspended. For example, ESC or TCS may be deactivated.

The mechanical (hydraulic) brake system is also monitored for potential faults. Depending on the system design, the CHB control module may monitor the mechanical brake system for faults or faults may be reported directly to domain controllers (e.g., body control module) to illuminate MILs.

3.4.8 Related Systems: Accelerator Control System With Electronic Throttle Control

As described in Sections 3.4.5 and 3.4.6, the CHB system may have the ability to request changes in the engine torque to support brake system functions. The ACS/ETC is responsible for implementing these torque requests. The ACS/ETC may arbitrate torque modification requests from the CHB system with other torque requests and internal ACS/ETC functions.

3.4.9 Related Systems: Yaw Rate Stabilization Coordination

The CHB system is the primary vehicle system responsible for implementing yaw rate stabilization. However, other vehicle systems, such as the steering system and active differential system, are also capable of performing yaw rate stabilization. The CHB system and these other vehicle systems would need to coordinate their yaw rate stabilization efforts to ensure their net action results in the correct vehicle dynamics.

3.4.10 Related Systems: Emergency/Parking Brake System

Both mechanical and electronic emergency/parking brake systems may have shared authority over the rear wheel brake pads/drums. With mechanical emergency/parking brake systems, the driver's control is connected to a cable that engages the rear brakes. In an electronic emergency/parking brake system, the driver's control operates motors at the rear wheels that engage the rear brakes. Some electronic emergency/parking brake systems are also designed to automatically activate (e.g., when the ignition is turned off). In both instances, unintended activation of the emergency/parking brake system may affect the ability for the CHB system to properly control the rear brakes.

---

different friction coefficients affect transmission of forces from the tires to the road surface and may induce unintended yaw.

4 VEHICLE-LEVEL HAZARD ANALYSIS

This study performed two types of hazard analyses — HAZOP and STPA. Section 4.1 presents the synthesized vehicle-level hazards from both analyses. Sections 4.2 and 4.3 provide additional details about the HAZOP study and STPA.

4.1 Vehicle-Level Hazards

The HAZOP study identified nine vehicle-level hazards and the STPA method identified thirteen vehicle-level hazards. The analysts reconciled the hazards identified using the HAZOP and STPA methods to generate the synthesized list of potential vehicle hazards in Table 1.

Table 1. Synthesized List of Potential Vehicle-Level Hazards

	ID	Potential Hazard (Synthesized Term)	Potential Hazard Description
Lateral Motion and Yaw Related Hazards	H1	Unintended Vehicle Lateral Motion/Unintended Yaw	The vehicle moves laterally/yaws more than, at a faster rate than, or in the opposite direction of what is commanded by the driver or another vehicle system controller. Specifically, this hazard considers cases where the wheels do not lock up.
	H2	Insufficient Vehicle Lateral Motion/Insufficient Yaw	The vehicle moves laterally/yaws, but less than or at a slower rate than what is commanded by the driver or another vehicle system controller. Specifically, this hazard considers cases where the wheels do not lock up.
	H3	Loss of Vehicle Lateral Motion Control	The vehicle does not respond to steering inputs from the driver or other vehicle systems (i.e., loss of steerability). Specifically, this hazard considers the case where the wheels lock up.
Longitudinal Motion Related Hazards	H4	Unintended Vehicle Deceleration	The vehicle decelerates more than or at a faster rate than what is commanded by the driver or another vehicle system controller.
	H5	Insufficient Vehicle Deceleration[1]	The vehicle decelerates, but less than or at a slower rate than what is commanded by the driver or another vehicle system controller.
	H6	Loss of Vehicle Longitudinal Motion Control[1]	The vehicle does not respond to braking inputs from the driver or other vehicle systems (i.e., loss of braking).
	H7	Unintended Vehicle Propulsion	The vehicle accelerates more than or at a faster rate than what is commanded by the driver or another vehicle system controller.

H8	Insufficient Vehicle Propulsion	The vehicle does not accelerate to the level commanded by the driver. This includes cases where the vehicle's propulsion is reduced below the driver's set point.
H9	Vehicle Movement in an Unintended Longitudinal Direction	The vehicle moves in a direction that is not expected by the driver, including rolling forward/backward when the vehicle should be stopped.

[1] Hazards H5 and H6 may also be considered as a single hazard, as shown in the example provided in Appendix F3 of SAE J-2980 [12]. However, the analysts opted to consider H5 and H6 as separate hazards in this study to ensure both conditions are considered explicitly in the ASIL assessment. If the ASIL assessment reveals that these hazards are similar, they may be considered together when developing the functional safety concept.

The key differences in hazards identified using the two methods are outlined below.

- The HAZOP determined the loss of the electronic braking function while the "Hill Holder" feature was active could result in a unique hazard – potential unintended vehicle motion in the incorrect direction. The analysts agreed this was a unique hazard and it is included in Table 1.
- The STPA results differentiated between hazards resulting from improper resolution of conflicting commands (e.g., improper arbitration or unintended driver override of an active safety system) and hazards resulting from other electronic failures. The analysts determined that these are special cases that could be combined with the hazards H1, H2, H4, and H5 in Table 1. The improper resolution of conflicting commands will be considered in more detail during development of the functional safety requirements.
- The STPA results differentiated between insufficient vehicle propulsion and propulsion power reduction/loss or vehicle stalling. These hazards were considered as unique hazards in a separate project that assessed the functional safety of the ACS/ETC system.[22] For the CHB system, the analysts agreed that these hazards could be considered jointly under H8 without impacting the risk assessment or functional safety concept.

In addition to the differences between the two methods outlined above, the analysts also refined the definitions of hazards H1, H2, and H3 to clearly differentiate between hazards where an electronic malfunction may result in the wheels locking up and electronic malfunctions where the wheels do not lock up. Refining the hazards in this manner removes overlap between the hazards, in particular for cases where loss of lateral motion control (H3) leads to unintended lateral motion/yaw (H1) or insufficient lateral motion/yaw (H2).

- Hazards H1 and H2 only consider cases where the wheels do not lock up. For example, hazard H1 may consider cases where an electronic failure causes unwanted activation of

[22] Safety Analysis of Automotive Accelerator Control Systems with Electronic Faults (Volpe Projects #HS7BA1 and HS7BA2; NHTSA #DTNH22-13-V-00114 and DTNH22-15-V-00010).

the ESC function, leading to potential unintended lateral motion/yaw. Similarly, hazard H2 may consider cases where an electronic failure prevents ESC from intervening during a critical driving maneuver, resulting in potential insufficient lateral motion/yaw.

- Hazard H3, potential loss of lateral motion control, considers the case where an electronic failure leads to the wheels locking up. For example, if an electronic failure causes the front wheels to lock up, the vehicle may lose steerability resulting in a loss of lateral motion control. Under this hazard, the vehicle may experience any range of deviations from the driver's intended course.

4.2 Hazard and Operability Study

4.2.1 System Description

The HAZOP analysis used the block diagram provided in Figure 5 to visually represent the CHB system, and identified the CHB system functions based on the description provided in Section 3.4.

4.2.2 System Functions

The HAZOP study identifies 23 system functions for the CHB system. The HAZOP analysis notes that all functions may need to comply with performance parameters and system design requirements specified in existing standards.[23]

Mechanical (Hydraulic) Braking Functions

1. Provide overdamped (non-oscillatory) brake torque in response to driver operated control, including over multiple braking events.
2. Provide overdamped (non-oscillatory) release of brake torque in response to driver operated control.
3. Provide redundancy and/or backup braking function.[24]
4. Provide driver with feedback about the system status.[25]
5. Provide the maximum braking torque with a maximum brake application force.
6. Provide a brake force that is greater than the propulsion force when the brake pedal and accelerator pedal have the same degree of pedal depression (i.e. driver's foot presses down both accelerator and brake in the same plane).[26]
7. Ensure an attainable brake pedal position exists where the brake force is greater than the propulsion force for all engine speeds/transmission operating points.

[23] Existing standards relevant to the brake system include FMVSS 135, FMVSS 126, and United Nations Economic Commission for Europe (UNECE) Regulation 13-H.
[24] This function is part of the failure mitigation strategy and is only included in the HAZOP analysis for completeness.
[25] This function is part of the driver warning strategy and is only included in the HAZOP analysis for completeness.
[26] This function is part of the failure mitigation strategy and is only included in the HAZOP analysis for completeness.

Electronic Braking Functions

8. Proportion brake force between front and rear wheels to maximize braking effectiveness.
9. Proportion brake force between left and right wheels to maximize braking effectiveness.
10. Control brake fluid pressure to prevent vehicle wheels from locking-up under braking during ABS events.
11. Provide selective wheel braking during TCS events.
12. Control brake fluid pressure to each wheel to provide vehicle control during ESC events, including during extreme dynamic maneuvers and in adverse roadway conditions.
13. Provide brake force to support other advanced braking features (e.g., hill holder).
14. Implement braking requests to support other vehicle systems (e.g. ACC, CIB, etc.).
15. Measure and provide the vehicle speed using available sensors and models.[27]
16. Coordinate yaw rate stabilization with the steering system and other vehicle systems.
17. Communicate with internal subsystems and external vehicle systems.
18. Request an increase in torque from the ACS/ETC to prevent wheel lock during sudden deceleration.
19. Request a reduction in propulsion/throttle from the ACS/ETC when needed to support a TCS or ESC event.
20. Store relevant data.

Fault Detection

21. Disengage ABS, TCS, and/or ESC when not functioning properly. [28]
22. Provide diagnostics.
23. Provide fault detection and mitigation.[28]

Certain functions included in this section are part of the failure mitigation or driver warning strategies (Functions 3, 4, 6, 21, and 23). These functions are included in the HAZOP analysis for completeness.

4.2.3 System Malfunctions and Hazards

The seven HAZOP study guidewords presented in Section 2.2.1 were applied to each of the 23 CHB functions listed above. This process generated a list of 171 malfunctions.[29] Each of these malfunctions was then assessed to determine if they may lead to one of the vehicle-level hazards; 159 of the 171 malfunctions lead to one or more of the vehicle-level hazards.

[27] This assumes that the CHB system is responsible for computing the vehicle speed based on individual wheel speed measurements. Other vehicle architectures may obtain the vehicle speed from other systems (e.g., transmission system).
[28] This function is part of the failure mitigation strategy and is only included in the HAZOP analysis for completeness.
[29] This does not represent an exhaustive list of all possible CHB system malfunctions. Identification of malfunctions is dependent on the item definition (e.g., system functions), the interpretation of the guidewords, and the judgement of the analyst.

Table 2 provides an example of how malfunctions are derived from one of the CHB functions and are assigned vehicle-level hazards. Table 3 shows the number of malfunctions identified for each of the CHB functions. Appendix C provides the complete results of the HAZOP study.

Table 2. Derivation of Malfunctions and Hazards Using HAZOP Study (Example)

HAZOP Guideword	***Malfunction***	***Potential Vehicle Level Hazard***
Loss of function	Does not control brake fluid pressure to prevent lock-up during ABS events	H1: Unintended Vehicle Lateral Motion/Yaw H2: Insufficient Vehicle Lateral Motion/Yaw H3: Loss of Lateral Motion Control H5: Insufficient Vehicle Deceleration
More than intended	"Over-corrects" pressure, reducing braking force more than necessary or when unnecessary during ABS events	H1: Unintended Vehicle Lateral Motion/Yaw H2: Insufficient Vehicle Lateral Motion/Yaw H5: Insufficient Vehicle Deceleration
Less than intended	"Under-corrects" pressure, resulting in lock-up and loss of steerability during ABS events	H1: Unintended Vehicle Lateral Motion/Yaw H2: Insufficient Vehicle Lateral Motion/Yaw H3: Loss of Lateral Motion Control H5: Insufficient Vehicle Deceleration
Intermittent/ Wrong Timing	Controls brake fluid pressure too early in ABS events	H5: Insufficient Vehicle Deceleration
	Controls brake fluid pressure too late in ABS events	H1: Unintended Vehicle Lateral Motion/Yaw H2: Insufficient Vehicle Lateral Motion/Yaw H3: Loss of Lateral Motion Control H5: Insufficient Vehicle Deceleration
Incorrect direction	Controls brake fluid pressure in wrong direction during ABS events (i.e., increases brake pressure when it should be reduced)	H1: Unintended Vehicle Lateral Motion/Yaw H2: Insufficient Vehicle Lateral Motion/Yaw H3: Loss of Lateral Motion Control H5: Insufficient Vehicle Deceleration
Not requested	Controls brake fluid pressure as if responding to an ABS event when the action is not necessary	H1: Unintended Vehicle Lateral Motion/Yaw H2: Insufficient Vehicle Lateral Motion/Yaw H5: Insufficient Vehicle Deceleration
Locked function	Brake fluid pressure remains in the system even after request for braking is removed	H1: Unintended Vehicle Lateral Motion/Yaw H4: Unintended Vehicle Deceleration

Table 3. Number of Identified Malfunctions for Each HAZOP Function

HAZOP Function	Number of Mal-functions	Mal-functions Leading to Hazards
Provide overdamped (non-oscillatory) brake torque in response to driver operated control, including over multiple braking events.	8	8
Provide overdamped (non-oscillatory) release of brake torque in response to driver operated control.	9	9
Provide redundancy and/or backup braking function.[1]	7	7
Provide driver with feedback about the system status.[1]	9	6
Provide the maximum braking torque with a maximum brake application force.	9	9
Provide a brake force that is greater than the propulsion force when the brake pedal and accelerator pedal have the same degree of pedal depression (i.e. driver's foot presses down both accelerator and brake in the same plane).[1]	9	8
Ensure an attainable brake pedal position exists where the brake force is greater than the propulsion force for all engine speeds/transmission operating points.	9	7
Proportion brake force between front and rear wheels to maximize braking effectiveness.	9	9
Proportion brake force between left and right wheels to maximize braking effectiveness.	9	9
Control brake fluid pressure to prevent vehicle wheels from locking-up under braking during ABS events.	8	8
Provide selective wheel braking during TCS events.	8	8
Control brake fluid pressure to each wheel to provide vehicle control during ESC events, including during extreme dynamic maneuvers and in adverse roadway conditions.	8	8
Provide brake force to support other advanced braking features (e.g., hill holder).	7	7
Implement braking requests to support other vehicle systems (e.g. ACC, CIB, etc.).	7	7
Measure and provide the vehicle speed using available sensors and models.[2]	7	7
Coordinate yaw rate stabilization with the steering system and other vehicle systems.	7	7
Communicate with internal subsystems and external vehicle systems.	4	4
Request an increase in torque from the ACS/ETC to prevent wheel lock during sudden deceleration.	9	9
Request a reduction in propulsion/throttle from the ACS/ETC when needed to support a TCS or ESC event.	9	8
Store relevant data.	5	0
Disengage ABS, TCS, and/or ESC when not functioning properly.[1]	5	5
Provide diagnostics.	3	3
Provide fault detection and mitigation.[1]	6	6

[1] This function is part of the failure mitigation or driver warning strategy and is only included in the HAZOP analysis for completeness.

[2] This function assumes the CHB system is responsible for computing the vehicle speed.

4.3 Systems-Theoretic Process Analysis: Step 1

4.3.1 Detailed Control Structure Diagram

Figure 9 illustrates the detailed control structure diagram used in the STPA method to represent a generic CHB system and its interfacing systems and components. The low voltage (e.g., 12-volt) power supply is only shown on this diagram as an effect of the driver's action on the ignition key. However, the impact of the low voltage power supply on the operation of the system electronics is considered in detail as part of STPA Step 2.

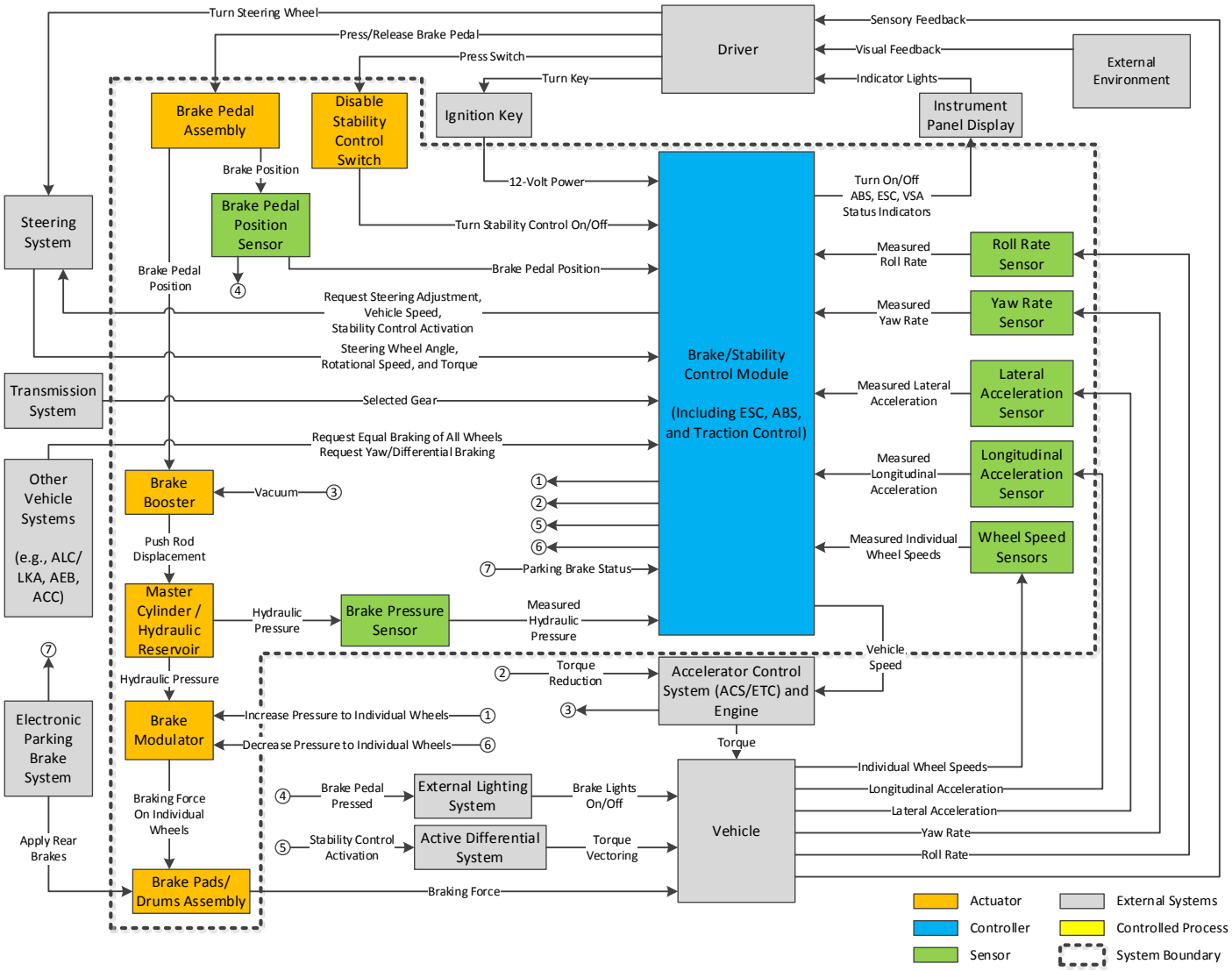


Figure 9. Detailed Control Structure Diagram for a Generic CHB System with ABS, TCS, and ESC

4.3.2 Vehicle-Level Loss and Initial Hazards

STPA begins by identifying specific losses that the control system is trying to prevent. In the STPA method, these losses result from a combination of a hazardous state along with a worst-case set of environmental conditions [5]. The vehicle-level loss relevant to this study is a vehicle crash.

An initial list of vehicle-level hazards is generated based on a literature search and engineering experiences. As the analyst identifies UCAs as part of STPA Step 1, the initial hazard list may be refined. Section 4.3.3 and Section 4.3.4 provide the details of this process. Then, the hazards generated from both HAZOP and STPA are synthesized to produce the hazard list shown in Section 4.1.

4.3.3 Control Actions and Context Variables

STPA Step 1 studies ways in which control actions in the system may become unsafe, leading to vehicle-level hazards. This study identifies eleven control actions issued by the CHB control module related to the CHB system function:

- Two control actions relate to implementing the ABS function.
    - **Allow Hydraulic Pressure to Increase at an Individual Wheel for the ABS Function** – The CHB control module issues this command to adjust the valve positions in the brake modulator (e.g., open the hold valve and close the release valve) so that the hydraulic brake pressure delivered to the brake pad/drum increases. (Note: the ABS function does not generate brake pressure above the set point established by the driver or other vehicle systems.)
    - **Allow Hydraulic Pressure to Decrease at an Individual Wheel for the ABS Function** – The CHB control module issues this command to adjust the valve positions in the brake modulator (e.g., open the release valve) so that the hydraulic brake pressure delivered to the brake pad/drum decreases.

Table 4 lists three context variables and relevant context variable states used for the analysis of the control actions related to the ABS function.

Table 4. STPA Context Variables for Implementing the ABS Function

Context Variable	Context Variable States
Mu-Slip Curve Region	Stable region
	Peak
	Unstable region - braking torque (T_b) is greater than the maximum road-surface frictional torque (T_r)[1]
	Unstable region - braking torque is less than the maximum road-surface frictional torque[1]
Driver's Braking Command	Brake is applied
	Brake is not applied
Braking Requests From Other CHB System Functions or Other Vehicle Systems	No braking request
	Increase braking force to the wheel
	Decrease braking force to the wheel
	Both increase and decrease braking force to the wheel

[1] The road-surface frictional torque is the torque that acts against the wheel resulting from fiction at the tire and road surface. [9]

- Two control actions relate to implementing the TCS function.
    - **Increase Hydraulic Pressure at an Individual Wheel for the TCS Function** – The CHB control module issues this command to increase the hydraulic brake pressure delivered to the brake pad/drum at a specific wheel. The CHB control module needs to generate hydraulic brake pressure independent of the driver, for instance by using a pump in the hydraulic modulator, in addition to controlling the valve positions in the brake modulator.
    - **Decrease Hydraulic Pressure at an Individual Wheel for the TCS Function** – The CHB control module issues this command to decrease the hydraulic brake pressure delivered to the brake pad/drum at a specific wheel by opening the release valve in the brake modulator.

Table 5 presents the context variables and context variable states used to assess the TCS function.

Table 5. STPA Context Variables for Implementing the TCS Function

Context Variable	Context Variable States
Mu-Slip Curve Region	Stable region
	Peak
	Unstable region – engine torque (T_e) is greater than the maximum T_r[1]
	Unstable region – T_e is less than the maximum T_r [1]
Acceleration Request	Yes
	No

[1] The road-surface frictional torque is the torque that acts against the wheel resulting from fiction at the tire and road surface. [9]

- One control action relates to implementing the ESC function.
    - **Adjust Hydraulic Pressure at Wheels to Induce Yaw in θ Direction** – The CHB control module controls the hydraulic brake pressure at one or more wheels to generate a differential braking force that causes the vehicle to rotate in the θ direction. For the purposes of this report, θ is used to indicate the direction of the vehicle's yaw (either clockwise or counterclockwise) in response to ESC intervention.

Table 6 presents the context variables and context variable states used to assess the ESC function.

Table 6. STPA Context Variables for Implementing the ESC Function

Context Variable	Context Variable States
Driver's Braking Command	Brake is applied
	Brake is not applied
Yaw Error between Driver's Command and Vehicle Response	No error
	Error in the θ direction
	Error in the -θ direction
Yaw/Differential Braking Requests From Other CHB System Functions or Other Vehicle Systems	No yaw/differential braking request
	Yaw/differential braking request in the θ direction
	Yaw/differential braking request in the -θ direction
	Yaw/differential braking requests in both the θ and -θ directions

- Two control actions relate to implementing braking requests involving all four wheels. For example, this control action would include implementing a braking request from ACC.
    - **Increase Hydraulic Pressure to Increase Braking to All Wheels** – The CHB control module issues this command to increase the hydraulic brake pressure delivered to the brake pad/drum at all four wheels. The CHB control module needs to generate hydraulic brake pressure independent of the driver, for instance by using a pump in the hydraulic modulator, in addition to controlling the valve positions in the brake modulator.
    - **Decrease Hydraulic Pressure to Decrease Braking to All Wheels** – The CHB control module issues this command to decrease the hydraulic brake pressure delivered to the brake pad/drum at all four wheels by opening the release valve in the brake modulator.

Table 7 presents the context variables and context variable states used to assess the control actions related to braking all four wheels.

Table 7. STPA Context Variables for Implementing Braking to All Wheels

Context Variable	Context Variable States
Driver's Braking Command	Brake is applied
	Brake is not applied
Braking Requests From Other CHB System Functions or Other Vehicle Systems	No braking
	Increase braking on all wheels
	Decrease braking on all wheels
	Both increase and decrease braking on all wheels
	Yaw/differential braking
	Increase braking on all wheels and yaw/differential braking
	Decrease braking on all wheels and yaw/differential braking
	Both increase and decrease braking on all wheels, and yaw/differential braking

- Two control actions relate to requesting adjustments in engine torque to support brake system functions (e.g., TCS).
    - **Request Propulsion Torque Increase** – The CHB control module issues this request to the ACS/ETC system to increase the net propulsion torque delivered to the drivetrain.
    - **Request Propulsion Torque Decrease** – The CHB control module issues this request to the ACS/ETC system to decrease the net propulsion torque delivered to the drivetrain.

Table 8 presents the context variables and context variable states used to assess propulsion torque adjustment requests to the ACS/ETC.

Table 8. STPA Context Variables for Requesting Propulsion Torque Adjustments

Context Variable	Context Variable States
Propulsion Torque Increase/Decrease Needed to Support CHB System Function	Yes
	No

- One control action relates to requesting a steering adjustment to support brake system functions (e.g., ESC).

- **Request Steering Adjustment** – The CHB control module issues this request to the steering system to provide a steering adjustment. For example, the CHB control module may request steering to counteract unintended yaw produced during heavy braking on a split-mu surface.

Table 9 presents the context variables and context variable states used to assess steering adjustment requests to the steering system.

Table 9. STPA Context Variables for Requesting Steering Adjustments

Context Variable	Context Variable States
Steering Adjustment Needed to Support CHB System Function	Yes
	No

- One control action relates to computing the vehicle speed. This control action only applies to vehicle architectures where the CHB system is responsible for computing the vehicle speed and broadcasting the vehicle speed information to other vehicle systems.
    - **Compute the Vehicle Speed** – The CHB control module computes the vehicle speed using available vehicle dynamics information, such as individual wheel speeds.

No context variables were used in assessing this control action.

In addition to the control actions of the CHB control module described above, this study models the driver as a high-level controller that can also issue control actions to the CHB system. In particular, the control actions issued by the driver cover the mechanical (hydraulic) braking pathway.

- Two control actions are related to the driver's braking command.
    - **Increase Application of the Brake Pedal** – the driver increases the angular position of the brake pedal to request more brake force from the CHB system.
    - **Decrease Application of the Brake Pedal** – the driver decreases the angular position of the brake pedal to reduce brake force produced by the CHB system.

Table 10 shows the context variable considered in assessing this control action. There are numerous conditions that could influence why the driver may issue a braking command, and it is not practical for this study to consider all possible combinations of these conditions. Therefore, this study assumes a competent driver and considers only whether the driver perceives the need for braking; this study does not analyze why the driver may arrive at that conclusion.

Table 10. STPA Context Variable for the Driver Issuing a Braking Command

Context Variable	Context Variable States
Is a Braking Adjustment Needed	Yes
	No

- Two control actions are related to the driver's operation of the "disable stability control switch." Some vehicle designs may include this switch to allow the driver to manually enable or disable the stability control features (i.e., ESC and TCS).[30]
    - **Activate Switch to Enable Stability Control** – the driver activates the switch to enable stability control if stability control is currently disabled.
    - **Activate Switch to Disable Stability Control** – the driver activates the switch to disable stability control if stability control is currently enabled.

Table 10 shows the context variable considered in assessing this control action.

Table 11. STPA Context Variable for Pressing the Disable Stability Control Switch

Context Variable	Context Variable States
Stability Control Status	Enabled
	Disabled

4.3.4 Unsafe Control Actions

The six UCA guidewords (Figure 4) were applied to each combination of context variable states for the five control actions listed in the previous section. The analysts then assessed whether the control action would result in a vehicle-level hazard under that particular scenario. Table 12 shows how this is done for one of the control actions – "Command an Increase in Hydraulic Pressure to Increase Braking to All Wheels." Appendix D contains all of the UCA assessment tables for the fifteen control actions.

[30] In some instances, for example when the vehicle is stuck in mud or if the vehicle is equipped with snow tires, the driver may want to disable the stability control features. [51]

Table 12. UCA Assessment Table (Example)

Control Action: Increase Hydraulic Pressure to Increase Braking to All Wheels

Context Variables		**Guidewords for Assessing Whether the Control Action May Be Unsafe**								
Driver's Braking Command	**Braking Requests From Other Functions or Vehicle Systems**	**Not provided in this context**	**Provided in this context**	**Provided, but duration is too long**	**Provided, but duration is too short**	**Provided, but the intensity is incorrect (too much)**	**Provided, but the intensity is incorrect (too little)**	**Provided, but executed incorrectly**	**Provided, but the starting time is too soon**	**Provided, but the starting time is too late**
…	…	…	…	…	…	…	…	…	…	…
Brake is applied	Both Increase and Decrease Braking on All Wheels	H5B	H4B	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided
Brake is applied	Yaw/Differential Braking	Not hazardous	H2, H4	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided
Brake is not applied	No Braking	Not hazardous	H4	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided	Hazardous if provided
Brake is not applied	Increase Braking on All Wheels	H5	Not hazardous	H4	H5	H4	H5	H1, H4, H5	N/A	H5
…	…	…	…	…	…	…	…	…	…	…

Note: This control action only refers to generation of additional hydraulic brake pressure independent of the driver. The control action assumes that the brake force commanded by the driver is still delivered via the mechanical (hydraulic) pathway.

Vehicle-Level Hazards:

H1: Potential unintended vehicle lateral motion/unintended yaw
H2: Potential insufficient vehicle lateral motion/insufficient yaw
H4: Potential unintended vehicle deceleration
H4B: Potential unintended vehicle deceleration from improper resolution of conflicting commands
H5: Potential insufficient vehicle deceleration
H5B: Potential insufficient vehicle deceleration from improper resolution of conflicting commands

Each cell in Table 12 represents a UCA. For example, application of the guideword "provided in this context" to the third row of context variables in Table 12 results in the following UCA statement:

> *The CHB control module commands an increase in hydraulic pressure to increase braking to all wheels when:*
> - *The driver is not applying the brakes, and*
> - *Other brake functions or other vehicle systems are not requesting braking.*
>
> *This may result in unintended vehicle deceleration.*

However, writing each cell of the table into a UCA statement would create a very long list of UCAs and many of these UCAs would have overlapping logical states. Therefore, this study uses the Quine-McCluskey minimization algorithm [8] to consolidate and reduce the overall number of UCA statements.

STPA Step 1 identifies a total of 159 UCAs for the generic CHB system. All 159 UCAs lead to one or more vehicle-level hazard. Table 13 provides the breakdown of these UCAs by control action.

Table 13. Number of Identified UCAs for Each STPA Control Action

STPA Control Action	Number of UCAs
CHB Control Module	
Allow Hydraulic Pressure to Increase at an Individual Wheel for ABS Function	14
Allow Hydraulic Pressure to Decrease at an Individual Wheel for ABS Function	26
Increase Hydraulic Pressure to Increase at an Individual Wheel for TCS Function	9
Decrease Hydraulic Pressure to Decrease at an Individual Wheel for TCS Function	10
Adjust Hydraulic Pressure at the Wheels to Induce Yaw in the θ Direction	21
Increase Hydraulic Pressure to Increase Braking to All Wheels	12
Decrease Hydraulic Pressure to Decrease Braking to All Wheels	15
Request Propulsion Torque Increase	8
Request Propulsion Torque Decrease	8
Request Steering Adjustment	8
Compute Vehicle Speed	5
Driver/Vehicle Operator	
Increase Application of Brake Pedal	7
Decrease Application of Brake Pedal	4
Activate Switch to Enable Stability Control	6
Activate Switch to Disable Stability Control	6

Appendix E presents a complete list of the UCAs identified in STPA Step 1. Tables 14 and 15 show examples of UCA statements and their associated vehicle-level hazards.

Table 14. Example UCA Statement for Increasing Hydraulic Pressure to Increase Braking on All Wheels

Hazard	Potential Insufficient Vehicle Deceleration
UCA (Example)	The CHB control module does not increase the hydraulic pressure to increase the braking force on all wheels when: • other vehicle systems or internal brake functions request an increase in braking on all wheels.

This UCA describes a situation where the CHB control module does not command an increase in the hydraulic brake pressure when another vehicle system, such as ACC or CIB, requests braking. In particular, there is no conflicting command from the driver, internal brake functions, or other vehicle systems.

Table 15. Example UCA Statement for Allowing Hydraulic Pressure to Decrease at an Individual Wheel for the ABS Function

Hazard	Potential Unintended Vehicle Lateral Motion/Unintended Yaw Potential Insufficient Vehicle Lateral Motion/Insufficient Yaw Potential Insufficient Vehicle Deceleration
UCA (Example)	The CHB control module allows the brake pressure to decrease at an individual wheel for the ABS function when: • the mu-slip curve is in the unstable region where $T_b > T_r$, and • the brake is applied, but the command is issued for too long.

T_b – Braking torque

T_r – Maximum road-surface frictional torque

This UCA describes a situation where the CHB control module intervenes during an ABS event by allowing the hydraulic brake pressure to decrease at a slipping wheel. However, the CHB control module allows the brake pressure to decrease for too long (i.e., the brake pressure continues to decrease as the wheel transitions back to the stable region).

5 RISK ASSESSMENT

The objective of the ISO 26262 functional safety process is to deliver a system that is free of "unreasonable risk."[31] In the context of ISO 26262, unreasonable risk is mitigated by fulfilling the recommendations of the ISO 26262 standard. This does not mean that the system is risk-free. Instead, it means that the residual risk is considered acceptable by industry standards.

This study follows the risk assessment approach in ISO 26262. The assessment derives the ASIL for each of the nine identified vehicle-level hazards. The ASIL classification assigned to each hazard depends on the exposure, severity, and controllability (see Section 5.1.2). Following the ASIL assessment process, it is possible for a hazard with the highest severity (S3) to have a low ASIL, such as ASIL A or QM. This does not indicate that the hazard is any less severe. Rather, it reflects a situation that has lower exposure or is more controllable. The ISO 26262 process does not automatically assign a high ASIL to hazards with high severity.

Finally, the ASIL is assessed in the context of the operational situation and item under consideration. The same hazard may have different ASILs under different operational scenarios. Similarly, the same hazard may have different ASILs for different systems or items.[32]

5.1 Automotive Safety Integrity Level Assessment Steps

The ASIL assessment contains the following steps.

1. Identify vehicle operational scenarios
2. For each identified vehicle-level hazard, apply the ISO 26262 risk assessment framework:
    a. Assess the probability of exposure to the operational scenario.
    b. Identify the potential crash scenario.
    c. Assess the severity of the harm to the people involved if the crash occurred.
    d. Assess the controllability of the situation and the vehicle in the potential crash scenario.
    e. Look up the ASIL per ISO 26262 based on the exposure, severity, and controllability.
3. Assign the worst-case ASIL to the hazard.

[31] ISO 26262 defines "unreasonable risk" as risk judged to be unacceptable in a certain context according to valid societal moral concepts (Part 1, Clause 1.136). [1]

[32] For example, the potential hazard "unintended lateral motion/yaw" may have a lower ASIL as a brake system hazard because of the assumption that a fully functional steering system is available to the driver for controlling the vehicle. When assessing the steering system, however, this same potential hazard may have a higher ASIL because the assumption in this case is that the steering system may not be available to the driver (although the brake system is assumed to be available to stop the vehicle).

5.1.1 Vehicle Operational Scenarios

Operational scenarios describe situations that can occur during a vehicle's life (Part 1 Clause 1.83 in ISO 26262). This study generates 201 vehicle operational scenarios that are provided in Appendix F. Below are two examples.

- Driving at high speed (130 kph ≥ V > 100 kph), with heavy traffic and negligible pedestrian presence; good road conditions; sharp road bends; the vehicle steers sharply.
- Driving at medium speed (100 kph ≥ V > 40 kph), with heavy traffic and negligible pedestrian presence, split-mu conditions; moderate road bends; the vehicle steers sharply.

These 201 scenarios cover six variables and their states as shown in Table 16. These variables and their states were identified following current industry practices. Not all combinations of variable states in Table 16 produce viable operational scenarios. For example, the vehicle speed state "very high speed" combined with the roadway state "parking lot/driveway" does not produce a viable operational scenarios.

For some combinations of variable states, only the more conservative combination of states was assessed. For example, operational scenarios involving light pedestrian traffic in a low-speed city setting were not assessed in lieu of the more conservative case involving heavy pedestrian traffic. Both the light and heavy pedestrian traffic scenarios would have the same exposure and controllability values, but the heavy pedestrian traffic scenario would have a higher severity value.

Table 16. Variables and States for Description of Vehicle Operational Scenarios

Variable	States
Vehicle Speed	Very High Speed (V > 130 kph)
	High Speed (130 kph ≥ V > 100 kph)
	Medium Speed (100 kph ≥ V > 40 kph)
	Low Speed (V ≤ 40 kph)
Road Surface/ Condition	Dry
	Wet/Snow
	Split Mu
Road Geometry	Straight
	Moderate Road Bends
	Sharp Road Bends
	Hill/Incline
Maneuver	Light Braking/Decelerating
	Heavy Braking/Emergency Stop
	Evasive Maneuver (No Braking)
	Evasive Maneuver (Light Braking)
	Evasive Maneuver (Heavy Braking)
	Overtaking
	Cornering/Hard Cornering
	Turning
	Reversing (No Braking)
	Reversing (Heavy Braking)
	Driving Straight (No Maneuver)
	Starting to Move
Traffic	Light
	Heavy
	Stop-and-Go
Pedestrian Presence	Light
	Heavy

The visibility variable is not considered in this analysis. Typically, visibility is considered when assessing the start of the braking action as part of the controllability analysis (e.g., low visibility may reduce controllability by delaying the start of braking). However, in this ASIL assessment the operational scenarios assume braking is already occurring and malfunctions in braking are the basis for the hazards.

Other road surface conditions, such as ice, standing water, and gravel/dirt roads were considered during development of the operational scenarios. However, the analysts deemed the exposure level associated with these conditions would be E1 and the resulting ASIL would be subordinate to similar higher exposure scenarios, such as a wet or snow-covered surface.

5.1.2 Automotive Safety Integrity Level Assessment

ISO 26262 assesses the ASIL of identified hazards according to the severity, exposure, and controllability (Part 3 in ISO 26262).

Exposure is defined as the state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis (Part 1 Clause 1.37 in ISO 26262). Table 17 is a reproduction of Table 2 in Part 3 of the ISO 26262 standard.

Table 17. Exposure Assessment

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability
E = Exposure					

Severity is defined as the estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation (Part 1 Clause 1.120 in ISO 26262). Table 18 is directly quoted from ISO 26262 Part 3 Table 1.

Table 18. Severity Assessment

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries
S = Severity				

Table 19 is one method for assessing severity that is provided in ISO 26262 (Part 3 Clause 7.4.3.2 and Annex B Table B.1).

Table 19. Example Method for Assessing Severity

	Class of Severity			
	S0	**S1**	**S2**	**S3**
Reference for single injuries (from AIS scale)	• AIS 0 and Less than 10% probability of AIS 1-6 • Damage that cannot be classified safety-related	More than 10% probability AIS 1- 6 (and not S2 or S3)	More than 10% probability of AIS 3-6 (and not S3)	More than 10% probability of AIS 5-6

AIS: Abbreviated Injury Scale

ISO 26262 defines controllability as the "ability to avoid a specified harm or damage through the timely reactions of the persons[33] involved, possibly with support from external measures" (Part 1 Clause 1.19 in ISO 26262). Table 20 is ISO 26262's approach to assessing controllability (Table 3 in Part 3 in ISO 26262). Table 21 shows how ASIL is assessed based on exposure, severity, and controllability (Table 4 in Part 3 of ISO 26262).

Table 20. Controllability Assessment

	Class			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

C = Controllability

[33] Persons involved can include the driver, passengers, or persons in the vicinity of the vehicle's exterior.

Table 21. ASIL Assessment

Severity Class	Probability Class (Exposure)	Controllability Class		
		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D
QM: Quality Management **E: Exposure** **S: Severity** **C: Controllability**				

Table 22 and Table 23 provide two examples of how this study assesses the ASIL for each hazard under identified operational situations.

Table 22: Example ASIL Assessment for Hazard H1

Vehicle-Level Hazard	Potential Unintended Vehicle Lateral Motion/Unintended Yaw		
Operational Situation	Driver performs an evasive maneuver with heavy braking while driving at high speed (130 kph > V ≥ 100 kph) with heavy traffic, negligible pedestrian presence, and good road conditions.		
Potential Crash Scenario	Collision with another vehicle or barrier		
ASIL Assessment	Severity	S3	Life-threatening injuries (survival uncertain) or fatal injuries
	Exposure	E2	Evasive maneuvers with heavy braking is not a common occurrence
	Controllability	C3	Difficult to control or uncontrollable[1]
Assigned ASIL Value	**B**		

[1] The assumption for this scenario is that a malfunction prevents ESC from intervening during an aggressive driving maneuver, making the situation more difficult to control.

Table 23: Example ASIL Assessment for Hazard H6

Vehicle-Level Hazard	Loss of Longitudinal Motion Control		
Operational Situation	The driver brakes hard while driving at medium speed (100 kph > V ≥ 40 kph) with heavy traffic, light pedestrian traffic, good road conditions, and moderate road bends.		
Potential Crash Scenario	Side/Front collision with a stationary object or another vehicle at medium speed		
ASIL Assessment	Severity	S3	Life-threatening injuries (survival uncertain) or fatal injuries.
	Exposure	E4	Occurs often (>10% of driving time is not unexpected)
	Controllability	C3	Difficult to control or uncontrollable
Assigned ASIL Value	**D**		

Appendix G contains the full ASIL assessment.

5.2 Automotive Safety Integrity Level Assignment for Each Hazard

The ASIL assessment for each operational situation forms the basis for the ASIL assignment to each of the nine vehicle-level hazards. ISO 26262 requires the most severe ASIL be chosen for each hazard. Table 24 shows the resulting ASIL values for each hazard.

Table 24. Vehicle-Level Hazards and Corresponding ASIL

	Hazard	ASIL
H1	Unintended Vehicle Lateral Motion/Unintended Yaw	B[1]
H2	Insufficient Vehicle Lateral Motion/Insufficient Yaw	B[1]
H3	Loss of Vehicle Lateral Motion Control	D
H4	Unintended Vehicle Deceleration	D
H5	Insufficient Vehicle Deceleration	D
H6	Loss of Vehicle Longitudinal Motion Control	D
H7	Unintended Vehicle Propulsion	C[2,3]
H8	Insufficient Vehicle Propulsion	C[2]
H9	Vehicle Movement in an Unintended Longitudinal Direction	QM[4]

[1] This ASIL only considers malfunctions in the braking system which may lead to this hazard. Similar hazards in the steering system may have a higher ASIL rating.

[2] This ASIL only considers malfunctions in the braking system which may lead to this hazard. Similar hazards in the ACS/ETC system may have a higher ASIL rating.

[3] Analysts did not reach consensus on the ASIL assessment for this hazard.

[4] This ASIL is specific to the Hill Holder feature. Other situations related to insufficient braking while on an incline are covered in hazards H5 and H6.

For Hazard H7, Unintended Vehicle Propulsion, the analysts did not reach consensus on the assignment of the controllability parameter for this hazard. For example, one analyst assigned the following operating scenario a controllability value of C2, while another analyst assigned the same operating scenario a controllability value of C3 for Hazard H7.

- Driving at high speed (130 kph > V ≥ 100 kph), with heavy traffic and negligible pedestrian presence; good road conditions; moderate road bends.

Both analysts agreed on the exposure and severity values assigned to all operating scenarios for this hazard.

6 VEHICLE-LEVEL SAFETY GOALS

Based on the hazard analysis and risk assessment, this study established the safety goals (SGs; i.e., vehicle-level safety requirements) listed in Table 25.

Table 25. Safety Goals for the CHB System

ID	Safety Goals	ASIL
SG 1	Prevent unintended vehicle lateral motion and/or unintended yaw under all vehicle operating conditions.	B[1,2]
SG 2	Provide sufficient lateral motion under all vehicle operating conditions.	B[1,2]
SG 3	Prevent CHB system failures that lead to loss of lateral motion control under all vehicle operating conditions.	D
SG 4	Prevent unintended vehicle deceleration[3] under all vehicle operating conditions.	D
SG 5	Prevent insufficient braking and loss of braking under all vehicle operating conditions.	D
SG 6	Prevent CHB system failures that lead to unintended acceleration under all vehicle operating conditions.	C[2,4]
SG 7	Prevent CHB system failures that lead to insufficient propulsion or propulsion power reduction/loss under all vehicle operating conditions.	C[2]
SG 8	Prevent CHB system failures that lead to unintended vehicle motion (e.g., rolling backward) under all vehicle operating conditions.	QM[5]

[1] This ASIL is based on the assumption that the wheels do not lock for this hazard. Situations where wheel lock-up affects the vehicle's lateral motion are considered in SG 3.
[2] This ASIL is based on failures in the CHB system that may lead to this potential hazard. Hazards in other vehicle systems that may lead to this hazard may have different ASILs.
[3] Some manufacturers may specify threshold values for "unintended vehicle deceleration" (e.g., 0.2g).
[4] Analysts did not reach consensus on the ASIL assessment for this hazard.
[5] This ASIL is specific to the Hill Holder feature. Other situations related to insufficient braking while on an incline are covered in hazards H5 and H6.

The SGs listed in Table 25 correspond to the vehicle-level hazards and ASILs listed in Table 24, with the following exceptions.

- Hazards H5 (Insufficient Vehicle Deceleration) and H6 (Loss of Longitudinal Motion Control) were combined into SG 5. Both hazards H5 and H6 are ASIL D and describe similar phenomena – loss of longitudinal motion control could be considered an extreme case of insufficient vehicle deceleration. In this context, the analysts agreed one SG could cover both hazards.
- SG 7 covers hazard H8 (Insufficient Vehicle Propulsion). As described in Section 4.1, STPA identified "Propulsion Power Reduction/Loss" as a related hazard that was ultimately incorporated into hazard H8. The wording for SG 7 explicitly mentions both conditions for completeness.

7 SAFETY ANALYSIS

This study uses the functional FMEA and STPA to complete the safety analysis.

7.1 Functional Failure Modes and Effects Analysis

This study carried out a functional FMEA for all of the potential vehicle-level hazards identified in Table 24. Overall, the functional FMEA covers 15 CHB subsystems and components, and 5 interfacing systems or subsystems. The functional FMEA identifies 86 failure modes and 195 potential faults. Note that some potential faults may lead to one or more failure modes Table 26 shows a breakdown of failure modes and potential faults by the systems, subsystems, and components.

Table 26. Breakdown of Identified Failure Modes and Potential Faults

System/Subsystem/Component	Number of Failure Modes	Number of Potential Faults
CHB Subsystems and Components		
CHB Control Module (including ABS, TCS, ESC)	31	36
Brake Modulator	18	14
Disable Stability Control Switch	1	1
Brake Booster	1	1
Brake Pads/Drums	2	0[1]
Brake Pedal Assembly	1	0[1]
Master Cylinder/Hydraulic Reservoir	1	0[1]
Brake Pedal Position Sensor	4	19
Brake Pressure Sensor	2	19
Lateral Acceleration Sensor	3	20
Longitudinal Acceleration Sensor	3	20
Roll Rate Sensor	3	20
Yaw Rate Sensor	4	20
WSSs	6	20
Interfacing Systems or Subsystems		
ACS/ETC System	1	1
Active Differential System	1	1
Electronic Parking Brake System	1	1
Steering System	2	1
Other Vehicle Systems with Braking Authority (e.g., ACC)	1	1

[1] Only mechanical faults were identified. Mechanical fault are outside the scope of ISO 26262.

Table 27 shows a few examples of the functional FMEA. Appendix H provides the complete functional FMEA results

Table 27. Portion of the Functional FMEA for H4: Potential Unintended Vehicle Deceleration

System/Subsystem	Potential Failure Mode	Potential Cause(s) or Mechanism(s) of Failure	Current Process Controls		
			Safety Mechanism	**Diagnostics**	**Diagnostic Trouble Code**
CHB Control Module	Commands brake modulator to provide too much brake pressure to rear wheels	Hardware fault (sensors, integrated circuits (ICs), circuit components, circuit boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in CHB input/output (I/O) connections	Critical messages/data transfer qualification	Stuck open/shot	I/O Fault
		Short in CHB I/O connections to ground or voltage	Critical messages/data transfer qualification	Stuck open/shot	I/O Fault
		Short in CHB I/O connections to another connection		Stuck open/shot	
		Signal connector connection failure		Hardware diagnostics	
		Firmware crash/failure (software parameters corrupted)		Periodic checks	
		Arbitration logic fault	Three-level monitoring		System Fault

7.2 System Theoretic Process Analysis: Step 2

STPA Step 1 identified 159 UCAs and 13 vehicle-level hazards, which were then integrated with the HAZOP results to yield the 9 vehicle-level hazards described in Section 4. The goal of STPA Step 2 is to identify CFs that may lead to the UCAs, which then may result in 1 or more of the 9 synthesized vehicle-level hazards. Each of the 26 CF guidewords and the detailed causes (Appendix B) are applied to the components and interactions depicted in the STPA control structure diagram (Figure 9). Specifically, the STPA Step 2 analysis includes the following components and interactions.

- Components within the CHB system – defined as any component within the CHB scope boundary shown in Figure 5.
- Interactions within the CHB system – defined as any interaction between components entirely within the CHB scope boundary. Types of interactions include wired or communication bus connections used to transmit data, or physical connections (e.g., to transmit hydraulic brake pressure).
- Interactions with interfacing components and systems – defined as any interaction which involves a component within the CHB system boundary and a component external to the CHB system. Types of interactions include wired or communication bus connections used to transmit data, or physical connections.

The choices of these components and interactions enable the analysis to focus on the defined scope of this study while still considering critical interfaces between the CHB system and other vehicle systems. For example, other vehicle systems – such as ACC – may issue a braking request to the CHB system. This analysis will consider faults in the transmission of the braking request to the CHB control module (e.g., over the CAN bus). However, failures within other vehicle systems that may lead to an incorrect request for braking are not considered in the analysis of the CHB system.

Each identified CF relates to one or more of the UCAs identified in STPA Step 1, providing a traceable pathway from CFs up to vehicle-level hazards (Figure 10).

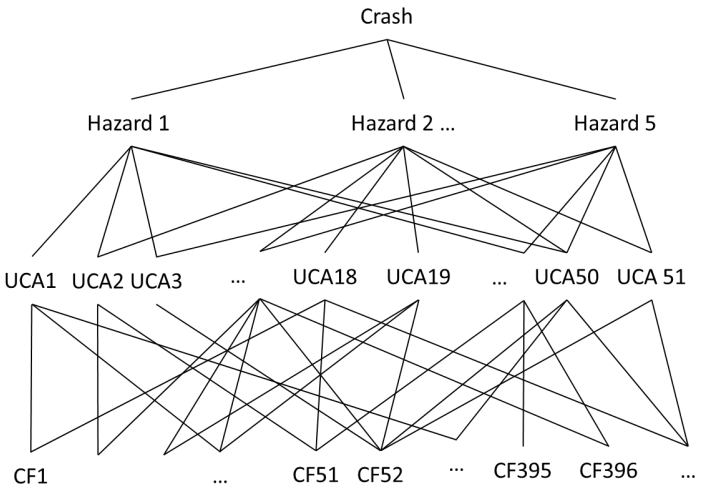


Figure 10. Traceability in STPA Results

The STPA Step 2 analysis identifies a total of 722 unique CFs. Below is a breakdown of CFs by the category of UCAs they affect.

- 245 CFs may lead to UCAs related to CHB control of the ABS function
- 281 CFs may lead to UCAs related to CHB control of the TCS function
- 405 CFs may lead to UCAs related to CHB control of the ESC function
- 255 CFs may lead to UCAs related to CHB control for braking all four wheels
- 191 CFs may lead to UCAs related to CHB request for propulsion torque adjustments
- 239 CFs may lead to UCAs related to CHB request for steering adjustments
- 121 CFs may lead to UCAs related to CHB calculation of vehicle speed
- 120 CFs may lead to UCAs related to the driver's braking input
- 43 CFs may lead to UCAs related to the driver's actuation of the disable stability control switch

As shown in Figure 10, a CF may lead to more than one UCA. Therefore, the totals listed above exceed the number of unique CFs identified in this study.

Table 28 shows a breakdown of the identified CFs by the 26 CF guidewords applied in this study. Appendix I provides the complete list of CFs identified in this study.

Table 28. Number of Identified Causal Factors by Causal Factor Category

Causal Factor Category	Number of Causal Factors
Actuation delivered incorrectly or inadequately: Actuation delayed	2
Actuation delivered incorrectly or inadequately: Hardware faulty	5
Actuation delivered incorrectly or inadequately: Incorrect connection	2
Actuator inadequate operation, change over time	5
Conflicting control action	2
Controlled component failure, change over time	7
Controller hardware faulty, change over time	8
Controller to actuator signal ineffective, missing, or delayed: Communication bus error	12
Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	18
Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	6
External control input or information wrong or missing	7
External disturbances	200
Hazardous interaction with other components in the rest of the vehicle	162
Input to controlled process missing or wrong	3
Output of controlled process contributes to system hazard	2
Power supply faulty (high, low, disturbance)	18
Process model or calibration incomplete or incorrect	77
Sensor inadequate operation, change over time	25
Sensor measurement delay	3
Sensor measurement inaccurate	5
Sensor measurement incorrect or missing	5
Sensor to controller signal inadequate, missing, or delayed: Communication bus error	33
Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	48
Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	16
Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	51

Table 29 shows three examples of CFs that may result in a UCA related to controlling the ABS function. In this UCA, the CHB control module commands the brake modulator to reduce the hydraulic brake pressure at an individual wheel. However, the command persists for too long and the hydraulic brake pressure continues to decrease after the wheel stops slipping.

Table 29. Examples of Causal Factors for a UCA Related to Implementing the ABS Function

<table>
<tr><td>Hazard</td><td colspan="2">Potential Unintended Vehicle Lateral Motion/Unintended Yaw

Potential Insufficient Vehicle Lateral Motion/Insufficient Yaw

Potential Insufficient Vehicle Deceleration</td></tr>
<tr><td>UCA
(Example)</td><td colspan="2">The CHB control module allows the brake pressure to decrease at an individual wheel for the ABS function when:

• the mu-slip curve is in the unstable region where $T_b > T_r$, and
• the brake is applied,

but the command is issued for too long.</td></tr>
<tr><td rowspan="4">Potential
Causal Factors
(Example)</td><td>Component</td><td>Potential Causal Factors</td></tr>
<tr><td>CHB Control Module</td><td>The control algorithm may continue in its previous state (e.g., decrease pressure) if it does not receive updated data (e.g., WSS reading).</td></tr>
<tr><td>WSS</td><td>The WSS may have an internal hardware failure (e.g., an internal short), affecting its ability to accurately measure the wheel speed.</td></tr>
<tr><td>WSS to CHB Control Module

Connection</td><td>The communication bus signal priority for the WSS may be too low, causing a delay before the CHB control module receives updated wheel speed data.</td></tr>
</table>

1. The first example CF in Table 29 describes a condition where the CHB control module algorithm logic continues to issue the same command until new data is received. In this particular case, the CHB control module continues to allow the hydraulic brake pressure at an individual wheel to decrease until new wheel speed information is received.

2. The second example CF in Table 29 describes an internal hardware failure in the WSS that could affect the accuracy of the wheel speed measurement provided to the CHB control module. An incorrect wheel speed measurement may result in the CHB control module continuing to decrease the hydraulic brake pressure at the affected wheel.

3. The third example CF in Table 29 describes how incorrect prioritization of signals on the communication bus may prevent critical data from reaching the CHB control module. For example, if the CHB control module does not receive updated wheel speed data, the CHB control module may not be able to properly control the ABS function.

8 FUNCTIONAL SAFETY CONCEPT

ISO 26262 defines functional safety as *the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electric/electronic systems* (Part 1 Clause 1.51 in ISO 26262). Functional safety is one aspect of the overall system safety. The primary focus of functional safety is to address systemic protection from electronic faults, which may include adding functionality to the system to specifically address safety. In particular, functional safety covers the safety behaviors or safety measures implemented by the system, such as fault detection, physical or systemic redundancy, or transitioning to a safe state, that reduce the overall risk due to faults in the electronic system. [13]

The objective of the functional safety concept is to derive a set of functional safety requirements from the safety goals, and to allocate them to the preliminary architectural elements of the system, or to external measures (Part 3 Clause 8.1 in ISO 26262). Figure 11 illustrates how the functional safety concept takes into consideration the results from the safety analysis; applies safety strategies, industry practices, and engineering experiences; and derives a set of safety requirements following the established process in ISO 26262.

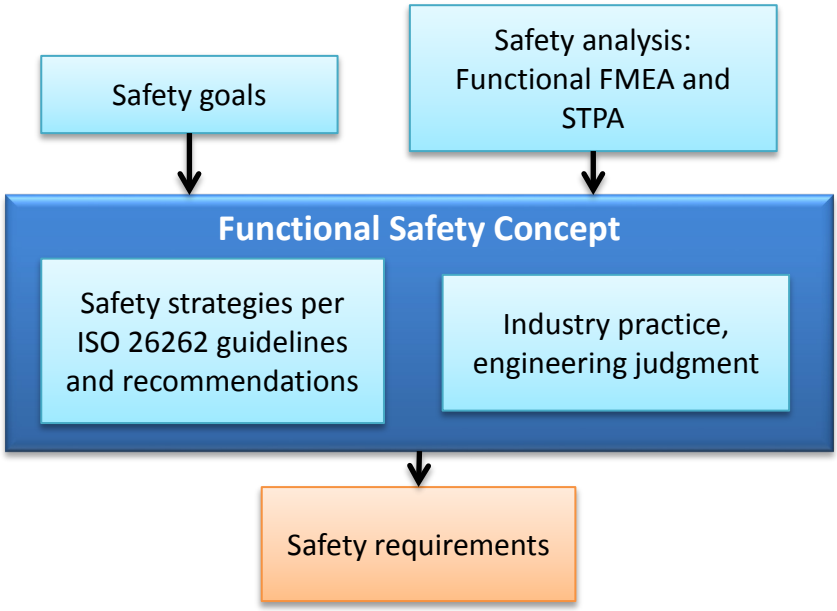


Figure 11. Functional Safety Concept Process

8.1 Safety Strategies

As stated in ISO 26262 Part 3 Clause 8.2, "*the functional safety concept addresses:*

- *Fault detection and failure mitigation;*
- *Transitioning to a safe state;*
- *Fault tolerance mechanisms, where a fault does not lead directly to the violation of the safety goal(s) and which maintains the item in a safe state (with or without degradation)*

- *Fault detection and driver warning in order to reduce the risk exposure time to an acceptable interval (e.g., engine malfunction indicator lamp, anti-lock brake fault warning lamp);*
- *Arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by different functions*."

Typical safety strategy elements may include the following:

1. Ensure that the system elements are functioning correctly.
2. Ensure that the critical sensors' inputs to the main controller are valid and correct (redundant measurements paths).
3. Validate[34] the health of the main controller (using an auxiliary processor).
4. Ensure the validity and correctness[35] of critical parameters (mitigate latent faults through periodic checks).
5. Ensure the validity and correctness of the critical communication signals internal and external to the CHB system (Quality factors[36]).
6. Ensure that the correct braking torque (in terms of magnitude and direction) is delivered to the road wheels at the correct time.
7. Ensure that low-voltage power is available until the safe state is reached under all safety hazards conditions.
8. Mitigate the safety hazards when an unsafe condition is detected.
9. Ensure that the safe state is reached on time when a hazard is detected.
10. Ensure driver warnings are delivered when an unsafe condition is detected.
11. Ensure the correctness and timeliness of the arbitration strategy.

8.2 Example Safe States

A safe state is an operating mode of the item without an unreasonable risk. A safe state may be the intended operating mode, a degraded operating mode, or a switched off mode (Part 1 Clause 1.102 of ISO 26262). The developer of the functional safety concept attempts to maximize the availability of the vehicle while ensuring the safety of its operation. Therefore, careful consideration is given to selecting the safe states in relation to the potential failure modes.

The safe states for the CHB system can be either full operation, degraded operation (e.g., loss of certain CHB system functions), or switched off mode (e.g., the electronic portion of the CHB

[34] "Validate" means to ensure that the value of a parameter or the state of an element falls within a valid set of values or states.
[35] "Correctness" means that the value of a parameter is the correct one from the valid set.
[36] Quality factors refer to techniques for error detection in data transfer and communication including checksums, parity bits, cyclic redundancy checks, error correcting codes, etc.

system is disabled). Possible safe states for the CHB system may include (but are not limited to) those listed in Table 30.

Table 30. Possible CHB System Safe States

Safe State	CHB System Behavior	Example Triggering Events
1	Disable TCS • Other unaffected CHB features may continue to operate	Fault in the TCS subsystem or in sensors critical to TCS operation
2	Disable ESC • Other unaffected CHB features may continue to operate	Fault in the ESC subsystem or in sensors critical to ESC operation
3	Disable ABS • Other unaffected CHB features may continue to operate	Fault in the ABS subsystem or in sensors critical to ABS operation
4	Limit the brake torque authority of electronic CHB features.	Fault in one of the brake pedal position sensors
5	Disable all electronic CHB features • Limit braking to the mechanical service brake	High severity hardware fault, CHB control module fault, low voltage power supply fault
6	Limit electronic portion of CHB system to implementing core braking functions (ABS, TCS, ESC). • Disable advanced features relying on the brake system (AEB, ACC, Hill Holder, Lane Keeping, etc.)	Communication system fault, arbitration logic fault

The objective of the safe states is to reduce the overall risk at the vehicle level. Some of the safe states listed in Table 30 include degraded operating modes of the CHB system, which may indirectly contribute to hazardous vehicle states. However, disabling these malfunctioning CHB functions may be preferable to allowing malfunctioning CHB functions from affecting the vehicle's dynamics. Furthermore, by transitioning to a safe state, degradation of the CHB system functionality is controlled and the driver is notified.

For example, disabling the ESC function as part of Safe State 2 may contribute to unintended or insufficient lateral motion/yaw since ESC may not be available to intervene in an oversteer or understeer condition. However, this may be preferable to allowing a malfunctioning ESC system from inadvertently inducing yaw in the vehicle. In addition, notifying the driver as part of the

safety strategy may allow the driver to better control the vehicle (e.g., by taking more conservative driving maneuvers).

8.3 Example Driver Warning Strategies

In addition to the safe states listed in Section 8.2, driver notification is a key element for ensuring that the driver takes the proper course of action. The following is an example of driver warning strategies commonly seen in the automotive industry:

- Amber Light:
  - Potential violation of a safety goal is detected, but the probability of violating a safety goal is moderate.
  - An Amber Light may be paired with Safe States 1, 2, 3, and 5.
- Red Light:
  - Potential violation of a safety goal is detected and the probability of violating a safety goal is high.
  - A violation of a safety goal is detected.
  - A Red Light may be paired with Safe States 4 and 6.
- Audio:
  - Chime: Audible notification of the driver is implemented whenever the conditions for the Red Light driver warning are identified. The chime may continue until the fault is removed.
  - Specific recorded (or simulated) verbal warning to the operator.
- Messages: Messages are displayed to the driver at least with the Red Light driver warning. The messages inform the driver of the absence of CHB system functions (e.g., ABS, ESC, or TCS) and the status of the service brake subsystem.

9 APPLICATION OF THE FUNCTIONAL SAFETY CONCEPT

This study identifies eight vehicle-level safety requirements (Safety Goals) and derives 198 CHB system and component functional safety requirements by following the Concept Phase (Part 3) in the ISO 26262 standard. Sections 9.1 and 9.2 present these requirements.

9.1 Vehicle-Level Safety Requirements (Safety Goals)

Vehicle-level safety requirements for the CHB system correspond to the safety goals presented in Section 6. The vehicle-level safety requirements for the CHB system are summarized below, along with the recommended safety strategies.

SG 1: Prevent unintended vehicle lateral motion/unintended yaw under all vehicle operating conditions in accordance with ASIL B classification.

- This safety goal covers:
  - Any lateral motion/yaw resulting from unintended activation of the CHB system functions, including the ABS, TCS, and ESC functions, including:
    - Lateral motion/yaw in the wrong direction
    - Any amount of lateral motion/yaw that exceeds the yaw amount expected during normal system operation by a yaw of to-be-determined (TBD) radians.
    - Any rate of change in lateral motion/yaw that exceeds the yaw rate expected during normal system operation by a yaw rate of TBD radians/sec.[37]
  - Failures in the CHB system that prevent intervention (e.g., absence of ESC) to correct the vehicle's yaw.
- This safety goal does not cover:
  - Failures in the vehicle's steering system or any vehicle system that commands or requests steering from the steering system.
  - Unintended lateral motion or unintended yaw resulting from wheel lock-up.

SG 2: Provide sufficient lateral motion/yaw all vehicle operating conditions in accordance with ASIL B classification.

- This safety goal covers:
  - Any amount of lateral motion/yaw that is below the yaw amount expected during normal system operation by a yaw of TBD radians.
  - Any rate of change in lateral motion/yaw that is below the yaw rate expected during normal system operation by a yaw rate of TBD radians/sec.[37]
  - Failures in the CHB system that prevent intervention (e.g., absence of ESC) to correct the vehicle's yaw.

[37] The allowable yaw rate deviation may be speed dependent (i.e., allowable yaw rate deviation is less than TBD radians/sec at TBD kph).

- This safety goal does not cover:
    - Failures in the vehicle's steering system or any vehicle system that commands or requests steering from the steering system.
    - Insufficient lateral motion or insufficient yaw resulting from wheel lock-up.

SG 3: Prevent CHB system failures that lead to loss of lateral motion control under all vehicle operating conditions in accordance with ASIL D classification.

- The CHB system is to prevent or minimize false positive loss of lateral motion control conditions (e.g., incorrect disabling of the ABS function).
- This safety goal includes:
    - Wheel lock-up, resulting in a loss of lateral motion control (i.e., steerability).
    - Changes in lateral motion when no change is expected by the vehicle dynamics (e.g., roll rate, yaw rate, vehicle speed, etc.).
    - No change in lateral motion when a change is expected based on the vehicle dynamics.
- This safety goal does not cover failures in the vehicle's steering system or any vehicle system that commands or requests steering from the steering system.

SG 4: Prevent unintended vehicle deceleration[38] under all vehicle operating conditions in accordance with ASIL D classification.

- This safety goal covers:
    - Any amount of vehicle deceleration that exceeds the deceleration commanded by the driver or another vehicle system by TBD m/s^2.[38]
    - Any degree of braking when braking is not requested by the driver or another vehicle system.

SG 5: Prevent insufficient and loss of braking under all vehicle operating conditions in accordance with ASIL D classification.

- The CHB system is to prevent or minimize false positive insufficient or loss of braking conditions (e.g., incorrect disabling of the ABS function).
- This safety goal covers:
    - Any amount of braking that results in violating regulatory requirements for stopping distance.[39]
    - Any vehicle deceleration that is less than the deceleration commanded by the driver or another vehicle system by TBD m/s^2.

[38] Some manufacturers may specify a threshold for "unintended vehicle deceleration" (e.g., 0.2g or 2 m/s^2).
[39] Federal Motor Vehicle Safety Standard (FMVSS) 135 specifies performance parameters in terms of minimum stopping distance for CHB systems. See Section 11.1 of this report for additional details.

- This safety goal does not include:
    - Mechanical failures in the hydraulic portion of the brake system, which are outside the scope of ISO 26262. Failures in these mechanical components are addressed through other industry practices.

SG 6: Prevent CHB system failures that lead to unintended vehicle propulsion under all vehicle operating conditions in accordance with ASIL C classification.

- This safety goal covers:
    - CHB system malfunctions that result in requests for propulsion torque that exceed the required torque to support a braking function by TBD m/s^2.[40]
    - Any amount of reduction in the braking torque that exceeds the requested amount and results in an unintended vehicle propulsion condition (i.e., the propulsion torque exceeds the braking torque).
- This safety goal does not cover:
    - Failures in the vehicle's ACS/ETC system or any vehicle system that commands or requests propulsion from the ACS/ETC system.

SG 7: Prevent CHB system failures that lead to insufficient vehicle propulsion or propulsion power reduction/loss under all vehicle operating conditions in accordance with ASIL C classification.

- This safety goal covers:
    - CHB system malfunctions that result in the vehicle failing to achieve the intended increase in propulsion torque by more than TBD sigma.[41]
- This safety goal does not cover:
    - Failures in the vehicle's ACS/ETC system or any vehicle system that commands or requests propulsion from the ACS/ETC system.

SG 8: Prevent CHB system failures that result in the vehicle rolling backward when not intended under all vehicle operating conditions in accordance with QM classification.[42]

In addition to any specific safety strategies listed for the safety goals above, the following general safety strategies are to be followed for each of the safety goals:

- The safety goals cover faults resulting from malfunctions of the CHB system or its subsystems, including the ABS, TCS, and ESC functions.
- CHB system is to prevent or detect faults and failures that could lead to the vehicle-level hazards.

[40] Some manufacturers may specify a threshold for "unintended vehicle propulsion" (e.g., 0.2g or 2 m/s^2).
[41] TBD sigma represents a deviation from the correctly functioning speed increase in profile for the ACS/ETC.
[42] This hazard is QM and therefore is not required to be addressed per ISO 26262.

- In case of the detection of any failure that could lead to vehicle-level hazards, the CHB system is to transition into a safe state within the fault tolerant time interval (FTTI).[43]
    - The FTTI is to be set based on established empirical data, system analysis, or engineering judgment.
    - The safe state is to be appropriate for the detected failure.
- In case of the detection of any failure that could lead to vehicle-level hazards, a warning is to be sent to the driver, and when necessary, any actions required by the driver are to be communicated to them.

9.2 Functional Safety Requirements for a CHB System

Following the Concept Phase (Part 3) in the ISO 26262 standard, this study identifies 198 functional safety requirements for a CHB system and its components. The distribution of these requirements is as follows:

1. General CHB System – 15 requirements
2. CHB Control Module – 91 requirements
3. Brake Pedal Assembly – 9 requirements
4. Brake Modulator – 10 requirements
5. Brake Pressure Sensor – 8 requirements
6. WSS – 8 requirements
7. Vehicle Dynamics Sensors – 27 requirements
8. Power Supply – 7 requirements
9. Communication System – 6 requirements
10. Interfacing System – 7 requirements
11. Mechanical CHB System Components – 10 requirements

Table 31 shows examples of safety requirements associated with the CHB control module, the safety analysis results from which the requirements are derived, and how the vehicle-level safety goal (SG 1 in this example) is allocated to one of the components in the system. The safety analysis identifies many failure modes and CFs for the CHB control module which could potentially lead to the violation of SG 1. Two CHB control module failures are chosen as examples in Table 31 to illustrate the development process of the safety requirements.

[43] ISO 26262 defines the FTTI as the time-span in which a fault or faults can be present in a system before a hazardous event occurs (Part 1, Clause 1.45) [1]. The FTTI consists of two parts (1) the time-span for detecting the fault, which is less than or equal to the diagnostic test interval, and (2) the fault reaction time, which is the time-span needed to transition to a safe state.

Table 31. Examples of Safety Requirements for the CHB Control Module

Safety Goal	Prevent insufficient braking and loss of braking under all vehicle operating conditions in accordance with ASIL D.
ASIL	D
Component	CHB Control Module
Safety Analysis (Examples)	• Hardware fault (sensors, ICs, etc.) • Arbitration algorithm fault
Safety Strategy	**Potential Safety Requirements (Examples)**
Detection	The ABS function is to be checked periodically based on the correct FTTI in order to prevent violation of any safety goals. • A fault tolerant strategy is to be applied for the ABS function. Fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the ABS function.
Fault Tolerance	If redundant elements are used, they are to be verified against common cause failures. 1. Failures in the electric power supply of one element are not to affect the power supply of the other element. 2. Failures in the communication path of one element are not to affect the communication path of the other element.
Safe State Warning	The CHB system command and control communication channel(s) with the components supporting the ABS, TCS, and ESC functions are to be validated at start up. Electronic braking commands are not to be issued until the validation of the communication channel(s) is successful. • In case of failure of validation, the CHB system is to transition into Safe Sate 1 for TCS associated faults, Safe State 2 for ESC associated faults, or Safe State 3 for ABS associated faults within a FTTI of TBD seconds, and an amber level driver warning is to be issued.

- The first safety requirement presented in Table 31 provides an example of a detection safety strategy. This requirement specifies periodic checks of the ABS function based on the FTTI. The frequency of the periodic checks will depend on the diagnostic measures implemented as part of the design, and would be derived from a detailed safety analysis of the specific hardware and software implementation for the ABS function. The periodic checks could range from power-on tests to continuous monitoring.
- The second safety requirement in Table 31 provides an example of a fault tolerance safety strategy. This requirement specifies the need for independence of redundant elements.
- The third safety requirement in Table 31 provides another example of a detection safety strategy for internal CHB system communications. In addition to the detection safety strategy, this requirement also incorporates two other safety strategies – transitioning to a safe state and warning the driver – in the event the communication system cannot be validated.

The rest of this section lists the 198 CHB functional safety requirements derived through this process. A functional safety requirement may have more than one ASIL associated with it, because the same requirement may cover more than one safety goal and these safety goals may have various levels of ASILs. The requirement may be implemented using different ASIL classification if independence among the implementation solutions can be demonstrated (Part 9 Clause 5.2 of ISO 26262).

9.2.1 General CHB System Functional Safety Requirements

This study derived 15 general functional safety requirements related to the CHB system. These requirements may cover the whole CHB system or may apply to all components within the CHB system. Each of the general CHB system functional safety requirements is listed in Table 32 along with the safety goals supported by the requirement and the associated ASILs.

Table 32. General Functional Safety Requirements

FSR ID	SG	ASIL	Functional Safety Requirement
1.1	3, 4, 5, 6, 7	D, C	The CHB system is to perform Power On tests, periodic tests or continuous monitoring tests to ensure the correctness of safety critical parameters, the integrity of critical system elements, and the integrity of the safety critical signals. • Critical parameters are those that are used to calculate the braking torques or the requests for propulsion torque increase or decrease. These include: o Brake pedal position o Brake fluid pressure o Yaw rate o Roll rate o Lateral acceleration o Longitudinal acceleration o Vehicle speed o Individual wheel speeds o Low voltage power supply o The steering wheel torque angle versus vehicle speed maps • Other critical parameters may include calculation and comparison results that confirm the proper operation of the system. • The proper operation of the followings critical system elements is to be checked before any braking or propulsion torque requests or commands are issued by the CHB system: o The BPPS o The WSS o The yaw rate sensor o The roll rate sensor o The lateral acceleration sensor o The longitudinal acceleration sensor o The brake pressure sensor • The critical interfacing sensors including: o The accelerator pedal sensor o The steering wheel torque and angle sensors • The communications channels between: o The critical sensors listed above and associated CHB system controllers o The CHB system controllers and the propulsion system controller o The CHB system controllers and the steering system controller. • A confirmation of the health and sanity of the CHB system control module, including the ABS, TCS, and ESC functions, is to be confirmed via an acceptable strategy before any requests or command for braking or propulsion torques are issued by the CHB system. o State of Health (SOH) checks may include: ▪ Random Access Memory (RAM) / Read-Only Memory (ROM) / Electronically Erasable Programmable Read Only Memory (EEPROM) Tests ▪ Analog to Digital (A/D) Converter Test o Shut Down TestSanity Checks may include: ▪ Quizzer or Seed & Key strategies • The frequency of the periodic tests is to be selected based on the FTTI[1], the fault detection time interval, and the fault reaction time interval. In case of failure in the periodic self-tests, the CHB system is to transition to the appropriate safe state within TBD ms.

FSR ID	SG	ASIL	Functional Safety Requirement
1.2	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system is to deliver the braking torque required to the vehicle wheels at the correct level under all vehicle operating conditions. • The CHB system is to deliver the correct level of braking within a tolerance that does not result in violation of any safety goals. The CHB system is to deliver the braking required to each of the vehicle wheels at the correct time for the correct duration under all vehicle operating conditions.
1.3	1, 2, 3, 4, 5, 6, 7	D, C, B	The braking torque applied by the CHB system is to result in a vehicle stopping distance that meets industry standards and regulatory requirements.
1.4	1, 2, 3, 4, 5, 6, 7	B, A, QM	Diagnostics of all safety critical components functions are to be conducted. In case of detected faults, the CHB system is to take mitigation action to prevent failures that lead to a violation of a safety goal, and appropriate DTCs are to be set. The diagnostics are to cover: • Hardware: yaw rate sensor, roll sensor, lateral acceleration sensor, longitudinal acceleration sensor, BPPS, brake pressure sensor, WSS, CHB system control module, and communications hardware. Software Functions: braking torque calculations, braking torque command, requested propulsion torque calculations, propulsion torque request.
1.5	1, 2, 3, 4, 5, 6, 7	QM	DTC(s) are to be set every time a safety goal is violated.
1.6	1, 2, 3, 4, 5, 6, 7	D, C, B, A, QM	To recover from a safe state, the CHB system is to reset and pass the power on self-test.
1.7	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	The hardware architectural Single Point Fault and Latent Fault metrics targets per ISO 26262 are to be demonstrated for the each safety goal.
1.10	1, 2, 3, 4, 5, 6, 7	D, C, B	If redundant elements are used and both elements fail, or if only one element is used and it fails, then the CHB system is to transition into Safe State 5 within the FTTI of TBD seconds, and a red light driver warning is to be issued.
1.11	1, 2, 3, 4, 5, 6, 7, 8	B, A, QM	Diagnostics covering the safety related functionality of the CHB system controller are to be instituted with a level of coverage corresponding to the ASIL of the safety goal that is affected. ISO 26262 diagnostics coverage guidelines for Low, Medium, and High are to be adhered to in order to comply with the hardware architectural metrics targets.
1.12	1, 2, 3, 4, 5, 6, 7, 8	B, A, QM	Diagnostics mechanisms are to adhere to ASIL B classification for ASIL D related elements and ASIL A classification for ASIL C related elements.

FSR ID	SG	ASIL	Functional Safety Requirement
1.13	1, 2, 3, 4, 5, 6, 7, 8	B, A, QM	Diagnostics covering the following failure modes shall be implemented: • Brake pressure sensor: o Integrated circuit faults o Open/short I/Os o Stuck on the same reading o Out of range o Offset o State of Health • WSS: o Integrated circuit faults o Open/short I/Os o Stuck on the same reading o Out of range o Offset o State of Health • Yaw rate sensor: o Integrated circuit faults o Open/short I/Os o Stuck on the same reading o Out of range o Offset o State of Health • Longitudinal acceleration sensor: o Integrated circuit faults o Open/short I/Os o Stuck on the same reading o Out of range • Roll rate sensor: o Integrated circuit faults o Open/short I/Os o Stuck on the same reading o Out of range • Lateral acceleration sensor: o Integrated circuit faults o Open/short I/Os o Stuck on the same reading o Out of range • Brake Modulator Motor: o Electromagnetic circuit faults • Brake Modulator Valves: o Stuck open o Stuck closed • Harnesses and Connectors: Open/short circuits

FSR ID	SG	ASIL	o Functional Safety Requirement
1.14	4, 5	D	Loss of the electronic portion of the CHB system is not to interfere with operation of the mechanical braking pathway.
1.15	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	The CHB system is to have a means for applying braking force to the wheels in the event of a failure of the primary service brake system. • The primary service brake system and secondary brake system are to be independent.

[1] The FTTI and TBD time intervals for transitioning into a safe state are typically determined by the manufacturers and may be defined based on the criticality of the sensor, the system architecture, and the limitations of the technology. Typically these FTTIs may be on the order of 150-250 ms.

9.2.2 CHB Control Module Functional Safety Requirements

This study derived 91 functional safety requirements related to the CHB control module. Of the 72 functional safety requirements derived for the CHB control module, 13 relate specifically to the ABS function, 14 relate specifically to the ESC function, and 11 relate specifically to the TCS function. The remaining 53 functional safety requirements cover the CHB control module.

Each of the CHB control module functional safety requirements is listed in Table 33 along with the safety goals supported by the requirement and the associated ASILs.

Table 33. Functional Safety Requirements for the CHB Control Module

FSR ID	SG	ASIL	Functional Safety Requirement
2.1	3, 4, 5, 6, 7	D, C	The health and sanity of the CHB system control module is to be ensured. • Power-on Self Tests are to be implemented to check the health of the controller. These tests may include: o Central Processing Unit (CPU) and Register Tests to check the internal working of the CPU. All CPU registers associated with the braking functions are to be checked during this test. o Interrupt and Exception Tests to check the interrupt and exception processing of the processor. o EEPROM Checksum Tests to check the EEPROM health. o Device Tests to check the peripheral devices connected to the microcontroller.
2.2	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module's I/Os pins are to be monitored for shorts to system voltages or ground.

FSR ID	SG	ASIL	Functional Safety Requirement
2.3	1, 2, 3, 4, 5, 6, 7	D, C, B	All single point CHB system controller hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the system is to transition to the corresponding safe state. • Hardware faults include those occurring in the ICs, circuit components, printed circuit boards, I/O pins, signal connectors, and power connectors.
2.4	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module is to have a mechanism to prevent unauthorized access to the CHB system control calculations and command path.
2.5	1, 2, 3, 4, 5, 6, 7	D, C, B	All single point faults that result in a failure to prevent unauthorized access to the CHB control module are to be detected and mitigated. • In case of unauthorized access to the CHB system control module, the CHB system is to transition to Safe State 5 within TBD ms, and a red light driver warning is to be issued. • A DTC is to be set.
2.6	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system is to transition into the corresponding safe state within TBD ms after the diagnostics detect a safety-critical failure.
2.7	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module is to have a mechanism for determining wheel conditions (e.g., low pressure, incorrect tire size, etc.) that affect the safe operation of the CHB system functions (e.g., ABS, TCS, and ESC). • If the ABS, TCS, or ESC functions cannot be provided, the CHB system is to transition into the appropriate safe state.
2.8	1, 2, 3, 4, 5, 6, 7	D, C, B	The braking torque applied to the wheels by the CHB system is not to lead to vehicle instability under all vehicle operating conditions
2.9	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The braking torque applied by the CHB system is to be controlled and updated within the correct time duration. The time duration required to update the braking torque is not to result in the violation of safety goals

FSR ID	SG	ASIL	Functional Safety Requirement
2.10	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The CHB system control module is to calculate the braking torque based on the BPP input, the inputs from the ABS, TCS, and ESC functions, and/or braking requests from other vehicle systems.
2.11	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module is to include metrics that clearly define the limits of vehicle stability (e.g., lateral acceleration limits). The braking torque computed by the control algorithms are to be validated against the vehicle stability metrics before any electronic braking command is issued. • In case of a failure, the CHB system is to transition into Safe State 1 (TCS fault), Safe State 2 (ESC fault), Safe State 3 (ABS fault), or Safe State 6 (other braking function faults) within a FTTI of TBD seconds and an amber level driver warning is to be issued. Appropriate warnings to the driver from affected interfacing systems are to be issued.
2.12	1, 2, 3, 4, 5, 6, 7	D, C, B	The braking command and control communication channel(s) are to be validated at start up. Electronic braking commands are not to be issued until the validation of the communication channel(s) is successful. • In case of failure in validating the communication channels, the CHB system is to transition into Safe State 4 within a FTTI of TBD seconds, and a red level driver warning is to be issued.
2.13	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system command and control communication channel(s) with the components supporting the ABS, TCS, and ESC functions are to be validated at start up. Electronic braking commands are not to be issued until the validation of the communication channel(s) is successful. • In case of failure of validation, the CHB system is to transition into Safe Sate 1 for TCS associated faults, Safe State 2 for ESC associated faults, or Safe State 3 for ABS associated faults within a FTTI of TBD seconds, and an amber level driver warning is to be issued.
2.14	1, 2, 3, 4, 5, 6, 7	D, C, B	All electrical hardware and software elements associated with the delivery of the braking function are to comply with ASIL D classification for SG 3, 4, and 5, ASIL C classification for SG 6 and 7, and ASIL B classification for SG 1 and 2 • If independence of the elements (per ISO 26262) cannot be demonstrated, then the higher ASIL classification is to be adopted. • If torque maps/look up tables are used, their content are to be checked for validity and correctness at the correct frequency.

FSR ID	SG	ASIL	Functional Safety Requirement
2.15	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module is to qualify the yaw rate sensor input for validity and correctness (plausibility and rationality).
2.16	1, 2, 3, 4, 5, 6, 7	B	The CHB system control module is to qualify the roll rate sensor input for validity and correctness (plausibility and rationality).
2.17	1, 2, 3, 4, 5, 6, 7	B	The CHB system control module is to qualify the lateral acceleration sensor input for validity and correctness (plausibility and rationality).
2.18	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module is to qualify the WSS(s) input(s) for validity and correctness (plausibility and rationality).
2.19	1, 2, 3, 4, 5, 6, 7	B	The CHB system control module is to qualify the longitudinal acceleration sensor input for validity and correctness (plausibility and rationality).
2.20	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	Communication and data transfer between the CHB system control module and the BPPS are to be qualified for validity and correctness (plausibility and rationality). • In case of a fault, the correct failure mode effect mitigation strategy is to be applied. • The critical communications include the braking torque and the diagnostics of the BPPS.
2.21	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module's algorithm or method for calculating the braking torque is to be validated.
2.22	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module's algorithm or method for calculating the distribution of the braking torque to the individual wheels is to be validated.

FSR ID	SG	ASIL	Functional Safety Requirement
2.23	1, 2, 3, 4, 5, 6, 7	D, C, B	The braking torque corresponding to the BPPS input or braking requests from other vehicle systems is to be calculated correctly, and the results are to be qualified for validity and correctness under all vehicle operating conditions.
2.24	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	The braking torque applied to each wheel by the CHB system is to be applied to the correct wheel, at the correct time, for the correct duration, and at the correct magnitude under all vehicle operating conditions.
2.25	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	The braking command to each wheel is to be controlled and updated with the correct brake force distribution, in the correct direction (e.g., increase or decrease), and within the correct time duration.
2.26	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	The time duration required to update the braking command is not to result in violation of a safety goal. • The time duration is to be reflected in the relevant software functions' execution time, and the transient response of the mechanical and hydraulic system components.[1]
2.27	3, 4, 5, 6, 7	D, C	The braking control algorithm is to be checked periodically based on the correct FTTI in order to prevent violation of any safety goals.[2] • The braking control algorithm is to employ validity checks to prevent unintended braking commands. • A fault tolerant strategy is to be applied for the braking control. Fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the braking control algorithm.
2.28	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	In case of a fault in the braking control algorithm that leads the CHB system control module to become unable to control the braking torque, the CHB system is to transition into Safe State 5 within TBD ms and the red level driver warning is to be issued.[3] • DTCs are to be set.
2.29	1, 2, 3, 4	D, C, B	The braking pressure applied to each wheel via the ABS function is to be validated. • If this is done via a non-electrical/electronic means, then this requirements falls outside the scope of ISO 26262.
2.30	3, 4, 5, 6, 7	D, C	All other critical parameters used by the CHB system control module are to be checked periodically based on the FTTI requirements.

FSR ID	SG	ASIL	Functional Safety Requirement
2.31	1, 2, 3, 5, 8	D, C, B, A, QM	The CHB control module is to be capable of responding to braking requests from other vehicle systems or internal brake functions regardless of the brake pedal position.
2.32	1, 2, 3, 4, 5	D, C, B	The CHB system control module is to have a mechanism for determining which wheel is braked in response to a braking command.
2.33	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	The CHB system control module is to be able to properly increase and decrease the hydraulic pressure when the brake pedal is not pressed.
2.34	1, 2, 3	D, B	The ABS function is to include a control algorithm that determines the conditions for wheel lock under all braking conditions. • The ABS control is to prevent the wheel lock conditions while maximizing transfer of braking force to the road surface. • Wheel lock may be permissible on deformable surfaces if the ABS function is specifically designed to allow the wheels to lock to minimize stopping distance. The ABS function is to have an algorithm to identify deformable surfaces.
2.35	1, 2, 3, 4, 5, 6, 7	D, C, B	When active, the ABS function is not to result in the CHB system failing to meet the requirements for minimum stopping distance. • The ABS function is not to activate when not required.
2.36	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The ABS function's control of the brake pressure is to be updated such that the resultant transient in the brake pressure does not translate into feedback that confuses the driver and results in unsafe braking action by the driver.
2.37	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The ABS function is to validate that the updated brake pressure is in the correct direction (increase or decrease).
2.38	1, 2, 3, 5	D, C, B	The ABS function's command to control the brake pressure at each wheel is to be qualified for rationality and plausibility.

FSR ID	SG	ASIL	Functional Safety Requirement
2.39	1, 2, 3, 5	D, C, B	The inputs from the vehicle sensors used by the ABS function are to be qualified for validity and correctness (plausibility and rationality). • In case of a fault that leads to a failure in the ability to validate the input from any sensor critical to the ABS function, the CHB system is to transition to Safe State 3 within a FTTI of TBD seconds, and an amber level driver warning is to be issued.
2.40	1, 2, 3, 5	D, C, B	The input parameters to the ABS function from other CHB system functions, and the interfacing systems and subsystems are to be qualified for validity and correctness (plausibility and rationality).
2.41	1, 2, 3, 5	D, C, B	The ABS function's method for calculating the braking pressure is to be validated
2.42	3, 5	D, C	The ABS function is to be checked periodically based on the correct FTTI in order to prevent violation of any safety goals.[2] • A fault tolerant strategy is to be applied for the ABS function. Fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the ABS function.
2.43	1, 2, 3, 5	D, C, B	In case of a fault that prevents the ABS function from controlling the braking pressure, the CHB system is to transition into Safe State 3 within TBD ms time, and the amber level driver warning is to be issued. • DTCs are to be set.
2.44	3, 5	D	When the ABS function is deactivated, the CHB system is to deliver a message to the driver indicating that the ABS function is off.
2.45	1, 2, 3, 4, 5	D, C, B	The ABS function is to prevent wheel lock-up when braking is requested by other vehicle systems (e.g., ACC, CIB, etc.).
2.46	1, 2, 3, 4, 5	D, C, B	The ABS function is to control the brake pressure at the correct time, for the correct duration, and with the correct magnitude under all vehicle operating conditions.
2.47	1, 2, 3, 4, 5, 6, 7	D, C, B	The TCS function is to include a control algorithm that determines the conditions for wheel spinning under all braking conditions. • The TCS function is to prevent the wheel spinning conditions while maximizing transfer of propulsion force to the road surface.

FSR ID	SG	ASIL	Functional Safety Requirement
2.48	4, 6, 7	D, C	The TCS function when activated is not to prevent the intended acceleration of the vehicle as requested by the driver or other vehicle systems.
2.49	1, 2, 3, 4, 5, 6, 7	D, C, B	The inputs from the vehicle sensors used by the TCS function are to be qualified for validity and correctness (plausibility and rationality). • In case of a fault that leads to a failure in the ability to validate the input from any sensor critical to the TCS function, the CHB system is to transition to Safe State 1 within a FTTI of TBD seconds, and an amber level driver warning is to be issued.
2.50	1, 2, 3, 4, 5, 6, 7	D, C, B	The input parameters to the TCS function from other CHB system functions, and the interfacing systems and subsystems are to be qualified for validity and correctness (plausibility and rationality).
2.51	1, 2, 3, 4, 5, 6, 7	D, C, B	The TCS function's command to modify the braking and/or propulsion torque for each wheel is to be qualified for rationality and plausibility.
2.52	1, 2, 3, 4, 5, 6, 7	D, C, B	The TCS function's method for calculating the required modification to braking and/or propulsion torque is to be validated.
2.53	1, 2, 3, 4, 5, 6, 7	D, C, B	The TCS function is to command the correct braking and/or propulsion torque to the correct wheel, at the correct magnitude, at the correct time, and for the correct duration under all vehicle operating conditions.
2.54	3, 4, 5, 6, 7	D, C	The TCS function is to be checked periodically based on the correct FTTI in order to prevent violation of any safety goal.[2] • A fault tolerant strategy is to be applied for the TCS function. Fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the TCS function.
2.55	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	In case of a fault in the TCS function that prevents controlling the braking and/or propulsion torque applied to the wheel, the CHB system is to transition into Safe State 1 within TBD ms time, and the amber light driver warning is to be issued. • DTCs are to be set.

FSR ID	SG	ASIL	Functional Safety Requirement
2.56	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	When the TSC function is deactivated, the CHB system is to deliver message to the driver indicating that the TSC function is off.
2.57	1, 2, 3, 4, 5, 7	D, C, B	The TCS function is not to activate if the wheels are not spinning.
2.58	1, 2, 3, 4, 5, 6, 7	D, C, B	The ESC function is to have a control algorithm that determines the conditions for vehicle stability at the limits of traction under all vehicle operating conditions. • The ESC function is to maintain the vehicle's longitudinal velocity, lateral velocity and yaw velocity within safe limits (e.g., vehicle stability limits) under all vehicle operating conditions.
2.59	4, 6	D, C	When activated, the ESC function is not to result in unintended deceleration or unintended acceleration of the vehicle.
2.60	1, 2, 3, 4, 5, 6, 7	D, C, B	The inputs from the vehicle sensors used by the ESC function are to be qualified for validity and correctness (plausibility and rationality). • In case of a fault that leads to a failure of the ability to validate the input from any sensor critical to the ESC function, the brake system is to transition to Safe State 2 within a FTTI of TBD seconds and an amber light driver warning is to be issued.
2.61	1, 2, 3, 4, 5, 6, 7	D, C, B	The input parameters to the ESC function from other CHB system functions, and the interfacing systems and subsystems are to be qualified for validity and correctness (plausibility and rationality).
2.62	1, 2, 3, 4, 5, 6, 7	D, C, B	The ESC function's command to modify braking or propulsion torque for each wheel is to be qualified for rationality and plausibility.
2.63	1, 2, 3, 4, 5, 6, 7	D, C, B	The ESC function's method for calculating changes to the braking or propulsion torque is to be validated.

FSR ID	SG	ASIL	Functional Safety Requirement
2.64	1, 2, 3, 4, 5, 6, 7	D, C, B	The ESC function's commands to change the braking or propulsion torque are to be applied to the correct wheel, at the correct magnitude, at the correct time, and for the correct duration under all vehicle operating conditions.
2.65	3, 4, 5, 6, 7	D, C	The ESC function is to be checked periodically based on the correct FTTI in order to prevent violation of any safety goal.[2] • A fault tolerant strategy is to be applied for the ESC function. Fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the ESC function.
2.66	1, 2, 3, 4, 5, 6, 7	D, C, B	In case of a fault that leads the ESC function to be unable to control the braking or propulsion torque applied to the wheels, the CHB system is to transition into Safe State 2 within TBD ms time, and the amber light driver warning is to be issued. • DTCs are to be set.
2.67	1, 2, 3, 4, 5, 6, 7	D, C, B	When the ESC function is deactivated, the CHB system is to deliver message to the driver indicating that the ESC function is off.
2.68	1, 2	B	The ESC function is to determine the yaw error between the intended vehicle heading and actual vehicle heading.
2.69	1, 2	B	The ESC function is to control the vehicle's yaw rate to minimize any yaw error between the intended vehicle heading and actual vehicle heading. • The yaw rate correction is to be provided in the correct direction, at the correct magnitude, and for the correct duration so as to prevent violation of any safety goals.
2.70	1, 2	C	The ESC function is to have a mechanism for determining the driver's steering input. • The driver's steering request may be provided by steering wheel angle and torque sensors in the steering system.
2.71	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	The ESC function is to have calculation algorithms for estimating the vehicle side slip or side slip derivative.

FSR ID	SG	ASIL	Functional Safety Requirement
2.72	8	QM	The CHB system is to prevent vehicle roll back conditions by more than the distance allowed by existing regulations when internal brake system functions intended to maintain the vehicle position on an incline are engaged.
2.73	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The CHB system control module is to have an arbitration strategy for braking requests from the driver and other vehicle systems.
2.74	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The CHB system control module is to have an arbitration strategy for braking requests from the driver and internal brake subsystems (i.e., TCS and ESC). • In case of a failure in this arbitration strategy, the CHB system is to transition into Safe Sate 1 for TCS associated faults and Safe State 2 for ESC associated faults within a FTTI of TBD seconds and an amber level driver warning is to be issued.
2.75	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The CHB system control module is to have an arbitration strategy for braking requests from other vehicle systems and internal brake subsystems (TCS and ESC). • In case of a failure in this arbitration strategy, the CHB system is to transition into Safe Sate 1 for TCS associated faults, Safe State 2 for ESC associated faults, or Safe State 6 for faults associated with requests from other vehicle systems within a FTTI of TBD seconds and an amber level driver warning is to be issued. • Appropriate warnings to the driver from affected interfacing systems are to be issued.
2.76	1, 2, 3, 4, 5, 6, 7	D, C, B	The CHB system control module is to arbitrate between multiple requests for braking from interfacing vehicle systems, the driver, and internal CHB system functions. • The control module's arbitration logic strategy and algorithm are to be checked for health and sanity periodically based on the FTTI.
2.77	1, 2, 3, 4, 5, 6, 7	D, C, B	The output of the CHB system controller arbitration logic is to be qualified for validity and correctness.
2.78	1, 2, 3, 4, 5, 6, 7	D, C, B	The arbitration strategy is to clearly define the action of the CHB system when there are conflicting braking requests from interfacing vehicle systems, the driver, and/or internal brake system functions.

FSR ID	SG	ASIL	Functional Safety Requirement
2.79	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	Execution time for the arbitration logic is not to result in violation of any safety goals.
2.80	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The CHB system is to deliver the request for propulsion torque increase or decrease to the ACS/ETC at the correct level under all vehicle operating conditions. • The CHB system is to request the correct level of propulsion torque within a tolerance that does not result in violation of any safety goals. • The CHB system is to request the propulsion torque required to each of the vehicle wheels at the correct time for the correct duration under all vehicle operating conditions.
2.81	1, 2, 3, 4, 5, 6, 7	D, C, B	The propulsion torque requested from the ACS/ETC by the CHB system is not to lead to vehicle instability under all vehicle operating conditions. • Conditions for determining vehicle instability are to be defined (e.g., yaw rate or lateral acceleration thresholds).
2.82	1, 2, 5	D, C, B	The CHB system is to deliver the request for steering angle modifications to the steering at the correct level under all vehicle operating conditions. • The CHB system is to request the correct level of steering angle modification within a tolerance that does not result in violation of any safety goals. • The CHB system is to request the steering angle modification at the correct time and for the correct duration under all vehicle operating conditions.
2.83	1, 2, 5	D, C, B	The steering angle requested from the steering system by the CHB system is not to lead to vehicle instability under all vehicle operating conditions
2.84	1, 2, 5	D, C, B	Steering angle adjustment requests issued by the CHB system to the steering system are to be qualified for validity and correctness (plausibility and rationality) by the CHB system control module.
2.85	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	If the CHB system is responsible for determining the vehicle speed, the CHB system control module is to have algorithms to determine the vehicle speed based on individual wheel speed measurement.
2.86	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	If the CHB system is responsible for determining the vehicle speed, the CHB system control module is to validate the vehicle speed prior to broadcasting the vehicle speed to other vehicle systems.

FSR ID	SG	ASIL	Functional Safety Requirement
2.87	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	If the CHB system is responsible for determining the vehicle speed, the vehicle speed calculation is to be updated with TBD frequency to prevent violation of any safety goals.
2.88	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	If the CHB system is responsible for determining the vehicle speed, the vehicle speed calculation algorithm is to account for wheels that may be slipping or spinning.
2.89	1, 2, 3, 4, 5, 6, 7	D, C, B	The controller is to have diagnostics for safety relevant failures caused by electromagnetic compatibility/electromagnetic interference, electrostatic discharge, single event effects, contamination, and other environmental conditions.

2.90	1, 2, 3, 4, 5, 6, 7, 8	B, A, QM	Diagnostics covering the failures for the following parts of the CHB system control module are to be implemented:
			• Execution logic (wrong coding, wrong or no execution, execution out of order, execution too fast or too slow, stack overflow or underflow).
			• On-chip communication and bus arbitration
			• The main controller's:
			  o CPU
			  o Processor memory
			  o Arithmetic Logic Unit
			  o Registers
			  o A/D converter
			  o Software program execution
			  o Connections (I/O) faults (short/open/drift/oscillation)
			  o Power supply
			• If an auxiliary processor is used, its:
			  o CPU
			  o Processor memory
			  o Arithmetic Logic Unit
			  o Registers
			  o A/D converter
			  o Software program execution
			  o Connections (I/O) faults (short/open/drift/oscillation)
			  o Power supply
			• The wiring harnesses and connectors for open and short circuits
			• Critical messages, including communication bus messages

FSR ID	SG	ASIL	Functional Safety Requirement
2.91	1, 2, 3, 4, 5, 6, 7, 8	QM	The CHB system control module is to log and save the following data every time a transition to safe state is executed due to a violation of a safety goal: • The diagnostics information of the fault(s) including the time at which the fault was detected and the nature of the fault. • The time interval from the detection of the fault to reaching safe state. • The time the system degradation strategy started, including the start and end of each phase if applicable and the values of the system metrics for each phase (e.g., braking torque output level). • The time the driver warning strategy started, including the start and end of each phase, if applicable, and the values of the system metrics for each phase. • The data are to be retained until they are accessed by authorized personnel.

[1] Some CHB systems may use a software execution time on the order of 10 to 20 ms for safety relevant requirements. This time duration is dependent on the software architecture.

[2] CHB systems may use hardware and software watchdog timers to monitor the algorithm execution sequence. The timer is dependent on the software architecture, but may be on the order of 300 to 500 ms.

[3] The transition time is design dependent. An example transition time may be on the order of 200 ms.

9.2.3 Brake Pedal Assembly Functional Safety Requirements

This study derived nine functional safety requirements related to the brake pedal assembly. Each of the functional safety requirements for the brake pedal assembly is listed in Table 34 along with the safety goals supported by the requirement and the associated ASILs.

Table 34. Functional Safety Requirements for the Brake Pedal Assembly

FSR ID	SG	ASIL	Functional Safety Requirement
3.1	1, 2, 3, 4, 5, 6, 7	D, C, B	The BPP corresponding to the braking torque requested by the driver is to be mapped correctly and consistently, and the results are be qualified for validity and correctness under all vehicle operating conditions, over the usable life of the vehicle.
3.2	3, 4, 5, 6, 7	D, C	The health and sanity of the BPPS is to be monitored and confirmed under all operating vehicle conditions.

FSR ID	SG	ASIL	Functional Safety Requirement
3.3	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The BPP value is to be measured, and the value shall be valid and correct.
3.4	1, 2, 3, 4, 5, 6, 7	D, C, B	The BPP to electrical conversion method is to be validated
3.5	1, 2, 3, 4, 5, 6, 7	D, C, B	The value of the BPP shall be communicated to the CHB system control module. The communication message or data transfer is to be qualified for validity (sent and received signals are the same) and correctness (plausibility (within range) and rationality (does not contradict with previous or other related signals/messages)). • The updated value of the BPP is to be received within TBD seconds. This time shall be specified to support the timely update of the brake torque command in order to prevent the violation of any safety goals.
3.6	1, 2, 3, 4, 5, 6, 7	D, C, B	In case of a fault that violates a safety goal, the BPPS is to communicate the fault to the CHB system control module.
3.7	1, 2, 3, 4, 5, 6, 7	B, A, QM	The BPPS is to have diagnostics for safety relevant failures caused by EMC/EMI, ESD, contamination, and other environmental conditions.

FSR ID	SG	ASIL	Functional Safety Requirement
3.8	1, 2, 3, 4, 5, 6, 7	D, C, B	All single point BPPS hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the system is to transition to the corresponding safe state. • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.
3.9	1, 2, 3, 4, 5, 6, 7	QM	The BP assembly mechanical faults that result in incorrect measurement of the BPP are to be detected and mitigated (not covered by ISO 26262). • Incorrect measurements include deviations from the correct BPP value or being stuck at the same value permanently or intermittently

[1] The FTTI and TBD time intervals for transitioning into a safe state are typically determined by the manufacturers and may be defined based on the criticality of the sensor, the system architecture, and the limitations of the technology. Typically these FTTIs may be on the order of 150-250 ms.

9.2.4 Brake Modulator Functional Safety Requirements

This study derived ten functional safety requirements related to the brake modulator, which is the primary actuator that regulates the hydraulic brake pressure delivered to each wheel. Each of the functional safety requirements for the brake modulator is listed in Table 35 along with the safety goals supported by the requirement and the associated ASILs.

Table 35. Functional Safety Requirements for the Brake Modulator

FSR ID	SG	ASIL	Functional Safety Requirement
4.1	3, 4, 5, 6	D, C	The command for braking from the CHB system control module is to be qualified for rationality and plausibility.
4.2	1, 2, 3, 4, 5, 6, 8	D, C, B	The brake modulator is to apply the correct hydraulic pressure at the correct wheel for the correct duration under all vehicle operating conditions
4.3	1, 2, 3, 4, 5, 6, 8	D, C, B	The brake modulator is to communicate the hydraulic pressures applied to each wheel to the CHB system control module within the correct time.

FSR ID	SG	ASIL	Functional Safety Requirement
4.4	1, 2, 3, 4, 5, 6	D, C, B	The brake modulator's transient response is not to result in a violation of any safety goal.
4.5	1, 2, 3, 4, 5, 6	D, C, B	The brake modulator is to have diagnostics to monitor the current draw of the motor.
4.6	3, 4, 5, 6	D, C	The brake modulator is to have diagnostics to monitor the back electromotive force of the motor.
4.7	1, 2, 3, 4, 5, 6	D, C, B	The brake modulator is to validate the hydraulic pressure applied to the wheels.
4.8	1, 2, 3, 4, 5, 6	D, C, B	In case of a fault that leads prevents the brake modulator from delivering the required hydraulic pressure to the wheels, the CHB system is to transition to Safe State 5 within a FTTI of TBD seconds, and a red light driver warning is to be issued. • DTCs are to be set.
4.9	1, 2, 3, 4, 5, 6	D, C, B	In case of a fault that prevents the brake modulator from validating the hydraulic pressure delivered to the wheels, the CHB system is to transition to Safe State 4 within a FTTI of TBD seconds, and a red light driver warning is to be issued. • DTCs are to be set.
4.10	1, 2, 3, 4, 5, 6	D, C, B	The brake modulator is to communicate the status of the valves and pump motor to the CHB control module with TBD frequency.

[1] The FTTI and TBD time intervals for transitioning into a safe state are typically determined by the manufacturers and may be defined based on the criticality of the sensor, the system architecture, and the limitations of the technology. Typically these FTTIs may be on the order of 150-250 ms.

9.2.5 Brake Pressure Sensor Functional Safety Requirements

This study derived eight functional safety requirements related to the brake pressure sensor, which measures the hydraulic brake pressure in the CHB system. Each of the functional safety requirements for the brake pressure sensor is listed in Table 36 along with the safety goals supported by the requirement and the associated ASILs.

Table 36. Functional Safety Requirements for the Brake Pressure Sensor

FSR ID	SG	ASIL	Functional Safety Requirement
5.1	1, 2, 3, 4, 5, 6, 7	D, C, B	The brake pressure sensor is to measure the master cylinder pressure and the value is to be qualified for validity and correctness.
5.2	1, 2, 3, 4, 5, 6, 7	D, C, B	The brake pressure sensor's pressure to electrical conversion method is to be validated.
5.3	3, 4, 5, 6, 7	D, C	The brake pressure sensor's input voltage is to be monitored for over and under voltage conditions whenever the CHB system is on. In case of failure in the input voltage, the CHB system is to transition into Safe State 4 within TBD ms, and a red light driver warning is to be issued. • DTCs are to be set.
5.4	1, 2, 3, 4, 5, 6, 7	D, C, B	The brake pressure sensor's measurement of the hydraulic pressure is to be communicated to the CHB system control module. The communication message or data transfer is to be qualified for validity, correctness, and rationality. • The updated value of the brake pressure sensor is to be received within TBD seconds. This time is to be specified to support the timely update of the CHB system in order to prevent the violation of any safety goals.
5.5	3, 4, 5, 6, 7	D, C	The health and sanity of the brake pressure sensor is to be monitored and confirmed under all operating vehicle conditions.
5.6	1, 2, 3, 4, 5, 6, 7	D, C, B	In case of a fault that violates a safety goal, the brake pressure sensor is to communicate the fault to the CHB system control module. • The brake system is to transition to Safe States 2 and 3 (deactivate ESC and ABS) within a FTTI of TBD ms and an amber light driver warning is to be issued.
5.7	1, 2, 3, 4, 5, 6, 7	B, A, QM	The brake pressure sensor is to have diagnostics for safety relevant failures caused by EMC/EMI, ESD, contamination, and other environmental conditions.

FSR ID	SG	ASIL	Functional Safety Requirement
5.8	1, 2, 3, 4, 5, 6, 7	D, C, B	All single point hardware faults in the brake pressure sensor that lead to violation of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the system is to transition to the corresponding safe state. • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.

[1] The FTTI and TBD time intervals for transitioning into a safe state are typically determined by the manufacturers and may be defined based on the criticality of the sensor, the system architecture, and the limitations of the technology. Typically these FTTIs may be on the order of 150-250 ms.

9.2.6 Wheel Speed Sensor Functional Safety Requirements

This study derived eight functional safety requirements related to the WSS, which measures the rotational speed of individual wheels. Each of the functional safety requirements for the WSS is listed in Table 37 along with the safety goals supported by the requirement and the associated ASILs.

Table 37. Functional Safety Requirements for the WSS

FSR ID	SG	ASIL	Functional Safety Requirement
6.1	1, 2, 3, 4, 5, 6, 7	D, C, B	The WSSs are to measure the speeds of individual vehicle wheels and the values are to be qualified for validity and correctness.
6.2	1, 2, 3, 4, 5, 6, 7	D, C, B	The WSS's method for converting the rotational speed to an electrical signal is to be validated.
6.3	1, 2, 3, 4, 5, 6, 7	D, C, B	The WSS's input voltage is to be monitored for over and under voltage conditions whenever the CHB system is on. In case of a failure in the input voltage, the CHB system is to transition into Safe States 1, 2, and 3 (deactivate TCS, ESC, and ABS) within TBD ms, and an amber light driver warning is to be issued. • DTCs are to be set.

FSR ID	SG	ASIL	Functional Safety Requirement
6.4	1, 2, 3, 4, 5, 6, 7	D, C, B	The individual wheel speed measurements by the WSS are to be communicated to the CHB system control module. The communication message or data transfer is to be qualified for validity and correctness. • The updated value of the WSS is to be received within TBD seconds. This time is to be specified to support the timely update of the CHB system in order to prevent the violation of any safety goals.
6.5	1, 2, 3, 4, 5, 6, 7	D, C, B	The health and sanity of the WSSs are to be monitored and confirmed under all operating vehicle conditions.
6.6	1, 2, 3, 4, 5, 6, 7	D, C, B	In case of a fault that violates a safety goal, the WSS is to communicate the fault to the CHB system control module. • The CHB system is to transition to Safe States 1 and 3 (deactivate TCS and ABS) within a FTTI of TBD ms and an amber light driver warning is to be issued.
6.7	1, 2, 3, 4, 5, 6, 7	D, C, B	The WSS is to have diagnostics for safety relevant failures caused by EMC/EMI, ESD, contamination, and other environmental conditions.
6.8	1, 2, 3, 4, 5, 6, 7	D, C, B	All single point WSS hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the CHB system is to transition to the corresponding safe state. • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.

[1] The FTTI and TBD time intervals for transitioning into a safe state are typically determined by the manufacturers and may be defined based on the criticality of the sensor, the system architecture, and the limitations of the technology. Typically these FTTIs may be on the order of 150-250 ms.

9.2.7 Vehicle Dynamics Sensors Functional Safety Requirements

This study derived 27 functional safety requirements related to the vehicle dynamics sensors, which includes the yaw rate sensor, lateral accelerator sensor, roll rate sensor, and longitudinal acceleration sensor. These sensors provide the CHB system with critical data regarding the vehicle's current state. Each of the functional safety requirements for the vehicle dynamics sensors is listed in Table 38 along with the safety goals supported by the requirement and the associated ASILs.

Table 38. Functional Safety Requirements for the Vehicle Dynamics Sensors

FSR ID	SG	ASIL	Functional Safety Requirement
7.1	1, 2, 3, 4, 5, 6, 7	D, C, B	The yaw rate sensor is to measure the yaw rate of the vehicle and the value is to be qualified for validity and correctness.
7.2	1, 2, 3, 4, 5, 6, 7	D, C, B	The yaw rate sensor's conversion method from the yaw rate to an electrical signal is to be validated.
7.3	3, 4, 5, 6, 7	D, C	The yaw rate sensor's input voltage is to be monitored for over and under voltage conditions whenever the CHB system is on. In case of failure in the input voltage, the CHB system is to transition into Safe State 1 and 2 (TCS and ESC disabled) within the FTTI of TBD ms, and an amber light driver warning is to be issued. • DTCs are to be set.
7.4	1, 2, 3, 4, 5, 6, 7	D, C, B	The yaw rate measurement by the yaw rate sensor is to be communicated to the CHB system control module. The communication message or data transfer is to be qualified for validity and correctness. • The updated value of the yaw rate sensor is to be received within TBD seconds. This time is to be specified to support the timely update of the CHB system in order to prevent the violation of any safety goals.
7.5	3, 4, 5, 6, 7	D, C	The health and sanity of the yaw rate sensor are to be monitored and confirmed under all operating vehicle conditions.
7.6	1, 2, 3, 4, 5, 6, 7	D, C, B	In case of a fault that violates a safety goal, the yaw rate sensor is to communicate the fault to the CHB system control module. • The CHB system is to transition to Safe State 2 (deactivate ESC) within a FTTI of TBD ms and an amber light driver warning is to be issued.
7.7	1, 2, 3, 4, 5, 6, 7	B, A, QM	The yaw rate sensor is to have diagnostics for safety relevant failures caused by EMC/EMI, ESD, contamination, and other environmental conditions.

FSR ID	SG	ASIL	Functional Safety Requirement
7.8	1, 2, 3, 4, 5, 6, 7	D, C, B	All single point yaw rate sensor hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the system is to transition to the corresponding safe state. • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.
7.9	1, 2, 3, 4, 5, 6, 7	B	The lateral acceleration sensor is to measure the lateral acceleration of the vehicle and the value is to be qualified for validity and correctness.
7.10	1, 2, 3, 4, 5, 6, 7	B	The lateral acceleration sensor's conversion method from the lateral acceleration to an electrical signal is to be validated.
7.11	1, 2, 3, 4, 5, 6, 7	B	The lateral acceleration measurement by the lateral acceleration sensor is to be communicated to the CHB system control module. The communication message or data transfer is to be qualified for validity and correctness. • The updated value of the lateral acceleration sensor is to be received within TBD seconds. This time is to be specified to support the timely update of the CHB system in order to prevent the violation of any safety goals
7.12	1, 2, 3, 4, 5, 6, 7	B	In case of a fault that violates a safety goal, the lateral acceleration sensor is to communicate the fault to the CHB system control module. • An amber light driver warning is to be issued.
7.13	1, 2, 3, 4, 5, 6, 7	B	In case of a fault that violates a safety goal, the lateral acceleration sensor is to communicate the fault to the CHB system control module. • The brake system is to transition to Safe State 1 and 2 (deactivate TCS and ESC) within a FTTI of TBD ms and an amber light driver warning is to be issued.
7.14	1, 2, 3, 4, 5, 6, 7	QM	The lateral acceleration sensor is to have diagnostics for safety relevant failures caused by EMC/EMI, ESD, contamination, and other environmental conditions.

FSR ID	SG	ASIL	Functional Safety Requirement
7.15	1, 2, 3, 4, 5, 6, 7	B	All single point lateral acceleration sensor hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the system is to transition to the corresponding safe state. • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.
7.16	1, 2, 3, 4, 5, 6, 7	B	The roll rate sensor is to measure the roll of the vehicle, and the value is to be qualified for validity and correctness.
7.17	1, 2, 3, 4, 5, 6, 7	B	The roll rate sensor's conversion method from the roll rate to an electrical signal is to be validated.
7.18	1, 2, 3, 4, 5, 6, 7	B	The roll rate measurement by the roll rate sensor is to be communicated to the CHB system control module. The communication message or data transfer is to be qualified for validity and correctness. • The updated value of the roll rate sensor is to be received within TBD seconds. This time is to be specified to support the timely update of the CHB system in order to prevent the violation of any safety goals.
7.19	1, 2, 3, 4, 5, 6, 7	B	In case of a fault that violates a safety goal, the roll rate sensor is to communicate the fault to the CHB system control module.
7.20	1, 2, 3, 4, 5, 6, 7	QM	The roll rate sensor is to have diagnostics for safety relevant failures caused by EMC/EMI, ESD, contamination, and other environmental conditions.
7.21	1, 2, 3, 4, 5, 6, 7	B	All single point roll rate sensor hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the CHB system is to transition to the corresponding safe state. • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.

FSR ID	SG	ASIL	Functional Safety Requirement
7.22	1, 2, 3, 4, 5, 6, 7	B	The longitudinal acceleration sensor is to measure the longitudinal acceleration of the vehicle, and the value is to be qualified for validity and correctness.
7.23	1, 2, 3, 4, 5, 6, 7	B	The longitudinal acceleration sensor's conversion method from the longitudinal acceleration to an electrical signal is to be validated.
7.24	1, 2, 3, 4, 5, 6, 7	B	The longitudinal acceleration measurement by the longitudinal acceleration sensor is to be communicated to the CHB system control module. The communication message or data transfer is to be qualified for validity and correctness. • The updated value of the longitudinal acceleration sensor is to be received within TBD seconds. This time is to be specified to support the timely update of the CHB system in order to prevent the violation of any safety goals.
7.25	1, 2, 3, 4, 5, 6, 7	B	In case of a fault that violates a safety goal, the longitudinal acceleration sensor is to communicate the fault to the CHB system controller.
7.26	1, 2, 3, 4, 5, 6, 7	QM	The longitudinal acceleration sensor is to have diagnostics for safety relevant failures caused by EMC/EMI, ESD, contamination, and other environmental conditions.
7.27	1, 2, 3, 4, 5, 6, 7	B	All single point longitudinal acceleration sensor hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the fault tolerant time interval. In case of a failure, the system is to transition to the corresponding safe state. • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.

[1] The FTTI and TBD time intervals for transitioning into a safe state are typically determined by the manufacturers and may be defined based on the criticality of the sensor, the system architecture, and the limitations of the technology. Typically these FTTIs may be on the order of 150-250 ms.

9.2.8 Power Supply Functional Safety Requirements

This study derived seven functional safety requirements related to providing power to the CHB system. Each of the functional safety requirements for the CHB system power supply is listed in Table 39 along with the safety goals supported by the requirement and the associated ASILs.

Table 39. Functional Safety Requirements for the Power Supply

FSR ID	SG	ASIL	Functional Safety Requirement
8.1	3, 4, 5, 6, 7	D, C	The CHB system is to have a redundant low voltage power supply. In case of a fault in the vehicle's low voltage power supply system, the redundant power supply for the CHB system is to activate within TBD ms and sustain the power for a duration greater than the longest FTTI.
8.2	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The low voltage power supply is to provide the CHB system with the required power supply for operation.
8.3	3, 4, 5, 6, 7	D, C	The supply voltage and current are to meet the quality parameters (levels (min, max), ripple, transient, and overshoot) as set by the CHB system components. The ASIL classification of this requirement is to be based on the safety analysis and the safety goal impacted.
8.4	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The CHB system is to be notified of any malfunction or disruption in the low voltage power supply system operation.
8.5	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	All communications and data transfer sent by the low voltage power system to the CHB system are to be qualified for validity and correctness (plausibility and rationality). This includes the low voltage power system diagnostics information.
8.6	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	In case of a malfunction, the low voltage power supply is to maintain the low voltage power supply to the CHB system for a time that is longer than the longest FTTI.
8.7	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	All single point failure modes that cause the loss of low voltage power are to be prevented or mitigated. • The CHB system is to transition to Safe State 5 in case of a loss or malfunction of the vehicle’s low voltage power system and red light driver warning is to be issued.

FSR ID	SG	ASIL	Functional Safety Requirement

[1] The FTTI and TBD time intervals for transitioning into a safe state are typically determined by the manufacturers and may be defined based on the criticality of the sensor, the system architecture, and the limitations of the technology. Typically these FTTIs may be on the order of 150-250 ms.

9.2.9 Communication System Functional Safety Requirements

This study derived six functional safety requirements related to the vehicle's communication system supporting the CHB system. This includes both communication between subsystems in the CHB system as well as communication with interfacing vehicle systems and sensors that provide safety-critical data to the CHB system. Each of the functional safety requirements for the vehicle communication system is listed in Table 40 along with the safety goals supported by the requirement and the associated ASILs.

Table 40. Functional Safety Requirements for the Vehicle Communication System

FSR ID	SG	ASIL	Functional Safety Requirement
9.1	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	Critical communications and data transfer between the CHB system control module and other vehicle systems or components are to be qualified for validity and correctness (plausibility and rationality). This includes the steering wheel angle and torque sensors (ASIL D), accelerator pedal position sensor (ASIL C), vehicle directional sensor (QM), and all other inputs that are used by the CHB system control module.
9.2	1, 2, 3, 4, 5, 6, 7, 8	D, C, B, A, QM	All critical communication signals are to be qualified for validity and correctness (plausibility and rationality). The ASIL classification for the signal is to correspond to the safety goal it is associated with. If a signal is associated with more than one safety goal, then it is to adhere to the higher ASIL classification.
9.3	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The communication bus is to support the communication of the CHB system with the rest of the vehicle systems in order to support the safe operation of the CHB system.
9.4	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The communication bus is to support the qualification of all critical communication bus signals between the CHB system and the interfacing vehicle systems.

FSR ID	SG	ASIL	Functional Safety Requirement
9.5	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The communication bus is to prevent the corruption of the critical communication bus signals during transmission between the CHB system and the interfacing vehicle systems.
9.6	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	In case of malfunction of the communication bus or communication bus module, the communication bus system is to inform the CHB system.

9.2.10 Interfacing Systems Functional Safety Requirements

This study derived seven functional safety requirements related to interfacing vehicle systems capable of requesting braking torque from the CHB system. The functional safety requirements related to interfacing vehicle systems are listed in Table 41, along with the safety goals supported by the requirement and the associated ASILs.

Table 41. Functional Safety Requirement for Interfacing Vehicle Systems

FSR ID	SG	ASIL	Functional Safety Requirement
10.1	1, 2, 3, 4, 5, 6, 7	D, C, B	All communications and data transfer regarding requests or commands for braking sent by interfacing vehicle systems to the CHB system are to be qualified for validity and correctness (plausibility and rationality) by the sending systems.
10.2	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	All requests or commands for braking torque modifications from interfacing vehicle systems are to be sent to the CHB system controller. This includes: • Requests for braking torque from the ACC system, the CIB system, the Pedestrian Emergency Braking system, and other driver assistance systems.
10.3	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	All communications and data transfer regarding requests or commands for braking torque modifications sent by the interfacing vehicle systems to the CHB system are to be qualified for validity and correctness (plausibility and rationality) by the sending system.
10.4	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	All interfacing systems are to inform the CHB system in case of any failure that may cause the system to transition into a degraded mode of operation.

FSR ID	SG	ASIL	Functional Safety Requirement
10.5	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	In case of a fault in the transmitted information to the CHB system from the interfacing system, the correct failure mode effect mitigation strategy is to be applied.
10.6	1, 2, 3, 4, 5, 6, 7, 8	D, C, B	The electronic parking brake status is to be conveyed to the CHB control module. • The status of the rear wheel parking brake is to be validated by the electronic parking brake system.
10.7	1, 2	C	The CHB system control module is to coordinate yaw stabilization with other vehicle systems capable of correcting the vehicle yaw in order to prevent violation of any safety goals.

9.2.11 Mechanical CHB System Components Functional Safety Requirements

This study derived 10 functional safety requirements related to the mechanical braking pathway from the driver to the wheels. Since these are mechanical components, they fall outside the scope of ISO 26262. However, they are critical for the overall safety of the CHB system.

The functional safety requirements related to the mechanical CHB system components are listed in Table 42, along with the safety goals supported by the requirement. Since these components are outside the scope of ISO 26262, no ASIL was assigned to the functional safety requirements.

Table 42. Functional Safety Requirement for Mechanical CHB System Components

FSR ID	SG	ASIL	Functional Safety Requirement
11.1	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The brake booster is to prevent incorrect brake pressure to be applied to any wheel under all vehicle operating conditions.
11.2	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The brake booster transient response is to support the timely application and timely update of the brake pressure to the wheels.

FSR ID	SG	ASIL	Functional Safety Requirement
11.3	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The brake booster is to prevent any failure that leads to a violation of any safety goal.
11.4	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The master cylinder is to prevent any faults that lead to a failure in the hydraulic pressure sensor measurements.
11.5	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The master cylinder is to prevent incorrect brake pressure from being applied to any wheel under all vehicle operating conditions.
11.6	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The master cylinder transient response is to support the timely application and timely update of the hydraulic pressure to the wheels.
11.7	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The master cylinder is to prevent any failure that leads to a violation of any safety goal.
11.8	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The brake pads/drums assembly is to prevent any failure that leads to incorrect brake torque applications to the any wheel.
11.9	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	The brake is to prevent any failure that leads to a violation of any safety goal, including loss of braking or locked wheels.
11.10	1, 2, 3, 4, 5, 6, 7, 8	No ASIL	In case of wear in the brake pads/drum assembly, the driver is to be provided with an alert or feedback.

10 DIAGNOSTICS AND PROGNOSTICS

10.1 Metrics for Diagnostics

The diagnostics presented in this section are limited to the sensing and evaluation elements of the CHB system and critical interfaces, as described in Section 3.1. While failures in other vehicle systems may be amenable to diagnostic evaluation, this report focuses on methodologies for identifying existing and potential problems within the CHB system and critical interfaces.

Many diagnostic functions are characterized by detecting when a key parameter strays out of its normal operating range. In any electronic system, short-term anomalies are possible in both the electronic components and the communications network. The safety analysis for a system should identify FTTIs over which a fault has to be identified and mitigated. For many serious malfunctions, these FTTIs are significantly less than one second. Therefore continually rechecking abnormal readings is an important part of verifying the diagnostic system integrity. The CHB system might also use three-level monitoring, as described in Appendix J.

ISO 26262 provides diagnostic coverage guidelines, including diagnostic coverage levels that correspond to the ASILs of the affected safety goals. Diagnostics coverage levels are associated with the number of failure modes detected by the specific technique. For example, a low diagnostics coverage level for a sensor might only detect out-of-range and stuck-in-range conditions. A medium diagnostics coverage level for a sensor might also detect offsets, in addition to out-of-range and stuck-in-range conditions. A high diagnostics coverage level might detect oscillations in addition to offsets, out-of-range, and stuck-in-range conditions. Diagnostics coverage supports several metrics required by ISO 26262, including the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures.

The diagnostic coverage guidelines in ISO 26262 can provide the basis for diagnostic coverage for the CHB system. ISO 26262 specifies how to implement diagnostic coverage for the safety-related functionality of critical CHB sensors, harnesses, and connectors based on the ASIL of the safety goal that is affected. For example, a diagnostic coverage strategy may include the following elements of the CHB system.

- Main and auxiliary controllers:
    - CPU
    - Processor memory
    - Arithmetic Logic Unit
    - Registers
    - A/D converter
    - Software program execution
    - Connections (I/O) faults (short or open circuits)
    - Power supply

- Critical communication bus messages
- Harnesses and connectors (short or open circuits)

10.2 Common Diagnostic Trouble Codes for the CHB System

10.2.1 Assessment of Selected Generic Diagnostic Trouble Codes

DTCs are part of a safety system that senses, diagnoses, and controls situations, using driver warnings when appropriate. SAE Recommended Practice J2012 defines standardized DTCs, including DTCs pertaining to the CHB system.

SAE J2012 uses a five-digit format for DTCs. Powertrain codes always start with the letter "P," whereas network codes start with "U," chassis codes start with "C," and body system codes start with "B." The second digit is numeric - typically 0, 1, 2, or 3. Predefined SAE (i.e., "controlled" non-OEM-specific) powertrain codes have a 0 or 2 as the second digit. Manufacturer-defined powertrain codes have a 1 or 3 in the second digit. For instance, P0XXX and P2XXX are SAE-controlled powertrain codes while P1XXX and P3XXX are unique to the manufacturer. Predefined SAE network codes, chassis codes, and body system codes have a 0 as the second digit whereas manufacturer-specific network codes, chassis codes, and body system codes have a 1 or 2 as the second digit. Thus, the first two digits can generally be used to determine whether the CHB system DTCs are SAE-controlled codes.

The codes are characterized by the phenomenon they represent. Some DTCs indicate an existing or emerging hazardous state, while others indicate a situation that requires attention to prevent the system from moving toward an unsafe state. System responses to DTCs, such as issuing a driver warning transitioning to a safe state is determined by the manufacturer.

Table C1 in Appendix C0 (Chassis Systems) of SAE J2012 lists DTCs specific to the brake and traction control system. [14] Review of SAE J2012 identified 93 DTCs that cover CHB-related components and interfaces. SAE J2012 also includes 187 DTCs that cover critical CHB system interfaces. Tables 43 and 44 provide a breakdown of these DTCs by the CHB system component or connection, and interfacing system or subsystem. Appendix K summarizes the DTCs relevant to the CHB system.

Table 43. Breakdown of Identified DTCs by CHB System Component or Connection

CHB System Component or Connection	Number of DTCs
Brake Booster	14
Brake Pads/Drum Assembly	2
Brake Pedal Position Sensor	9
Brake Pressure Sensor	3
CHB Control Module	20
CHB Stability Control Disable Switch	1
Hydraulic Modulator	17
WSS	17
Vehicle Dynamics/Inertial Sensors	10

Table 44. Breakdown of Identified CHB-Relevant DTCs by Interfacing System or Subsystem

Interfacing System Component or Connection	Number of DTCs
ACS/ETC System[1]	51
Brake Fluid Level Sensor	1
Differential System	3
Instrument Panel Display	6
Low Voltage Power Supply	1
Other Vehicle Systems (e.g., ACC, Park Assist, etc.)	7
Rain Sensor	1
Vehicle Communication System	97
Vehicle Speed Sensor[2]	11

[1] Includes the accelerator pedal position sensor, if used by the TCS function to determine acceleration.
[2] If vehicle speed is not calculated by the CHB system control module.

10.2.2 Potential Additional Generic Diagnostic Trouble Code Needs

The diagnostic coverage for the CHB system specified in SAE J2012 covers the majority of components and interfaces identified in this study. More refined DTC coverage of failure modes of the CHB control module could supplement the existing DTC coverage in SAE J2012. These possible DTC coverage areas are listed in Table 45. The DTCs in Table 45 are based on similar DTC types listed in SAE J2012 for the powertrain control module.

Table 45. Possible Areas for Additional DTC Coverage in the CHB System

Phenomenon	System or Component
Internal CHB Control Module Memory Check Sum Error	CHB Control Module
CHB Control Module Programming Error	CHB Control Module
Internal CHB Control Module Keep Alive Memory (KAM) Error	CHB Control Module
Internal CHB Control Module RAM Error	CHB Control Module
Internal CHB Control Module ROM Error	CHB Control Module
CHB Control Module Processor	CHB Control Module
CHB Control Module Performance	CHB Control Module
Internal CHB Control Module Monitoring Processor Performance	CHB Control Module
Internal CHB Control Module A/D Processing Performance	CHB Control Module
Internal CHB Control Module Main Processor Performance	CHB Control Module
CHB Control Module Vehicle Options Error	CHB Control Module

11 PERFORMANCE PARAMETERS AND TEST SCENARIOS

11.1 Relationship With Current FMVSS

NHTSA has established two Federal Motor Vehicle Safety Standards that are relevant to the CHB system considered in this study. FMVSS 135 specifies minimum performance parameters for braking systems in light vehicles. FMVSS 126 specifies the basic operational requirements and minimum performance parameters for ESC systems in light vehicles.

The performance tests incorporated into these FMVSSs are discussed briefly below.

- FMVSS 126 describes performance tests for the ESC system using a sine with dwell test. These performance tests assume that the ESC system is operating correctly; FMVSS 126 does not include performance tests with ESC malfunctions. With respect to ESC malfunctions, FMVSS 126 performance tests focus on ensuring proper illumination of the malfunction indicator light. [10]
- FMVSS 135 describes performance tests for the service brake system, with a focus on ensuring minimum stopping distances are achieved under a range of conditions. Unlike FMVSS 126, which assumes ESC is operating correctly, FMVSS 135 includes performance tests for brake systems with certain malfunctions including:
    - Failure of the ABS function, if equipped (Section 7.8)
    - Failure of the variable brake proportioning valve (Section 7.9)
    - Failure of the hydraulic circuit (Section 7.10) and
    - Failure of the power unit or power assist unit (a.k.a., brake booster; Section 7.11) [11]

The example test scenarios described in the following section are intended to evaluate whether the CHB system achieves the functional safety requirements outlined in Sections 6 and 9 of this report. In particular, these test scenarios may be used to ensure the SGs in Section 6 are not violated in the presence of system faults. The example test scenarios presented in this report may be complementary to the performance tests included in FMVSS 126 and 135, but are not intended to replace or supersede the performance tests included in FMVSS 126 and 135. For instance, the performance requirements specified in FMVSS 126 and 135 may be used as performance targets for the test scenarios in the following section.

11.2 Test Scenario Development

This section describes potential test scenarios based on the each of identified vehicle-level hazards and results of the hazard and safety analyses. This section of the report is intended to illustrate how the results of this study may be used to develop a range of possible test scenarios. These test scenarios may be used to verify that the functional safety requirements are achieved. However, these test scenarios should not be interpreted as comprehensive set of test scenarios

and additional test scenarios may be necessary to adequately verify the functional safety requirements are achieved.

Each test scenario includes the following:

- **Test Goals**: Each of the safety goals identified in this study serves as the testing goal for a test scenario. The test objective is to ensure that the safety goal is not violated.
- **Driving Scenarios**: The driving scenario is developed using a combination of the vehicle's operating scenario and key inputs to the system. Together, this represents the situation under which the system should avoid entering a hazardous state when a fault is injected. The two components of the driving scenario are described below.
    - The operating scenarios are generated as part of the ASIL assessment and describe the operating environment of the vehicle. The operating scenarios considered in these test scenarios are based on the variables listed in Table 16. In particular, the ASIL operating scenarios that lead to the highest ASIL value for a hazard may represent worst-case driving situations under which the system should avoid entering a hazardous state. Note that test procedures may deviate from the "worst case" driving situation in the ASIL assessment for the purposes of testing safety. For example, test procedures may be developed that implement lower vehicle speeds if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.
    - The context variables used for deriving the UCAs represent key inputs to the system. Certain system behaviors are expected based on the combinations of these context variables to avoid entering a hazardous state.
- **Fault Injection**: The CFs identified in STPA, and failure modes and faults identified in the functional FMEA may be used as the basis for determining faults to inject at the component and connection levels. Examples of potential faults that could be introduced to the system include inducing hardware failures in system components, transmitting erroneous measurements from sensors, or issuing incorrect controller commands (e.g., to simulate a flaw in the software algorithm).
- **Expected Safe Behavior**: The test scenarios can be evaluated by monitoring for expected safe behaviors. The following are examples of possible safe behaviors:
    - The system may transition into one of the identified safe states within the FTTI. As described in Section 8.2, safe states are operating modes of the system that do not present an unreasonable risk.
    - The system's controller may still be capable of issuing the correct command when a fault is injected. For example, the CHB control module may be capable of using other sensor data to determine the correct amount of differential braking to provide when there's a disruption in the voltage supply to the yaw rate sensor.

Although the role of the driver was considered in the hazard and safety analyses, the test scenarios presented in this section focus on the behavior of the electronic control system. Evaluation of driver behavior when certain faults are injected into the vehicle would require a human factors study.

11.2.1 Potential Test Scenarios for SG 1

Safety Goal 1 states that the CHB system prevent unintended lateral motion/yaw under all vehicle operating conditions. Table 46 describes two possible driving scenarios to test this safety goal. Both driving scenarios are based on the same operating scenario, identified as the worst-case scenario from the ASIL assessment. The driving scenarios differ based on the system input:

Table 46. Example Driving Scenarios for SG 1

Test Goal		Prevent unintended lateral motion or yaw under all vehicle operating conditions.
ASIL		B
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [44]
	System Input #1	• Driver brakes hard while steering. • There is no yaw error between the driver's steering input and the vehicle response. • Other vehicle systems are not requesting differential braking.
	System Input #2	• Driver executes an evasive maneuver (e.g., rapid clockwise and counter-clockwise steering) that induces a yaw error between the driver's steering input and the vehicle response. • Other vehicle systems are not requesting differential braking.

- *Driving Scenario 1:* The driver applies a hard braking force while steering around a moderate road bend. However, the vehicle remains within the limits of roadway traction. This scenario is intended to determine if an induced fault may cause the CHB system to apply differential braking that could lead to a violation of the safety goal (e.g., inadvertent ESC activation).

[44] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

- *Driving Scenario 2:* The driver executes an evasive maneuver that results in the vehicle reaching the limits of roadway traction. This scenario is intended to determine if an induced fault may prevent the CHB system from intervening, resulting in a violation of the safety goal (e.g., ESC does not activate).

For each of the two test scenarios listed in Table 46, potential faults could be simulated in the CHB system to determine if these faults result in violation of the safety goal. The induced faults presented in Tables 47 and 48 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Tables 47 and 48 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in the test scenarios.

Table 47. Examples of Simulated Faults to Test SG 1 Under Driving Scenario 1

Test Goal		Prevent unintended lateral motion or yaw under all vehicle operating conditions.
ASIL		B
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [45]
Injected Fault (Examples)	System Input	• Driver brakes hard while steering. • There is no yaw error between the driver's steering input and the vehicle response. • Other vehicle systems are not requesting differential braking.
	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Issue a differential braking command from the CHB control module to the brake modulator (e.g., a simulated software fault). *(CF #172, 310, 311)*
	Yaw Rate Sensor	• Simulate internal shorts in the yaw rate sensor (e.g., to ground, battery, etc.). *(CF #362)* • Report an inverted yaw rate signal (e.g., a clockwise yaw rate while the driver is steering counterclockwise) to the CHB control module. *(CF #369, 567, 568)*
	Incoming Connection from Steering System	• Report an inverted steering input (e.g., a clockwise signal while the driver is steering counterclockwise) to the CHB control module. *(CF #338, 345, 447)* • Subject the connection between the steering wheel sensors and CHB control module to a range of EMI disturbances. *(CF #478, 486)*
	Incoming Connection From Other Vehicle Systems	• Issue an errant signal on the communication bus that mimics a differential braking request. *(CF #164, 528)*
Expected Safety Strategies		• Detects fault and does not apply differential braking. • Transitions to Safe State 2 or Safe State 6, and alerts the driver.

[45] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 48. Examples of Simulated Faults to Test SG 1 Under Driving Scenario 2

Test Goal		Prevent unintended lateral motion/yaw under all vehicle operating conditions.
ASIL		B
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [46]
	System Input	• Driver executes an evasive maneuver (e.g., rapid clockwise and counter-clockwise steering) that induces a yaw error between the driver's steering input and the vehicle response. • Other vehicle systems are not requesting differential braking.
Injected Fault (Examples)	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Simulate a power supply disruption to the CHB control module. *(CF #12)* • Terminate the signal from the CHB control module to the brake modulator (e.g., simulate a software fault that prematurely terminates ESC). *(CF #171, 307)*
	Yaw Rate Sensor	• Simulate internal shorts in the yaw rate sensor (e.g., to ground, battery, etc.). *(CF #362)* • Simulate a loss of power to the yaw rate sensor. *(CF #382)*
	Brake Pressure Sensor	• Subject the connection between the brake pressure sensor and CHB control module to a range of EMI disturbances. *(CF #478, 486)* • Simulate shorts in the connection between the brake pressure sensor and CHB control module. *(CF #385)*
	Incoming Connection From Disable Stability Control Switch	• Simulate shorts (e.g., to ground, battery, etc.) in the connection between the disable stability control switch and CHB control module. *(CF #385)*
Expected Safety Strategies		• CHB system detects fault and intervenes appropriately to correct yaw error. • Transitions to Safe State 2 and alerts the driver.

11.2.2 Potential Test Scenarios for SG 2

Safety Goal 2 states that the CHB system provide sufficient vehicle lateral motion/yaw under all vehicle operating conditions. Table 49 describes two possible driving scenarios to test this safety goal. The driving scenarios differ based on the system input.

Table 49. Example Driving Scenarios for SG 2

Test Goal		Provide sufficient vehicle lateral motion/yaw under all vehicle operating conditions.
ASIL		B
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [47]
	System Input #1	• Driver brakes hard while steering, inducing understeer.
	System Input #2	• The driver is not steering. • Other vehicle systems request yaw/differential braking.

- *Driving Scenario 1:* The driver applies a hard braking force while steering around a moderate road bend in a manner that results in an understeer condition. This scenario is intended to determine if an induced fault may prevent the CHB system from intervening, resulting in a violation of the safety goal (e.g., ESC does not activate).
- *Driving Scenario 2:* The driver is not issuing a steering command, but another vehicle system – such as a lane keep assist system – is requesting differential braking to control the vehicle's lateral position. This test scenario is intended to determine if an induced fault may affect the ability of the CHB system to respond to braking requests from other vehicle systems, resulting in a violation of the safety goal.

For each of the test scenarios listed in Table 49, potential faults could be simulated in the CHB system to determine if these faults result in violation of the safety goal. The induced faults presented in Tables 50 and 51 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Tables 50 and 51 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in the test scenarios.

[46] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

[47] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 50. Examples of Simulated Faults to Test SG 2 Under Driving Scenario 1

Test Goal		Provide sufficient vehicle lateral motion/yaw under all vehicle operating conditions.
ASIL		B
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [48]
Injected Fault (Examples)	System Input	• Driver brakes hard while steering, inducing understeer.
	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Simulate a power supply disruption to the CHB control module. *(CF #12)* • Provide inputs to the CHB control module that trigger a conflicting brake system function (e.g., ABS). *(CF #308)*
	Yaw Rate Sensor	• Simulate internal shorts in the yaw rate sensor (e.g., to ground, battery, etc.). *(CF #362)* • Simulate a loss of power to the yaw rate sensor. *(CF #382)*
	Brake Pressure Sensor	• Subject the connection between the brake pressure sensor and CHB control module to a range of EMI disturbances. *(CF #478, 486)* • Simulate shorts in the connection between the brake pressure sensor and CHB control module. *(CF #385)*
	Incoming Connection from Steering System	• Introduce a delay in the signal from the steering wheel sensors to the CHB control module. *(CF #341, 473)* • Subject the connection between the steering wheel sensors and CHB control module to a range of EMI disturbances. *(CF #478, 486)*
Expected Safety Strategies		• CHB system detects fault and intervenes appropriately to correct understeer. • Transitions to Safe State 2 and alerts the driver.

[48] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 51. Examples of Simulated Faults to Test SG 2 Under Driving Scenario 2

Test Goal		Provide sufficient vehicle lateral motion/yaw under all vehicle operating conditions.
ASIL		B
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [49]
	System Input	• The driver is not steering. • Other vehicle systems request yaw/differential braking.
Injected Fault (Examples)	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Simulate a power supply disruption to the CHB control module. *(CF #12)* • Provide a set of inputs to the CHB control module that trigger a conflicting brake system function (e.g., ABS). *(CF #309)*
	Incoming Connection From Other Vehicle Systems	• Subject the connection between the requesting system and CHB control module to a range of EMI disturbances. *(CF #164)* • Issue conflicting differential braking requests from multiple vehicle systems. *(CF #168)*
Expected Safety Strategies		• CHB system detects fault and intervenes appropriately to implement the differential braking request. • Transitions to Safe State 6 and alerts the driver.

11.2.3 Potential Test Scenarios for SG 3

Safety Goal 3 states that the CHB system prevent the unintended loss of lateral motion control under all vehicle operating conditions. As described in Section 6 of this report, this safety goal considers the case where the front wheel lock-up, causing a loss of steering control. This study derives one possible driving scenario to test this safety goal, shown in Table 52.

[49] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 52. Example Driving Scenario for SG 3

Test Goal		Prevent loss of lateral motion control.
ASIL		D
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [49]
	System Input	• Driver brakes hard (with enough force to activate ABS) while steering.

- *Driving Scenario 1:* The driver brakes hard while steering around a moderate bend at high vehicle speeds in heavy traffic, with good road conditions. This test scenario is intended to determine if an induced fault may cause the front wheels to lock-up, ultimately resulting in a loss of steerability.

The induced faults presented in Table 53 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Table 53 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in the test scenario.

Table 53. Examples of Simulated Faults to Test SG 3 Under Driving Scenario 1

Test Goal		Prevent loss of lateral motion control.
ASIL		D
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [50]
Injected Fault (Examples)	System Input	• Driver brakes hard (with enough force to activate ABS) while steering.
	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Simulate a power supply disruption to the CHB control module. *(CF #12)* • Issue a command to the brake modulator to close the release valve while ABS is active (e.g., simulate a software fault that prematurely terminates ABS). *(CF #27, 171)*
	WSS	• Simulate internal shorts in the WSS (e.g., to ground, battery, etc.). *(CF #34)* • Reverse the connections between the WSSs and CHB control module (e.g., switch the left and right WSSs). *(CF #76)* • Subject the connection between the WSS and CHB control module to a range of EMI disturbances. *(CF #78, 86)* • Misalign the WSS relative to the wheel. *(CF #38, 39, 42, 47, 49)*
	Brake Modulator	• Simulate a power supply loss or disruption to the brake modulator. *(CF #105, 106)* • Prevent the brake modulator from changing the valve positions. *(CF #98, 99, 224)* • Reverse the connections between the brake modulator and brake circuits (e.g., switch the front and rear brake hoses). *(CF #152, 154)*
Expected Safety Strategies		• CHB system detects the fault and ensures that the front wheels do not lock-up. • Transitions to Safe State 3 and alerts the driver.

[50] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

11.2.4 Potential Test Scenarios for SG 4

Safety Goal 4 states that the CHB system prevent unintended vehicle deceleration[51] under all vehicle operating conditions. This study derived two possible driving scenarios to test this safety goal, which are shown in Table 54.

Table 54. Example Driving Scenarios for SG 4

Test Goal		Prevent unintended vehicle deceleration under all vehicle operating conditions.
ASIL		D
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [52]
	System Input #1	• Driver brakes lightly.
	System Input #2	• The driver is not applying the brakes • Another vehicle system requests braking.

- *Driving Scenario 1:* The driver applies the brakes lightly, while the vehicle is travelling at high speeds in heavy traffic and with good road conditions. This test scenario is intended to determine if an induced fault could cause the brake system to provide more braking than commanded by the driver (e.g., inadvertent activation of panic brake assist).
- *Driving Scenario 2:* The driver is not applying the brakes, but another vehicle system – such as adaptive cruise control – is requesting braking. This test scenario is intended to determine if an induced fault could cause the brake system to provide more braking than requested.

The induced faults presented in Tables 55 and 56 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Tables 55 and 56 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in the test scenarios.

[51] An example threshold for unintended vehicle deceleration may be any deceleration that exceeds 0.2g.
[52] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 55. Examples of Simulated Faults to Test SG 4 Under Driving Scenario 1

Test Goal		Prevent unintended vehicle deceleration under all vehicle operating conditions.
ASIL		D
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [53]
	System Input	• Driver brakes lightly.
Injected Fault (Examples)	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Issue a braking command from the CHB control module to the brake modulator (e.g., a simulated software fault). *(CF #166, 167, 172, 584)*
	Brake Pressure Sensor	• Subject the connection between the brake pressure sensor and CHB control module to a range of EMI disturbances. *(CF #478, 486)* • Simulate shorts in the connection between the brake pressure sensor and CHB control module. *(CF #385)*
Expected Safety Strategies		• CHB system detects the fault and provides the appropriate braking response. • Transitions to Safe State 4 or Safe State 6, and alerts the driver.

[53] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 56. Examples of Simulated Faults to Test SG 4 Under Driving Scenario 2

Test Goal		Prevent unintended vehicle deceleration under all vehicle operating conditions.
ASIL		D
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [54]
	System Input	• The driver is not applying the brakes • Another vehicle system requests braking.
Injected Fault (Examples)	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Issue a command to the brake modulator to accumulate more brake pressure than requested (e.g., a simulated software fault). *(CF #166, 167, 584)*
	Brake Modulator	• Simulate a power supply loss or disruption to the brake modulator. *(CF #105, 106)* • Prevent the brake modulator from changing the valve positions. *(CF #98, 99, 224)*
	Incoming Connection From Other Vehicle Systems	• Subject the connection between the requesting system and CHB control module to a range of EMI disturbances. *(CF #164)* • Issue an errant signal on the communication bus that mimics a braking request. *(CF #528)*
Expected Safety Strategies		• CHB system detects the fault and provides the appropriate braking response. • Transitions to Safe State 4 or Safe State 6, and alerts the driver.

11.2.5 Potential Test Scenarios for SG 5

Safety Goal 5 states that the CHB system prevent insufficient and loss of braking under all vehicle operating conditions. This study derived one possible driving scenario to test this safety goal, which is shown in Table 57.

[54] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 57. Example Driving Scenario for SG 5

Test Goal		Prevent insufficient and loss of braking under all vehicle operating conditions.
ASIL		D
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends.[54]
	System Input	• Driver brakes hard.

- *Driving Scenario 1:* The driver applies the brakes hard while at high vehicle speeds in heavy traffic, with good road conditions. This test scenario is intended to determine if an induced fault may prevent the CHB system from generating sufficient brake force.

The induced faults presented in Table 58 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Table 58 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in test scenarios.

Table 58. Examples of Simulated Faults to Test SG 5 Under Driving Scenario 1

Test Goal		Prevent insufficient and loss of braking under all vehicle operating conditions.
ASIL		D
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [55]
Injected Fault (Examples)	System Input	• Driver brakes hard.
	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Issue a command to the brake modulator to open the release valves (e.g., a simulated software fault). *(CF #165, 167, 172, 276, 577, 584)*
	WSS	• Simulate internal shorts in the WSS (e.g., to ground, battery, etc.). *(CF #34)* • Reverse the connections between the WSSs and CHB control module (e.g., switch the left and right WSSs). *(CF #76)* • Subject the connection between the WSS and CHB control module to a range of EMI disturbances. *(CF #78, 86)*
	Brake Modulator	• Simulate a power supply loss or disruption to the brake modulator. *(CF #105, 106)* • Prevent the brake modulator from changing the valve positions. *(CF #98, 99, 224)* • Reverse the connections between the brake modulator and brake circuits (e.g., switch the front and rear brake hoses). *(CF #152, 154)*
	Brake Pads/Drum Assembly	• Simulate degraded brake pad effectiveness (e.g., brake fade, wear, etc.). *(CF #113, 115, 117)*
Expected Safety Strategies		• CHB system detects the fault and provides an appropriate amount of brake force. • Transition to Safe State 3 or Safe State 5, and alerts the driver.

[55] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

11.2.6 Potential Test Scenarios for SG 6

Safety Goal 6 states that the CHB system prevent system failures that lead to unintended vehicle propulsion under all vehicle operating conditions. This study derived one possible driving scenario to test this safety goal, which is shown in Table 59.

Table 59. Example Driving Scenario for SG 6

Test Goal		Prevent system failures that lead to unintended vehicle propulsion under all vehicle operating conditions.
ASIL		C[1]
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [56]
	System Input	• Driver releases the accelerator pedal suddenly.

[1] Analysts did not reach consensus on the ASIL assessment for this hazard.

- *Driving Scenario 1:* While travelling at high vehicle speeds, the driver releases the accelerator pedal suddenly activating the engine drag torque control function. This test scenario is intended to determine if an induced fault may cause the CHB system to request an increase in engine torque that results in a violation of the safety goal.

The induced faults presented in Table 60 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Table 60 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in test scenarios.

[56] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 60. Examples of Simulated Faults to Test SG 6 Under Driving Scenario 1

Test Goal		Prevent system failures that lead to unintended vehicle propulsion under all vehicle operating conditions.
ASIL		C[1]
Driving Scenarios	Operating Scenario	Driving at high speeds (130 kph ≥ V > 100 kph), heavy traffic, good road conditions, moderate road bends. [57]
	System Input	• Driver releases the accelerator pedal suddenly.
Injected Fault (Examples)	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Issue a command to increase the engine torque (e.g., simulate a software fault). *(CF #595, 586)*
	Brake Pedal Position Sensor	• Simulate a power supply loss or disruption to the brake pedal position sensor. *(CF #187, 188)* • Simulate shorts in the connection to the CHB control module (e.g., ground, battery, etc.). *(CF #198)*
	WSS	• Simulate internal shorts in the WSS (e.g., to ground, battery, etc.). *(CF #34)* • Subject the connection between the WSS and CHB control module to a range of EMI disturbances. *(CF #78, 86)* • Misalign the WSS relative to the wheel. *(CF #38, 39, 42, 47, 49)*
Expected Safety Strategies		• CHB system detects the fault and provides appropriate engine torque control. • Transition to Safe State 2 or Safe State 5, and alerts the driver.

[1] Analysts did not reach consensus on the ASIL assessment for this hazard.

11.2.7 Potential Test Scenarios for SG 7

Safety Goal 7 requires that the CHB system prevent system failures that lead to insufficient vehicle propulsion and propulsion power reduction/loss under all vehicle operating conditions.

[57] High speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

This study derived one possible driving scenario to test this safety goal, which is shown in Table 61.

Table 61. Example Driving Scenario for SG 7

Test Goal		Prevent system failures that lead to insufficient vehicle propulsion or propulsion power reduction/loss under all vehicle operating conditions.
ASIL		C
Driving Scenarios	Operating Scenario	Driving at very high speeds (V > 130 kph), heavy traffic, good road conditions, moderate road bends. [58]
	System Input	• Driver maintains the accelerator pedal position.

- *Driving Scenario 1:* The driver maintains the accelerator pedal position (i.e., neither accelerating nor decelerating) while driving at very high speeds with heavy traffic and good road conditions. This test scenario is intended to determine if an induced fault may cause the CHB system to request a decrease in engine torque that results in a violation of the safety goal.

The induced faults presented in Table 62 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Table 62 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in test scenarios.

[58] Very high speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 62. Examples of Simulated Faults to Test SG 7 Under Driving Scenario 1

Test Goal		Prevent system failures that lead to insufficient vehicle propulsion or propulsion power reduction/loss under all vehicle operating conditions.
ASIL		C
Driving Scenarios	Operating Scenario	Driving at very high speeds (V > 130 kph), heavy traffic, good road conditions, moderate road bends. [59]
Injected Fault (Examples)	System Input	• Driver maintains the accelerator pedal position.
	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Issue a command to decrease the engine torque (e.g., simulate a software fault). *(CF #27, 595, 586)*
	WSS	• Simulate internal shorts in the WSS (e.g., to ground, battery, etc.). *(CF #34)* • Subject the connection between the WSS and CHB control module to a range of EMI disturbances. *(CF #78, 86)* • Misalign the WSS relative to the wheel. *(CF #38, 39, 42, 47, 49)*
Expected Safety Strategies		• CHB system detects the fault and provides appropriate engine torque control. • Transition to Safe State 1 or Safe State 5, and alerts the driver.

11.2.8 Potential Test Scenarios for SG 8

Safety Goal 8 states that the CHB system prevent the vehicle from rolling backward when not intended under all vehicle operating conditions. This study derived one possible driving scenario to test this safety goal, which is shown in Table 63.

[59] Very high speed is the "worst case" or most critical condition. Test procedures may be developed that implement lower vehicle speeds for the purposes of testing safety if it can be shown that failure modes are independent of speed or if the protocol implements incremental speed increases.

Table 63. Example Driving Scenario for SG 8

Test Goal		Prevent the vehicle from rolling backward when not intended under all vehicle operating conditions.
ASIL		QM
Driving Scenarios	Operating Scenario	Vehicle in traffic, on an incline, facing upwards, with pedestrians present.
	System Input	• Driver activates the hill holder feature. • Driver releases the brake pedal.

- *Driving Scenario 1:* The driver activates the hill holder feature while the vehicle is stopped on an incline, facing upwards. This test scenario is intended to determine if an induced fault may prevent the CHB system from maintaining the vehicle's position, resulting in a violation of the safety goal.

The induced faults presented in Table 64 are examples of potential faults that can be derived from the STPA and functional FMEA results. The lists of potential faults in Table 64 are not intended to be exhaustive. The full STPA and functional FMEA results in Appendix H and Appendix I can be used to identify additional faults to include in test scenarios.

Table 64. Examples of Simulated Faults to Test SG 8 Under Driving Scenario 1

Test Goal		Prevent the vehicle from rolling backward when not intended under all vehicle operating conditions.
ASIL		QM
Driving Scenarios	Operating Scenario	Vehicle in traffic, on an incline, facing upwards, with pedestrians present.
	System Input	• Driver activates the hill holder feature. • Driver releases the brake pedal.
Injected Fault (Examples)	CHB Control Module	• Subject the CHB control module to a range of EMI and ESD disturbances. *(CF #2, 13)* • Issue a command to reduce the brake pressure. *(CF #169, 232)*
	Brake Pedal Position Sensor	• Simulate a power supply loss or disruption to the brake pedal position sensor. *(CF #187, 188)* • Simulate shorts in the connection to the CHB control module (e.g., ground, battery, etc.). *(CF #198)*
	Incoming Connection From Longitudinal Acceleration Sensor	• Simulate shorts in the connection to the CHB control module (e.g., ground, battery, etc.). *(CF #164)*
Expected Safety Strategies		• CHB system detects the fault and provides adequate brake force to maintain the vehicle's position. • Transition to Safe State 5 or Safe State 6, and alerts the driver.

12 CONCLUSIONS

This study followed the Concept Phase process (Part 3) in ISO 26262 standard to derive a list of potential safety requirements for the CHB system. Specifically, this research:

1. Identified eight vehicle-level safety goals and assessed their ASIL:

ID	Safety Goals	ASIL
SG 1	Prevent unintended vehicle lateral motion and/or unintended yaw under all vehicle operating conditions.	B[1,2]
SG 2	Provide sufficient lateral motion under all vehicle operating conditions.	B[1,2]
SG 3	Prevent CHB system failures that lead to loss of lateral motion control under all vehicle operating conditions.	D
SG 4	Prevent unintended vehicle deceleration[3] under all vehicle operating conditions.	D
SG 5	Prevent insufficient braking and loss of braking under all vehicle operating conditions.	D
SG 6	Prevent CHB system failures that lead to unintended acceleration under all vehicle operating conditions.	C[2,4]
SG 7	Prevent CHB system failures that lead to insufficient propulsion or propulsion power reduction/loss under all vehicle operating conditions.	C[2]
SG 8	Prevent CHB system failures that lead to unintended vehicle motion (e.g., rolling backward) under all vehicle operating conditions.	QM[5]

[1] This ASIL is based on the assumption that the wheels do not lock for this hazard. Situations where wheel lock-up affects the vehicle's lateral motion are considered in SG 3.
[2] This ASIL is based on failures in the CHB system that may lead to this potential hazard. Hazards in other vehicle systems that may lead to this hazard may have different ASILs.
[3] Some manufacturers may specify threshold values for "unintended vehicle deceleration" (e.g., 0.2g).
[4] Analysts did not reach consensus on the ASIL assessment for this hazard.
[5] This ASIL is specific to the Hill Holder feature. Other situations related to insufficient braking while on an incline are covered in hazards H5 and H6.

2. Developed the functional safety concept and identified 198 functional safety requirements by following the Concept Phase in the ISO 26262 standard, combining the results of the two safety analyses (functional FMEA and STPA), and leveraging industry practice experiences. The breakdown of the number of requirements is as follows.
   - General CHB System – 15 requirements
   - CHB Control Module – 91 requirements
   - Brake Pedal Assembly – 9 requirements
   - Brake Modulator – 10 requirements
   - Brake Pressure Sensor – 8 requirements
   - WSS – 8 requirements
   - Vehicle Dynamics Sensors – 27 requirements
   - Power Supply – 7 requirements

- Communication System – 6 requirements
- Interfacing System – 7 requirements
- Mechanical CHB System Components – 10 requirements

3. Identified 93 generic DTCs included in SAE J2012 that provide coverage of the CHB system and 187 DTCs that provide coverage for safety-critical interfacing components and communication systems. In addition, this study identified 11 potential DTCs that could provide additional coverage of the CHB system.

4. Developed 11 example test scenarios which could be used to validate the safety goals and functional safety requirements. The results from this study could also be used to develop a more comprehensive set of test scenarios.

REFERENCES

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

[2] Walker Jr., J. (2005). *Introduction to Brake Control Systems: An SAE Professional Development e-Seminar.* Warrendale, PA: SAE International.

[3] International Organization for Standardization. (2011). Road vehicles - functional safety(Final Draft). (ISO 26262). Geneva: Author.

[4] International Electrotechnical Commission. (2001). Hazard and operability studies (HAZOP Studies) - Application guide, Edition 1.0. (IEC 61882-2001). Geneva: Author.

[5] Leveson, N. (2012). *Engineering a safer world*, Cambridge, MA: MIT Press.

[6] Society of Automotive Engineers. (1994). Potential failure mode and effects analysis in design and potential failure mode and effects analysis in manufacturing and assembly processes. (SAE J1739). Warrendale, PA: Author. [Editor's note: In 2006 the Society of Automotive Engineers changed its name to SAE International.]

[7] Thomas, J. (2013). Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis (Ph.D. dissertation). Cambridge, MA: Massachusetts Institute of Technology.

[8] Coudert, O. (1994). Two-level logic minimization: An overview, *Integration, the VLSI Journal, 17*(2), pp. 97-140.

[9] K. Reif, Ed.(2014). *Brakes, brake control and driver assistance systems: Function, regulation and components* (Bosch Professional Automotive Information), Heidelberg, Germany: Springer Vieweg.

[10] 49 CFR Parts 571 and 585. FMVSS 126: Electronic Stability Control Systems; Controls and Displays..

[11] 49 CFR Part 571. FMVSS 135: Passenger Car Brake Systems,

[12] SAE International. (2015) *Considerations for ISO 26262 ASIL Hazard Classification* (SAE J2980) Warrendale, PA: Author.

[13] International Electrotechnical Commission. Functional Safety - IEC 61508 Explained (IEC 61508) Geneva: Author.Available at www.iec.ch/functionalsafety/explained/

[14] SAE International. (2007). *Diagnostic Trouble Code Definitions* (SAE J2012) Warrendale, PA: Author.

[15] Transport Canada. (2007, January). Electronic Stability Control - Frequently Asked Questions Web page). Retrieved from www.tc.gc.ca/eng/motorvehiclesafety/tp-tp14651-vs200701-faq-742.htm

[16] Kade, A., Bartz, D., Hudas, G., & D. G. Mikulski, D. G. (2014, October 28). *Tank Automotive Research, Development and Engineering Center Subject Matter Expert Interview on Automated Lane Centering.* [Interview].

[17] Miller, J., Seewald, A., Heitzer, H.-D., Wegner, M., Kristofik, J., & Standtke, P. (2014, October 29). Interviewees, *TRW Automotive Subject Matter Expert Interview on Automated Lane Centering.* [Interview].

[18] Stanyer, T., & Chutorash, R. (2014, October 27). Interviewees, *ESG Automotive Subject Matter Expert Interview on Automated Lane Centering.* [Interview].

DOT HS 812 574
August 2018

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

13497a-080318-v2