U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

DOT HS 812 640

December 2018

Functional Safety Assessment Of a Generic Accelerator Control System With Electronic Throttle Control in Fuel Cell Hybrid Electric Vehicles

DISCLAIMER

This publication is distributed by 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 United States Government assumes no liability for its contents or use thereof. If trade names, manufacturers' names, or specific products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Suggested APA Format Citation:

Becker, C., Nasser, A., & Attioui, F. (2018, December). *Functional safety assessment of a generic accelerator control system with electronic throttle control in fuel cell hybrid electric vehicles* (Report No. DOT HS 812 640). 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
	December 2018	

4. TITLE AND SUBTITLE
Functional Safety Assessment of a Generic Accelerator Control System With Electronic Throttle Control in Fuel Cell Hybrid Electric Vehicles

5. FUNDING NUMBERS
Intra-Agency Agreement
DTNH22-15-V-00010
51HS7BA200

6. AUTHORS
Christopher Becker, Ahmad Nasser, and Fouad Attioui

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
John A. Volpe National Transportation Systems Center
Cambridge, MA 02142

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-NHTSA-16-09

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 812 640

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Document is available to the public through the National Technical Information Service, www.ntis.gov.

12b. DISTRIBUTION CODE

13. ABSTRACT
This report describes research assessing the functional safety of accelerator control systems with electronic faults, such as errant electronic throttle control signals, following an industry process standard. This study focuses specifically on errant signals in motor vehicles with fuel cell hybrid electric propulsion. This study follows the concept phase process in the ISO 26262 standard and applies a hazard and operability study, functional failure mode and effects analysis, and systems theoretic process analysis methods. In total, this study identifies 7 vehicle-level safety goals and 202 ACS/ETC system safety requirements (an output of the ISO 26262 and STPA processes). This study uses the results of the analysis to identify potential opportunities to improve the risk assessment approach in ISO 26262.

14. SUBJECT TERMS
accelerator control system, electronic throttle control, fuel cell, hazard and operability study, failure mode and effects analysis, systems theoretic process analysis, ISO 26262, hazard analysis, risk assessment, safety requirements.

15. NUMBER OF PAGES
115

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 motor vehicle 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 program 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 program 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 report describes the research effort to assess the functional safety of accelerator control systems with electronic faults, such as errant electronic throttle control signals, following an industry process standard. This study focuses specifically on errant signals in motor vehicles with fuel cell hybrid electric propulsion. This study follows the concept phase process in the ISO 26262 standard [2]and applies a hazard and operability study, functional failure mode and effects analysis, and systems theoretic process analysis methods. In total, this study identifies 7 vehicle-level safety goals and 202 ACS/ETC system safety requirements (an output of the ISO 26262 and STPA processes). This study uses the results of the analysis to identify potential opportunities to improve the risk assessment approach in the ISO 26262 standard.

This publication is part of a series of reports that describe NHTSA's initial work in the automotive electronics reliability program. This research specifically supports the first, second, fourth, and fifth goals of NHTSA's electronics reliability research program by gaining understanding on both the technical safety requirements for ACS/ETC systems and how the industry standard may enhance safety.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

A/D	analog-to-digital
ACC	adaptive cruise control
ACS	accelerator control system
AEB	automatic emergency braking
AIS	Abbreviated Injury Scale
AP	accelerator pedal
APP	accelerator pedal position
APPS	accelerator pedal position sensor
ASIL	automotive safety integrity level
BP	brake pedal
BPP	brake pedal position
BPP	brake pedal position sensor
BTO	brake throttle override
C	controllability
CAN	controller area network
CC	cruise control
CF	causal factor
CPU	central processing unit
DTC	Diagnostic Trouble Code
E	exposure
ECU	electronic control unit
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EPS	electric powertrain subsystem
ESD	electrostatic discharge
ETC	electronic throttle control
EV	electric vehicle
FMEA	failure mode and effects analysis
FMVSS	Federal Motor Vehicle Safety Standard
FTTI	fault tolerant time interval
HAZOP	Hazard and Operability Study
HEV	hybrid electric vehicle
HV	high voltage
HVIL	high voltage interlock loop
I/O	input/output
IC	integrated circuit
ICE	internal combustion engine
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization

kph	kilometers per hour
MISRA	Motor Industry Software Reliability Association
mph	miles per hour
NPRM	Notice of Proposed Rulemaking
PCM	powertrain control module
QM	quality management
RESS	rechargeable energy storage system
SAE	Society of Automotive Engineers
S	severity
STPA	systems theoretic process analysis
TBD	to-be-determined
TCS	traction control system
TICM	traction inverter control module
UCA	unsafe control action

EXECUTIVE SUMMARY

This report documents research by the Volpe National Transportation Systems Center (Volpe), in conjunction with the National Highway Traffic Safety Administration, to identify example safety requirements[1] related to the failures and countermeasures of the accelerator control system with electronic faults, such as errant electronic throttle control signals. ACS/ETC systems are the subset of ACS architectures where the throttle is controlled electronically, rather than through a mechanical connection to the driver-operated control.

Specifically, this report focuses on the identification of example safety requirements for the ACS/ETC systems in fuel cell hybrid electric vehicles.[2] In ACS the throttle for FCEV's is defined as the electric power delivery to the traction motor.

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 International Organization for Standardization 26262 [2] 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 recommends with respect to the identified automotive safety integrity level of the item under consideration.[3] 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. Based on their ASIL decomposition, manufacturers may employ a variety of techniques, such as driver warnings, fault detection mechanisms, plausibility checks, redundancies, etc., to achieve the necessary ASILs that effectively mitigate the underlying safety risks.

This research follows the Concept Phase process (Part 3) in ISO 26262 to derive a list of potential safety requirements. Specifically, this research:

1. Defines the scope and functions of a generic FCEV ACS/ETC, and represents the system in block diagrams.
2. Performs a vehicle-level hazard analysis using both the Hazard and Operability (HAZOP) study and the Systems Theoretic Process Analysis (STPA) method. By integrating the

[1] All requirements presented in this report are not actual compliance requirements currently in effect in an existing FMVSS. Instead, they are intended to illustrate a comprehensive set of requirements that could be derived from the safety analysis results. These safety requirements are not intended to represent NHTSA's official position or regulatory requirements for production ACS/ETC systems.

[2] Vehicle-level hazards and requirements identified in this study are based on the analysis of a generic FCEV ACS/ETC. More complex systems (e.g., with integrated Advanced Driver Assist Systems) may result in additional hazards and functional safety requirements.

hazards identified in both the HAZOP study and STPA, the process establishes seven vehicle-level hazards (Table ES-1).

   a. The HAZOP study identifies 146 malfunctions from analysis of the 21 ACS/ETC functions (see Section 4.2.3, Table 3 for details).
   b. The STPA identifies 95 unsafe control actions (UCAs) from analysis of the 13 ACS/ETC control actions (see Section 4.3.4, Table 13 for details).

3. Applies the ASIL assessment[3] approach in the ISO 26262 standard to evaluate the risks associated with each of the identified hazards. In total, 73 operational situations are developed to assess the seven vehicle-level hazards. Following the practice in the ISO 26262 process, the most severe ASIL is chosen for each vehicle-level hazards. Table ES-1 summarizes the outcome.

Table ES-1. Vehicle-Level Hazards and Corresponding ASIL

	Hazards	**ASIL**
H1	Potential uncontrolled vehicle propulsion	D
H1.a	Potential uncontrolled vehicle propulsion when the vehicle speed is zero	B[i]
H2	Potential insufficient vehicle propulsion	C[ii]
H3	Potential vehicle movement in an unintended direction	C
H4	Potential propulsion power reduction/loss or vehicle stalling	D
H5	Potential insufficient vehicle deceleration	C[ii]
H6	Potentially allowing driver's command to override active safety systems[iv]	D[iii]
H7	Potential electric shock	B[v]

i. For certain control system features that only operate when vehicle speed is zero, the ASIL of this hazard is B. This ASIL is based on a reduced severity from impact occurring at a low speed (i.e., impact occurs before the vehicle reaches high speeds). An example of such a feature is the hill-holder that prevents a car from rolling backward on a hill when the brake pedal is released. However, it is recognized that under certain conditions anomalous vehicle behavior, such as unintended acceleration, may pose a danger to people close to the vehicle.

ii. The ASIL assessment for this hazard varied among safety analysts in the absence of objective data. This research finds that objective data are not readily available for the assessment of the three dimensions used to determine the ASIL--severity, exposure, and controllability.

iii. The effects of H6 are contained in H1, H2, H4, and H5. Therefore, H6 takes on the most severe ASIL value among those four hazards.

iv. This hazard may not apply in ACS/ETC systems designed to give the driver's command priority over all active safety systems.

v. This hazard is not likely to occur for passengers and pedestrians in contact with the vehicle due to an electrical failure. The hazard is primarily limited to people conducting maintenance on the vehicle, or first responders following an incident that has caused physical damage to the vehicle/battery.

[3] 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. There are four ASIL levels that are assigned a letter value "A" to "D" according to increasing hazard criticality.

4. Performs a safety analysis using both the FMEA and the STPA method.
   a. The Functional FMEA identifies 33 failure modes and 93 causes (see Section 7.1, Table 25 for details).
   b. The STPA identifies 1,052 causes that may lead to 95 UCAs (see Section 7.2, Table 27 for details).

5. Identifies 202 example safety requirements for the ACS/ETC system and components by combining the results of the two safety analyses (Functional FMEA and STPA) and leveraging industry practice experiences.
   a. This study derived 114 example functional safety requirements by following the Concept Phase in the ISO 26262 standard
   b. This study derived 88 examples of additional safety requirements by following the additional safety strategy in MIL-STD-882E [3]. These 88 requirements are out of the scope of the Functional Safety Concept phase in ISO 26262 (Part 3 of ISO 26262). However, subsequent steps in the ISO 26262 process — Systems Engineering (Part 4), Hardware Development (Part 5), and Software Development (Part 6) — cascade the Functional Safety Concept requirements into additional development-specific safety requirements, and may identify these 88 requirements.

   Table ES-2 provides a breakdown of the 114 example functional safety requirements and 88 examples of additional safety requirements.

Table ES-2. Breakdown of Safety Requirements

ACS/ETC System/Subsystem	Number of Functional Safety Requirements	Number of Additional Safety Requirements
General ACS/ETC System	11	17
Accelerator Pedal Assembly	8	3
Fuel Cell Electric Vehicle Powertrain Control Module	50	27
Electric Powertrain System	28	13
Communication Signals	5	4
Power Supply (Low and High Voltage)	7	3
Interfacing Systems	5	21

While following the ISO 26262 process, this research also makes the following observations:

- Although ISO 26262 requires a hazard to take the most severe ASIL among all operational situations, if a vehicle feature only operates in a subset of all operational situations, its ASIL could be lower. For example, although *H1-Uncontrolled Vehicle Propulsion* has an ASIL D for all operational situations considered, *H1.a-Uncontrolled Vehicle Propulsion when Vehicle Speed is Zero* has a lower ASIL (B). This lower ASIL

is based on a reduced severity value from impact occurring at a low speed (i.e., the vehicle does not reach high speeds). Therefore, an electronic control system feature such as hill-holder that only operates when the vehicle speed is zero may receive ASIL B for the *Uncontrolled Vehicle Propulsion* hazard.

- The generation of operational situations could be improved by leveraging the variables and codes in the NHTSA crash databases and naturalistic driving datasets.
- Without the support of objective data, the ASIL assessment may vary among safety analysts.
    - Statistics from the NHTSA crash databases are available to support the assessment of severity.
    - Statistics are not readily available for the assessment of exposure, but may be derived from the naturalistic driving data sets.
    - Statistics are not publicly available for the assessment of controllability.

The results of this study may be used to:

- Benchmark safety requirements for the FCEV ACS/ETC system.
- Illustrate how STPA may be incorporated as one of the potential hazard and safety analysis methods that can support the ISO 26262 process.
- Provide inputs to the development of performance testing.

1 INTRODUCTION

1.1 Research Objectives

In conjunction with the National Highway Traffic Safety Administration, the Volpe National Transportation Systems Center is working on a project that supports the need for additional safety requirements[4] related to the failures and countermeasures of the accelerator control system with electronic faults, such as errant electronic throttle control signals. This project focuses on the ACS/ETC, which is the subset of ACS architectures where the throttle is controlled electronically, rather than through a mechanical connection to the driver-operated control.

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. Conduct a hazard analysis for electronic-related ACS/ETC failures; and
2. Derive example safety requirements and safety constraints for different ACS/ETC propulsion system variants in accordance with ISO 26262 Concept Phase (Part 3) and other system safety standards, such as MIL-STD-882E.

In this project, Volpe is examining the ACS/ETC for the following propulsion system variants.

1. Gasoline Internal Combustion Engine
2. Diesel ICE
3. Electric vehicle
4. Hybrid electric vehicle with a gasoline ICE for three common architectures:
   a. Series
   b. Parallel
   c. Series-parallel
5. Fuel Cell HEV

This report covers the study of the FCEV ACS/ETC in light motor vehicles (i.e., passenger cars, vans, minivans, SUVs, and pickup trucks with gross vehicle weight ratings of 10,000 pounds or less). This report documents the approach and the findings of the analysis.

[4] All requirements presented in this section are not actual compliance requirements currently in effect in an existing FMVSS. Instead, they are intended to illustrate a comprehensive set of requirements that could be derived from the safety analysis results. These safety requirements are not intended to represent NHTSA's official position on or regulatory requirements for producing ACS/ETC systems.

1.2 Report Outline

In addition to the Introduction, this 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 ACS/ETC system in FCEVs. 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 on the identified vehicle-level hazards.
- Section Six summarizes the vehicle-level safety goals as the result of 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 safety requirements.
- Section Ten discusses observations on the application of the ISO 26262 standard.
- Section Eleven considers potential uses of the results of this study.

Sections Two and Eleven of this report are essentially unchanged from a previous report published as part of this project, *Functional Safety Assessment of a Generic Accelerator Control System With Electronic Throttle Control in Gasoline-Fueled Vehicles* [34]. These sections are reproduced here so that this report can serve as a stand-alone document.

2 ANALYSIS APPROACH

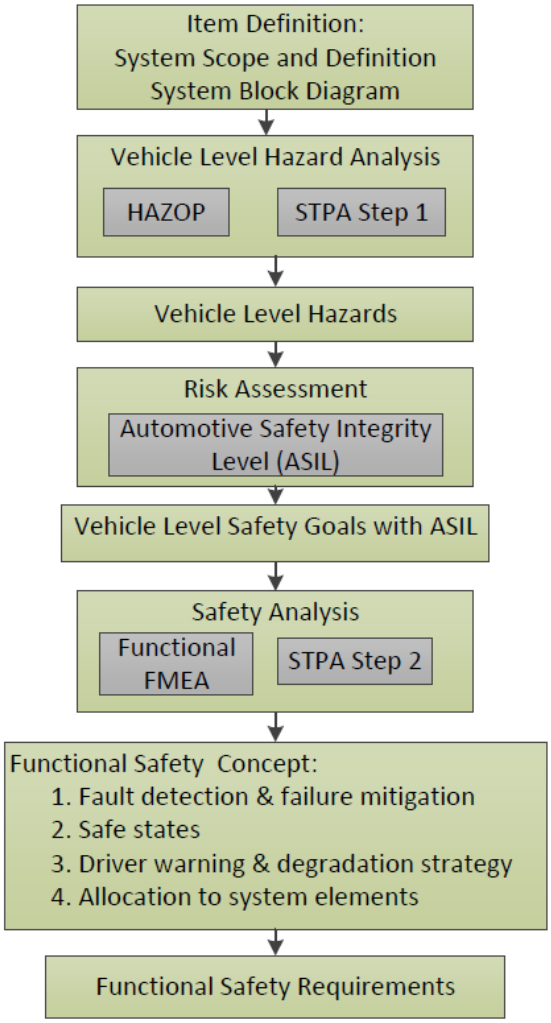
The primary purpose of this work is to study and analyze the potential hazards that could result from cases of electrical or electronic failures impacting the functions of vehicular control systems. The study follows the ISO 26262 process to identify the integrity requirements of these functions at the concept level, independent of implementation variations. ISO 26262 is a functional safety standard adapted from the International Electrotechnical Commission Standard 61508, and is intended for application to electrical and electronic systems in motor vehicles (Introduction in Part 1 of ISO 26262). Part 3 of ISO 26262 describes the steps for applying the 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. Based on their ASIL decompositions, manufacturers may employ a variety of techniques, such as 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. The process shown in Figure 1 was developed in part based on learnings from applying Part 3 of ISO 26262 in a previous study.[5]

[5] Brewer, J., Nasser, A., Hommes, Q. V. E., Najm, W., Pollard, J., & Jackson, C. (2018). *Safety management of automotive rechargeable energy storage systems: The application of functional safety principles to generic rechargeable energy storage systems* (Report No. DOT HS 812 556). Washington, DC: National Highway Traffic Safety Administration.

.



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 and 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.
2. Carry out the hazard analysis using both the HAZOP study [4] and the STPA method [5]. The output of the hazard analysis is a list of vehicle-level hazards.
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 vehicle-level safety goal.
5. Perform safety analyses on the relevant system components and interactions as defined in the first step of this process. This project applies both a Functional FMEA [6] and STPA in the safety analysis.
6. Develop a functional safety concept and functional safety requirements for the ACS/ETC at the system and component levels by following the ISO 26262 process. The functional safety concept and safety requirements are based on results from the hazard and safety analyses, ISO 26262 guidelines, and industry practice experiences.

2.2 Hazard and Safety Analysis Methods

This project uses multiple analysis methods to generate a list of hazard and safety analysis results.[6] These methods are described in this section.[7]

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.

[6] 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.
[7] 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 description to better explain how the analysis is performed.

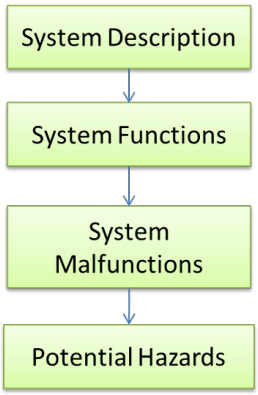


Figure 2. HAZOP Study Process

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 is designed to perform. This step is also accomplished in the first step of the overall project (Figure 1).
3. Apply a set of guidewords to each of the identified functions to describe the various ways in which the function may deviate from its design intent. IEC 61882[8] 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
    - Incorrect direction
    - Not requested
    - Locked function
4. Assess the effect of these functional deviations at the vehicle level. If a deviation from an intended function may result in a vehicle-level hazard, the hazard is then documented.

[8] IEC 61882:2001, *Hazard and operability studies (HAZOP studies) - Application guide*, provides a guide for HAZOP studies of systems using 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.

2.2.2 Functional Failure Mode 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 potentially lead to the vehicle-level hazards. The failure modes identified by the Functional FMEA are used to derive the safety requirements.

SAE Standard J1739 by the Society of Automotive Engineers[9] provides guidance on applying the Functional FMEA method [6]. The analysis includes the following steps.

1. List each function of the item on a 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.
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 performed during the Concept Phase of ISO 26262, the analysis is not based on a specific design and does not assume controls or mitigation measures are present; there are not enough data to support Steps 5 through 7. The completed Functional FMEA worksheet is intended to be a living document that is continually updated throughout the development process.

2.2.3 Systems Theoretic Process Analysis

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.

[9] In 2006 the Society of Automotive Engineers, well known as SAE, changed its formal name to SAE International.

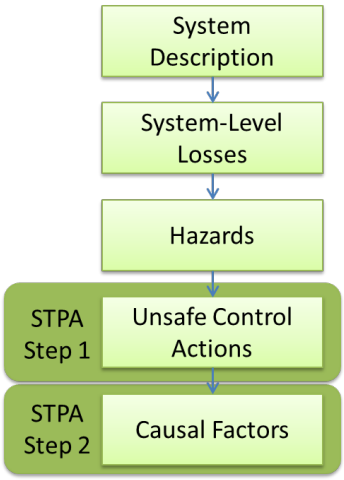


Figure 3. STPA Process

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 (controllers, sensors, actuators, controlled processes, and communications links). This control structure is a generic representation of the functions for a typical system.
    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 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, the losses include the occurrence of a vehicle crash and electrocution.
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 worst-case environmental conditions, will lead to a system-level loss [5]. Initially, based on engineering experience and a literature search, a preliminary hazard list is generated. This list is further refined through iterations in STPA Steps 1 and 2 — UCA and causal factor identification.

4. **STPA Step 1**: Identify potential UCAs issued by each of the system controllers that could lead to vehicle-level hazards. Four sub-steps are involved.

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

    b. For each control action, develop a set of context variables[10]. 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. A recent enhancement to the STPA method [7] enumerates the process model variable states in the first step of STPA. Process model variables refer to variables that the control algorithm uses to model the physical system it controls. This study does not assume the detailed algorithm design is known, and hence, modifies this STPA approach to focus on context variables instead of process model 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.

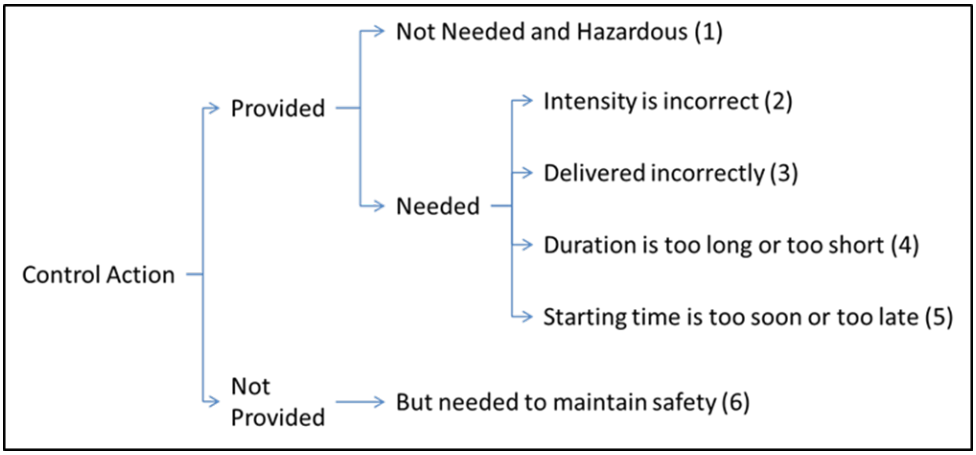


Figure 4. Guidewords for UCAs

For each control action, assess each of the six guidewords against each of the context variable combinations to determine if it could lead to one or more of the

[10] The context variables describe the context in which the control commands act in. For example, the control command "enter BTO mode" may operate in the context of the "driver presses both AP and BP."

vehicle-level hazards. If new hazards are identified, add these hazards 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 overall 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 CFs for each UCA identified in STPA Step 1.

   Each component and interaction in the control structure representation of the system is analyzed 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 used an expanded list of 26 guidewords for identifying CFs. Appendix A 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 (Figure 1) stage.

3 SYSTEM DEFINITION

3.1 System Analysis Scope

In ACS:

> *"all vehicle components, including both mechanical and electrical/electronic components and modules, that operate a vehicle's throttle in response to movement of the driver-operated control and that, upon removal of actuating force on the driver-operated control, return both the throttle and the driver-operated control to their idle or rest positions".*

Furthermore, the components and connections in the ACS mean:

> *"a series of linked components extending from the driver-operated control to the throttling or fuel-metering device on the engine or motor."*

In addition, this analysis also considers incoming torque requests from other vehicle systems, such as cruise control or the traction control system. However, this analysis assumes that these other vehicle systems correctly issue torque requests to the ACS/ETC; failures in other vehicle systems that could result in incorrect torque 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 components leading from the driver-operated control to the high voltage power supply connection to the traction motor, including the following.
   - Accelerator pedal
   - Accelerator pedal position sensor
   - FCEV powertrain control module
   - Traction inverter control module
   - Gate drive board
   - Inverter/converter (also known as the power stage)
   - Phase/current sensor
   - Motor position and speed sensor
   - Inverter temperature sensor
2. All connections between the components listed above, including:
   - Wired connections
   - Communication over the vehicle bus (e.g., controller area network)
3. Brake throttle override function
4. Incoming torque requests from other vehicle systems
5. Interfaces with the rechargeable energy storage system and fuel cell system, including:
   - HV power supply to the inverter / converter
   - High voltage interlock loop information
   - Requests to discharge the HV bus

6. Interfaces with the vehicle cooling system
7. Interfacing sensors, including:
    - Vehicle speed data
    - Brake pedal position sensor
    - Vehicle direction data (forward or reverse gear)

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

- Torque generation by the traction motor and downstream torque transmission (e.g., reduction gears).
- Hazards not directly caused by malfunctioning behavior of the electronic control system, such as fire hazards.
- Brake system malfunctions that may lead to acceleration- or deceleration-related hazards, including regenerative braking malfunctions.
- Malfunctions in other vehicle systems leading to incorrect torque requests.
- Malfunctions in other parts of the high voltage system, including the RESS and fuel cell system.
- Notifications from the ACS/ETC to the driver, such as malfunction indicator lights.
- Driver errors, such as incorrect pedal application or gear selection.
- Failures due to improper maintenance over the lifetime of the vehicle (e.g., incorrect parts, incorrect assembly, and failure to conduct scheduled inspections).
- Multiple point failures in the ACS/ETC system or interfacing systems.

3.2 Analysis Assumptions

In addition to the system scope described in Section 3.1, this analysis includes several assumptions regarding the operation of the FCEV ACS/ETC 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 fuel cell system and RESS both provide DC directly to the inverter/converter. This architecture is currently employed in production vehicles from Toyota, Hyundai, and Honda [9] [10] [11].
    - *Some other system architectures may employ a series HEV style architecture where the fuel cell system is only used to charge the HV battery* [12, pp. 375-377]. *Other system architectures may pair an internal combustion engine with the fuel cell system in a parallel HEV style architecture* [13]. *These other architectures are not considered in this study. Additional analysis may be required for ACS/ETC systems with architectures that differ from the system description in Section 3.4 of this report.*
- The FCEV powertrain operates a single traction motor that is used to provide torque to the drivetrain.

- *Additional analysis may be required for architectures with multiple traction motors (e.g., wheel hub motors) to ensure coordination and proper supply of HV power to each motor.*
- The vehicle speed is primarily provided to the FCEV PCM by a dedicated sensor in the drivetrain, with secondary sources of speed provided by the brake/stability[11] control module. Some system architectures may obtain the vehicle speed from other components. *Requirements related to vehicle speed would apply to whichever component is responsible for providing this information to the FCEV PCM.*

- In order to exit BTO mode and resume acceleration, the driver needs to not only remove the pedal conflict, but also explicitly increase the AP angle. This assumption is based on a brake override process flow diagram published by Toyota [14]. Other manufacturers may have different strategies for exiting BTO mode.
  - *Manufacturers implementing other BTO strategies may require a separate analysis to identify requirements related to the safe functioning of their BTO algorithm.*
- The driver's intent for acceleration and deceleration is only conveyed via the AP and brake pedal (BP). Furthermore, this analysis assumes the driver input is correct and does not examine why the driver may incorrectly or unintentionally press the pedals. It also does not examine other sources of unintentional pedal input such as pedal interference or entrapment by objects inside the vehicle
  - *Requirements related to other types of driver-operated controls for acceleration and braking may require additional analysis. Additional analysis is also needed to understand why the driver may incorrectly or non-intuitively apply the AP or the BP.*
- Cooling for the inverter/converter is provided by a separate vehicle cooling system that is not part of the ACS/ETC. This analysis assumes that the ACS/ETC requests cooling from the cooling system based on the inverter/converter temperature. Some system designs may have other cooling strategies, such as permanent cooling (e.g., immersion).
  - *The requirements related to the cooling system identified in this study would apply to architectures where the inverter/converter has a dedicated cooling system. However, additional analysis may be required to identify requirements related to other types of cooling strategies.*
- The RESS and fuel cell system are responsible for monitoring their respective parts of the HV system, and disconnecting the HV system in the event of a failure. The ACS/ETC is responsible for discharging the HV bus when requested by either the RESS or fuel cell system.
  - *Requirements related to the incoming request to discharge the bus apply to whichever system issues this request to the ACS/ETC. If discharging the HV bus is not performed through the ACS/ETC, then these requirements would not apply.*

[11] Vehicle stability control may include antilock braking system, electronic stability control system, TCS, etc.

- The FCEV PCM is responsible for opening the contactors when the vehicle is in a crash or when the HVIL is violated. In other designs, the contactors may be controlled through the RESS and fuel cell system.
  - *If the system design does not use the FCEV PCM to open the HV contactors in the event of a crash or HVIL violation, requirements related to opening the contactors would not apply.*
- The motor position and speed are provided to the TICM, which communicates the traction motor health to the FCEV PCM. Some system architectures may have relevant motor data provided directly to the FCEV PCM.
  - *Requirements related to the traction motor position and speed would apply regardless of whether this information is provided to the TICM or FCEV PCM. Similarly, requirements related to the communication of this data can be readily adapted to other system architectures.*
- Safety strategies, such as redundant sensors, are not considered in the hazard analysis or safety analysis stages.
  - *Once specific design strategies have been adopted, additional hazard and safety analyses should be performed.*

3.3 System Block Diagram

The FCEV ACS/ETC operates in a similar manner to the EV ACS/ETC.[12] The FCEV powertrain converts electrical energy supplied by the RESS and fuel cell system to mechanical energy, which provides propulsion for the vehicle. The FCEV ACS/ETC regulates the electric power supply to the traction motor to control the motor torque output in response to changes in the driver-operated control.

Figure 5 shows a block diagram representation of the FCEV ACS/ETC system considered in this study. The dashed line indicates the system boundary for the ACS/ETC. Other vehicle systems, shown in gray, are treated as black boxes with respect to the ACS/ETC and are assumed to be functioning correctly. Interfaces between these systems and the ACS/ETC are shown as lines that cross the ACS/ETC system boundary.

[12] Details of the EV ACS/ETC operation can be found in a separate report prepared as part of this research project (Becker, C., Nasser, A., & Attioui, F. [in press]. Functional safety assessment of a generic accelerator control system with electronic throttle control in electric vehicles. Washington, DC: National Highway Traffic Safety Administration.).

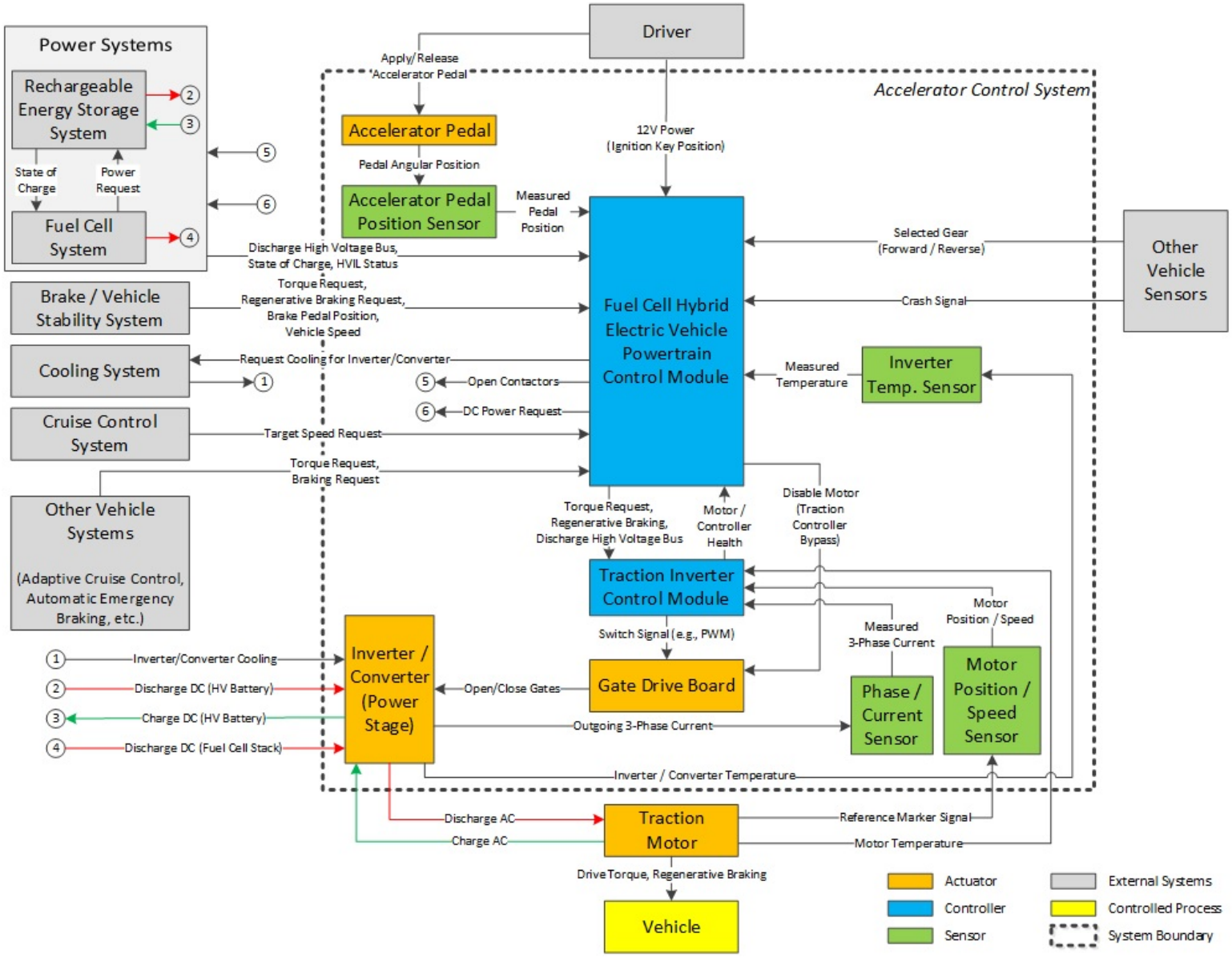


Figure 5. Block Diagram of the ACS/ETC in FCEVs

3.4 System Description

The following description outlines the functions of an FCEV ACS/ETC system. [11] [10] [12] [9] [15] [16] [17]

3.4.1 Driver-Operated Control and Other Torque Requests

The AP assembly allows the driver to command a desired torque from the traction motor. When the driver presses the AP, an integrated sensor – the APPS – measures the angular displacement of the AP. The APPS converts the angular displacement of the AP to a voltage signal, which is transmitted to the FCEV PCM. The signal may be transmitted via a direct connection between the APPS and FCEV PCM or over the vehicle communication bus (e.g., CAN bus).

The FCEV PCM converts the voltage signal from the APPS to a desired traction motor torque.[13] The FCEV PCM then reconciles the torque requested by the driver with torque requests from other vehicle systems. These systems vary depending on the vehicle design and features, but typically include:

- Torque requests from the brake/stability system
- Torque requests from the CC or adaptive cruise control system
- Torque requests from the automatic emergency braking system

In addition to requesting torque via the AP, the driver also determines the desired vehicle direction (e.g., drive or reverse) using the gear selector. The transmission range sensor communicates the gear selector position to the FCEV PCM. The FCEV PCM then commands torque from the traction motor in the direction that corresponds to the driver's selection.

3.4.2 Traction Motor Current Control

After the FCEV PCM computes the direction and amount of torque necessary to meet the driver's request and other vehicle demands, the FCEV PCM sends a torque command to the TICM. The FCEV PCM also issues a DC power or current request to the energy management system, which provides the RESS and fuel cell system with target operating points. The TICM regulates the electrical current supplied to the traction motor to meet the torque command from the FCEV PCM. The electrical current supplied to the traction motor determines both the direction and amount of torque produced by the traction motor.

The TICM causes current to flow to the traction motor by sending switching signals to the gate drive board. The gate drive board serves as a power amplifier that switches the transistors in the inverter/converter according to the TICM's command. The gate drive board may also electrically

[13] Some FCEV ACS/ETC systems may be designed to operate in the power domain (i.e., the driver requests a certain power output via the AP). In these types of ACS/ETC systems, torque requests from other vehicle systems may need to be converted to the power domain prior to being implemented. Otherwise, the system description outlined in this section generally applies to both torque and power domain ACS/ETC systems.

isolate the TICM from the high-voltage inverter/converter to prevent damage to the microcontroller.

The power output from the fuel cell system may not be suitable for direct use by the traction motor. Therefore the inverter/converter may include voltage regulators or direct current/DC converters (e.g., boost and buck converters) to condition the power output from the fuel cell system. The inverter/converter may also contain additional converters that convert high-voltage DC to the low-voltage DC needed for the vehicle's auxiliary systems.

Depending on the FCEV architecture, the traction motor may operate using either HV DC or alternating current. The inverter/converter is designed to provide the appropriate HV power supply to the traction motor. For FCEVs with DC motors, the inverter/converter converts the HV DC from the RESS to the appropriate voltage level for the traction motor. For FCEVs with AC motors, the inverter/converter converts the HV DC from the RESS to the three-phase AC required by the traction motor.

A phase/current sensor measures the current supply from the inverter/converter to the traction motor. The phase/current sensor measurement provides feedback to the TICM allowing closed-loop control of the switching signal provided to the gate drive board. The inverter/converter also provides current and voltage feedback to the fuel cell system.

The traction motor provides torque to the transaxle of the driven wheels, providing propulsion for the vehicle. The traction motor position and speed is measured by an integrated sensor in the motor assembly (e.g., a resolver). The traction inverter controller uses feedback from the motor position and speed sensor to adjust the switching signal provided to the gate drive board to achieve the desired torque output from the traction motor.

3.4.3 Idle Speed Control

When the driver releases the AP, mechanical components (e.g., springs) in the AP assembly return the pedal to the idle (i.e., undepressed) position. In an FCEV, the traction motor torque output can be reduced to zero when the AP is released. This is in contrast to vehicles with ICEs that maintain an idle speed when the AP is released.[14] In order to simulate the "creep" speed found in ICEs, some FCEV PCMs are designed to provide current to the traction motor when the AP is released based on a pre-programmed idle torque level.

If the AP is released when the vehicle speed is above the idle creep speed, the FCEV PCM may either coast down to the idle creep speed or may activate regenerative braking to slow the vehicle at a faster rate. This latter approach is typically used to simulate the effect of engine braking

[14] In ICEs, the engine runs at an idle speed to provide torque to vehicle accessories and prevent engine stalling from drag torque. A portion of the idle torque gets transmitted through the transmission and produces a low "creep" speed.

found on vehicles with ICEs. Regenerative braking also serves to re-charge the RESS, as noted later in this report.

3.4.4 Brake Throttle Override Function

As an example OEM strategy, when the driver presses the BP, the BPPS sends a signal to the FCEV PCM. If both the AP and BP are pressed, algorithms in the FCEV PCM determine if the driver's intent is to stop the vehicle. To accomplish this, the FCEV PCM may consider other factors in addition to the accelerator pedal position and brake pedal position, such as vehicle speed, the sequence of brake and accelerator pedal application, and the duration with which both pedals are pressed. If it appears that the driver is trying to stop the vehicle, the FCEV PCM engages the BTO feature.

In BTO mode the FCEV PCM will override the torque request from the driver via the AP and either reduce the current supply to the pre-set current level for BTO mode or reduce the current supply to zero. Since regenerative braking relies on the traction motor, it is possible that the FCEV PCM engages regenerative braking while in BTO mode, effectively overriding the AP torque request. The FCEV PCM will maintain the current supply to the traction motor at the BTO level until BTO mode is disengaged. The FCEV PCM should not exit BTO mode while a conflict between the AP and BP still exists.

3.4.5 Fault Detection

In addition to regulating the traction motor torque output, the FCEV PCM is also responsible for monitoring the ACS/ETC electronic system components to determine if faults are present. If the FCEV PCM detects a fault in the system, the FCEV PCM will log a diagnostic trouble code and may force the ACS/ETC into a safe state, such as the "limp-home mode." The FCEV PCM may also issue a command to turn on the malfunction indicator light on the vehicle's instrument display panel.

Some examples of system faults include the following.[15]

- APPS voltage signals exceeding the calibration range
- Faults in the TICM or inverter/converter
- Faults in the HV supply
- Internal software or hardware faults in the FCEV PCM

[15] These examples are faults within the ACS/ETC system. For faults within the fuel cell system itself, such as low performing cells (i.e., low individual cell voltages), the fuel cell system control module may issue separate commands to illuminate malfunction indicator lights.

If the TICM has a fault, the FCEV PCM may be able to bypass the TICM and communicate directly with the gate drive board to disable current flow to the traction motor.

3.4.6 Related System: Braking System

In addition to providing vehicle propulsion, the traction motor is responsible for supporting the FCEV brake/stability system through regenerative braking. Regenerative braking occurs when the traction motor is operated as a generator, creating a braking effect at the driven wheels and converting the kinetic energy of the vehicle into electrical energy stored by the RESS. This dissipates the vehicle's kinetic energy, slowing the vehicle.

When the BP is pressed, the BPPS measures the angular displacement of the BP. This measurement is converted to an electrical signal that is sent to the FCEV PCM. The FCEV PCM then develops a braking strategy that meets the demanded level of braking while maximizing energy recovery through regenerative braking. When the available regenerative braking force is not sufficient to meet the braking demand, the FCEV PCM can request braking from traditional mechanical (i.e., friction) brakes. Note that in some vehicle configurations, the braking strategy may be developed by another vehicle controller, such as the brake/stability control module, and the FCEV PCM only receives a request to supply a certain level of regenerative braking.

The FCEV PCM sends a request for regenerative braking to the TICM. Similar to the traction motor control described above, the TICM determines the appropriate current flow from the traction motor to achieve the required level of regenerative braking. The electrical energy generated by the traction motor is converted to HV DC suitable for the RESS through the inverter/converter.

Although regenerative braking uses many of the same components as the FCEV ACS/ETC, as described in Section 3.1 of this report, regenerative braking is outside the scope of this study.

3.4.7 Related System: Fuel Cell System

The fuel cell system is not considered part of the ACS/ETC, but is essential for supplying the DC power to the ACS/ETC that allows the traction motor to operate. There are several types of fuel cell systems. However, the type of fuel cell system currently used in most production vehicles is the hydrogen-fueled proton exchange membrane. This type of fuel cell system combines hydrogen and oxygen to produce an electrical current.

The core element of the fuel cell system is the "fuel cell stack." The fuel cell stack is comprised of numerous fuel cells, each of which consist of two electrodes (an anode and cathode) separated by an electrolyte. As hydrogen gas from on-board fuel tanks passes through the anode, it becomes ionized. The positive ions pass through the electrolyte to the cathode, while the electrons flow through an external circuit and supply power to the vehicle. The HV circuit is closed at the cathode, where the hydrogen ions react with oxygen from the ambient air to produce water as a byproduct. The voltage output from an individual fuel cell is relatively low

(e.g., on the order of one to two volts) and so multiple fuel cells are required to produce the voltage required to power the vehicle.

In addition to the fuel cell stack, the fuel cell system includes ancillary equipment that ensures proper operation of the system. This equipment may include compressors, humidifiers, heat exchangers, pumps and valves for regulating flow of gasses through the fuel cell stack, temperature monitoring equipment, and hydrogen leak detectors.

In addition to supplying HV DC to the ACS/ETC system, the fuel cell system must also regulate several other parameters (temperature, humidity, etc.) to ensure proper operation and prevent damage to the fuel cell stacks. As a result, operation of the fuel cell system does not necessarily track the APP. For example, if the AP is released suddenly (e.g., a sudden reduction in power demand), the fuel cell system may reduce the power output more gradually to ensure the humidity levels are maintained as the fuel cell stack cools. The excess power produced may be diverted to the RESS to charge the HV battery.

If a problem in the fuel cell system is detected or in the event of a vehicle crash, the fuel cell system may send a signal to the FCEV PCM to discharge the HV bus. The FCEV PCM transmits the request to discharge the HV bus to the TICM. The TICM commands the inverter/converter, through the gate drive board, to discharge the HV bus across resistors integrated into the inverter/converter. In the event of a vehicle crash, the fuel cell system itself typically consumes the residual hydrogen and oxygen in the fuel cell stacks, as well as the residual energy in the fuel cell system; aside from the hydrogen storage tanks, there is relatively little stored energy in the fuel cell system itself.

3.4.8 Related System: Rechargeable Energy Storage System

The RESS is not considered part of the ACS/ETC, but it is a closely related system and is also essential for achieving the desired torque output from the traction motor. The RESS is responsible for controlling both the charging and discharging the high-voltage battery, including charging the battery through regenerative braking and from the fuel cell system. Coordination between the RESS, fuel cell system, and ACS/ETC is critical for ensuring proper power management for the vehicle; critical information shared between these systems may include the battery state of charge and DC power required by the ACS/ETC.

Depending on the vehicle's design, the fuel cell system may be capable of providing the majority of the required power to operate the traction motor. The RESS may supply the inverter/converter with high-voltage DC when the power demand exceeds the fuel cell system's current power output, such as during vehicle start-up or heavy acceleration. In addition, the RESS may compensate for short-term fluctuations in the ACS/ETC power demand, allowing the fuel cell system to remain at more efficient operating points. In some designs, the RESS may also provide the power necessary to start up some of the fuel cell system components (e.g., compressors and pumps).

In addition to supplementing the DC power supplied by the fuel cell system, the RESS also manages recharging of the battery. The RESS coordinates with the ACS/ETC to receive high-voltage DC from the inverter/converter during regenerative braking. The RESS also coordinates with the fuel cell system to recharge the battery using the power output from the fuel cell system.

When a voltage or current abnormality is detected or when the RESS receives a signal from the occupant restraint system crash sensors, the RESS may send a signal to the FCEV PCM to discharge the HV bus. The FCEV PCM implements this command in the same manner as described in Section 3.4.7.

4 VEHICLE-LEVEL HAZARD ANALYSIS

This study performs two types of hazard analysis – HAZOP study 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

In this study, HAZOP and STPA identify similar vehicle-level hazards. These hazards were synthesized to produce a consistent list. Table 1 shows the vehicle-level hazards and their definitions.

Table 1. Vehicle-Level Hazards and Definitions

	Driver Action	Vehicle Response	Hazards
Acceleration-Related	Does not command acceleration or commands less than the provided acceleration	Accelerates in the direction chosen by driver (forward or reverse)	**H1: Potential Uncontrolled Vehicle Propulsion** - is analogous with Unintended Acceleration, defined as "any vehicle acceleration that the driver did not purposely cause to occur" **H1.a: Potential Uncontrolled Vehicle Propulsion When the Vehicle Speed is Zero**
	Commands acceleration	Does not accelerate or accelerates at a rate that is less than the specified speed increase profile	**H2: Potential Insufficient Vehicle Propulsion** - refers to incidents where the vehicle does not accelerate to the level commanded by the driver or at the rate commanded by the driver.
		Accelerates in a direction other than chosen by the driver	**H3: Potential Vehicle Movement in an Unintended Direction** – refers to vehicle acceleration in response to the driver's command. However, the vehicle accelerates in a direction other than the direction selected by the driver.
Deceleration-Related	Does not command deceleration or commands less than the provided deceleration	Decelerates	**H4: Potential Propulsion Power Reduction/Loss or Vehicle Stalling** - refers to incidents where there is any degree of deceleration of the vehicle that the driver did not purposely cause to occur.
	Commands deceleration	Does not decelerate or decelerates at a rate that is less than the specified speed decrease profile	**H5: Potential Insufficient Vehicle Deceleration** - refers to incidents where the vehicle does not decelerate to the level commanded by the driver or at the rate commanded by the driver when the driver reduces the angular position of the AP.
Applicable to both Acceleration and Deceleration	Commands either acceleration or deceleration	Accelerates or decelerates following driver's command, and overrides active safety function	**H6: Potentially Allowing Driver's Command to Override Active Safety Systems** - refers to situations where the ACS/ETC system follows the driver's input when the system design specifies the ACS/ETC should follow an active safety system's torque request.[1]
Not Motion Related			**H7: Potential Electric Shock** – refers to situations where the FCEV ACS fails to discharge an HV circuit and individuals (such as someone performing vehicle repairs or first responder emergency personnel) who might come in contact with an exposed HV circuit.

[1] This hazard may not apply in ACS/ETC systems designed to give driver's command priority over all active safety systems.

This study considers "Potential Electric Shock" as an FCEV ACS/ETC vehicle-level hazard even though it is not related to vehicle motion. This hazard results directly from the function of the ACS/ETC system and therefore falls within the scope of the ACS/ETC according to ISO 26262 (Part 3 Clause 1).

4.2 Hazard and Operability Study

4.2.1 System Description

The HAZOP study uses a block diagram as a visual representation of the FCEV ACS/ETC system. The HAZOP study block diagram identifies the key system elements, internal interfaces, and high-level external interfaces. Figure 6 illustrates the block diagram used in the HAZOP study.

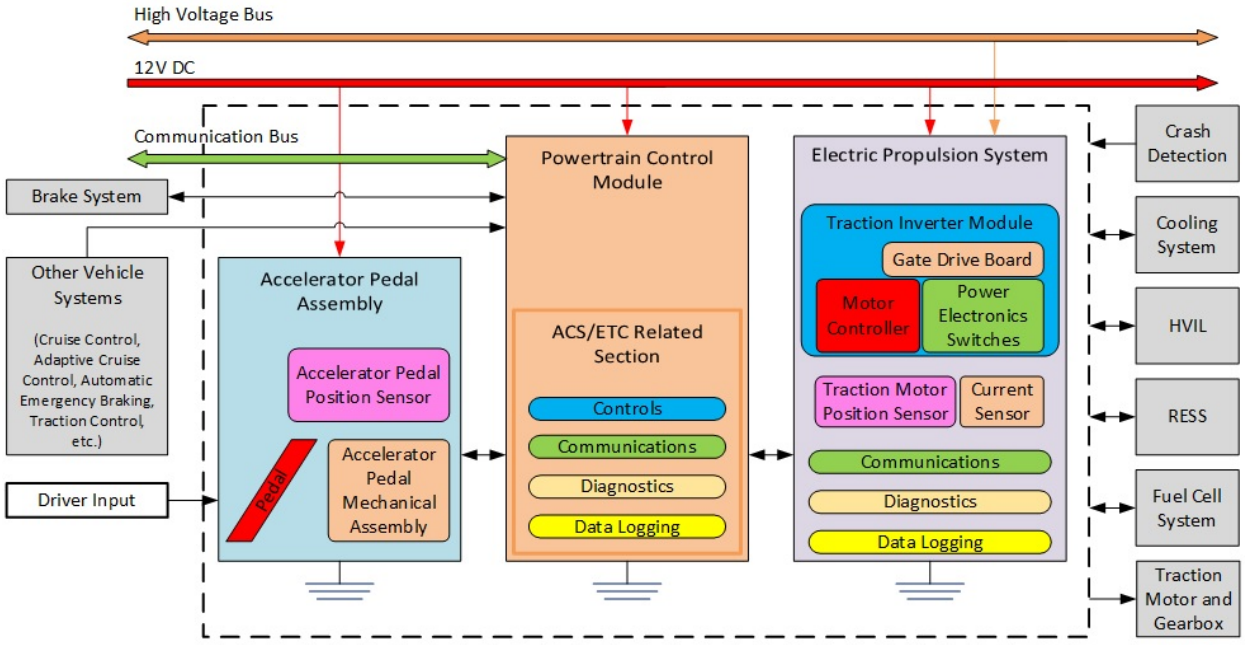


Figure 6. Block Diagram of the FCEV ACS/ETC System for the HAZOP Study

The dashed line in Figure 6 defines the boundary of the ACS/ETC system considered in the HAZOP study. The ACS/ETC contains three main subsystems.

- AP Assembly
- FCEV PCM
- EPS

The AP in the AP assembly receives the driver's input, which is communicated to the FCEV PCM by the APPS. The FCEV PCM determines the corresponding torque output from the traction motor, considering relevant parameters of the vehicle operating conditions, such as vehicle speed, vehicle direction, and torque requests from other vehicle systems. The ACS/ETC receives torque requests from systems such as:

- CC/ACC,
- AEB, and
- TCS.

The FCEV PCM transmits the desired torque to the EPS. The EPS includes the TICM, motor current sensors, motor position sensors, and other hardware and software necessary to drive and control the motor torque. The EPS supplies current to the traction motor, which provides torque to the drivetrain.

In addition to torque requests, the ACS/ETC has other interfaces with the following vehicle systems.

- Brake system – regenerative braking, vehicle speed data, etc.
- Cooling system – inverter/converter cooling
- HVIL – high voltage circuit faults
- Fuel Cell System – system health, discharge bus requests, available power, etc.
- RESS – system health, discharge bus requests, etc.
- Occupant restraint system – crash detection

The ACS/ETC is also connected to the low voltage power supply, the HV power supply, and communication bus (e.g., CAN bus).

4.2.2 System Functions

The HAZOP study identifies 21 system functions for the FCEV ACS/ETC.

1. Command torque from the EPS
2. Receive energy from the HV DC bus.
3. Deliver current to the traction moto
4. Control the RESS HV contactor[16]
5. Control the fuel cell system HV contactor[16]
6. Provide the APP to the FCEV PCM
7. Return the AP to the at-rest (i.e., undepressed) position within the specified time
8. Provide AP request rate limiting

[16] In some topologies, the ACS/ETC may have some control over the contactors. In other topologies, only the RESS and fuel cell systems may have control over the contactors. This study adopts the more conservative approach by including these functions as part of the ACS/ETC.

9. Communicate the delivered torque magnitude and direction to the FCEV PCM
10. Return the torque output to the creep value within the specified time[17]
11. Establish the creep torque value[18]
12. Provide creep state control[18]
13. Provide BTO control
14. Store the APP and motor speed torque maps
15. Provide bus capacitance discharge requests to the EPS
16. Discharge the bus capacitance
17. Communicate with internal subsystems and external vehicle systems
18. Provide diagnostics
19. Provide fault detection and failure mitigation
20. Store relevant data
21. Provide traction motor current values

Functions 19, 20, and 21 are shown here for completeness. Function 19 is part of the design to mitigate hazards resulting from other malfunctions in the system. The HAZOP study concludes that malfunctions derived from Function 20 would not result in vehicle-level hazards. Function 21 is part of the design implementation and may be considered by some analysts to be integral to the TICM.

4.2.3 System Malfunctions and Hazards

The application of the seven HAZOP study guidewords presented in Section 2.2.1 to each of the 21 ACS/ETC functions listed above results in a list of 146 malfunctions.[19] Each of these malfunctions is assessed to determine if the malfunction could lead to one or more of the potential vehicle-level hazards.

Table 2 provides an example of how malfunctions were derived from one of the ACS/ETC functions. Table 3 shows the number of malfunctions identified for each of the 21 ACS/ETC functions. Appendix B provides the complete results of the HAZOP study.

[17] If the FCEV ACS/ETC is not designed to simulate an idle creep speed, the analogous function would be to return the torque output to zero within the specified time.
[18] This function may not apply if the FCEV ACS/ETC is not designed to simulate an idle creep speed.
[19] This does not represent an exhaustive list of all possible FCEV malfunctions. Identification of malfunctions is dependent on the item definition (e.g., system functions), the interpretation of the guidewords, and the judgment of the analyst.

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

Function: Provide the APP to the FCEV PCM.

HAZOP Guidewords	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
Loss of function	Does not provide the APP to the FCEV PCM	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2, 3, 4) Potential insufficient vehicle propulsion 1, 2) Potential insufficient vehicle deceleration 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2) Potential vehicle movement in the wrong direction
More than intended	Provides larger AP travel position than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential uncontrolled vehicle propulsion 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling
Less than intended	Provides smaller AP travel position than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential insufficient vehicle propulsion 1, 2) Potential insufficient vehicle deceleration
Intermittent	Provides APP intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2, 3, 4) Potential insufficient vehicle propulsion 1, 2) Potential insufficient vehicle deceleration 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2) Potential vehicle movement in the wrong direction
Incorrect direction	Provides AP travel position in the wrong direction	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2, 3, 4) Potential uncontrolled vehicle propulsion
Not requested	Provides AP travel position when not intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None. This condition is for unintended but correct information.
Locked function	Does not update AP travel position (stuck)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2) Potential insufficient vehicle propulsion 1, 2) Potential insufficient vehicle deceleration 3, 4) Potential propulsion power reduction/loss or vehicle stalling

ON: Engine on; **D**: Drive; **R**: Reverse

Table 3. Number of Identified Malfunctions for Each HAZOP Function

HAZOP Function	Number of Identified Malfunctions
Command torque from the EPS	7
Receive energy from the HV DC bus	7
Deliver current to the traction motor	7
Control the RESS HV contactor	7
Control the fuel cell system HV contactor	7
Provide the APP to the FCEV PCM	7
Return AP to the at-rest (i.e., undepressed) position within a specified time	9
Provide AP request rate limiting	7
Communicate the delivered torque magnitude and direction to the FCEV PCM	7
Return the torque output to the creep value within a specified time [i]	9
Establish creep torque value [ii]	7
Provide creep torque control [ii]	7
Provides BTO control	7
Stores the APP and motor speed torque maps	7
Provide bus capacitance discharge request	7
Discharge the bus capacitance	7
Communicate with internal subsystems and external vehicle systems	6
Provide diagnostics	6
Provide fault detection and failure mitigation [iii]	6
Store relevant data [iii]	6
Provide traction motor current values [iii]	6

[i] If the ACS/ETC is not designed to simulate an idle creep speed, the analogous function would be to return the torque output to zero within the specified time.
[ii] This function may not apply if the ACS/ETC is not designed to simulate an idle creep speed.
[iii] This function is only included for completeness.

4.3 Systems Theoretic Process Analysis: Step 1

4.3.1 Detailed Control Structure Diagram

Figure 7 illustrates the detailed control structure diagram used in the STPA method to represent a generic FCEV ACS/ETC system and its interfacing systems and components. The ACS/ETC components are delineated by the dashed line. The low voltage 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 system is considered in detail as part of STPA Step 2.

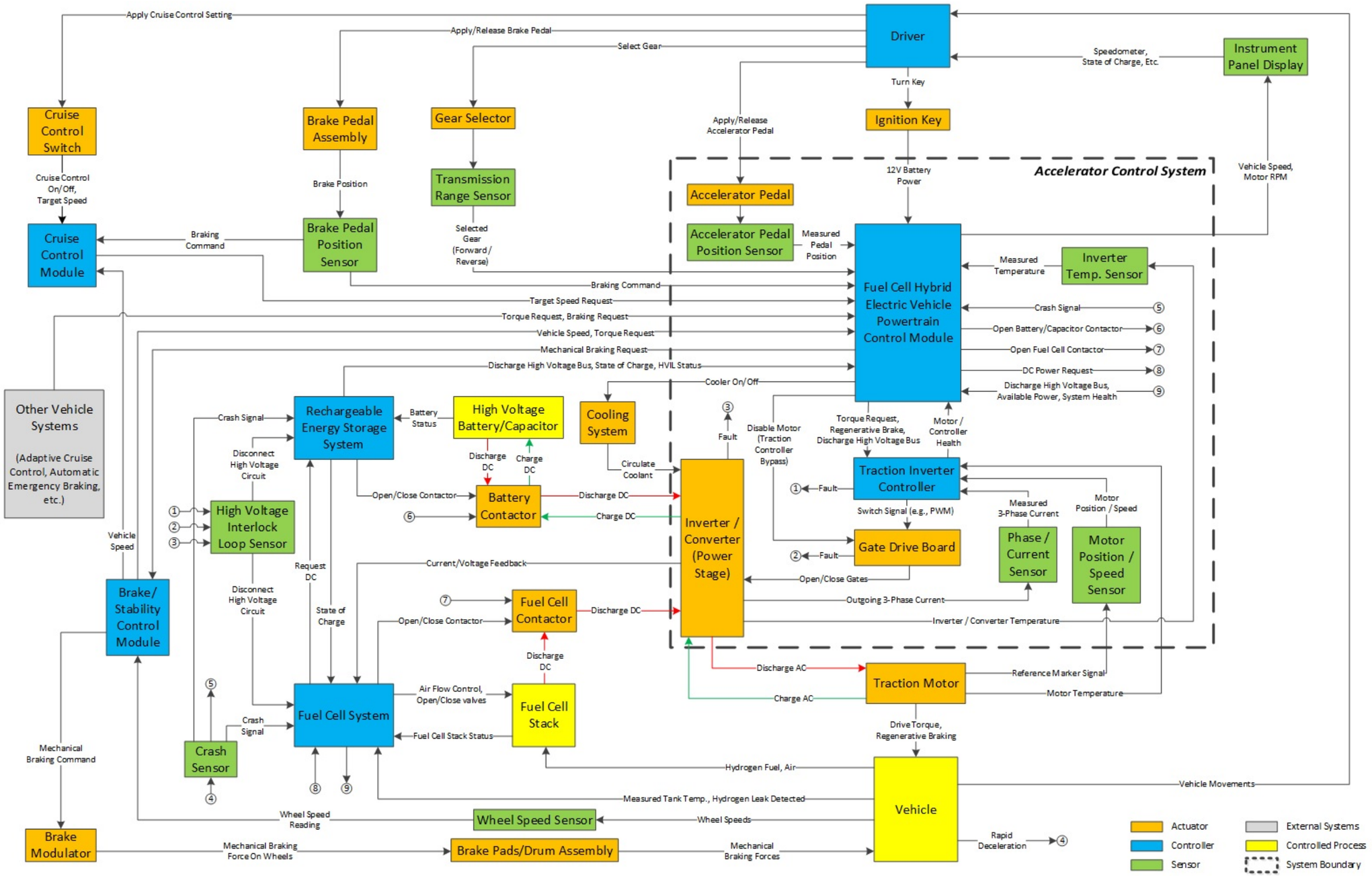


Figure 7. Detailed Control Structure Diagram for the FCEV ACS/ETC System

4.3.2 Vehicle-Level Loss and Initial Hazards

STPA begins by identifying specific losses that the study 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 losses relevant to this study are a vehicle crash and electrocution.

An initial list of vehicle-level hazards is generated based on literature search and engineering experience. As the analyst identifies UCA 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 the HAZOP study and STPA are synthesized to produce the hazard list shown in Table 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 11 control actions issued by the FCEV PCM and two control actions issued by the TICM related to the ACS/ETC function. The 11 FCEV PCM control actions include the following:

1. Two control actions are related to mode switching. These control actions are internal to the FCEV PCM and result in a change in the FCEV PCM operating state.
    i. **Enter BTO mode** – the FCEV PCM issues this control action to enter an operating state that causes the driver's request for braking to override the AP command.
    ii. **Enter normal mode** – the FCEV PCM issues this control action to resume normal ACS/ETC operation (i.e., exit BTO mode).

    The context variable states used to analyze the mode switching control actions are listed in Table 4. The vehicle speed states in Table 4 are based on the maximum speed above which BTO should engage. Manufacturers may elect to have lower vehicle speed threshold values.

Table 4. STPA Context Variables for the Mode Switching Control Actions

Context Variable	Context Variable States
Accelerator Pedal	Pedal is pressed
	Pedal is released
Brake Pedal	Pedal is pressed
	Pedal is released
Vehicle Speed	≥ 10 mph
	< 10 mph

2. Two control actions are related to controlling the magnitude of the torque output from the traction motor. These control actions are issued to the TICM, which controls the current flow to the traction motor to achieve the desired amount of torque.
    i. **Increase the traction motor torque** – the FCEV PCM issues this control action to increase the torque output from the traction motor.
    ii. **Decrease the traction motor torque** – the FCEV PCM issues this control action to decrease the torque output from the traction motor.

    These control actions assume that the traction motor torque output is in the correct direction. The context variable states used to analyze the control actions related to the traction motor torque output are listed in Table 5.

Table 5. STPA Context Variables for the Control Actions Related to Torque Magnitude

Context Variable	Context Variable States
Accelerator Pedal Position	Driver is not pressing the pedal
	Driver reduces the pedal angular position
	Driver maintains the pedal angular position
	Driver increases the pedal angular position
FCEV PCM Operating Mode	BTO mode
	Normal mode
	BTO transitioning to normal mode
	Normal mode transitioning to BTO mode
Torque Requests from Other Vehicle Systems	None
	Reduce torque
	Increase torque
	Both reduce and increase torque

3. Two control actions are used to controlling the direction of the torque supplied by the traction motor. As described in Section 3.4, the FCEV traction motor is capable of directly supplying torque in both the forward and reverse directions. These control actions are issued to the TICM, which controls the current flow to the traction motor to provide the correct direction of rotation.
    i. **Provide torque in the forward direction** – the FCEV PCM issues this control action to provide torque from the traction motor that propels the vehicle in the forward direction.
    ii. **Provide torque in the reverse direction** – the FCEV PCM issues this control action to provide torque from the traction motor that propels the vehicle in the reverse direction.

    These control actions assume that the magnitude of the traction motor torque output is correct based on the inputs from the driver and other vehicle systems. The context

variable states used to analyze the control actions related to the direction of the torque output from the traction motor are listed in Table 6.

Table 6. STPA Context Variables for the Control Actions Related to the Direction of Torque Output

Context Variable	Context Variable States
Gear Selector Position	Driver has selected park
	Driver has selected reverse
	Driver has selected neutral
	Driver has selected drive/low

4. Two control actions are related to requesting cooling for the inverter/converter from the vehicle's cooling system, based on the inverter/converter temperature. The FCEV PCM issues these control actions to maintain the inverter/converter within an allowable temperature range.[20]
    i. **Turn cooling on** – the FCEV PCM issues this control action to request cooling for the inverter/converter from the vehicle's cooling system. For example, this request may cause the vehicle cooling system to activate a cooling pump.
    ii. **Turn cooling off** – the FCEV PCM issues this control action to stop the cooling supplied to the inverter/converter.

    The specific threshold temperature value for requesting cooling depends on the design of the cooling system as well as the inverter/converter. Therefore, this analysis simply refers to a threshold value and it is up to manufacturers to specify this value for their specific design. Table 7 lists the context variable states used to analyze the request for inverter/converter cooling control action.

Table 7. STPA Context Variables for the Inverter/Converter Cooling Control Actions

Context Variable	Context Variable States
Inverter Temperature	Above Threshold Value
	At Threshold Value
	Below Threshold Value

5. One control action is related to discharging the HV bus in response to a request from either the RESS or fuel cell system. The logic for determining when to discharge the HV bus resides in the RESS and fuel cell system control modules; the FCEV PCM simply executes these requests. The command is issued by the FCEV PCM to the TICM, which controls the current flow in the inverter/converter to discharge the HV bus.

[20] As described in Section 3.2, this report assumes that the cooling system is actively controlled (i.e., can be turned on and off).

i. **Discharge the HV bus** – the FCEV PCM issues this control action to discharge stored energy on the HV bus.

Table 8. STPA Context Variables for the Control Action to Discharge the HV Bus

Context Variable	Context Variable States
RESS/Fuel Cell System Request to Discharge HV Bus	Yes
	No

6. One control action is related to opening the contactors for the HV power supply. Depending on the vehicle design, this control action may be issued by the FCEV PCM or may be part of the RESS or fuel cell system.
   i. **Open the contactor** – the FCEV PCM issues this control action to disconnect the RESS and/or the fuel cell system from the ACS/ETC in the event of a vehicle crash or when the HVIL is violated.

Table 9. STPA Context Variables for the Control Action to Open the Contactors

Context Variable	Context Variable States
Vehicle Crash Detected	Yes
	No
HVIL Status	Fault
	No Fault

7. One control action is related to requesting DC power from the energy management system.[21] Along with other high voltage power requests from other vehicle systems, this control action enables the energy management system to establish a target operating points for the fuel cell system or RESS. As described in Section 3.4, additional coordination between the fuel cell system and RESS is not considered part of the ACS/ETC.
   i. **Request DC Power** – the FCEV PCM issues this control action to inform the energy management system of the power required to meet the driver's torque request.

Table 10. STPA Context Variables for the Control Action to Request DC Power

Context Variable	Context Variable States
Request DC Power	Torque Requested
	Torque Not Requested

[21] The energy management system may be a dedicated control module or may be incorporated with either the RESS or fuel cell system controllers.

There are two control actions issued by the TICM:

1. Two control actions are related to controlling the current supply to the traction motor. The TICM issues these control actions to the gate drive board, which operates the transistors in the inverter/converter to regulate the HV power supply to flow to the traction motor.
    i. **Increase current supply to the traction motor** – the TICM issues this control action to increase the current supply to the traction motor, resulting in an increase in torque output.
    ii. **Decrease current supply to the traction motor** – the TICM issues this control action to decrease the current supply to the traction motor, resulting in a decrease in torque output.

Table 11. STPA Context Variables for Control Actions Regulating Current Supply

Context Variable	Context Variable States
FCEV PCM Torque Request	Increase torque
	Decrease torque

4.3.4 Unsafe Control Actions

The six UCA guidewords (Figure 4) are applied to each combination of context variable states for the 13 control actions listed in the previous section. Some control actions only have a single context variable. In these cases, the UCA guidewords are applied directly to the control action for each of the individual context variable states (i.e., there are no combinations of context variable states).

The analysts then assess whether the control action would result in a vehicle-level hazard, given the particular combination of context variable states. Table 12 shows how this is done for one of the control actions – "Enter BTO Mode." Appendix C contains all the UCA assessment tables for the 13 control actions studied.

Table 12. UCA Assessment Table (Example)

Control Action: Enter BTO Mode

Context Variables			Guidewords for Assessing Whether the Control Action May be Unsafe								
Accelerator pedal	**Brake pedal**	**Vehicle speed**	**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**
Not Pressed	Not Pressed	<10 mph	Not hazardous	H4	N/A	N/A	N/A	N/A	Hazardous if provided	Hazardous if Provided	Hazardous if Provided
Not Pressed	Not Pressed	≥10 mph	Not hazardous	H4	N/A	N/A	N/A	N/A	Hazardous if provided	Hazardous if Provided	Hazardous if Provided
Not Pressed	Pressed	<10 mph	Not hazardous	Not hazardous	N/A	N/A	N/A	N/A	Not hazardous	Not hazardous	Not hazardous
Not Pressed	Pressed	≥10 mph	Not hazardous	Not hazardous	N/A	N/A	N/A	N/A	Not hazardous	Not hazardous	Not hazardous
Pressed	Not Pressed	<10 mph	Not hazardous	H4	N/A	N/A	N/A	N/A	Hazardous if provided	Hazardous if Provided	Hazardous if Provided
Pressed	Not Pressed	≥10 mph	Not hazardous	H4	N/A	N/A	N/A	N/A	Hazardous if provided	Hazardous if Provided	Hazardous if Provided
Pressed	Pressed	<10 mph	Not hazardous	H4	N/A	N/A	N/A	N/A	Hazardous if provided	Hazardous if Provided	Hazardous if Provided
Pressed	Pressed	≥10 mph	H1	Not hazardous	N/A	N/A	N/A	N/A	H1	H4	H1

Vehicle-Level Hazards:

H1: Potential uncontrolled vehicle propulsion
H4: Potential propulsion power reduction/loss or vehicle stalling

Each cell in Table 12 represents a UCA. For example, the last row and fourth column of the table may generate the following UCA.

- *The FCEV PCM does not issue the Enter BTO Mode command when:*
  - *the AP is pressed,*
  - *the BP is pressed, and*
  - *the vehicle speed is 10 mph or greater.*

  This may result in potential uncontrolled vehicle Propulsion.

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

Overall, STPA Step 1 identifies a total of 95 UCAs for the generic FCEV ACS/ETC system studied. The breakdown of these UCAs by control action is provided in Table 13.

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

STPA Control Action	**Number of Identified UCAs**
Enter BTO Mode	6
Enter Normal Mode	4
Increase the Traction Motor Torque	12
Decrease the Traction Motor Torque	24
Provide Torque in the Forward Direction	4
Provide Torque in the Reverse Direction	4
Turn Cooling On	5
Turn Cooling Off	2
Discharge the HV Bus	5
Open Contactor	7
Request DC Power	6
Increase Current Supply to the Traction Motor	8
Decrease Current Supply to the Traction Motor	8

Appendix D presents a complete list of the UCAs identified in STPA Step 1. Table 14 and Table 15 show examples of UCAs for the FCEV PCM and their associated vehicle-level hazards. Table 16 shows an example of a UCA for the TICM and its associated vehicle-level hazard.

Table 14. STPA UCA Statement for Traction Motor Torque Magnitude Control (Example)

Hazard	Potential uncontrolled vehicle propulsion
UCA (Example)	The FCEV PCM issues the Increase Torque command when the driver reduces or maintains the angular position of the AP, or is not pressing the AP.

Table 15. STPA UCA Statement for the Direction of Torque Output Control (Example)

Hazard	Potential vehicle movement in an unintended direction Potential uncontrolled vehicle propulsion
UCA (Example)	The FCEV PCM provides torque in the reverse direction when the driver selects park, neutral, or drive/low.

Table 16. STPA UCA Statement for Traction Motor Current Control (Example)

Hazard	Potential propulsion power reduction or loss or vehicle stalling
UCA (Example)	The TICM decreases the current to the traction motor when the FCEV PCM requests a decrease in torque, but the current is decreased by too much.

5 RISK ASSESSMENT

This study follows the risk assessment approach in ISO 26262. The assessment derives the ASIL for each of the seven identified vehicle-level hazards.

5.1 Automotive Safety Integrity Level Assessment Steps

The ASIL assessment contains the following steps:

1. Identify vehicle operational situations
2. For each identified vehicle-level hazard, apply the ISO 26262 risk assessment framework:
    a. Assess the probability of exposure to the operational situation.
    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.

5.1.1 Vehicle Operational Situations

Operational Situations are scenarios that can occur during a vehicle's life (Part 1 Clause 1.83 in ISO 26262). This study generates 73 vehicle operational situations that are provided in Appendix E. Below are two examples:

- Driving at high speeds (100 kph) < V < 130 kph), heavy traffic, good visibility, and good road conditions.
- Driving in the city with heavy traffic and pedestrians present, stop-and-go driving above 16 kph, low visibility, and slippery road conditions.

Seventy of these 73 scenarios are described by 10 variables and their states as shown in Table 17. These variables and their states are identified following current industry practices.

Table 17. Variables and States for Description of Vehicle Operational Situations

Vehicle Speed	Very high speed (V>130 kph)	**Rail Road Track**	Near a rail road track
	High speed (100 kph<V≤130 kph)		Over a rail road track
	Medium speed (40 kph<V≤100 kph)		Not near or over a rail road track
	Inside city (16 kph<V≤40 kph)	**Road Condition**	Slippery
	Inside city very low speed (V≤16 kph)		Good
	Parking lot or drive way (V=0)	**Driving Maneuver**	Stop and go (applicable only at low speed)
	In a traffic stop (V=0)		Overtaking another vehicle
Traffic	Heavy		Evasive maneuver deviating from desired path
			Going straight without special driving maneuver or not moving
	Light		Sharp turn (inc. highway entry/exit ramps)
Visibility	Low/bad	**Brake Pedal**	Applied
	Good		Not applied
Pedestrian Presence	Negligible	**PRNDL**	Park
	Present		Reverse
	Heavy		Neutral
Country Road	Yes		Drive
	No		Drive with hill hold on

The hazard "Potential Electric Shock" does not result from the same operating scenarios as the vehicle motion related hazards. Therefore, the variables in Table 17 were not used to determine the ASIL for "Potential Electric Shock." Instead, three additional operating scenarios were developed to describe this hazard.

1. A person is handling the HV wires when the vehicle is on, but not driving. The vehicle may be on the road, in the garage, or in storage.
2. The vehicle is in a crash event with the HV bus exposed. The vehicle occupants or first responders are in or around the vehicle.
3. The vehicle is moving and enters a safe state that requires the discharge of the bus capacitance.

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 18 is directly copied from ISO 26262 Part 3 Table 2.

Table 18. 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 19 is directly quoted from ISO 26262 Part 3 Table 1.

Table 19. 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 20 is an acceptable approach to assess severity shown in ISO 26262 (Part 3 Clause 7.4.3.2 and Annex B Table B.1).

Table 20. Acceptable Approach to Assess 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
S = Severity

ISO 26262 defines controllability as the "ability to avoid a specified harm or damage through the timely reactions of the persons[22] involved, possibly with support from external measures" (Part 1

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

Clause 1.19 in ISO 26262). Table 21 is ISO 26262's approach to assessing controllability (Table 3 in Part 3 in ISO 26262). Table 22 shows how ASIL is assessed based on exposure, severity, and controllability (Table 4 in Part 3 of ISO 26262).

Table 21. Controllability Assessment

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

C = Controllability

Table 22. ASIL Assessment

Severity Class	**Probability Class**	**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

Below are two examples of how this study assesses the ASIL for each hazard under identified operational situations.

Example 1:

- **Hazard:** Potential uncontrolled vehicle propulsion
- **Operational situation:** Driving at high speeds (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.
- **ASIL assessment:**
  - Exposure = **E4** (This operational situation occurs often, > 10 percent of the vehicle average operating time.)
  - Crash scenario: The vehicle runs into another vehicle in a rear-end crash or an object by departing the road.
  - Severity = **S3** (Front/rear collision or frontal impact with an object with passenger compartment deformation. More than 10 percent probability of AIS 5-6.)
  - Controllability = **C3** (This is the situation with rear-wheel drive vehicles. While at high speeds, the driver's reaction is braking. This situation is difficult to control. For front-wheel drive vehicles, Controllability = C2. The rear-wheel drive vehicles represent the more severe ASIL assessment.)
- ASIL = **D**

Example 2:

- **Hazard**: Potential propulsion power reduction/loss or vehicle stalling
- **Operational situation**: Driving at very high speeds (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.
- **ASIL assessment:**
  - Exposure = **E2** (Operational situation occurs about 1 percent of the operating time of the vehicle.)
  - Crash scenario: Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.
  - Severity = **S3** (Front/rear collision with passenger compartment deformation. More than 10 percent probability of AIS 5-6.)
  - Controllability = **C3** (While at high speeds, the driver's reaction is to steer the vehicle out of traffic and apply additional braking if necessary. This situation is hard to control.)
- ASIL = **B**

Appendix F contains the full ASIL assessment table.

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 seven vehicle-level hazards. ISO 26262 requires the most severe ASIL be chosen for each hazard. Table 23 shows the resulting ASIL values for each hazard.

Table 23. Vehicle-Level Hazards and Corresponding ASIL

	Hazard	ASIL
H1	Potential uncontrolled vehicle propulsion	D
H1.a	Potential uncontrolled vehicle propulsion when the vehicle speed is zero	B[i]
H2	Potential insufficient vehicle propulsion	C[ii]
H3	Potential vehicle movement in an unintended direction	C
H4	Potential propulsion power reduction/loss or vehicle stalling	D
H5	Potential insufficient vehicle deceleration	C[ii]
H6	Potentially allowing driver's command to override active safety systems[iv]	D[iii]
H7	Potential electric shock	B

i. *For certain control system features that only operate when vehicle speed is zero, the ASIL of this hazard is B. This ASIL is based on a reduced severity from impact occurring at a low speed (i.e., impact occurs before the vehicle reaches high speeds). An example of such a feature is the hill-holder that prevents a car from rolling backward on a hill when the BP is released.*

ii. *The ASIL assessment for this hazard varied among safety analysts in the absence of objective data. This study finds that objective data are not readily available for the assessment of the three dimensions used to determine the ASIL--severity, exposure, and controllability.*

iii. *The effects of H6 are contained in H1, H2, H4, and H5. Therefore, H6 takes on the most severe ASIL value among those four hazards.*

iv. *This hazard may not apply in ACS/ETC systems designed to give driver's command priority over all active safety systems.*

6 VEHICLE-LEVEL SAFETY GOALS

Based on the hazard analysis and risk assessment, the safety goals (i.e., vehicle-level safety requirements) are established as listed in Table 24. Each safety goal corresponds to the potential hazards in Table 23.

Table 24. Safety Goals with ASIL

ID	Safety Goals	ASIL
SG 1	Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than to-be-determined m/s^2 for a period greater than TBD seconds is to be mitigated in accordance with the identified ASIL.	D
SG 1a	Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 with zero speed at start is to be mitigated in accordance with the identified ASIL.	B
SG 2	Potential insufficient vehicle propulsion[i] is to be mitigated in accordance with the identified ASIL.	C[ii]
SG 3	Potential vehicle movement in the wrong direction is to be mitigated in accordance with the identified ASIL.	C
SG 4	Potential propulsion power loss/reduction resulting in vehicle deceleration greater than TBD m/s^2 is to be mitigated in accordance with the identified ASIL.	D
SG 5	Potential insufficient vehicle deceleration[i] is to be mitigated in accordance with the identified ASIL.	C[ii]
SG 6	The ACS/ETC control algorithm is to choose the torque command that has the highest priority for safety in accordance with the identified ASIL.	D
SG 7	Potential electric shock is to be mitigated in accordance with the identified ASIL.	B

i. *Insufficient vehicle propulsion/deceleration is defined as the vehicle deviating from the correctly functioning speed increase/decrease profile under any operating conditions by more than TBD sigma. These hazards specifically relate to speed increases or decreases that result from the driver increasing or decreasing the angular position of the AP.*

ii. *The ASIL assessment for the hazard associated with this safety goal varied among safety analysts in the absence of objective data. This study finds that objective data are not readily available for the assessment of the three dimensions used to determine the ASIL--severity, exposure, and controllability.*

7 SAFETY ANALYSIS

This study performs two types of safety analysis — Functional FMEA and STPA.

7.1 Functional Failure Mode and Effects Analysis

This study carried out Functional FMEA for hazards H1, H1a, H2, H3, H4, H5, and H7 (Table 1). Because the consequences of H6 are captured in hazard H1, H2, H4, and H5, a separate Functional FMEA was not performed for H6. Overall, the Functional FMEA covers three ACS/ETC subsystems and nine interfacing systems. The Functional FMEA identifies 33 failure modes and 93 potential causes of failures. Table 25 shows the number of identified causes for each of the failure modes.

Table 25. Number of Identified Faults by Failure Mode

System / Subsystem	Failure Mode	Number of Identified Faults
AP Assembly	APP value interpreted higher than actual	19
	APP value interpreted lower than actual	19
	AP is not returned to idle position correctly	1[i]
	APP communicates with FCEV PCM incorrectly	19
FCEV PCM	Commands a larger amount of torque than requested by the driver	20
	Commands a smaller amount of torque than requested by the driver	20
	Commands torque in the wrong direction	20
	Misinterprets the APPS input	20
	APP-Torque map corrupted	18
	APP rate limiting fault (over-limiting/under-limiting)	20
	Incorrectly establishes idle torque [ii]	20
	BTO control fault	5
	Miscommunicates with internal subsystems	4
	Miscommunicates with external systems	5
	Commands incorrect amount of DC power	20
	Fails to command a discharge of the HV bus capacitance	19
	Diagnostics fault	1[iii]
EPS	Delivers more torque than requested by the FCEV PCM	28
	Delivers less torque than requested by the FCEV PCM	30
	Delivers torque in the opposite direction of the FCEV PCM command	28
	Fails to maintain idle torque [ii]	30
	Does not discharge the HV bus capacitance	21
Motor Speed Sensor	Provides incorrect motor speed to FCEV PCM	1
Vehicle speed sensor	Provides incorrect vehicle speed to FCEV PCM	1
Vehicle direction sensor	Provides incorrect vehicle direction to FCEV PCM	1
BPPS	Provides incorrect input to FCEV PCM	1
Other interfacing vehicle systems	Provides request for incorrect (more) propulsion torque	1
	Provides request for incorrect (less) propulsion torque	1
RESS controller	Communicates incorrect state of charge to FCEV PCM	1
	Incorrectly communicates HV bus capacitance discharge request to FCEV PCM	1
Fuel Cell System controller	Communicates incorrect power availability to FCEV PCM	1
	Incorrectly communicates HV bus capacitance discharge request to FCEV PCM	1
Vehicle communication system (e.g., CAN bus)	Communication messages corrupted during transfer within the ACS/ETC, or between the ACS/ETC and interfacing vehicle systems	1

Note: Some faults may potentially result in multiple failure modes.
[i] These faults are mechanical in nature and are outside the scope of ISO 26262.
[ii] This failure mode only applies to designs where the FCEV PCM simulates an idle creep speed.
[iii] This failure mode is only considered as part of a multiple point failure analysis.

The Functional FMEA also identified the possibility of faults within interfacing vehicle systems. However, as described in Section 3.2, other vehicle systems are assumed to be operating correctly. Therefore, these faults are not included in Table 25.

Table 26 shows a few examples of the Functional FMEA. Appendix G provides the complete Functional FMEA results.

Table 26. Sample Functional FMEA for Potential Uncontrolled Vehicle Propulsion (H1) (Not Complete)

System/Subsystem	Potential Failure Mode (Potential Uncontrolled Vehicle Propulsion)	Potential Cause(s) Mechanism(s) of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code (DTC)
FCEV PCM	Commands a larger amount of torque than requested by the driver	FCEV PCM fault:	Three-level monitoring		FCEV PCM Fault
		Hardware fault (sensors, integrated circuits, circuit components, circuit boards…)		Hardware diagnostics	FCEV PCM Fault
		Internal connection fault (short or open)		Hardware diagnostics	FCEV PCM Fault
		Break in FCEV PCM I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in FCEV PCM I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in FCEV PCM I/O connections to another connection	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Torque command calculation algorithm fault	Three-Level Monitoring	Software diagnostics	System Fault
		Software parameters corrupted		Periodic Checks	
		Arbitration logic fault	Three-Level Monitoring		System Fault

7.2 Systems Theoretic Process Analysis: Step 2

STPA Step 1 identifies UCAs and vehicle-level hazards. The goal of STPA Step 2 is to identify CFs that may lead to the UCAs, which then may result in one or more of the seven vehicle-level hazards. Each of the 26 CF guidewords and the detailed causes (Appendix A) are applied to the components and connections depicted in the STPA control structure diagram (Figure 7). Specifically, the STPA Step 2 analysis includes the following components and connections.

- ACS/ETC components – defined as any component within the ACS/ETC scope boundary
- ACS/ETC interactions – defined as any interaction entirely within the ACS/ETC scope boundary (e.g., a connection between two components)
- Interfacing interaction – defined as an interaction between an ACS/ETC system component and a component outside the ACS/ETC system scope boundary
- Interfacing components – defined as a component where an interfacing interaction originates

The choices of these components and connections enable the analysis to focus on the defined scope of this study while still considering critical interfaces between the ACS/ETC system and other vehicle systems. For example, the vehicle speed signal from the brake/stability system is considered by analyzing the brake/stability control module and the connection between the brake/stability control module and the FCEV PCM. However, other failures in the brake system, such as faults in the wheel speed sensor, are not considered as part of this study.

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 8).

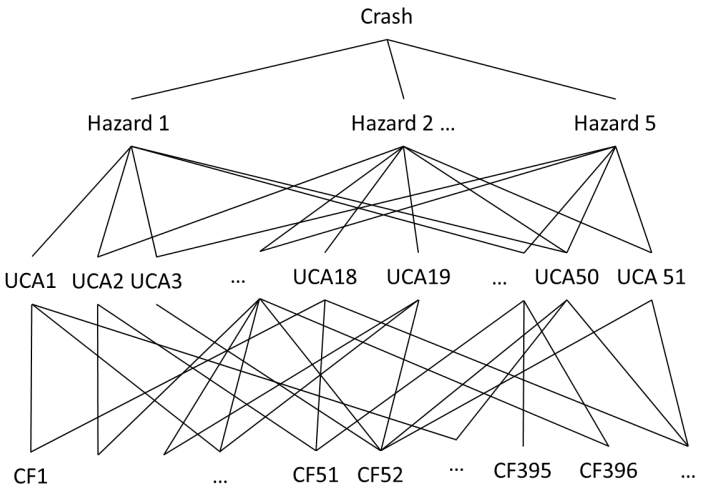


Figure 8. Traceability in STPA Results

The STPA Step 2 analysis identifies a total of 1052 unique CFs. Below is a breakdown of CFs by the type of UCAs they affect. As shown in Figure 8, each CFs can potentially lead to more than one type of UCA. Therefore the breakdown below exceeds the number of unique CFs.

- 214 CFs may lead to UCAs related to mode switching
- 196 CFs may lead to UCAs related to commanding the traction motor torque output
- 446 CFs may lead to UCAs related to converting the torque request to a current
- 82 CFs may lead to UCAs related to providing torque in the requested direction
- 164 CFs may lead to UCAs related to controlling the inverter/converter temperature
- 205 CFs may lead to UCAs related to discharging the HV bus
- 81 CFs may lead to UCAs related to opening the HV contactor
- 84 CFs may lead to UCAs related to requesting DC power

Table 27 shows a breakdown of the identified CFs by the 26 CF guidewords applied in this study.

Table 27. Number of Identified Causal Factors by Causal Factor Category

Causal Factor Category	Number of Identified Causal Factors
Actuation delivered incorrectly or inadequately: Actuation delayed	2
Actuation delivered incorrectly or inadequately: Hardware faulty	4
Actuation delivered incorrectly or inadequately: Incorrect connection	3
Actuator inadequate operation, change over time	30
Conflicting control action	1
Controlled component failure, change over time	3
Controller hardware faulty, change over time	23
Controller to actuator signal ineffective, missing, or delayed: Communication bus error	24
Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	31
Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	10
External control input or information wrong or missing	9
External disturbances	322
Hazardous interaction with other components in the rest of the vehicle	307
Input to controlled process missing or wrong	3
Output of controlled process contributes to system hazard	2
Power supply faulty (high, low, disturbance)	29
Process model or calibration incomplete or incorrect	19
Sensor inadequate operation, change over time	28
Sensor measurement delay	5
Sensor measurement inaccurate	5
Sensor measurement incorrect or missing	7
Sensor to controller signal inadequate, missing, or delayed: Communication bus error	38
Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	65
Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	22
Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	60

Appendix H provides the complete list of CFs. Table 28 shows two examples of CFs for a UCA related to commanding a torque increase.

Table 28. Examples of Causal Factors for a Torque Increase UCA

Hazard	Potential uncontrolled vehicle propulsion	
UCA (Example)	The FCEV PCM issues the increase torque command when: • the FCEV PCM is in BTO mode or is transitioning from normal mode to BTO mode.	
Potential Causal Factor (Examples)	**Component**	**Potential Causal Factor**
	FCEV PCM	Electromagnetic interference or electrostatic discharge from other vehicle components could affect the FCEV PCM.
	FCEV PCM	The FCEV PCM may respond to requests from other vehicle systems to increase the torque output while the FCEV PCM is in BTO mode or is transitioning from normal mode to BTO mode.

- The first CF describes an interaction between vehicle components, where EMI or ESD generated by another vehicle component (e.g., the traction motor) affects the function of the FCEV PCM.
- The second CF describes a flaw in the software logic design where the FCEV PCM responds to a request to increase the traction motor torque from another vehicle system while the FCEV PCM is in BTO mode or is transitioning into BTO mode.

Table 29 shows three examples of CFs for a UCA related to decreasing the current supply to the traction motor.

Table 29. Examples of Causal Factors for a UCA for Decreasing the Current Supply

Hazard	Potential propulsion power reduction / loss or vehicle stalling	
UCA (Example)	The TICM decreases the current to the traction motor when: • the FCEV PCM requests a decrease in torque, but the current is decreased by too much.	
Potential Causal Factor (Examples)	**Component**	**Potential Causal Factor**
	Motor Position / Speed Sensor to TICM	Moisture, corrosion, or contamination could affect the connection terminals of the motor position/speed sensor or the TICM, resulting in an incorrect motor position/speed reported to the TICM.
	TICM	A programming error or flaw in software logic may cause the traction inverter controller to disconnect the high voltage and discharge the high voltage bus (e.g., incorrectly perceives a fault in the system).
	Motor Position / Speed Sensor	The reporting frequency of the motor position / speed sensor may be too low.

- The first CF describes moisture or other contamination affecting the connection between the motor position speed sensor and TICM. If the TICM has the incorrect motor position or

speed information, this could affect how the TICM computes the current required by the traction motor.

- The second CF describes a fault where the TICM disconnects the high voltage system after incorrectly perceiving a faulted state in the ACS/ETC.
- The third CF describes a delay in the transmission of critical sensor data to the TICM. If the TICM does not receive the motor position or speed data in a timely manner and continues to operate using the old data, the TICM may continue to decrease the current supplied to the motor.

8 FUNCTIONAL SAFETY CONCEPT

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 9 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.

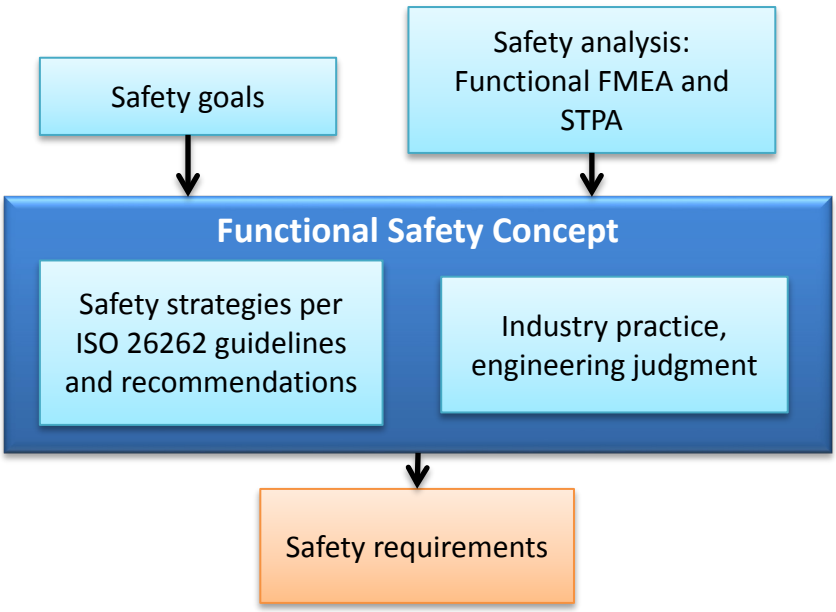


Figure 9. Functional Safety Concept Process

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[23] the health of the main controller (using an auxiliary processor).
4. Ensure the validity and correctness[24] 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 ACS/ETC (Quality factors[25]).
6. Ensure the correct torque, in terms of magnitude and direction, is delivered to the drivetrain with the correct timing.
7. Ensure the health and sanity of the BTO control algorithm.
8. Ensure that low-voltage power is available until the safe state is reached under all safety hazard conditions.
9. Mitigate the safety hazards when an unsafe condition is detected.
10. Ensure that the safe state is reached on time when a hazard is detected.
11. Ensure driver warnings are delivered when an unsafe condition is detected.
12. Ensure the correctness and timeliness of the arbitration strategy.

8.2 Example Safe States

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 item while ensuring the safety of the vehicle operation. Therefore, careful consideration is given to selecting the safe states in relation to the potential failure modes.

The safe states for the FCEV ACS/ETC are either full operation (full torque availability), degraded operation (0 < Torque < Full), or switched off mode (zero torque). The degraded operation may include different levels depending on the potential failure mode.

For example, in cases where the APPS signal is good, but cannot be confirmed, the safe state may allow full torque but at a ramp rate[26] slower than normal in order to give the driver more time to react in case of unintended vehicle behavior. On the other hand, if the APPS signal is unreliable but the vehicle can still be controlled by the brakes and the EPS, the FCEV PCM may allow a torque level higher than creep torque.

---

[23] "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.
[24] "Correctness" means that the value of a parameter is the correct one from the valid set.
[25] Quality factors refer to techniques for error detection in data transfer and communication including checksums, parity bits, cyclic redundancy checks, error correcting codes, etc.
[26] The ramp rate refers to the speed increase and decrease profiles.

Safe states may include the following states commonly used in the automotive industry.

- Safe State 1: Disable input from other vehicle systems, such as ACC and AEB.
- Safe State 2: Limit the maximum allowable propulsion torque to the propulsion torque level that was computed at the instant immediately prior to when the fault occurred.
- Safe State 3: Slow torque ramp rate in response to AP input (single APPS fault)
- Safe State 4: Torque produced without AP input; speed limited to TBD mph, which is greater than the creep speed (two APPS faults; FCEV PCM fault with EPS still able to control throttle)
- Safe State 5: Torque produced at zero AP input value of the torque map (two APPS faults plus BPPS fault)
- Safe State 6: Zero torque output (vehicle disabled; system is unable to mitigate the hazards or ensure Safe States 1-5).
- Safe State 7: Disconnection of the HV bus from the RESS and fuel cell system.

The safe states listed above describe propulsion reduction (Safe States 2, 4, 5, and 6) or deviations from the specified speed decrease or increase profiles (Safe State 3). While these vehicle responses may be similar to vehicle behaviors resulting from the identified hazards H2, H4, and H5, there are key differences:

- The propulsion reduction or modified speed decrease/increase profiles are controlled when entering a safe state, while the hazards describe uncontrolled changes in propulsion (e.g., changes may not be smooth or consistent).
- When entering a safe state, the driver is informed that the vehicle is in a degraded operating state and can take appropriate action. The driver may not be notified of the degraded operating state when hazard H2, H4, and H5 manifests.

8.3 Example Driver Warning Strategies

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 the safety goal is moderate (e.g., single APPS fault, BTO algorithm fault regardless of the need to execute the BTO algorithm).
- Red Light: Potential violation of a safety goal is detected and probability of violating the safety goal is high (e.g., AP torque map corruption, AP or BP communication/data transfer fault), or a violation of a safety goal is detected.
- 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.

- Messages: Messages are displayed to the driver when the red-light driver warning is issued. Manufacturers may also elect to display messages in other situations, such as when the amber light driver warning is issued. The messages include instructions to the driver, such as exiting or staying away from the vehicle.
- Haptic warning: Haptic warnings may be an additional driver warning strategy. Dashboard lights and audible chimes are commonly used in conjunction with haptic warning. It may be beneficial to assess the drivers' reactions to haptic warning at the same time the system attempting to reach a safe state and degraded operation mode.

9 APPLICATION OF THE FUNCTIONAL SAFETY CONCEPT

This study uses the example safety goals identified for the generic FCEV ACS/ETC system introduced in this research and exercises the functional safety concept process depicted on Figure 9. Through this process, this study identifies a total of 202 illustrative safety related engineering requirements for the concept ACS/ETC system and its components.[27]

These include 114 FCEV ACS/ETC system and component functional safety requirements identified by following the Concept Phase (Part 3) in ISO 26262. Sections 9.1 and 9.2 present these findings.

Furthermore, this study identifies an additional 88 safety requirements related to the generic ACS/ETC system and components based on the use of STPA and the additional safety strategies suggested in MIL-STD-882E. These 88 requirements are out of the scope of the Functional Safety Concept in ISO 26262 (Part 3 of the standard). However, the subsequent parts in ISO 26262 — Systems Engineering (Part 4), Hardware Development (Part 5), and Software Development (Part 6) — cascade the Functional Safety Concept requirements into additional development-specific safety requirements, and may capture these additional safety requirements. Section 9.3 presents these additional 88 requirements.

9.1 Example Vehicle-Level Safety Requirements (Safety Goals)

Vehicle-level safety requirements for the generic FCEV ACS/ETC system correspond to the example safety goals presented in Table 24. The safety goals are summarized below, along with the recommended safety strategies.

SG 1: Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 for a period greater than TBD seconds is to be mitigated in accordance with ASIL D classification.

SG 1a: Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 with zero vehicle speed at start is to be mitigated in accordance with ASIL B classification.

SG 2: Potential insufficient vehicle propulsion is to be mitigated in accordance with ASIL C classification.

- Insufficient vehicle propulsion is defined as the vehicle deviating from the correctly functioning speed increase profile under any operating conditions (e.g., when the driver increases the angular position of the AP) by more than TBD sigma.

[27] All requirements presented in this section are intended to illustrate a comprehensive set 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 an ACS/ETC system.

SG 3: Potential vehicle movement in the wrong direction is to be mitigated in accordance with ASIL C classification.

SG 4: Potential propulsion power loss/reduction resulting in vehicle deceleration exceeding the driver's intent by TBD m/s^2 is to be mitigated in accordance with ASIL D classification.

SG 5: Potential insufficient vehicle deceleration is to be mitigated in accordance with ASIL C classification.

- Insufficient vehicle deceleration is defined as the vehicle deviating from the correctly functioning speed decrease profile under any operating conditions (e.g., when the driver reduces the angular position of the AP) by more than TBD sigma.

SG 6: The ACS/ETC control algorithm is to choose the torque command that has the highest priority for safety in accordance with ASIL D classification.

SG 7: Potential electric shock is to be mitigated in accordance with ASIL B classification.

The following outlines the framework used to derive the safety requirements for each of the example safety goals listed above:

- The ACS/ETC is to prevent or detect faults and failures that could lead to vehicle-level hazards that the safety goals intend to mitigate.
- The ACS/ETC is to prevent all failures that lead to the initiation of a propulsion torque increase or decrease when a change in propulsion torque is not requested by the driver or other vehicle systems.
- The ACS/ETC is to detect all faults in requests to modify the propulsion torque issued by other vehicle systems.
- The ACS/ETC is to acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended increase or decrease in speed, including faults communicated by systems such as the brake/stability control system, AEB, and ACC.
- In case of the detection of any failure that could lead to vehicle-level hazards, the ACS/ETC is to transition into a safe state within the fault tolerant time interval.
    - The FTTI is to be set based on established industry data.
    - In the absence of data, the safe state is to be reached as fast as the technology used can diagnose the fault and trigger the system actions.
    - The safe state is to correspond to the 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 any actions required by the driver are to be communicated to them.

9.2 FCEV ACS/ETC System and Components Functional Safety Requirements

Following the Concept Phase (Part 3) in ISO 26262, this study identifies 114 example functional safety requirements for the generic FCEV ACS/ETC system and its components. The distribution of these requirements is as follows.

1. General FCEV ACS/ETC System – 11 requirements
2. AP Assembly – 8 requirements
3. FCEV PCM – 50 requirements
4. EPS – 28 requirements
5. Communication Signals – 5 requirements
6. Power Supply (low and high voltage) – 7 requirements
7. Interfacing Systems – 5 requirements

Table 30 shows examples of safety requirements associated with the FCEV PCM and how they are developed, and how the vehicle-level safety goal (SG 1) is allocated to one of the components in the system — the FCEV PCM. The safety analysis identifies many FCEV PCM failure modes and CFs that could potentially lead to the violation of SG 1. Here, two FCEV PCM controller hardware failures are chosen as examples to illustrate the development process of safety requirements.

Table 30. Examples of FCEV PCM Safety Requirements

Safety Goal	SG 1: Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 for a period greater than TBD seconds is to be mitigated in accordance with the identified ASIL level.
ASIL	D
Component	FCEV PCM
Safety Analysis (Examples)	• Hardware fault (sensors, ICs, etc.) • Internal connection fault (short or open)
Safety Strategy	**Potential Safety Requirements (Examples)**
Detection Fault Tolerance Safe State	All single-point FCEV PCM hardware faults that lead to potential violations of a safety goal are to be detected within the fault detection time and mitigated within the FTTI (ASIL B/C/D). • 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.
Warning	The FCEV PCM is to log and save the following data every time a transition to safe state is executed due to a potential violation of a safety goal (ASIL QM). • The diagnostics information of the faults, 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 the 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 (i.e., 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 accessed by authorized personnel

In case of a controller hardware fault, the first mitigation strategy is for the system to be able to detect the abnormality and transition the system to a safe state. This requirement corresponds to the safety strategy that involves detection, fault tolerance, and transitioning to a safe state in Table 30. Additionally, if the vehicle is to transition to a safe state with reduced or very limited propulsion power (e.g., limp-home mode) the driver would need to be notified so that he or she can maneuver the vehicle to a safe location and get the needed repair service to the vehicle. Therefore, a potential additional requirement associated with a driver warning could be the one described in Table 30.

The rest of this section lists the 114 ACS/ETC 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 different 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 FCEV ACS/ETC System-Level Functional Safety Requirements

There are eleven general system-level functional safety requirements derived for the generic FCEV ACS/ETC system examined in this study. These requirements correspond to all established safety goals.

1. The ACS/ETC is to perform power-on tests, periodic tests, or continuous monitoring tests to ensure the correctness of safety-critical parameters and the integrity of critical system elements (**ASIL B/C/D**).
    a. Critical parameters include those that are used to calculate the magnitude and direction of the propulsion torque, the HV DC bus voltage, the low voltage, vehicle speed, motor speed, the vehicle direction (forward or reverse), and the safety of the HV power bus from unauthorized intrusion.
    b. Other critical parameters may include calculation and comparison results that confirm the proper operation of the system.
    c. The pedal position-speed torque maps are to be checked.
    d. The proper operation of the following critical system elements is to be checked before any propulsion torque command is issued by the ACS/ETC.
        - APPS
        - The motor position sensor
        - The communications channels between the APPS and the FCEV PCM, between the FCEV PCM and TICM, between the motor position sensor and the TICM, and between the brake/stability system and the FCEV PCM.
        - A confirmation of the sanity and health of the FCEV PCM and TICM is to be confirmed via an acceptable strategy before any propulsion torque command is issued by the ACS/ETC.
            - Sanity checks may include quizzer, or seed-and-key strategies[28]
            - State-of-health checks may include:
                - RAM/ ROM/ EEPROM tests
                - Analog-to-digital converter test
                - Shutdown test
    e. The frequency of the periodic tests is to be selected based on the FTTI, and the fault reaction time interval.
    f. In case of a failure in the periodic self-tests, the ACS/ETC is to transition to the appropriate safe state within TBD ms.

[28] Quizzer is also known as seed-and-key. It is a technique that is used to confirm the sanity (health) of a microcontroller. This is usually used as a redundancy technique to comply with ASIL C or D of ISO 26262. The technique uses sets of inputs that mimic a specific operating scenario. One controller (A), at predefined time intervals, presents a set of inputs to the controller (B) whose health is being checked. The set of inputs have a predefined response that is expected from controller B. If controller B responds within the specified time period correctly, then its health is confirmed. If controller B responds incorrectly, then a mitigation strategy is executed by controller A.

2. The hardware architectural single point fault and latent fault metrics targets per ISO 26262 are to be demonstrated for each safety goal (**ASIL B/C/D**).
3. If redundant elements are used, they are to be verified against common cause failures (**ASIL C/D**).
    - Failures in the electric power supply of one element are not to affect the power supply of the other element.
    - A failure in the communication path of one element is not to affect the communication path of the other element.
4. If redundant elements are used and one element fails, the ACS/ETC is to transition into Safe State 3 within the FTTI of TBD seconds and an amber light driver warning is to be communicated to the driver (**ASIL B/C/D**).
5. If redundant elements are used and both elements fail, or if only one element is used and it fails, then the ACS/ETC is to transition into Safe State 4 within the FTTI of TBD seconds, and a red-light driver warning is to be communicated to the driver (**ASIL B/C/D**).
6. Diagnostics of all safety-critical component functions are to be conducted. In case of detected faults, the system is to take mitigation action to prevent failures that lead to a potential violation of a safety goal and appropriate DTCs are to be set (**ASIL QM/A/B**). The diagnostics approach is to cover:
    - Hardware: APPS, FCEV PCM, EPS, and communication hardware, and
    - Software Functions: APP calculations, torque command determination, torque control, and BTO.
7. The ACS/ETC is to include diagnostics covering the following failure modes (**ASIL QM/A/B**).
    - APPS:
        - IC faults
        - Open/short I/Os
        - Stuck on the same reading
        - Out of range
        - Offset
        - State of health
    - Current sensor (if only two sensors are used):
        - IC faults
        - Open/short I/Os
        - Stuck on the same reading
        - Out of range (not required if three sensors are used)
        - Offset (not required if three sensors are used)
        - State of health (not required if three sensors are used)
    - Harnesses and Connectors
        - Open/short circuits

8. DTCs are to be set every time a safety goal may be violated (**ASIL QM**).
9. The ACS/ETC is to log and retain data that can be used to reconstruct the vehicle operating scenario prior to any faults that leads to a violation of a safety goal; the recording time period is TBD seconds before and TBD seconds after the safety goal violation event (**ASIL QM**).
    - This data may include sensors data, human-machine interface data, communication signals, and values of some critical parameters used in the propulsion torque calculations. For example, the following data may be considered.
        - Ignition switch status
        - Gear selector position
        - Vehicle speed and direction
        - APPS value
        - Status of driver assist and other vehicle systems (e.g., ACC, AEB, ESC, etc.)
        - Brake system state
        - Traction motor RPM
        - Traction motor current sensors readings
        - System low voltage value
        - Driver actions regarding vehicle systems capable of initiating and or commanding changes to propulsion torque, including driver override decisions of vehicle systems capable of initiating and/or commanding changes to propulsion torque
        - Arbitration logic decisions by the FCEV PCM
        - FCEV PCM torque request
        - EPS torque received request
        - EPS motor current command
        - Torque requests received from other vehicle systems
        - HV bus state of charge
        - Vehicle dynamics data
10. Diagnostics covering the safety related functionality of the ACS/ETC system components and connections (including the FCEV PCM, EPS, APPS, harnesses, and connectors) are to be instituted with a level of coverage corresponding to the ASIL of the safety goal that is affected. Adhere to ISO 26262 diagnostics coverage guidelines for Low, Medium, and High to comply with the hardware architectural metrics targets (**ASIL QM/A/B**).
11. Diagnostics mechanisms are to adhere to ASIL B classification for ASIL D related elements and ASIL A classification for ASIL C related elements (**ASIL QM/A/B**).

9.2.2 Accelerator Pedal Assembly Functional Safety Requirements

There are eight AP assembly functional safety requirements derived for the generic FCEV ACS/ETC system studied in this project. The AP assembly functional safety requirements correspond to all safety goals, unless otherwise specified.

1. The APP corresponding to the propulsion torque requested by the driver is to be mapped correctly and consistently, and the results are to be qualified for validity and correctness under all vehicle operating conditions, over the usable life of the vehicle (**ASIL B/C/D**).
2. The health and sanity of the APPS is to be monitored and confirmed under all operating vehicle conditions (**ASIL C/D**). **Safety Goals: 1 through 6**.
3. The APP value is to be measured and the value is to be valid and correct (**ASIL B/C/D**).
4. The APP to electrical conversion method is to be validated (**ASIL B/C/D**).
5. Critical communication and data transfer between the APPS and the FCEV PCM, including the APP and diagnostics of the APPS, 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 (**ASIL B/C/D**).
6. In case of a fault that violates a safety goal, the APPS is to communicate the fault to the FCEV PCM (**ASIL B/C/D**). Faults may include the following.
    - Internal hardware failure
    - Degradation over time
    - Overheating due to increased resistance in a subcomponent or internal short
    - Reporting frequency too low
7. The APPS is to have diagnostics for safety-relevant failures that could be caused by EMI/electromagnetic compatibility (EMC), ESD, contamination, and other environmental conditions (**ASIL A/B**).
8. All single point APPS hardware faults that could lead to potential violation of a safety goal are to be detected and mitigated within the FTTI. In case of the detection of a failure, the system is to transition to the corresponding safe state (**ASIL B/C/D**).
    - Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.

9.2.3 FCEV Powertrain Control Module Functional Safety Requirements

There are 50 FCEV PCM functional safety requirements that are derived in this project. Many of these requirements correspond to all established safety goals. However, some of the functional safety requirements only correspond to a subset of the established safety goals. These requirements have the specific safety goals listed in the end.

1. The health and sanity of the FCEV PCM controller are to be ensured (**ASIL C/D**). **Safety Goals: 1 through 6**
    - Power-on Self Tests are to be implemented to check the health of the controller. These test may include:
        i. CPU and Register Test to check the internal working of the CPU. All CPU registers associated with the torque control functions are to be checked during this test.
        ii. Interrupt and Exception Test to check the interrupt and exception processing of the controller.
        iii. EEPROM Checksum Test to check the EEPROM health.
        iv. Device Tests to check the peripheral devices connected to the microcontroller used on a board.
2. The FCEV PCM's I/O pins are to be monitored for shorts to high voltages or ground (**ASIL B/C/D**).
3. The FCEV PCM is to have diagnostics for potential safety relevant failures caused by EMI/EMC, ESD, contamination, organic growth, single event effects[29], and other environmental conditions (**ASIL B/C/D**).
4. All single point FCEV PCM hardware faults that lead to potential violations of a safety goal are to be detected and mitigated within the FTTI (**ASIL B/C/D**).
    - 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.
5. The motor torque output is to be controlled and updated in the correct direction within the correct time duration. The time duration required to update the motor torque output must not result in an uncontrolled propulsion condition (failure mode in SW execution, execution time, motor inertia) (**ASIL D**). **Safety Goal: 1**
6. The FCEV PCM is to arbitrate between multiple requests for propulsion torque modifications from interfacing vehicle systems and the driver (**ASIL B/C/D**). **Safety Goal: 1 through 6**
7. The FCEV PCM arbitration logic strategy and algorithm are to be checked for health and sanity periodically based on the FTTI (**ASIL B/C/D**). **Safety Goals: 1 through 6**
    - In case of a failure in this arbitration strategy, the ACS/ETC is to transition into Safe State 1 within a FTTI of TBD seconds.
    - An amber light driver warning is to be issued.
8. The arbitration strategy is to clearly define the action of the ACS/ETC when there are conflicting propulsion torque requests from interfacing vehicle systems, the driver, and/or internal ACS/ETC functions.

[29] Single-event effects are anomalies in microelectronics caused by single energetic particles, such as protons or cosmic rays. Several different types of single-event effects may occur, such as transient pulses in logic, bit flips, latch-up, or burnout of power transistors. [22]

9. The output of the FCEV PCM arbitration logic is to be qualified for validity and correctness (**ASIL B/C/D**). **Safety Goals: 1 through 6**
10. Critical communications and data transfer between the FCEV PCM and other vehicle systems that can request or command changes to the propulsion torque are to be qualified for validity and correctness (plausibility and rationality) (**ASIL B/C/D**). **Safety Goals: 1 through 6**
    - In case of the detection of a fault, the correct failure mode effect mitigation strategy is to be applied.
    - Critical communications and data transfer include communication signals that request propulsion torque modifications and diagnostics (failure) information of these systems.
11. Critical communications and data transfer between the FCEV PCM and other vehicle systems/components are to be qualified for validity and correctness (plausibility and rationality) including the BPPS (**ASIL D**), vehicle speed sensor (**ASIL D**), motor speed sensor (**ASIL D**), RESS (**ASIL D**), fuel cell system (**ASIL D**), vehicle direction sensor (**ASIL C**), and all other inputs that are used by the torque control function. **Safety Goals: 1 through 6**
    - If the vehicle speed and motor speed are used redundantly, then the ASIL classification may be applied based on a selected ASIL decomposition strategy.
    - If torque maps or look up tables are used, their content is to be checked for validity and correctness at the correct frequency.
12. The torque control function is to specify the inputs used to calculate the propulsion torque. The propulsion torque calculation is to be based on these inputs (**ASIL B/C/D**). **Safety Goals: 1 through 6**
    - Inputs may include, but are not limited to: AP, vehicle speed sensor, vehicle direction sensor, and inputs from other vehicle systems capable of requesting modifications in propulsion torque (e.g., ACC or AEB).
13. The FCEV PCM is to qualify the APP input(s) for validity and correctness (plausibility and rationality) (**ASIL D**). **Safety Goals: 1 through 6**

14. The FCEV PCM torque control algorithm is to include a ramp rate[30] profile. The torque calculation algorithm is to specify the parameters that form the basis for the ramp rate[30] profile (e.g., vehicle speed) (**ASIL C**). **Safety Goals: 2 and 5**
15. The APP to propulsion torque rate of change mapping is to be monitored for correctness (**ASIL C**). **Safety Goals: 2 and 5**
16. All other critical parameters used by the FCEV PCM are to be checked periodically based on the FTTI requirements (**ASIL B/C/D**). **Safety Goals: 1 through 6**
17. All electrical hardware and software elements associated with the delivery of the torque control function are to comply with ASIL D classification for Safety Goals 1, 4, and 6, ASIL C classification for Safety Goals 2, 3, and 5, and ASIL B classification for Safety Goals 1a and 7 unless otherwise specified. If independence of the elements (Part 9 Clause 5.2 of ISO 26262) cannot be demonstrated, then the higher ASIL classification is to be adopted.
18. The FCEV PCM torque command and control communication channel(s) with the EPS are to be validated at start up (**ASIL B/C/D**).
    - Torque commands are not to be issued until the validation of this communication channel(s) is successful.
    - In case of failure of validation, the ACS/ETC is to transition into Safe State 6 within a FTTI of TBD seconds.
    - A red-light driver warning is to be communicated to the driver.
19. The torque command is to be controlled and updated in the correct direction and within the correct time duration (**ASIL B/C/D**). **Safety Goals: 1 through 6**
20. The FCEV PCM algorithm or method for calculating the torque command is to be validated (**ASIL B/C/D**). **Safety Goals: 1 through 6**
21. The torque command corresponding to the propulsion torque requested by the driver is to be calculated correctly and the results are to be qualified for validity and correctness under all vehicle operating conditions (**ASIL B/C/D**). **Safety Goals: 1 through 6**
22. The ACS/ETC is to correctly adjust the propulsion torque in response to propulsion torque modification requests by other vehicle systems (e.g., ACC or AEB) (**ASIL B/C/D**). **Safety Goals 1 through 6**
23. The ACS/ETC is to correctly adjust the propulsion torque request when it receives a communication of a braking action by the brake/stability control system (**ASIL B/C/D**). **Safety Goals 1 through 6**
24. The FCEV PCM is to validate the propulsion torque computed by the control algorithm against propulsion torque limit requests issued by other vehicle systems (e.g., ESC) (**ASIL D**). **Safety Goals: 1 and 3**
    - In case the calculated propulsion torque exceeds the requested propulsion torque limit the ACS/ETC is to transition into Safe State 2 within a FTTI of TBD seconds and an amber light driver warning is to be issued.

[30] The ramp rate refers to the speed increase and decrease profiles.

- Appropriate warnings to the driver from affected interfacing systems are to be issued.

25. The FCEV PCM is to access the metrics that clearly define the limits of vehicle stability from the appropriate vehicle system. The propulsion torque computed by the FCEV PCM is to be validated against the vehicle stability metrics before any propulsion torque command is issued (**ASIL D**). **Safety Goals: 1 and 3**
26. The FCEV PCM is to qualify the stability metrics input(s) for validity and correctness (plausibility and rationality) (**ASIL D**). **Safety Goals: 1 and 3**
    - In case the calculated torque exceeds the vehicle stability limits, the ACS/ETC is to transition to Safe State 2 within a FTTI of TBD seconds. An amber light driver warning is to be issued. Appropriate driver warnings from affected interfacing systems are to be issued.
27. The FCEV PCM is to qualify propulsion torque limit requests issued by other vehicle systems for validity and correctness (plausibility and rationality) (**ASIL D**). **Safety Goals: 1 and 3**
28. The time duration required to update the torque command is not to result in violation of a safety goal. The time duration is to be reflected in the relevant software function's execution time and the transient response of the motor (**ASIL B/C/D**). **Safety Goals: 1 through 6**
29. The FCEV PCM torque control algorithm is to be checked periodically based on the correct TFFI in order to prevent violation of any safety goal (**ASIL C/D**). **Safety Goals 1 through 6**
    - The appropriate fault tolerant strategies are to be applied for the torque control function, such as redundancy, voting logic, or other techniques.
    - A control flow monitoring strategy is to be applied for the torque control function.
30. In case of a fault in the torque control function that results in the FCEV PCM becoming unable to control the torque command, the ACS/ETC is to transition into Safe Sate 6 within TBD ms time and the red-light driver warning is to be issued (**ASIL B/C/D**). **Safety Goals: 1 through 6**
    - In architectures with a simulated idle "creep" speed, failures that prevent the FCEV PCM from controlling the idle "creep" torque command may have a longer FTTI than the FTTI for operating speeds above the idle "creep" speed.
    - DTCs are to be set.
31. The FCEV PCM is to communicate the correct torque command to the EPS under all vehicle operating scenarios within TBD time (**ASIL B/C/D**).
32. Communications of the torque command between the FCEV PCM and EPS 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 (**ASIL B/C/D**).
33. The FCEV PCM is to have a mechanism to prevent unauthorized access to the propulsion torque control calculations and command path (**ASIL B/C/D**).

34. All single point faults that result in a failure to prevent unauthorized access to the FCEV PCM are to be detected and mitigated (**ASIL B/C/D**).
    - In case of unauthorized access to the FCEV PCM, the ACS/ETC 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.
35. The FCEV PCM is to be able to shut down the EPS (**ASIL C/D**).
36. The FCEV PCM is to provide BTO control (**ASIL C**). **Safety Goals: 1 through 6**
37. All electrical hardware and software elements associated with the delivery of the BTO function are to comply with **ASIL C** unless otherwise stated. **Safety Goals: 2 and 6**.
38. The FCEV PCM BTO control is to command a pre-determined torque output when both the AP and BP are pressed and when the vehicle speed is above the pre-determined threshold value, regardless of the amount of torque requested via the APPS (**ASIL C**). **Safety Goals: 1 through 6**
39. The FCEV PCM BTO control strategy is to include provisions, if necessary, for a modified control strategy if it is determined that simultaneous AP and BP applications are intended and confirmed by the driver. The modified strategy is to include a maximum allowable torque and a torque rate that will not lead to a potential violation of a safety goal (**ASIL C**). **Safety Goals: 1 through 6**
40. Critical communication and data transfer between the BPPS and the FCEV PCM 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 (**ASIL D**). **Safety Goals: 1 through 6**
41. The BTO control algorithm is to execute within TBD seconds (**ASIL C**). **Safety Goals: 1 through 6**
42. The FCEV PCM BTO control algorithm is to be checked periodically based on the correct FTTI to prevent potential violation of the safety goals (**ASIL C**). **Safety Goals: 1 through 6**
    - The appropriate fault tolerant strategies are to be applied for the BTO function, such as redundancy, voting logic, or other techniques.
    - A control flow monitoring strategy is to be applied for the BTO function.
    - In case of a fault in the BTO control algorithm that may lead to a potential failure and a potential violation of a safety goal, the system is to transition into Safe State 6 within TBD ms (200 ms is considered in the industry for similar safety goals), and the red-light driver warning is to be issued.
    - DTCs are to be set.
43. In case of a failure in the APPS and the BPPS, the ACS/ETC is to transition into Safe State 5, and a red-light driver warning is to be issued (**ASIL B/C/D**). **Safety Goals: 1 through 6**

44. All requests or commands for change in the propulsion torque by other vehicle systems are to be ignored when BTO is activated (**ASIL C**). **Safety Goals: 1 through 6**
45. In the event of FCEV PCM malfunction resulting in the loss of the BTO control function, the ACS/ETC is to be able to reduce the torque level to the pre-determined BTO level (**ASIL A/B/C**). **Safety Goals: 2 and 6**. Possible implementation strategies include:
    - Enter a safe state, and
    - Implement a BTO control function that is subordinate to the FCEV PCM BTO control function, for example in the EPS.

    The ASIL classification for this requirement depends on whether it is a part of ASIL decomposition or if it is a safety mechanism to the FCEV PCM BTO function.

46. The FCEV PCM is to open the contactors following a vehicle crash. If a HVIL fault is detected and the vehicle speed is below TBD mph, the FCEV PCM is to open the HV contactors. If the vehicle speed is above TBD mph when the HVIL fault is detected, the FCEV PCM is to send an amber warning to the driver (**ASIL B**). **Safety Goal: 7**
47. The FCEV PCM is to qualify the vehicle crash signal for validity and correctness (**ASIL B**). **Safety Goal: 7**
48. The FCEV PCM is to qualify the HVIL signal for validity and correctness (**ASIL B**). **Safety Goal: 7**
49. Diagnostics covering the failures for the following parts of the FCEV PCM are to be implemented (**ASIL QM/A/B**).
    - Execution logic (wrong coding, wrong or no execution, execution out of order, execution too fast or too slow, and stack overflow or underflow)
    - On-chip communication and bus arbitration
    - The main controller's:
        - CPU
        - processor memory
        - arithmetic logic unit
        - registers
        - A/D converter
        - signal conditioning and converting (e.g., signal filters)
        - software program execution
        - connections I/O faults (short/open/drift/oscillation)
        - power supply
        - temperature
    - If an auxiliary processor is used, then cover its:
        - CPU
        - processor memory (if auxiliary processor is used)
        - arithmetic logic unit
        - registers

    - A/D converter
    - signal conditioning and converting (e.g., signal filters)
    - software program execution
    - I/O faults (short/open/drift/oscillation)
    - power supply
    - temperature
  - The wiring harnesses and connectors for open and short circuits
  - Critical messages including CAN messages

50. The FCEV PCM is to log and save the following data every time a transition to safe state is executed due to a potential violation of a safety goal (**ASIL QM**):
    - The diagnostics information of the faults 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 the 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 (i.e., 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 is to be retained until accessed by authorized personnel.

9.2.4 Electric Powertrain Subsystem Functional Safety Requirements

As depicted in Figure 6, the EPS contains the power electronics used to drive the traction motor. This includes the TICM, gate drive board, inverter/converter, and relevant sensors. There are 28 EPS functional safety requirements derived in this project. These safety requirements correspond to all safety goals, except where otherwise noted.

1. The health and sanity of the EPS motor torque current calculation algorithm is to be checked periodically based on the correct FTTI to prevent violations of the safety goals (via an auxiliary processor or equivalent means) (**ASIL C/D**). **Safety Goals: 1 through 5**
    - The appropriate fault tolerant strategies are to be applied for the motor torque current calculation algorithm, such as redundancy, voting logic, or other techniques.
    - A control flow monitoring strategy is to be applied for the motor torque current calculation algorithm.
2. Critical communications and data transfer between the TICM and other EPS components are to be qualified for validity and correctness (plausibility and rationality). This includes the motor position sensor and diagnostics associated with the motor position determination/sensing mechanism (**ASIL B/C/D**). **Safety Goals: 1 through 5**
3. All single point EPS hardware faults that lead to potential violations of a safety goal are to be detected and mitigated within the FTTI (**ASIL B/C/D**).

- 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.

4. In case of a fault, the EPS is to communicate the fault to the FCEV PCM. The fault communication is to be checked for validity and correctness (**ASIL B/C/D**).
5. All electrical hardware and software elements associated with delivering the motor torque current to the traction motor or discharging the HV bus are to comply with A**SIL D** classification for Safety Goals 1, 4 and 6; **ASIL C** classification for Safety Goals 2, 3, and 5; and **ASIL B** classification for Safety Goals 1a and 7 unless otherwise specified. If independence of the elements (per ISO 26262) cannot be demonstrated, the higher ASIL classification is to be adopted.
6. The EPS is to deliver the motor torque current at the correct value, in the correct direction, at the correct ramp rate,[31] and at the correct time to the traction motor (**ASIL B/C/D**). **Safety Goals: 1 through 5**
    - The motor torque current direction is defined in terms of the intended direction of the output motor torque. This means that in case of a 3-phase current, the motor rotor position may have to be considered when establishing the current direction.
    - The transient response of the EPS is to be established to prevent a violation of any safety goal.
7. The EPS is to have motor torque current calculations and control algorithms for all motor speeds (**ASIL B/C/D**). **Safety Goals: 1 through 5**
8. The motor torque current calculations are to result in the correct motor torque ramp rate[32] (**ASIL C**). **Safety Goals 2 and 5**
9. If look up tables are used to determine the value of the motor torque current, the content of the tables is to be checked for correctness every time the ACS/ETC is started (**ASIL B/C/D**). **Safety Goals: 1 through 5**
10. The EPS is to deliver motor torque current to drive the motor in both the clockwise and counterclockwise directions (**ASIL B/C/D**). **Safety Goals: 1 through 5**
11. The EPS is to control the motor torque current such that the motor torque is controlled to within a pre-established tolerance band (both in magnitude and ramp rate[32]) based on the vehicle operating scenario. This tolerance band is not to result in a violation of a safety goal (**ASIL B/C/D**). **Safety Goals: 1 through 5**
12. The motor speed is to be validated against the vehicle speed (**ASIL B/C/D**). **Safety Goals: 1 through 5**
13. The motor speed and torque combination is to be validated for the driver's intended direction of travel (**ASIL B/C**). **Safety Goals: 1A and 3**
14. The motor torque current value, direction, and ramp rate[32] are to be qualified for validity and correctness (**ASIL B/C/D**). **Safety Goals: 1 through 5**

[31] The ramp rate refers to the speed increase and decrease profiles.
[32] The ramp rate refers to the speed increase and decrease profiles.

15. The motor position sensor input is to be checked for validity and correctness (**ASIL B/C/D**). **Safety Goals: 1 through 5**
16. The motor position sensor end of line calibration process capability is to be monitored (**ASIL B/C/D**). **Safety Goals 1 through 5**
17. The motor current sensor inputs are to be checked for validity and correctness (**ASIL B/C/D**). **Safety Goals: 1 through 5**
18. The transient response of the EPS is to be established to prevent a violation of any safety goal (**ASIL C/D**). **Safety Goals: 1 through 5**
19. All other critical parameters used by the motor torque current calculation algorithm that may lead to a violation of any safety goal when not correct are to be checked periodically based on the FTTI requirements (**ASIL B/C/D**). **Safety Goals: 1 through 5**
20. All faults that result in a failure to determine the motor torque current are to be detected and mitigated (**ASIL B/C/D**). **Safety Goals: 1 through 5**
    - In case of a failure to in establishing the validity and correctness of the motor torque current, the ACS/ETC is to transition into Safe State 4 and issue a red-light driver warning.
    - A DTC is to be set.
21. The EPS is to have a mechanism to prevent unauthorized access to the motor torque current calculations and command path (**ASIL B/C/D**).
22. All single point faults that result in a failure to prevent unauthorized access to the EPS are to be detected and mitigated (**ASIL B/C/D**).
    - In case of unauthorized access to the EPS, the ACS/ETC 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.
23. The EPS is to receive HV electric energy from the HV bus (**ASIL C/D**). **Safety Goals: 1 through 5**
    - If there is a fault in the HV system that may lead to a violation of a safety goal, the ACS/ETC is to transition into a safe state and a driver warning is to be issued.
24. The EPS is to have a mechanism to prevent unauthorized access to the HV bus (**ASIL B**). **Safety Goal: 7**
25. All single point faults that result in a failure to disconnect the EPS from the HV bus when unauthorized access occurs are to be detected and mitigated (**ASIL B**). **Safety Goal: 7**
    In case of a failure that leads the EPS to be unable to disconnect from the HV bus when unauthorized access occurs, the ACS/ETC is to:
    - Transition into Safe State 7 within TBD ms,
    - Issue a red-light driver warning, and
    - Set DTCs.
26. The EPS is to discharge the HV bus to a pre-determined level within the required time when requested by the FCEV PCM (**ASIL B**). **Safety Goal: 7**

27. All single point faults that result in a failure to discharge the HV bus when requested by the FCEV PCM are to be detected and mitigated (**ASIL B**). **Safety Goal: 7**
    In case of a failure that leads the EPS to be unable to disconnect from the HV bus when unauthorized access occurs, the ACS/ETC is to:
    - Transition into Safe State 7 within TBD ms,
    - Issue a red-light driver warning, and
    - Set DTCs.
28. Diagnostics covering the failures for the following parts of the EPS are to be implemented (**ASIL QM/A/B**).
    - 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:
        - CPU
        - processor memory
        - arithmetic logic unit
        - registers
        - A/D converter
        - signal conditioning and converting (e.g., signal filters)
        - software program execution
        - connections I/O faults (short/open/drift/oscillation)
        - power supply
        - temperature
    - If an auxiliary processor is used, then cover the following.
        - CPU
        - processor memory (if auxiliary processor is used)
        - arithmetic logic unit
        - registers
        - A/D converter
        - signal conditioning and converting (e.g., signal filters)
        - software program execution
        - I/O faults (short/open/drift/oscillation)
        - power supply
        - temperature
    - The motor position sensor
    - The motor current sensors
    - The wiring harnesses and connectors for open and short circuits
    - Critical messages, including CAN messages

9.2.5 Communication Signal Functional Safety Requirements

There are five functional safety requirements for the communication signals, each corresponding to all safety goals.

The critical communication signals include the following.

- APPS signals from the APPS to FCEV PCM
- APPS fault diagnostics signal
- BPPS signal to FCEV PCM
- Communication channel "secure" signals between FCEV PCM and EPS
- Communication channel "secure" signals between FCEV PCM and the following:
  - ACC/CC
  - AEB
  - RESS
  - Fuel cell system
  - Other systems that can request modification to the propulsion torque
- Commands/requests for propulsion torque modifications from interfacing systems to FCEV PCM
- Vehicle speed signal
- Vehicle direction signal
- Command for torque from the FCEV PCM to the EPS
- EPS fault diagnostics signals
- Motor speed sensor signal to TICM
- Motor position sensor signal to TICM
- Driver warning signals
- Unauthorized access to HV bus signal from the EPS to RESS controller
- Low voltage power loss from the low voltage power system to FCEV PCM signal
- Communication bus signal failure from the communication bus to the FCEV PCM

1. 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. In case of a fault in any critical signal, the system detecting the fault is to (**ASIL B/C/D**):
   - Inform the FCEV PCM of the fault, and
   - Invoke the correct failure mode effect mitigation strategy.
2. The communication bus is to support the communication of the ACS/ETC with the other vehicle systems in order to support the safe operation of the ACS/ETC (**ASIL B/C/D**).
3. The communication bus is to support the qualification of all critical communication signals between the ACS/ETC and the interfacing vehicle systems (**ASIL B/C/D**).

4. The communication bus is to prevent the corruption of the critical communication signals during transmission between the ACS/ETC and the interfacing vehicle systems (**ASIL B/C/D**).
5. In case of malfunction of the communication bus or communication bus module, the communication bus system is to inform the FCEV PCM (**ASIL B/C/D**).

9.2.6 Power Supply Functional Safety Requirements

There are seven functional safety requirements for the low and high voltage power supplies. These requirements correspond to all safety goals, except where otherwise specified.

1. The ACS/ETC is to have a redundant low voltage power supply (**ASIL C/D**). **Safety Goals: 1 through 5**
    - In case of a fault in the low voltage power system, the redundant power supply is to activate within TBD ms and sustain the low voltage power supply to the vehicle for a duration greater than the longest FTTI.
2. The low voltage power supply is to provide the ACS/ETC and interfacing systems and sensors with the required 12-volt power supply for operation (**ASIL B/C/D**).
3. The supply voltage and current are to meet the requirements on the quality parameters (levels (min, max), ripple, transient, and overshoot) as set by the ACS/ETC system components and interfacing systems and sensors. The ASIL classification of this requirement is to be based on the safety analysis and the safety goal impacted (**ASIL B/C/D**).
4. The ACS/ETC is to be notified of any malfunction or disruption in the 12-volt power supply system operation (**ASIL B/C/D**).
5. All communications and data transfer sent by the low voltage power system to the FCEV ACS/ETS are to be qualified for validity and correctness (plausibility and rationality). This includes the low voltage power system diagnostics information (**ASIL B/C/D**).
6. In case of a malfunction, the low voltage power supply is to maintain the 12-volt power supply to the ACS/ETC, interfacing systems, and sensors for a time that is longer than the longest FTTI of the ACS/ETC (**ASIL B/C/D**).
7. All single point failure modes that cause the loss of low voltage power are to be prevented or mitigated. The ACS/ETC is to transition to Safe State 4 in case of the loss or malfunction of the vehicle's low voltage power system and red-light driver warning is to be issued to the driver (**ASIL D**).

9.2.7 Interfacing Systems Functional Safety Requirements

There are five functional safety requirements for the interfacing systems. These functional safety requirements correspond to all safety goals unless otherwise noted.

1. All requests or commands for propulsion torque modifications or HV bus discharge from vehicle interfacing systems are to be sent to the FCEV PCM (**ASIL B/C/D**). This includes the following.
    - Requests for torque increases or decreases from the CC/ACC system
    - Requests for torque reduction from the braking system including the AEB module (directly or indirectly through the braking system module)
    - Requests for torque modification from the TCS
    - Requests for torque modification from the electronic stability control system
    - Requests for regenerative braking
    - Requests for discharging the HV bus
2. All communications and data transfer regarding requests or commands for propulsion torque modifications sent by the vehicle interfacing systems to the FCEV PCM are to be qualified for validity and correctness (plausibility and rationality) by the sending system (**ASIL D**). **Safety Goals: 1 through 6**
3. All interfacing systems are to inform the FCEV PCM in case of any failure that may cause the system, and the ACS/ETC, to transition into a degraded mode of operation (**ASIL B/C/D**).
4. In case of a fault in the transmitted information to the FCEV PCM from the interfacing system, the correct failure mode effect mitigation strategy is to be applied (**ASIL B/C/D**).
5. When opened following a vehicle crash or HVIL fault, the contactors are to remain open until the integrity of the HV system has been confirmed. Some examples for confirming the integrity of the HV system may include successful system self-checks and removal of faults (**ASIL B**). **Safety Goal: 7**

9.3 Additional Safety Requirements beyond the Scope of the ISO 26262 Functional Safety Concept

This study performs comprehensive hazard and safety analysis. In addition, this study also considers the risk reduction measures recommended by the system safety standard—MIL-STD-882E in order to ensure the generation of a comprehensive list of safety requirements.

- Eliminate hazards through design selection
- Reduce risk through design alteration

Subsequently, this study identifies additional 88 safety requirements related to the ACS/ETC system and components. Many of these requirements also support the main elements of the safety strategies listed in Section 8.1. They fall into the following categories.

1. General FCEV ACS/ETC System – 17 requirements
2. AP Assembly – 3 requirements
3. FCEV PCM – 27 requirements
4. EPS – 13 requirements

5. Communication Signals – 4 requirements
6. Power Supply (low and high voltage) – 3 requirements
7. Interfacing Systems – 21 requirements

9.3.1 General FCEV ACS/ETC System-Level Safety Requirements

This study identifies 17 general system-level safety requirements for the FCEV ACS/ETC system outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262). These requirements correspond to all safety goals, unless otherwise specified.

1. The packaging for the ACS/ETC components and connections is to provide sufficient static and dynamic clearances (**ASIL B/C/D**).
2. The ACS/ETC components and connections are to be protected from physical interference from foreign objects (e.g., road debris) (**ASIL B/C/D**).
3. The ACS/ETC assemblies are to be free of manufacturing defects. This includes both the component manufacturing quality as well as the quality of the connections between components in the assembly process (**ASIL B/C/D**).
4. The calibration of the safety critical sensors, safety critical actuators, and other safety critical parameters is to be checked and verified to be correct. This includes interfacing sensors and actuators that are critical to the safe functioning of the ACS/ETC (**ASIL B/C/D**).
   Typical safety critical sensors include the following.
   - APPS
   - BPPS
   - Motor speed/position sensor
   - Phase/current sensor
   - Inverter temperature sensor
   - Transmission range sensor
   - Vehicle speed sensor (may be provided by the brake/stability control module)
   - Battery state-of-charge (may be provided by the RESS control module)
   - Crash signal (may be provided by the occupant restraint system control module)

   Typical safety critical actuators include the following.
   - Inverter/converter (power stage)
   - Gate drive board

   Other typical safety critical components include the following.
   - Inverter cooler parameters
   - Traction motor parameters
5. ACS/ETC sensors are to have TBD reporting frequency such that safety critical data is updated with sufficient frequency to prevent violation of a safety goal (**ASIL B/C/D**).
   Safety Goals: 1 through 6

Typical ACS/ETC sensors include:

- APPS,
- Motor speed/position sensor,
- Phase/current sensor, and
- Inverter temperature sensor.

6. The ACS/ETC components are to meet the reliability and functional degradation requirements (**ASIL B/C/D**).
7. Safety critical ACS/ETC sensors and actuators are to have TBD failure rate for 100,000 miles and under all normal (TBD) vehicle operating conditions (temperature, vibration, moisture, etc.) (**ASIL C/D**).
   Failures may include the following.
   - Hardware failure
   - Degradation over time
   - Internal short and increased resistance

   Safety-critical sensors may include the following.
   - APPS
   - Motor speed/position sensor
   - Phase/current sensor
   - Inverter temperature sensor

   Safety-critical actuators may include the following.
   - Gate drive board
   - Inverter/converter (power stage)
8. The ACS/ETC components and connections are to meet the standards for EMI/EMC with the environment and the vehicle in order to prevent malfunctioning of the FCEV PCM, TICM, corruption of critical parameters including the torque maps, and corruption of software algorithms (**ASIL B/C/D**).
9. The ACS/ETC components and connections are to meet the contamination ingress protection requirements and the corrosion protection requirements. This includes moisture, corrosion, or contamination from the environment or other vehicle components (**ASIL B/C/D**).
10. The ACS/ETC components and connections are to meet the vibration and shock impact requirements (**ASIL B/C/D**).
11. The ACS/ETC components and connections are to meet the ambient temperature requirements considering the packaging location in the vehicle. The temperatures of the ACS/ETC components are to be monitored (**ASIL B/C/D**).
12. The ACS/ETC components and connections are to be designed to prevent organic growth from the external environment that affects the safe functioning of the ACS/ETC (**ASIL B/C/D**).

13. The ACS/ETC system and components are to mitigate the effects of magnetic interference from other vehicle components, as well as the external environment (**ASIL B/C/D**).
14. The ACS/ETC is to be designed to prevent damage to vehicle components and connections (including other ACS/ETC components and connections) by the HV circuit (e.g., electrical arcing, corona effects, back EMF, etc.). This includes damage to low-voltage electronic components, such as microprocessors (**ASIL B/C/D**).
15. Unused connection terminals are to be sealed to prevent the ingress of moisture, corrosion, and contamination from the external environment or other systems in the vehicle (**ASIL B/C/D**).
16. Third party manufactured accessories placed in the driver's foot well are not to interfere with the free movement of the AP or BP, or operation of the APPS or BPPS (**No ASIL - not within the scope of ISO 26262**). **Safety Goals: 1 through 6**
17. The AP and BP are to return to the at-rest (i.e., undepressed) position when released by the driver (**No ASIL - not within the scope of ISO 26262**). **Safety Goals: 1 through 6**

9.3.2 Accelerator Pedal Assembly Safety Requirements

This study identifies three safety requirements for the AP assembly outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262). These requirements correspond to all safety goals.

1. AP assembly mechanical faults that result in incorrect measurement of the APP are to be detected and mitigated (**ASIL QM**).
   - Incorrect measurements include deviations from the correct APP value or being stuck at the same value permanently or intermittently.
2. The AP assembly critical mechanical components, including the AP connection to the APPS, are to meet the life and durability requirements of TBD miles without any critical failures (**ASIL C/D**).
3. The AP assembly foot well is to allow for free AP movement and operation of the APPS in the presence of reasonable everyday objects (**No ASIL - not within the scope of ISO 26262**).

9.3.3 FCEV Powertrain Control Module Safety Requirements

This study identifies 27 FCEV PCM safety requirements outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262). These requirements correspond to all vehicle-level safety goals, unless otherwise specified.

1. In case of a fault in the activation delay or transition time, the ACS/ETC is to invoke the proper fault mitigation strategy including, if required, transitioning to a safe state (**ASIL B/C/D**).

2. The FCEV PCM is to monitor the CPU temperature and is to maintain the CPU temperature within the acceptable operating range (**ASIL B/C/D**).
3. The ACS/ETC software development process is to comply with the state-of-the-art standards for software development such as ISO/IEC 15504 and Motor Industry Software Reliability Association (MISRA) C/C++ (**ASIL B/C/D**).
4. The FCEV PCM software algorithm is to correctly write to memory (**ASIL B/C/D**). **Safety Goals: 1 through 6**
5. The FCEV PCM is to correctly calculate the motor torque required for maintaining the creep speed, and the results are to be qualified for validity and correctness under all vehicle operating conditions (**ASIL B/C/D**). **Safety Goals: 1 through 6**
6. The FCEV PCM is to have specific conditions for entering a degraded operating state (e.g., the "limp-home" mode), and is not to enter a degraded operating state unless these conditions are met. The driver is to be notified when the FCEV PCM enters a degraded operating state (**ASIL B/C/D**). **Safety Goals: 1 through 6**
7. The FCEV PCM software code is to be verified for correctness, including any automatically generated code (**ASIL B/C/D**).
8. The FCEV PCM is to verify the correctness of all clock or internal FCEV PCM timing signals (**ASIL B/C/D**).
9. Any unused circuits or pins in the FCEV PCM are to be properly managed to prevent unwanted signals or other interference with the FCEV PCM function (**ASIL B/C/D**).
10. The FCEV PCM is to have TBD reliability over the lifetime of the vehicle and under all vehicle operating conditions (such as temperature, vibration, moisture, etc.) (**ASIL C/D**). This includes, but is not limited to the following.
    - The IC board
    - The memory block
    - The CPU
    - Other electric/electronic subcomponents
11. The FCEV PCM is to detect erroneous torque commands issued by malicious intruders or aftermarket components (**ASIL C/D**). **Safety Goals: 1 through 6**
12. The FCEV PCM is to enter or exit BTO mode at the correct time when the conditions for entering or exiting BTO mode are met (dead-time, activation delay, vehicle speed, APP and BPP, etc.) (**ASIL C**). **Safety Goals: 1 through 6**
13. The FCEV PCM BTO control algorithm is to enter BTO mode when the driver presses both the AP and BP simultaneously and the vehicle speed is above the pre-set vehicle speed threshold value for BTO. If the vehicle speed is below the pre-set vehicle speed threshold value for BTO, then the FCEV PCM is not to enter BTO mode. The FCEV PCM is to monitor the vehicle speed (**ASIL C**). **Safety Goals: 1 through 6**
14. The FCEV PCM is not to enter BTO mode when the BP is not pressed (**ASIL C**). **Safety Goals: 1 through 6**

15. The FCEV PCM is not to exit BTO mode while both the AP and BP are still pressed (**ASIL C**). **Safety Goals: 1 through 6**
16. The FCEV PCM BTO control model design is to be verified and validated for correctness, including pedal sequencing, critical process parameters, and timing (**ASIL C**). **Safety Goals: 1 through 6**
17. Incorporating additional requirements into the BTO algorithm beyond the APP, BPP, and vehicle speed is not to prevent the FCEV PCM from entering BTO mode when the driver's intention is to stop the vehicle (**ASIL C**). **Safety Goals: 1 through 6**
18. Incorporating additional requirements into the BTO algorithm beyond the APP, BPP, and vehicle speed is not to prevent the FCEV PCM from exiting BTO mode when the driver's intention is to resume acceleration (**ASIL C**). **Safety Goals: 1 through 6**
19. The FCEV PCM is not to command an increase in the traction motor torque output while in BTO mode or while transitioning into BTO mode (**ASIL C**). **Safety Goals: 1 through 6**
20. Other vehicle systems are not to have the authority to command the FCEV PCM to exit BTO mode (**ASIL C**). **Safety Goals: 1 through 6**
21. The FCEV PCM is not to command an increase in the traction motor torque output when exiting BTO mode unless the driver increases the angular position of the AP and all other conditions for exiting BTO mode are met (**ASIL C**). **Safety Goals: 1 through 6**
22. When entering normal mode, the FCEV PCM is to resume responding to the driver's torque request via the AP (**ASIL C**). **Safety Goals: 1 through 6**
23. In case of a fault entering BTO mode or entering normal mode, the FCEV PCM is to invoke the proper fault mitigation strategy, including transitioning into a safe state, if required, and alerting the driver (**ASIL C**). **Safety Goals: 1 through 6**
24. If the FCEV PCM issues an HV DC power request to the HV power systems (i.e., RESS and fuel cell system), the required HV DC is to be properly calculated based on the desired propulsion torque output (**ASIL C/D**). **Safety Goals: 4 and 5**
25. If the FCEV PCM issues as HV DC power request to the HV power systems (i.e., RESS and fuel cell system), the HV DC power request is to be qualified for validity and correctness (**ASIL C/D**). **Safety Goals: 4 and 5**
    - In the event of a fault in requesting HV DC power, the ACS/ETC is to transition to the appropriate safe state and a red-light driver warning is to be issued.
26. The FCEV PCM is to supply the correct reference voltage to the ACS/ETC sensors (**ASIL B/C/D**).
27. The FCEV PCM is to detect disruptions in the reference voltage supplied to the ACS/ETC sensors (too high, too low, missing, etc.) and transition into the appropriate safe state (**ASIL A/B**).

9.3.4 Electric Powertrain Subsystem Safety Requirements

This study identifies 13 safety requirements for the EPS outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262). These requirements trace back to all safety goals.

1. The TICM is to have TBD reliability over the lifetime of the vehicle and under all vehicle operating conditions (temperature, vibration, moisture, etc.) (**ASIL C/D**). **Safety Goals: 1 through 5, and 7**
   This includes, but is not limited to the following.
   - The IC board
   - The memory block
   - The CPU
   - Other electric/electronic subcomponents
2. The TICM is to monitor its CPU temperature and is to maintain the CPU temperature within the acceptable operating range (**ASIL B/C/D**). **Safety Goals: 1 through 5, and 7**
3. Any unused circuits or pins in the TICM are to be properly managed to prevent unwanted signals or other interference with the TICM function (**ASIL B/C/D**). **Safety Goals: 1 through 5, and 7**
4. The TICM is to verify the correctness of all clock or internal timing signals (**ASIL B/C/D**). **Safety Goals: 1 through 5, and 7**
5. The TICM software code is to be verified for correctness, including any automatically generated code (**ASIL B/C/D**). **Safety Goals: 1 through 5, and 7**
6. The TICM software algorithm is to correctly write to memory (**ASIL B/C/D**). **Safety Goals: 1 through 5, and 7**
7. The TICM is to have specific conditions for entering a degraded operating state (e.g., "limp-home" mode) and is not to enter a degraded operating state unless these conditions are met. The FCEV PCM and the driver are to be notified when the TICM enters a degraded operating state (**ASIL B/C/D**).
8. The EPS is to detect erroneous torque commands issued by malicious intruders or aftermarket components, including commands to the gate drive board to disable the traction motor (**ASIL C/D**).
9. The HV power supply to the traction motor that meets the requirements for quality (e.g., transients, phase, spikes, noise, etc.) (**ASIL QM**). **Safety Goals: 1 through 5**
   - This includes any conditioning or converting (e.g., boost or buck conversion) of the voltage supply from the fuel cell system.
10. The ACS/ETC is to maintain the inverter/converter temperature within the operating range. This includes ensuring proper calibration of safety critical parameters for the cooling system (**ASIL B/C/D)**. **Safety Goals: 1 through 5**
    - If the inverter/converter temperature cannot be maintained within the acceptable operating range, the ACS/ETC is to enter the appropriate safe state and warn the driver.

- If the cooling system does not operate continually, this includes ensuring the cooling system is operated with the correct timing and duration.

11. The inverter cooling system is to provide sufficient cooling for the inverter/converter under all vehicle operating conditions. If the inverter cooling system also supplies cooling for other vehicle components (e.g., the traction motor), then cooling system is to be able to provide sufficient cooling for all connected components under all vehicle operating conditions (**ASIL B/C/D**). **Safety Goals: 1 through 5**
12. The ACS/ETC is to detect failures in the cooling system, including the coolant delivery mechanism (hoses, piping, ducts, etc.). In the event of a failure in the cooling system, the ACS/ETC is to enter the appropriate safe state to prevent further violation of any safety goals (**ASIL B/C/D**). **Safety Goals: 1 through 5**
13. The inverter temperature sensor is to be positioned to ensure accurate and representative measurements of the inverter/converter temperature (**ASIL A/B**). **Safety Goals: 1 through 5**

9.3.5 Communication Signals Safety Requirements

This study identifies four safety requirements for critical communication signals that are outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262). These requirements correspond to all safety goals.

The critical communication signals include the following.

- APPS signals from the APPS to FCEV PCM
- APPS fault diagnostics signal
- BPPS signal to FCEV PCM
- Communication channel "secure" signals between FCEV PCM and EPS
- Communication channel "secure" signals between FCEV PCM and the following:
  - ACC/CC
  - AEB
  - RESS
  - Fuel cell system
  - Other systems that can request modification to the propulsion torque
- Commands/requests for propulsion torque modifications from interfacing systems to FCEV PCM
- Vehicle speed signal
- Vehicle direction signal
- Command for torque from the FCEV PCM to the EPS
- EPS fault diagnostics signals
- Motor speed sensor signal to TICM
- Motor position sensor signal to TICM

- Driver warning signals
- Unauthorized access to HV bus signal from the EPS to the RESS and fuel cell system controllers
- Crash signal from the occupant restraint system control module to FCEV PCM
- Low voltage power loss from the low voltage power system to FCEV PCM signal
- Communication bus signal failure from the communication bus to the FCEV PCM

1. The communication bus signal prioritization strategy is to allow the TBD reporting frequency for data critical to the safe functioning of the ACS/ETC. The reporting frequency is to allow for the timely update of safety-critical data to prevent violation of any safety goals (**ASIL QM/A/B**).
2. The FCEV PCM is to detect intermittent communication signals in the ACS/ETC system (**ASIL QM/A/B**).
3. The communication bus is to be secured against unauthorized access (**ASIL B/C/D**).
4. Interfacing vehicle systems are to detect and inform the FCEV PCM of intermittent communication signals between safety critical sensors and the ACS/ETC (**ASIL QM/A/B**).

9.3.6 Power Supply Safety Requirements

This study identifies three safety requirements for the power supply that are outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262). These requirements correspond to all safety goals, unless otherwise specified.

1. In the event of a vehicle crash, the low voltage power supply is to maintain the low voltage power supply to the ACS/ETC for a sufficient duration to allow discharging of the HV bus and opening of the contactors (**ASIL B**). **Safety Goal: 7**
2. The necessary supply voltage is to be supplied to interfacing sensors critical to the safe operation of the ACS/ETC and is to meet the quality parameters (levels (min, max), ripple, transient, and overshoot) as set by these safety-critical sensors. The ASIL classification of this requirement is to be based on the safety analysis and the safety goal impacted (**ASIL B/C/D**). **Safety Goals: 1 through 5**
   Typical safety critical interfacing sensors include:
   - BPPS
   - Transmission range sensor
   - Vehicle speed sensor (may be provided by the brake/stability control module)
   - Battery state-of-charge sensor (may be provided by the RESS control module)
   - Crash sensor (may be provided by the occupant restraint system control module)

3. If the HV DC power supplied to the ACS/ETC cannot be increased at a rate to achieve the requested propulsion torque ramp rate,[33] the ACS/ETC is to transition into Safe State 3. An amber light driver warning is to be issued (**ASIL C**). **Safety Goals: 2 and 5**

9.3.7 Interfacing Systems Safety Requirements

This study identifies 21 safety requirements for interfacing vehicle systems that are outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262). These requirements correspond to all safety goals, unless otherwise specified.

1. The interfacing system components critical to the safe functioning of the ACS/ETC are to meet the reliability and functional degradation requirements (**ASIL B/C/D**).
2. Interfacing sensors critical to the safe functioning of the ACS/ETC are to have TBD failure rate for 100,000 miles and under all normal (TBD) vehicle operating conditions (temperature, vibration, moisture, etc.) (**ASIL QM**). **Safety Goals: 1 through 5**
   Sensor failures may include the following.
   - Hardware failure
   - Degradation over time
   - Internal short and increased resistance

   Typical safety critical interfacing sensors include the following.
   - BPPS
   - Transmission range sensor
   - Vehicle speed sensor (may be provided by the brake/stability control module)
   - Battery state-of-charge sensor (may be provided by the RESS control module)
   - Crash signal (may be provided by the occupant restraint system control module)
3. The packaging for interfacing system components and connections critical to the safe functioning of the ACS/ETC is to meet the standards for packaging clearances (**ASIL B/C/D**).
4. The interfacing system components and connections critical to the safe functioning of the ACS/ETC (e.g., vehicle speed, battery state-of-charge, transmission range, etc.) are to be designed to meet the ambient temperature requirements, considering the packaging location in the vehicle (**ASIL B/C/D**).
   - The temperatures of the interfacing system sensors critical to the safe functioning of the ACS/ETC (e.g., transmission range sensor, vehicle speed sensor, battery state of charge sensor, etc.) are to be monitored.
5. The interfacing system components and connections critical to the safe functioning of the ACS/ETC are to be protected from physical interference from foreign objects (e.g., road debris) (**ASIL B/C/D**).

[33] The ramp rate refers to the speed increase and decrease profiles.

6. The interfacing system assemblies critical to the safe functioning of the ACS/ETC are to be free from manufacturing defects. This includes component and connection manufacturing quality in the assembly process (**ASIL B/C/D**).
7. The interfacing vehicle system components and connections critical to the safe functioning of the ACS/ETC are to meet the standards for EMI/EMC and other electrical interference from the environment and other components in the vehicle (**ASIL B/C/D**).
8. The interfacing system components and connections critical to the safe functioning of the ACS/ETC are to meet the contamination ingress protection requirements and the corrosion protection requirements. This includes moisture, corrosion, or contamination from the environment or other vehicle components (**ASIL B/C/D**).
9. The interfacing system components and connections critical to the safe functioning of the ACS/ETC are to meet the vibration and shock impact requirements (**ASIL B/C/D**).
10. The interfacing system components and connections are to be designed to prevent organic growth from the external environment that could affect the safe functioning of the ACS/ETC (**ASIL B/C/D**).
11. The interfacing system components critical to the safe functioning of the ACS/ETC are to mitigate the effects of magnetic interference from other vehicle components, as well as the external environment (**ASIL B/C/D**).
12. Interfacing sensors critical to the safe functioning of the ACS/ETC are to have TBD reporting frequency so that the safety critical data is updated with sufficient frequency to prevent violation of a safety goal (**ASIL B/C/D**). **Safety Goals: 1 through 5**
    Typical safety critical interfacing sensors include the following.
    - BPPS
    - Transmission range sensor
    - Vehicle speed sensor (may be provided by the brake/stability control module)
    - Battery state-of-charge sensor (may be provided by the RESS control module)
    - Crash signal (may be provided by the occupant restraint system control module)
13. Software code for control modules in interfacing systems that are critical for the safe functioning of the ACS/ETC is to be verified for correctness, including any automatically generated code (**ASIL B/C/D**).
    This may include the following control modules.
    - Brake/stability control module (if used to process and communicate vehicle speed information)
    - RESS control module
    - Fuel cell system control module
    - Occupant restraint system controller (crash signal)
14. Propulsion torque modification capable systems are to correctly identify themselves according to the FCEV PCM prioritization strategy when issuing torque requests to the FCEV PCM (**ASIL B/C/D**). **Safety Goals: 1 through 6**

15. The traction motor is to prevent locked motor rotor conditions (**ASIL B/C/D**). **Safety Goals: 1 through 5**
    - In case of a failure to prevent a locked rotor condition, the vehicle system controller is to transition into Safe State 6, and a red-light driver warning is to be delivered to the driver.
16. The BPP value is to be measured, and the value is to be valid and correct (**ASIL B/C/D**). **Safety Goals: 1 through 5**
17. The BP assembly foot well is to allow for free pedal movement and operation of the BBPS in the presence of reasonable everyday objects (**No ASIL — not within the scope of ISO 26262**). **Safety Goals: 1 through 5**.
18. The BP assembly critical mechanical components, including the BP connection to the BPPS, are to meet the life and durability requirements without any critical failures (**No ASIL — not within the scope of ISO 26262**). **Safety Goals: 1 through 5**
19. BP mechanical assembly faults that result in incorrect measurement of the BPP are to be detected and mitigated (**No ASIL — not within the scope of ISO 26262**). **Safety Goals: 1 through 5**
    - Incorrect measurements include deviations from the correct BPP value or being stuck at the same value permanently or intermittently.
20. Interfacing sensors critical to the safe functioning of the ACS/ETC are to have the correct reference voltage supply (**ASIL B/C/D**). **Safety Goals: 1 through 5**
    Safety-critical interfacing sensors may include the following.
    - BPPS
    - Transmission range sensor
    - Vehicle speed sensor (may be provided by the brake/stability control module)
    - Battery state-of-charge sensor (may be provided by the RESS control module)
    - Crash signal (may be provided by the occupant restraint system control module)
21. Interfacing systems are to inform the FCEV PCM of any disruptions to the reference voltage supplied to sensors critical to the safe functioning of the ACS/ETC (too high, too low, missing, etc.) (**ASIL B/C/D**).

10 OBSERVATIONS

This study follows the process in the ISO 26262 Concept Phase to develop safety requirements for the FCEV ACS/ETC system. This section discusses three observations made from applying the ISO 26262's ASIL assessment approach.

10.1 Automotive Safety Integrity Level May Depend on a Feature's Operational Situations

In ISO 26262 the ASIL assessment approach requires the safety analyst to review every vehicle operational situation and assign an ASIL for the hazard of interest. At the end, the hazard takes the most severe ASIL among all operational situations.

However, for a feature that may not be used in all the vehicle operational situations, the ASIL could be too stringent. This project identified at least one feature that only operates in a subset of the operational situations — the hill-holder feature only operates when the vehicle speed is zero. The ASIL for operational situations when vehicle speed is zero is much less severe than the worst-case operational situation, mainly due to the lower severity at the lower speed (this assumes the vehicle does not reach high speeds, which may have higher severity). Therefore, H1.a has an ASIL B, while H1 has an ASIL D (Table 23).

Therefore, the following approach may be considered in future ASIL assessments.

1. Treat the vehicle as a black box with no assumptions about its designs and features. Choose the most severe ASIL for each hazard.
2. When designing a vehicle feature, review the operational situations used for the ASIL assessment. If the feature only operates in a subset of the operational situations, choose the ASIL for that feature based on the most severe ASIL within that subset of operational situations.

10.2 Generation of Operational Situations

The current industry practice generates the operational situations based on safety experts' experiences as well as known drive cycles. This study initially followed this approach. After reviewing the operational situations generated relying on industry knowledge, Table 17 was generated to characterize the variables considered. Using this variable list, this study generated an exhaustive combination of all the variables and their states, and compared this exhaustive combination with the operational situations identified using industry knowledge. The comparison found additional operational situations. These additional operational situations were then further assessed and added.

Furthermore, when reviewing the variables and their states in Table 17, this study also realized that it was possible to further extend and improve this list using the variables and codes specified in NHTSA's vehicle crash databases [18]. In addition, naturalistic driving data may also help

contribute to the variable list. The benefits of using the variables in the existing NHTSA databases could include:

- Leveraging prior work to help make the operational situations more comprehensive.
- Potentially only performing the analysis once for all vehicle motion-related hazards. The resulting comprehensive operational situations may be applicable to all current and future safety analyses.
- Connect the operational situations to crash data and naturalistic driving data, which may facilitate the quantitative analysis for severity and exposure.

Therefore, the following may be considered for future improvements of the ASIL assessment approach:

1. Develop a comprehensive variable list describing the vehicle operational situations based on NHTSA's crash databases and naturalistic driving data sets.
2. The exhaustive combinations of the identified variables and their states may create a long list of operational situations. Develop a method to efficiently examine the operational situations for each vehicle-level hazard.

10.3 Variations in the Automotive Safety Integrity Level Assessment

In the course of this study, not all safety analysts on the project team agreed to the same assessment for exposure and controllability. This is due to the fact that objective data typically do not exist to support the assessment, and expert opinions are often used. This observation corroborates previous assessments of ISO 26262 [19] [20].

ISO 26262 recommends the use of expert inputs when objective data are not available. This helps the completion of the ASIL assessment. However, there are drawbacks to this approach. With regards to exposure, psychologists studying human decision making have shown that humans are not good at predicting truly random events, especially rare events [21]. For example, the availability of an event in the risk analyst's mind, and how vividly the event is described, heavily influence the subjective probability assessment. Therefore, the assessment of exposure may vary among safety experts and it is difficult to decide who is right in the absence of objective data [19] [20].

In addition, ISO 26262 assesses controllability based on average/majority drivers' ability to retain control of the vehicle in a certain operational situation. However, the standard provides no definition on the ability of the average/majority driver.

The following may be considered to potentially improve the severity, exposure, and controllability assessments.

- Statistics from the NTHSA crash databases are available to support the assessment of severity.

- Statistics for the assessment of exposure could be derived from the naturalistic driving scenarios.
- Statistics are not publicly available for the assessment of controllability. Further investigations are needed to understand how to more rigorously assess controllability using objective data.

11 POTENTIAL USE OF STUDY RESULTS

The results of this study may be useful in the following ways:

- This study derives 202 potential safety requirements for the FCEV ACS/ETC system following the Concept Phase process (Part 3) in ISO 26262 standard. These requirements may serve as an illustration of the process for the automotive industry to review and compare with their own functional safety requirements.
- For practitioners who are not yet following the ISO 26262 process, this study may provide additional insights on the process of deriving functional safety requirements for an FCEV ACS/ETC system.
- This study applies three hazard and safety analysis methods — the HAZOP study, Functional FMEA, and STPA. While the automotive industry is familiar with the HAZOP study and Functional FMEA, STPA is a relatively new method. For those who are following the ISO 26262 process for functional safety, this study may serve as an example of the use and results of STPA.

12 CONCLUSIONS

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

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

ID	Safety Goals	ASIL
SG 1	Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 for a period greater than TBD s is to be mitigated in accordance to the identified ASIL level.	D
SG 1a	Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 with zero speed at start is to be mitigated in accordance to the identified ASIL level.	B
SG 2	Potential insufficient vehicle propulsion[i] is to be mitigated in accordance to the identified ASIL level.	C[ii]
SG 3	Potential vehicle movement in the wrong direction is to be mitigated in accordance to the identified ASIL level.	C
SG 4	Potential propulsion power loss/reduction resulting in vehicle deceleration greater than TBD m/s^2 is to be mitigated in accordance to the identified ASIL level.	D
SG 5	Potential insufficient vehicle deceleration[i] is to be mitigated in accordance to the identified ASIL level.	C[ii]
SG 6	The ACS/ETC control algorithm is to choose the torque command that has the highest priority for safety in accordance to the identified ASIL level.	D
SG 7	Potential electric shock is to be mitigated in accordance to the identified ASIL level.	B

i. *Insufficient vehicle propulsion/deceleration is defined as the vehicle deviating from the correctly functioning speed increase/decrease profile under any operating conditions by more than TBD sigma. These hazards specifically relate to speed increases or decreases that result from the driver increasing or decreasing the angular position of the AP.*

ii. *The ASIL assessment for the hazard associated with this safety goal varied among safety analysts in the absence of objective data. This study finds that objective data are not readily available for the assessment of the three dimensions used to determine the ASIL--severity, exposure, and controllability.*

As shown by SG 2 and SG 5 in the above table, ASIL assessments can vary between analysts without the support of objective data. Variations in the ASIL assessment may lead to different safety requirements for the same hazard.

- Data to support assessment of severity may be available from NHTSA's crash databases.
- Data to support assessment of exposure are not readily available, but may be derived from naturalistic driving data sets.
- No publicly available data are available to support assessment of controllability.

2. Developed the functional safety concept and identified 114 illustrative 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 FCEV ACS/ETC System – 11 requirements
    - AP Assembly – 8 requirements
    - FCEV PCM – 50 requirements
    - EPS – 28 requirements
    - Communication Signals – 5 requirements
    - Power Supply (low and high voltage) – 7 requirements
    - Interfacing Systems – 5 requirements

3. Identified an additional 88 illustrative safety requirements based on the comprehensive results of the safety analyses (Functional FMEA and STPA), and by following the additional safety strategy in the military standard MIL-STD-882E. The breakdown of the number of requirements is as follows.

    - General FCEV ACS/ETC System – 17 requirements
    - AP Assembly – 3 requirements
    - FCEV PCM – 27 requirements
    - EPS – 13 requirements
    - Communication Signals – 4 requirements
    - Power Supply (low and high voltage) – 3 requirements
    - Interfacing Systems – 21 requirements

    These 88 requirements are out of the scope of the Functional Safety Concept phase in ISO 26262 (Part 3 of ISO 26262). However, subsequent steps in the ISO 26262 process — Systems Engineering (Part 4), Hardware Development (Part 5), and Software Development (Part 6) — cascade the Functional Safety Concept requirements into additional development-specific safety requirements, and may identify these 88 requirements.

REFERENCES

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

[3] Department of Defense. (2012). Department of Defense Standard Practice: System Safety (MIT-STD-882E). Washington, DC: Author.

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

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

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

[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*, p. 97-140.

[9] Toyota Motor Sales, UCA, Inc. (2010, March 19). FCV Fuel Cell Vehicle (Web page). Retrieved on June 20, 2016, from the Toyota website at www.toyota-global.com/innovation/environmental_technology/fuelcell_vehicle/

[10] Hyundai Motor UK. (n.a.). Hydrogen Fuel Cell Powered Cars. (Web page). Retrieved from the Hyundai web site on June 20, 2016, from www.hyundai.co.uk/about-us/environment/hydrogen-fuel-cell#technology

[11] Honda Motor Co., Ltd. (2016). Clarity Fuel Cell Technology (Web page). Retrieved from the Honda web site on June 20, 2016, at http://world.honda.com/CLARITY/technology/index.html

[12] Larminie, J., & Dicks, A. (2003). *Fuel cell systems explained* (2nd ed.), West Sussex, UK: John Wiley & Sons Ltd.

[13] Abuelsamid, S. (2010, March 29). BMW technik working on hybrid fuel cell 1 series concept (Web log post). Retrieved from www.autoblog.com/2010/03/29/bmw-technik-working-on-hybrid-fuel-cell-1-series-concept/

[14] Toyota Motor Sales, UCA, Inc. (2010, March 19). Brake Override System (Web page). Retrieved from the Toyota website at http://toyota2.tekgroupweb.com/article_download.cfm?article_id=2390

[15] Chan, C. C. (2007). The state of the art of electric, hybrid, and fuel cell vehicles. *Proceedings of the IEEE, 95*, no. 4.

[16] Kim, M.-J., & Peng, H. Power management and design 0ptimization of fuel cell/battery hybrid vehicles. *Journal of Power Sources, 165*, no. 2.

[17] Wu, D., & Williamson, S. S. (2007). Status review of power control strategies for fuel cell based hybrid electric vehicles. In *IEE Canada Electrical Power Conference*, Montreal, October 25-26, 2007.

[18] National Highway Traffic Safety Administration. (n.a.) (National Automotive Sampling System (NASS) General Estimate System (GES) Analytical User's Manual, 1988-2012 (Unnumbered, undated report). Washington DC: National Highway Traffic Safety Administration. Available at ftp://ftp.nhtsa.dot.gov/GES/GES12/GES%20Analytical%20Users%20Manual%201988-2012_FINAL-2013-10-31.pdf

[19] Van Eikema Hommes, Q. D. (2012, April 16). Review and assessment of the ISO 26262 draft road vehicle - Functional safety (Paper No. SAE 2012-01-0025). SAE 2012 World Congress & Exhibition, Detroit, MI, April 24-26, 2012. DOI: 10.4271/2012-01-0025

[20] Van Eikema Hommes, Q. D. (2016, June). *Assessment of safety standards for automotive electronic control systems*. (Report No. DOT HS 812 285). Washington, DC: National Highway Traffic Safety Administration. Available at www.nhtsa.gov/sites/nhtsa.dot.gov/files/812285_electronicsreliabilityreport.pdf

[21] Kahneman, D. (2013, April). *Thinking, fast and slow*. New York: Farrar, Straus, and Giroux.

[22] Robert Bosch GmbH. (2013). Gasoline Port Fuel Injection (Web page). Retrieved from the Bosch web site at www.bosch-mobility-solutions.com/media/en/ubk_europe/db_application/downloads/pdf/antrieb/de_5/pfi_full_de.pdf

[23] Clemson University Vehicular Electronics Laboratory. (n.a.). Electronic Throttle Control (Web page). Retrieved from the Clemson University web site at www.cvel.clemson.edu/auto/systems/throttle_control.html

[24] NASA Engineering and Safety Center. (2011, January 11). National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation: Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation (NESC Assessment #: TI-10-00618). Hampton, VA: Author. Available at www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf

[25] Van Eikema Hommes, Q. D. (2014, March 27). Applying STAMP Framework to Analyze Automotive Recalls (PowerPoint presentation). MIT 3rd STAMP/STPA Workshop, Cambridge, MA, March 25-27, 2014. Available at http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Hommes-STAMP-2014-Presentation-140327.pdf

[26] Van Eikema Hommes, Q., Becker, C., Najm, W., & Won, C. (in press). *A scientific foundation for analyzing safety issues in automotive electronic control systems*. Washington, DC: National Highway Traffic Safety Administration.

[27] Rippel, W. (2007, January 9). Induction versus DC brushless motors (Web log post). Retrieved from www.teslamotors.com/blog/induction-versus-dc-brushless-motors

[28] Solberg, G. (2007, June 9). The magic of Tesla Roadster regenerative braking (Web page). Retrieved from the Tesla Motors web site at www.teslamotors.com/blog/magic-tesla-roadster-regenerative-braking

[29] Gordon-Bloomfield, N. (2011, June 15). Should electric cars mimic the gasoline driving experience (Green Car Reports web page). Retrieved from www.greencarreports.com/news/1061657_should-electric-cars-mimic-the-gasoline-driving-experience

[30] Lampton, C. (2009, January 23). How Regenerative Braking Works (HowStuffWorks website). Retrieved from http://auto.howstuffworks.com/auto-parts/brakes/brake-types/regenerative-braking.htm

[31] Alcala, I., Claudio, A., & Guerrero, G. V. (2005). Analysis of propulsion systems in electric vehicles. In *2nd International Conference on Electrical and Electronics Engineering*, Mexico City, Sept. 7-9, 2005.

[32] Krohn, K. (2013, September). Freescale - Building a basic inverter (Web page). Retrieved from www.freescale.com/files/training/doc/dwf/DWF13_AMF_AUT_T0144.pdf

[33] Whaling, C. (2013, December). Electric Drive Power Electronics: An Overview (Web page). IEEE Transportation Electrification. Available at https://tec.ieee.org/newsletter/december-2013/electric-drive-power-electronics-an-overview?highlight=WyJlbGVjdHJpYyIsIidlbGVjdHJpYyciLCJlbGVjdHJpYyciLCJkcml2ZSIsImRyaXZlJ3MiLCJwb3dlciIsImVsZWN0cm9uaWNzIiwiYW4iLCJvdmVydmlldyIsImVsZWN0cmljIGRyaXZlIiwiZWxlY3RyaWMgZHJpdmUgcG93ZXIiLCJkcml2ZSBwb3dlciIsImRyaXZlIHBvd2VyIGVsZWN0cm9uaWNzIiwicG93ZXIgZWxlY3Ryb25pY3MiLCJwb3dlciBlbGVjdHJvbmljcyBhbiIsImVsZWN0cm9uaWNzIGFuIiwiZWxlY3Ryb25pY3MgYW4gb3ZlcnZpZXciLCJhbiBvdmVydmlldyJd[34] Van Eikema Hommes, Q. D., & Becker, C. (2018, July). *Functional safety assessment of a generic accelerator control system with electronic throttle control in gasoline-fueled vehicles* (Report No. DOT HS 812 557). Washington, DC: National Highway Traffic Safety Administration.

DOT HS 812 640
December 2018

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

13781-121218-v3a