U.S. Department of Transportation

National Highway Traffic Safety Administration

NHTSA

DOT HS 812 557 July 2018

Functional Safety Assessment of a Generic Accelerator Control System With Electronic Throttle Control in Gasoline-Fueled Vehicles

Disclaimer

Suggested APA Format Citation:

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.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No.0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** July 2018	**3. REPORT TYPE AND DATES COVERED**

4. TITLE AND SUBTITLE Functional Safety Assessment of a Generic Accelerator Control System With Electronic Throttle Control in Gasoline-Fueled Vehicles **6. AUTHORS** Qi Van Eikema Hommes and Christopher Becker	**5. FUNDING NUMBERS** Intra-Agency Agreement DTNH22-13-V-00114 51HS7BA100
7. PERFORMING ORGANIZATION NAME AND ADDRESS John A. Volpe National Transportation Systems Center Cambridge, MA 02142	**8. PERFORMING ORGANIZATION REPORT NUMBER** DOT-VNTSC-NHTSA-15-06
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS National Highway Traffic Safety Administration 1200 New Jersey Avenue SE. Washington, DC 20950	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER** DOT HS 812 557
11. SUPPLEMENTARY NOTES	
12a. DISTRIBUTION/AVAILABILITY STATEMENT This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.	**12b. DISTRIBUTION CODE** Document is available to the public from the National Technical Information Service, www.ntis.gov.

13. ABSTRACT

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 powered by gasoline internal combustion engines. This study follows the concept phase process in the ISO 26262 standard and applies a hazard and operability study, functional failure modes and effects analysis, and systems theoretic process analysis methods. In total, this study identifies 5 vehicle-level safety goals and 179 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, hazard and operability study, failure modes and effects analysis, systems theoretic process analysis, ISO 26262, hazard analysis, risk assessment, and safety requirements.	**15. NUMBER OF PAGES** 404 **16. PRICE CODE**

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

Foreword

NHTSA's Automotive Electronics Reliability Research Program

The mission of the National Highway Traffic Safety Administration is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes. As part of this mission, NHTSA researches methods to ensure the safety and reliability of emerging safety-critical electronic control systems in motor vehicles. The electronics reliability research 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 5 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 powered by gasoline internal combustion engines. This study follows the concept phase process in the ISO 26262 standard [1] and applies a hazard and operability study, functional failure modes and effects analysis, and systems theoretic process analysis methods. In total, this study identifies 5 vehicle-level safety goals and 179 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.

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/C	air conditioning
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
BPPS	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
ECM	engine control module
EEPROM	electrically erasable programmable read-only memory
EDC	electronic diesel control
EGO	exhaust gas oxygen
EGR	exhaust gas recirculation
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ESD	electrostatic discharge
ETC	electronic throttle control
FMEA	failure mode and effects analysis
FMVSS	Federal Motor Vehicle Safety Standard
FPCV	fuel rail pressure control valve
FQC	fuel quantity control
FRPS	fuel rail pressure sensor
FTTI	fault tolerant time interval
HAZOP	hazard and operability study

HEV	hybrid electric vehicle
IC	integrated circuit
ICE	internal combustion engine
IEC	International Electrotechnical Commission
I/O	input/output
ISO	International Organization for Standardization
kph	kilometers per hour
MISRA	Motor Industry Software Reliability Association
mph	miles per hour
QM	quality management
RAM	random access memory
ROM	read only memory
rpm	revolutions per minute
S	severity
SAE	SAE International
SG	safety goal
STPA	systems theoretic process analysis
TBD	to-be-determined
UCA	unsafe control action

EXECUTIVE SUMMARY

This report describes a research effort by the Volpe National Transportation Systems Center, 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 position is controlled electronically. Specifically, this report focuses on the identification of example safety requirements for the ACS/ETC systems in motor vehicles powered by gasoline internal combustion engines.[2]

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 (ASIL) 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 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.

This research follows the Concept Phase process, Part 3 of ISO 26262 [1] to derive a list of potential safety requirements. Specifically, this research:

1. Defines the scope and functions of a generic gasoline ACS/ETC, and represents the system in block diagrams.
2. Performs a vehicle-level hazard analysis using both the Hazard and Operability study and the systems-theoretic process analysis method. By integrating the hazards identified in both the HAZOP study and STPA, the process establishes five vehicle-level hazards (Table ES-1).
    a. The HAZOP study identifies 103 malfunctions from analysis of the 15 ACS/ETC functions (see Section 4.2.3, Table 3 for details).

[1] 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 or regulatory requirements for ACS/ETC systems.

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

b. The STPA identifies 48 unsafe control actions from analysis of the four ACS/ETC control actions (see Section 4.3.4, Table 7 for details).

3. Applies the ASIL assessment[3] approach in ISO 26262 to evaluate the risks associated with each of the identified hazards. In total, 71 operational situations are evaluated for each vehicle-level hazard. Following the practice in the ISO 26262 process, the most severe ASIL is chosen for each of the five 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 propulsion power reduction/loss or vehicle stalling	D
H4	Potential insufficient vehicle deceleration	C[ii]
H5	Potentially allowing driver's command to override active safety systems[iv]	D[iii]

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 which 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 individuals in close proximity to the vehicle.*

ii. *The ASIL assessments 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 H5 are contained in H1, H2, H3, and H4. Therefore, H5 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.*

4. Performs safety analysis using both the functional failure mode and effects analysis and the STPA methods.
   a. The functional FMEA identifies 25 failure modes and 95 causes (see Section 7.1, Table 18 for details).
   b. The STPA identifies 505 causes that may lead to 48 UCAs (see Section 7.2, Table 20 for details).

[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" through "D" according to increasing hazard criticality.

5. Identifies 179 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 103 example functional safety requirements by following the Concept Phase in ISO 26262
   b. This study derived 76 examples of additional safety requirements by following the additional safety strategy in the military standard MIL-STD-882E [2]. These 76 requirements are out of the scope of the Functional Safety Concept phase in ISO 26262 Part 3. 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 76 additional requirements.

Table ES-2 provides a breakdown of the 103 example functional safety requirements and 76 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	18
Accelerator Pedal (AP) Assembly	8	5
Engine Control Module	64	35
Throttle Assembly Subsystem	–	1
Communication Signals	8	–
Power Supply	7	–
Brake Pedal (BP) Assembly	1	5
Interfacing Systems	4	12

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 (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 gasoline engine 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 position is controlled electronically.

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 [2].

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

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

This report covers the study of the 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) powered by the gasoline engines. 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 or regulatory requirements for production 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 motor vehicles powered by the gasoline internal combustion engine. 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 made from this study regarding application of ISO 26262.
- Section Eleven: considers potential uses of the results of this study.

2 ANALYSIS APPROACH

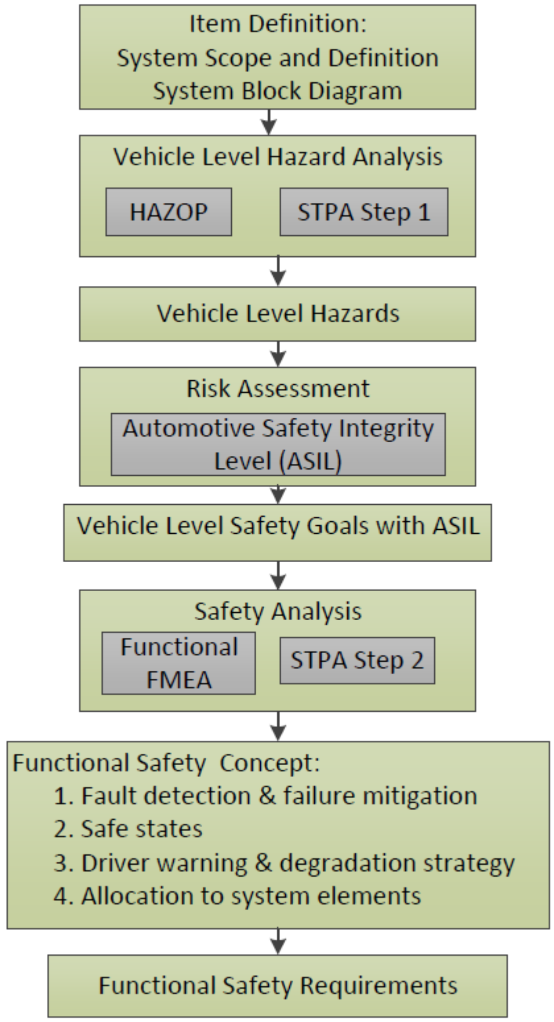
The primary purpose of this work is to study and analyze the potential hazards that could result from cases of electrical or electronic failures impacting the functions of vehicular control systems. The study follows the ISO 26262 process to identify the integrity requirements of these functions at the concept level, independent of implementation variations. ISO 26262 is a functional safety process adapted from the International Electrotechnical Commission 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 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.

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 in a previous study.[5]

---

[5] Brewer, J., Nasser, A., Van Eikema Hommes, Q. D., Najm, W., Pollard, J., & Jackson, C. (in press). *Safety management of automotive rechargeable energy storage systems: The application of functional safety principles to generic rechargeable energy storage systems*. Washington, DC: National Highway Traffic Safety Administration.



HAZOP: Hazard and Operability study
STPA: System Theoretic Process Analysis

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

FMEA: Failure Modes 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 analysis in the rest of the process.
2. Carry out hazard analysis using both the HAZOP study [3] and the STPA method [4]. 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 that 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 requirements.
5. Perform safety analyses on the relevant system components and interactions as defined in the first step of this process. This project performs both the functional FMEA [5] and STPA.
6. Follow the ISO 26262 process to develop a functional safety concept and functional safety requirements at the ACS/ETC system and components level, based on results from both functional FMEA and STPA, 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 descriptions to better explain how the analysis is performed.

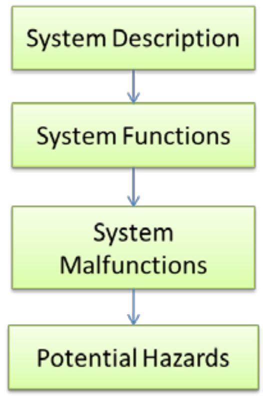


Figure 2. HAZOP Study Process

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 components are designed to perform. This step is also accomplished in the first step of the overall project (Figure 1).
3. For each of the identified functions, apply a set of guidewords that describe the various ways in which the function may deviate from its design intent. IEC 61882[8] lists 11 suggested guidewords, but notes that the guidewords can be tailored to the particular system being analyzed [3]. 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 utilizing the specific set of guide words defined in this standard; and also gives guidance on application of the technique and on the HAZOP study procedure, including definition, preparation, examination sessions, and resulting documentation.

2.2.2 Functional Failure Modes and Effects Analysis

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

Standard J1739 by SAE International provides guidance on applying the functional FMEA method [5]. 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 implemented at the concept phase and is not based on a specific design, the FMEA does not assume controls or mitigation measures are present; there are no 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

The STPA is a top-down systems engineering approach to system safety [4]. In STPA, the system is modelled as a dynamic control problem, where proper controls and communications in the system ensure the desired outcome for emergent properties, such as safety. In the STPA framework, a system will not enter a hazardous state unless an unsafe control action is issued by a controller, or a control action needed to maintain safety is not issued. Figure 3 shows a process flow diagram for the STPA method.

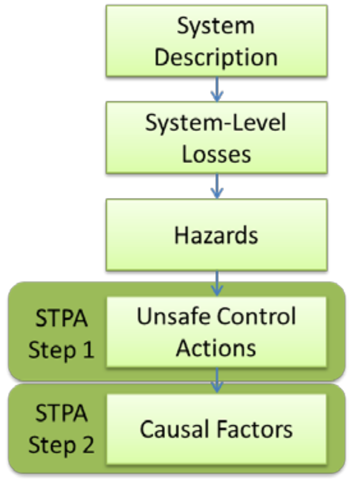


Figure 3. STPA Process

This project performs STPA following these steps:

1. Define the system of study and the scope of the analysis:
    a. Draw a hierarchical control structure of the system that captures the feedback control loops (controller, sensors, actuators, controlled process, and communications links). This control structure is a generic representation of the functions in most systems in use.
    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. [4]. For this project, the loss is defined as the occurrence of a vehicle crash.
3. Identify a preliminary list of vehicle-level hazards. STPA defines a hazard as a system state or set of conditions that, together with a set of worst-case environmental conditions, will lead to a system-level loss [4]. Initially, based on engineering experience and literature search, a preliminary hazard list is generated. This list is further refined through iterations in STPA Steps 1 and 2 — UCA and causal factors identification.
4. **STPA Step 1**: Identify potential UCAs issued by each of the system controllers that could lead to hazardous states for the system. Four sub-steps are involved:

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

b. For each control action, develop a set of context variables[9]. 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 [6] enumerates the process variable states in the first step of STPA. Process 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 the recently-enhanced STPA approach to focus on context variables instead of process variables.

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

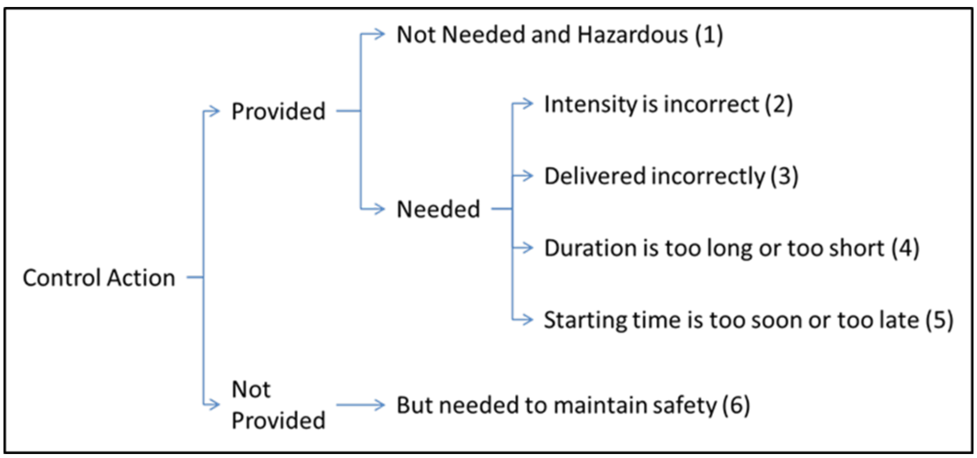


Figure 4. Guidewords for UCAs

For each control action, assess each of the six guidewords against each of the context variable combinations to determine if it could lead to vehicle-level hazards. If new hazards were identified, add it 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 [7] to reduce the number of UCA statements.

[9] The context variables describe the context in which the control commands act in. For example, the control command "increase throttle opening" may operate in the context of the "driver presses both accelerator pedal and brake pedal."

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 connection in the control structure representation of the system is analyzed to determine if the component or the connection may contribute to one of the UCAs identified in STPA Step 1. STPA literature provides 17 guidewords to assist the analyst in identifying CFs [4]. 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.

Please note 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.

This report describes how this study performs HAZOP study, functional FMEA, and STPA, including detailed analysis and results for the ACS/ETC system in light vehicles powered by the gasoline engine.

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 the incoming torque requests from other vehicle systems are correct; failures in other vehicle systems that could result in incorrect engine torque requests are out of scope for this study.

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

1. All components leading from the driver-operated control to the air-throttling device on the engine, including the following.
    - Accelerator pedal
    - Accelerator pedal position sensor
    - Engine control module, including the throttle position control functions
    - Throttle motor
    - Throttle valve
    - Throttle position sensor
2. All connections between the components listed above, including the following.
    - 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. Interfacing sensors, including
    - Vehicle speed data
    - Brake pedal position sensor
    - Engine sensors

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

- Torque and power delivery downstream of generation, including failures in the transmission system
- Hazards not related to vehicle acceleration or deceleration, such as fire hazards
- Malfunctions in fuel delivery or engine combustion
- Brake system malfunctions that may lead to acceleration- or deceleration-related hazards
- Malfunctions in other vehicle systems leading to incorrect engine torque requests
- Notifications from the ACS/ETC to the driver, such as malfunction indicator lights.
- Driver errors, such as incorrect pedal application.
- 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 gasoline engine 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 vehicle speed is primarily provided to the EV PCM by a dedicated sensor in the drivetrain, with secondary sources of speed provided by the brake/stability[10] 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 ECM.*
- The mass air flow sensor/manifold absolute pressure sensor provides the ECM with information regarding the ambient air pressure. Some system architectures may have a separate barometric pressure sensor that provides this information.
  - *Requirements related to ambient air pressure would apply to whichever component is responsible for providing this information to the ECM.*
- 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 [9]. 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 intentionally 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 will need additional analysis. Additional analysis is also needed to understand why the driver may incorrectly or non-intuitively apply the AP or the BP.*

- The engine idle speed is maintained solely by adjusting the throttle valve position. Some systems may use a separate idle bypass valve that allows air to flow to the intake manifold independent of the throttle valve position.
  - *Safety requirements related to the function of controlling the idle air flow also apply to the idle bypass valve. However, the specific safety requirements for the idle bypass valve control will require additional analysis.*
- Safety strategies, such as redundant sensors, are not considered in the hazard analysis or safety analysis stages. They are only considered as part of the functional safety concept and are reflected in the safety requirements
  - *Once specific design strategies have been adopted, additional hazard and safety analyses should be performed.*

3.3 System Block Diagram

The gasoline engine regulates the amount of air intake to control the engine power output in response to changes in the driver-operated control. In the older mechanical throttle control systems, the throttle valve position is controlled by a cam and cable system directly connected to the AP. In modern ACS/ETC systems, the air throttle valve position is controlled by a motor, which receives an electrical signal from the ECM.

Figure 5 shows a block diagram representation of the 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. Interfaces between these systems and the ACS/ETC system are shown as lines that cross the ACS/ETC system boundary.

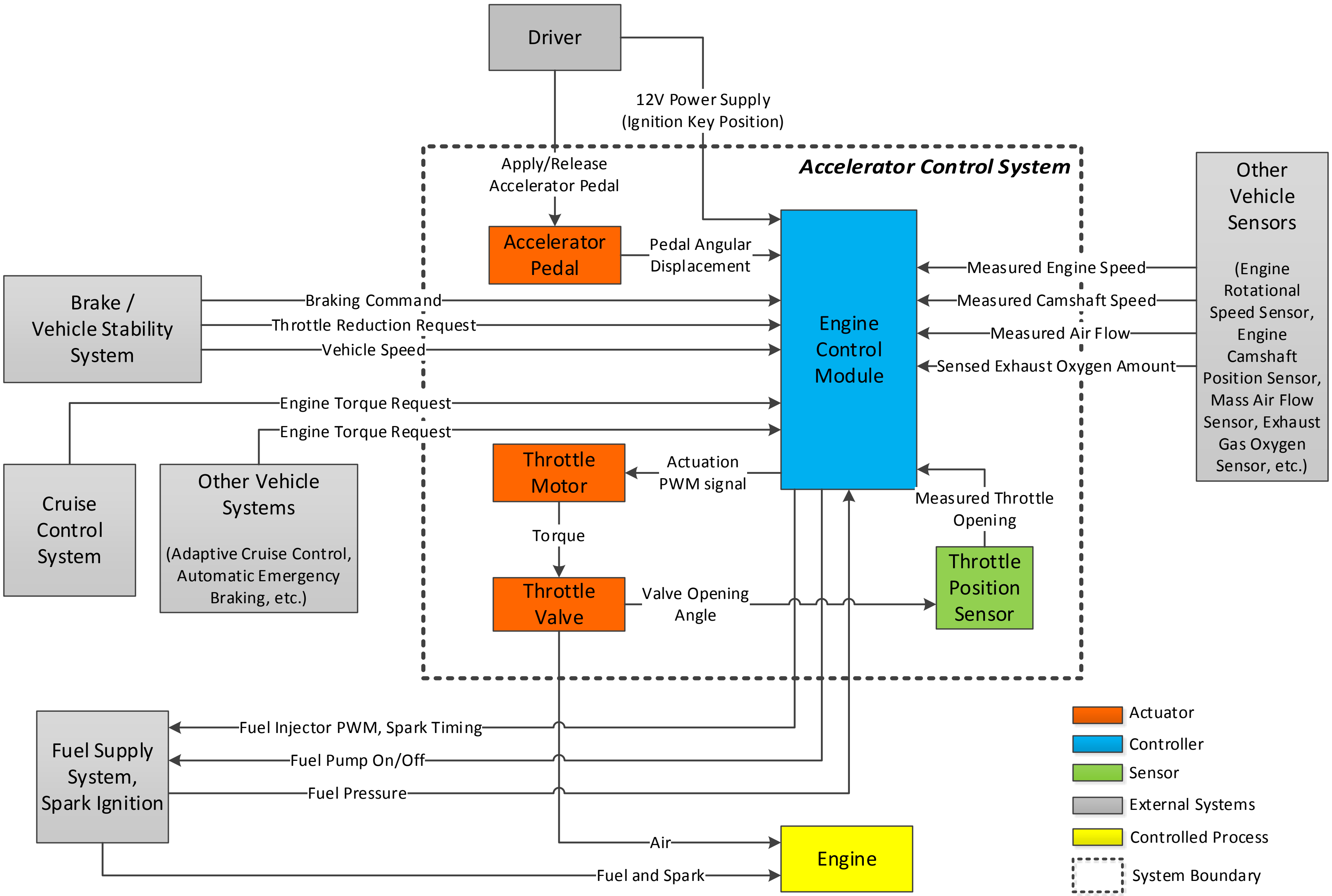


Figure 5. Block Diagram of ACS in Gasoline Internal Combustion Engine Vehicles

3.4 System Description

The following description outlines the functions of a gasoline engine ACS/ETC system [10] [11] [12].

3.4.1 Driver-Operated Control and Other Torque Requests

The AP assembly allows the driver to command a desired torque. When the driver presses the AP, the APPS measures the angular position of the AP. The APPS converts the angular position of the AP to a voltage signal, which is transmitted to the ECM. The signal may be transmitted via a direct analog input or a vehicle communication bus such as the CAN bus.

Using calibration maps, the ECM converts the voltage signal from the APPS to a desired engine torque. The ECM then reconciles the torque requested by the driver with requests from other vehicle systems and measurements from other vehicle sensors. These systems and sensors vary depending on the vehicle design, but typically include:

- Engine speed reduction requests from the TCS,
- Throttle opening requests from the CC system, and
- Engine speed adjustment requests from the transmission control system.

3.4.2 Throttle Position Control

The ECM computes the quantity of air required by the engine to achieve the torque necessary to meet the driver's request and other vehicle demands. To adjust the volume of air reaching the engine, the ECM uses pulse-width modulation to drive the throttle motor. As the throttle motor rotates the throttle valve, the throttle opening increases or decreases to regulate air flow to the intake manifold.

The TPS attached to the throttle valve assembly provides feedback to the ECM about the angular position of the throttle valve. This feedback signal enables the ECM to use closed-loop control to precisely adjust the angular position of the throttle valve.

In some gasoline engine architectures, the throttle position control may be performed by a separate throttle actuator controller. In this case, the desired throttle position would be determined by the ECM and communicated to the throttle actuator controller. The throttle actuator controller would be responsible for operating the throttle motor and communicating the throttle position to the ECM.

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 at-rest (i.e., undepressed) position. When the AP is in the at-rest position, the ECM commands the throttle valve to its idle angular position.

The idle angular position of the throttle valve is determined by the ECM based on the calibration data about the MAF required by the engine to run at the idle speed. As the vehicle ages, the ECM continuously updates the throttle valve idle angular position calibration to ensure that the engine receives the required air flow.

The engine rotational speed is measured in rpm by the engine rotational speed sensor, which is also known as engine rpm sensor. The ECM uses the engine speed as a feedback input to control the engine idle speed. If the measured engine idle speed does not match the expected engine idle speed programmed into the ECM software, the ECM can adjust the idle position of the throttle valve until the expected engine idle speed is reached. Some factors that may cause the actual engine idle speed to differ from the expected engine idle speed when the throttle valve is at the idle angular position include:

- Engine temperature,
- Engine load demands, such as A/C, and
- Ambient air temperature and pressure.

The ECM also uses the idle angular position as the baseline throttle valve position when determining the throttle opening needed to satisfy torque demands by the driver and vehicle.

3.4.4 Brake Throttle Override Function

As an example of OEM strategy, when the driver presses the BP, the BPPS sends a signal to the ECM. If both the AP and BP are pressed, the ECM must determine if the driver's intent is to stop the vehicle. To accomplish this, the ECM 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 ECM engages the BTO feature.

In BTO mode, the ECM will override the torque request from the driver via the AP and return the throttle valve to the idle angular position or a pre-set throttle position for BTO mode. The ECM will maintain the throttle valve at the idle angular position until BTO mode is disengaged. The ECM 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 throttle valve position, the ECM is also responsible for monitoring the ACS/ETC electronic system components to determine if faults are present. If the ECM detects a fault in the system, the ECM will log a diagnostic trouble code and may force the ACS/ETC into a safe state, such as the "limp-home mode." The ECM will also turn on the malfunction indicator light on the vehicle's instrument display panel.

Some examples of system faults include:

- APPS or TPS voltage signals exceeding the calibration range,
- Throttle motor exceeding the allowable electronic current limit, and
- Internal software or hardware faults in the ECM.

3.4.6 Related System: Fuel Delivery System

While the fuel delivery system is outside the gasoline engine ACS/ETC scope for this study, it is a closely related system and is essential for achieving the desired engine torque output. An overview of the relationship between the fuel delivery system and the gasoline engine ACS/ETC is provided below.

The MAF sensor measures the quantity of air entering the engine. The ECM uses the MAF as well as emissions data from the heated exhaust gas oxygen sensor to determine the appropriate quantity of fuel to command from the fuel supply system and to control spark timing. The ECM adjusts the fuel quantity and spark timing to achieve maximum engine torque output while meeting emission standards.

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 study 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 vehicle acceleration or commands less than the provided acceleration	Accelerates in 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 vehicle 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.
Deceleration-Related	Does not command vehicle deceleration or commands less than the provided deceleration	Decelerates	**H3: 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. This includes vehicle deceleration resulting from conditions such as engine stalling.
	Commands vehicle deceleration	Does not decelerate or decelerates at a rate that is less than the specified speed decrease profile	**H4: Potential Insufficient Vehicle Deceleration** - refers to incidents where the engine speed is not reduced to the level commanded by the driver when the driver reduces the angular position of the accelerator pedal.
Applicable to Both Acceleration and Deceleration	Command either acceleration or deceleration	Accelerates or decelerates following driver's command, and overrides active safety function	**H5: 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.[i]
[i] This hazard may not apply in ACS/ETC systems designed to give the driver's command priority over all active safety systems.			

4.2 Hazard and Operability Study

4.2.1 System Description

The HAZOP study uses a block diagram as a visual representation of the 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.

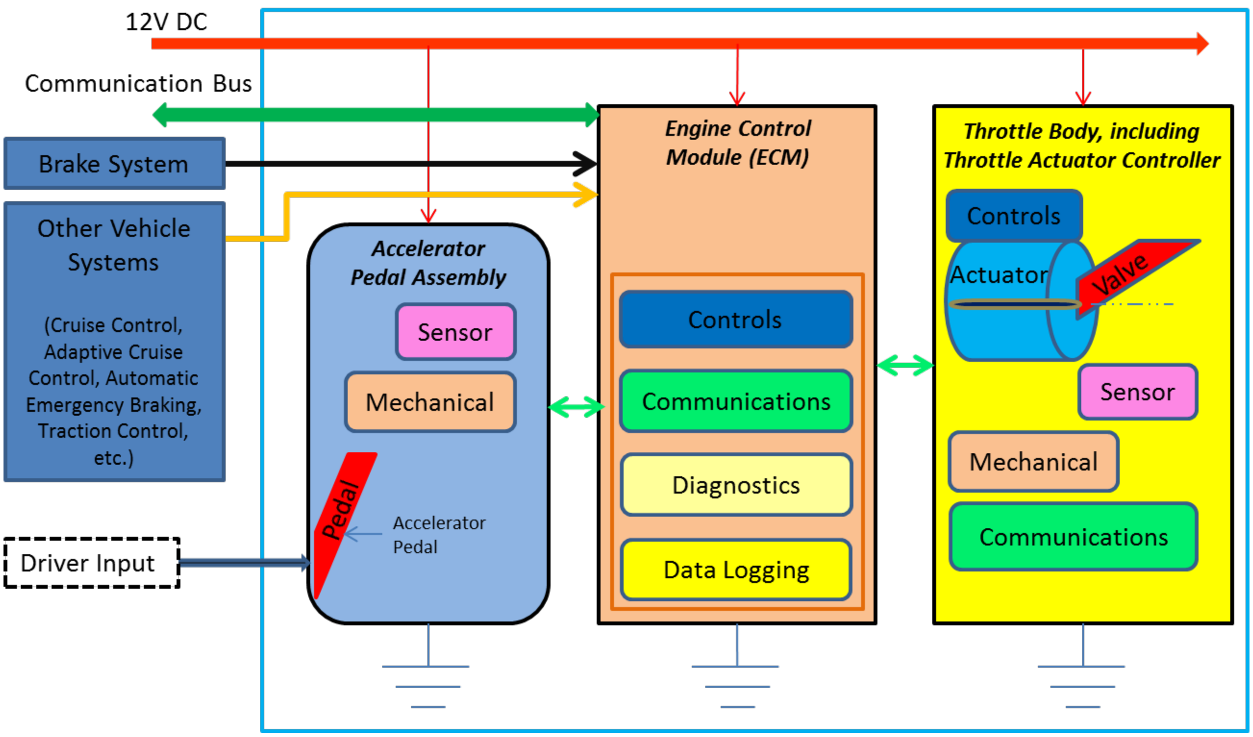


Figure 6. Block Diagram of the ACS/ETC System for the HAZOP Study

The light blue solid line defines the boundary of the ACS/ETC system that contains three main components.

- AP assembly
- ECM
- Throttle body, including the throttle actuator controller

The AP in the AP assembly receives the driver's input. The driver's input is communicated to the ECM, which in turn communicates a desired throttle position to the throttle actuator controller. The ACS/ETC also interfaces with other vehicle systems, such as:

- Brake system,
- Adaptive cruise control,

- Automatic emergency braking, and
- TCS.

In addition to the interfaces with other vehicle systems, the ACS/ETC is connected to the low voltage direct current power supply and communication bus (e.g., CAN bus).

4.2.2 System Functions

The HAZOP study identifies 15 system functions for the ACS/ETC.

1. Command torque from the propulsion system
2. Provide the APP to the ECM
3. Return the AP to the off (undepressed) position within the specified time
4. Provide AP request rate limiting
5. Control the throttle position
6. Communicate the throttle position to the ECM
7. Return the throttle to the idle position within the specified time
8. Establish the throttle idle position
9. Provide idle state control
10. Provide the BTO control
11. Store the APP torque maps
12. Communicate with internal subsystems and external vehicle systems
13. Provide diagnostics
14. Provide fault detection and failure mitigation
15. Store relevant data

Functions 14 and 15 are shown here for completeness. The HAZOP study concludes that malfunctions related to these 2 functions would not result in vehicle-level hazards.

4.2.3 System Malfunctions and Hazards

The 7 HAZOP study guidewords presented in Section 2.2.1 are applied to each of the 15 ACS/ETC functions listed above. They generate a list of 103 malfunctions. These malfunctions may lead to 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 ACS/ETC functions. Each of the identified malfunctions is assessed to determine if it could result in a vehicle-level hazard. Appendix B provides the complete results of the HAZOP study.

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

Function: Provide the APP to the ECM.

HAZOP Guidewords	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
Loss of function	Does not provide the APP to the ECM	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
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
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) 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
Commands Torque From the Propulsion System	8
Provides Accelerator Pedal Position to the Engine Control Module	7
Returns Accelerator Pedal to Off (undepressed) Position Within a Specified Time	9
Provides AP Request Rate Limiting	7
Controls the Throttle Position	7
Communicates the Throttle Position to the ECM	6
Returns Throttle to Idle Position Within Specified Time	9
Establishes Throttle Idle Position	5
Provides Idle State Control	7
Provides Brake-Throttle Override Control	7
Stores the APP Torque Maps	7
Communicates With Internal Subsystems and External Vehicle Systems	6
Provides Diagnostics	6
Provides Fault Detection and Failure Mitigation [i]	6
Stores Relevant Data [i]	6
[i] 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 ACS/ETC system (in the dashed line) and its interfacing systems and components. 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.

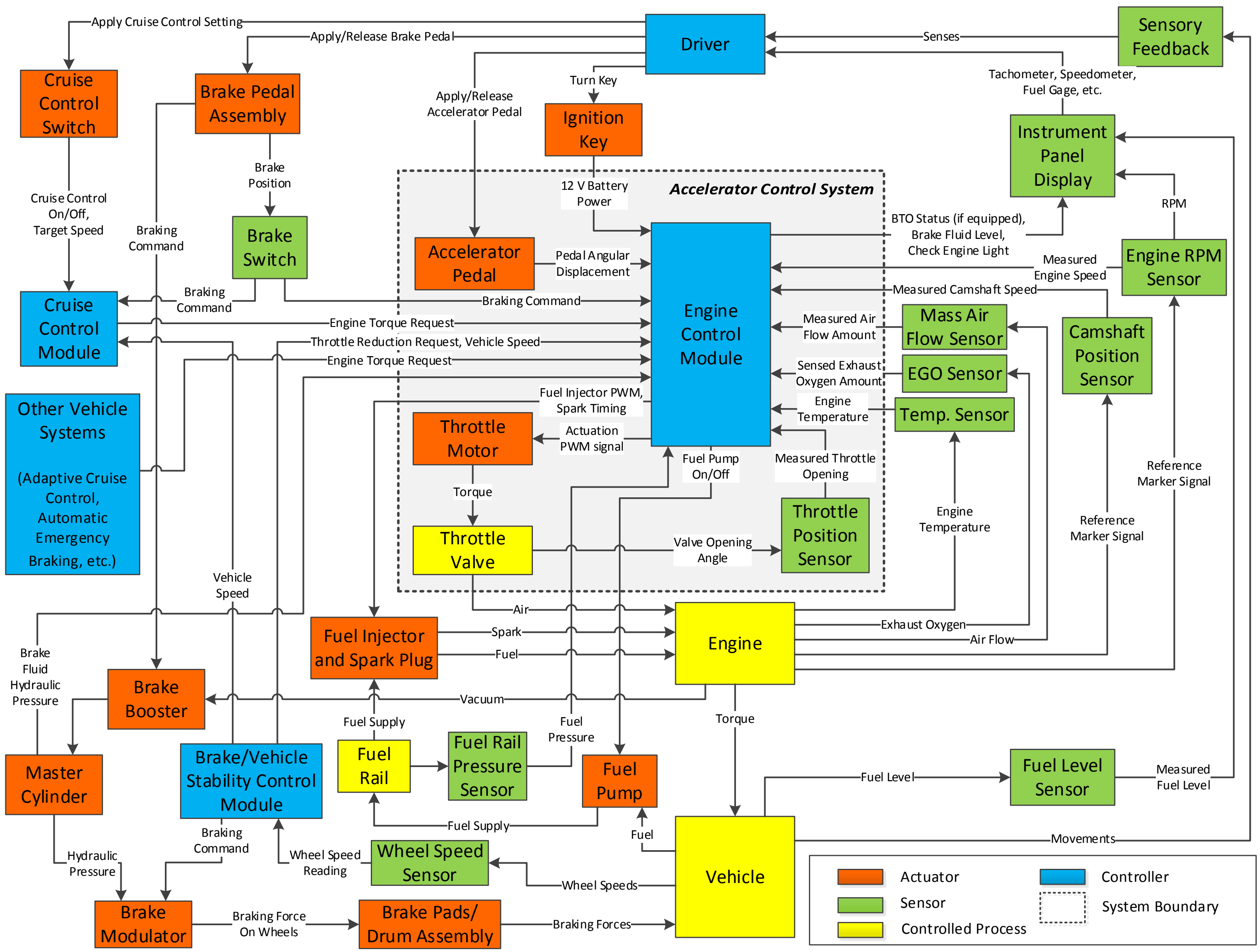


Figure 7. Detailed Control Structure Diagram for the Gasoline Engine ACS/ETC System

4.3.2 Vehicle-Level Loss and Initial Hazards

The vehicle-level loss of interest to this project is the prevention of a vehicle crash.

An initial list of vehicle-level hazards is generated based on literature search and engineering experience. STPA Step 1 helps refine the initial hazard list. 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 hazards 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 four control actions issued by the ECM related to the ACS/ETC function:

1. Two control actions are related to mode switching. These control actions are internal to the ECM and result in a change in the ECM operating state.
    i. **Enter BTO mode** – the ECM issues this control action to enter an operating state that allows the driver's request for braking to override the AP command.
    ii. **Enter normal mode** – the ECM 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 Analyzing 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 miles per hour (mph)
	< 10 mph

2. Two control actions are related to adjusting the throttle position. These control actions are issued to the throttle motor, which directly controls the throttle valve position.
    i. **Increase the throttle opening** – the ECM issues this control action to increase the air flow to the engine.
    ii. **Decrease the throttle opening** – the ECM issues this control action to decrease the air flow to the engine.

The context variable states used to analyze the throttle adjustment control actions are listed in Table 5.

Table 5. STPA Context Variables for Analyzing the Throttle Adjustment Control Actions

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
ECM 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

4.3.4 Unsafe Control Actions

The six UCA guidewords (Figure 4) are applied to each combination of context variable states for the four control actions listed in the previous section. It is then assessed whether the control action would result in a vehicle-level hazard. Table 6 shows how this is done for one of the control actions – "Enter BTO Mode." Appendix C contains all the UCA assessment tables for the four control actions studied.

Table 6. 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		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Not Pressed	Not Pressed	≥10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Not Pressed	Pressed	<10 mph			N/A	N/A	N/A	N/A			
Not Pressed	Pressed	≥10 mph			N/A	N/A	N/A	N/A			
Pressed	Not Pressed	<10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Not Pressed	≥10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Pressed	<10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Pressed	≥10 mph	H1		N/A	N/A	N/A	N/A	H1	H3	H1

Vehicle-Level Hazards:

H1: Potential uncontrolled vehicle propulsion
H3: Potential propulsion power reduction/loss or vehicle stalling

Each row of Table 6 represents a UCA. For example, the last row and fourth column of the table may generate the following UCA.

- *The ECM 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 Uncontrolled Vehicle Propulsion.

However, writing each cell of the table into a UCA statement will create a very long list of UCAs. Many of these UCAs have overlapping logical states. Therefore, this study further applies the Quine-McCluskey minimization algorithm [7] to consolidate and reduce the number of UCA statements.

Overall, STPA Step 1 identifies a total of 48 UCAs for the generic ACS/ETC system studied. The breakdown of these UCAs by control action is provided in Table 7.

Table 7. Number of Identified UCAs for Each STPA Control Action

STPA Control Action	**Number of Identified UCAs**
Increase Throttle Opening	12
Decrease Throttle Opening	26
Enter BTO Mode	6
Enter Normal Mode	4

Appendix D presents a complete list of the UCAs identified in STPA Step 1. Table 8 and Table 9 show examples of UCAs and their associated vehicle-level hazards.

Table 8. STPA UCA Statement for Mode Switching (Example)

Hazard	Potential propulsion power reduction/loss or vehicle stalling
UCA (Example)	The ECM issues the Enter Normal Mode command when the driver presses the AP and the driver does not press the BP, but the command is issued too late.

Table 9. STPA UCA Statement for Throttle Control (Example)

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

Prior to the UCA analysis, a preliminary list of vehicle-level hazards was identified. During the course of the STPA Step 1, the UCA analysis identified additional vehicle-level hazards and helped to improve the definition of some hazards.

5 RISK ASSESSMENT

This study follows the risk assessment approach in ISO 26262. The assessment derives the ASIL for each of the five 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 (E) to the operational situation.
    b. Identify the potential crash scenario.
    c. Assess the severity (S) of the harm to the people involved if the crash occurred.
    d. Assess the controllability (C) of the situation and the vehicle in the potential crash scenario.
    e. Look up the ASIL per ISO 26262 based on the E, S, and C.
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 69 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.

These 69 scenarios cover ten variables and their states as shown in Table 10. These variables and their states are identified following current industry practices.

Table 10. 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≤130kph)		Over a rail road track
	Medium speed (40kph<V≤100kph)		Not near or over a rail road track
	Inside city (16kph<V≤40kph)	**Road Condition**	Slippery
	Inside city very low speed (V≤16kph)		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
	Light		Going straight without special driving maneuver or not moving
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

5.1.2 Automotive Safety Integrity Level Assessment

ISO 26262 assesses the ASIL of identified hazards according to the S, E, and C (Part 3 in ISO 26262).

E 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 11 is directly copied from ISO 26262 Part 3 Table 2.

Table 11. Exposure Assessment

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

S 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 12 is directly quoted from ISO 26262 Part 3 Table 1.

Table 12. 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

Table 13 is an acceptable approach to assess severity shown in ISO 26262Part 3 Clause 7.4.3.2 and Annex B Table B.1.

Table 13. 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

ISO 26262 defines C[10] as the "ability to avoid a specified harm or damage through the timely reactions of the persons[11] involved, possibly with support from external measures" (Part 1 Clause 1.19 in ISO 26262). Table 14 is ISO 26262's approach to assessing C (Table 3 in Part 3 in ISO 26262). Table 15 shows how ASIL is assessed based on E, S, and C (Table 4 in Part 3 of ISO 26262).

Table 14. Controllability Assessment

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

[10] The parameter C in hazard analysis and risk assessment represents the potential for controllability.
[11] Persons involved can include the driver, passengers, or people close to the vehicle's exterior.

Table 15. 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:**
  - E = **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.
  - S = **S3** (Front/rear collision or frontal impact with an object with passenger compartment deformation. More than 10% probability of AIS 5-6.)
  - C = **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, C = 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:**
  - E = **E2** (Operational situation occurs about 1% of the operating time of the vehicle.)
  - Crash scenario: Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.
  - S = **S3** (Front/rear collision with passenger compartment deformation. More than 10% probability of AIS 5-6.)
  - C = **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 five vehicle-level hazards. ISO 26262 requires the most severe ASIL be chosen for each hazard. Table 16 shows the resulting ASIL values for each hazard.

Table 16. 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 propulsion power reduction/loss or vehicle stalling	D
H4	Potential insufficient vehicle deceleration	C[ii]
H5	Potentially allowing driver's command to override active safety systems[iv]	D[iii]

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 which prevents a car from rolling backward on a hill when the brake pedal 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 H5 are contained in H1, H2, H3, and H4. Therefore, H5 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 17. Each safety goal (SG) corresponds to the potential hazards in Table 16.

Table 17. 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 s is to be mitigated in accordance to 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 to the identified ASIL.	B
SG 2	Potential insufficient vehicle propulsion[i] is to be mitigated in accordance to the identified ASIL.	C[ii]
SG 3	Potential propulsion power loss/reduction resulting in vehicle deceleration greater than TBD m/s^2 or vehicle stalling is to be mitigated in accordance to the identified ASIL.	D
SG 4	Potential insufficient vehicle deceleration[i] is to be mitigated in accordance to the identified ASIL.	C[ii]
SG 5	The ACS/ETC control algorithm is to choose the throttle command that has the highest priority for safety in accordance to the identified ASIL.	D

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 accelerator pedal.*

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, and H4 (Table 1). Because the consequences of H5 are captured in the other four hazards, no separate functional FMEA is needed for H5. Overall, the functional FMEA covers 11 ACS/ETC system/ subsystems. The functional FMEA identifies 25 failure modes and 95 potential causes of failures. Table 18 shows the number of identified causes for each of the failure modes.

Table 18. Number of Identified Faults by Failure Mode

Failure Mode	Number of Identified Faults
APP communicates with ECM incorrectly	1
APP rate limiting fault (over-limiting/under-limiting)	1
AP is not returned to idle position correctly	1[i]
APP value interpreted/communicated higher than actual	19
APP value interpreted/communicated lower than actual	6
BTO control fault	5
Command/request for braking from automatic emergency braking to ECM failure	1
Command/request for braking from cruise control or adaptive cruise control to ECM failure	1
Commands incorrect throttle position	1
Commands larger throttle opening than required for the torque requested by the driver	20
Commands smaller throttle opening than required for the torque requested by the driver	20
Diagnostics fault	1[ii]
Drives the throttle to a larger opening than commanded by the ECM	22
Drives the throttle to a smaller opening than commanded by the ECM	8
Fails to maintain the throttle idle position	1
Incorrectly establishes the throttle idle position	3
Miscommunicates with external systems	6
Miscommunicates with internal subsystems	3
Misinterprets the communication message from the ECM	1
Misinterprets the APP	1
Provides incorrect engine rotational speed to the ECM	1
Provides incorrect brake pedal position input to the ECM	1
Provides incorrect pressure (elevation) value to the ECM	1
Provides incorrect vehicle speed to the ECM	1
Provides request for incorrect (more) propulsion torque	2
Torque map corrupted	2

Note: Some faults may result in one or more failure modes.
[i] These faults are mechanical in nature and are outside the scope of ISO 26262.
[ii] This failure mode is only considered as part of a multiple point failure analysis.

Table 19 shows a few examples of the functional FMEA. Appendix G provides the complete functional FMEA results.

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 five 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 connections – defined as any connection entirely within the ACS/ETC scope boundary
- Interfacing connections – defined as a connection which begins outside the ACS/ETC system boundary and terminates at an ACS/ETC system component
- Interfacing components – defined as a component where an interfacing connection 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 system is considered by analyzing the brake/stability control module and the connection between the brake/stability control module and the ECM. 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).

Table 19. Sample Functional FMEA for H1: Uncontrolled Vehicle Propulsion (Not Complete)

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands larger throttle opening than required by the requested torque by the driver	ECM fault:	Three-level monitoring		ECM Fault
		Hardware fault (sensors, integrated circuits, circuit components, circuit boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ECM Input/Output (I/O) connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to ground or voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		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

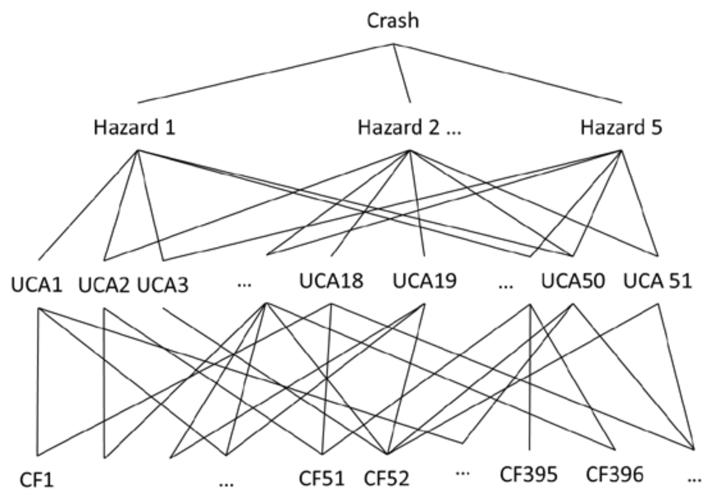


Figure 8. Traceability in STPA Results

The STPA Step 2 analysis identifies a total of 505 CFs. Below is a breakdown of CFs by the type of UCAs they affect.

- 294 CFs may lead to UCAs related to mode switching
- 501 CFs may lead to UCAs related to throttle position adjustment

Table 20 shows a breakdown of the identified CFs by the 26 CF guidewords applied in this study.

Table 20. Number of Identified Causal Factors by Causal Factor Category

Causal Factor Category	Number of Identified Causal Factors
Actuation delivered incorrectly or inadequately: Hardware faulty	2
Actuator inadequate operation, change over time	10
Conflicting control action	1
Controlled component failure, change over time	3
Controller hardware faulty, change over time	18
Controller to actuator signal ineffective, missing, or delayed: Communication bus error	4
Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	5
Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	2
External control input or information wrong or missing	4
External disturbances	158
Hazardous interaction with other components in the rest of the vehicle	114
Power supply faulty (high, low, disturbance)	20
Process model or calibration incomplete or incorrect	14
Sensor inadequate operation, change over time	25
Sensor measurement delay	1
Sensor measurement inaccurate	3
Sensor measurement incorrect or missing	3
Sensor to controller signal inadequate, missing, or delayed: Communication bus error	28
Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	35
Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	14
Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	41

As shown in Figure 8, many CFs may lead to both types of UCAs.

Appendix H provides the complete list of CFs. Table 21 shows three examples of CFs that may result in a mode switching UCA, and the associated vehicle-level hazard:

1. First example describes a potentially faulty BTO software logic in the ECM. If the ECM incorporates an incorrect pedal sequence requirement in the BTO algorithm, the ECM may think the driver intended to apply both pedals. The ECM may not enter BTO mode when the driver is trying to stop the vehicle.
2. Second example describes an interaction between a vehicle component in an interfacing system and the external environment. If the contamination ingress causes the brake/ stability control module to report an incorrect vehicle speed, the ECM may not enter BTO mode. This example illustrates the importance of understanding the interactions between vehicle systems.

3. Third example describes a case where physical interference with a connection between a sensor and the ECM may result in a lost or incorrect signal. If the BP position is not reported to the ECM, the ECM may not know that the driver is trying to apply the brakes and may not enter BTO mode.

Table 21. Examples of Causal Factors for a Mode Switching UCA

Hazard	Potential uncontrolled vehicle propulsion	
UCA (Example)	The ECM does not issue the *Enter BTO Mode* command when: • the driver presses the AP, • the driver presses the BP, and • the vehicle speed is 10 mph or greater.	
Potential Causal Factors (Example)	**Component**	**Potential Causal Factors**
	ECM	The sequence of pedal application is either not considered or is incorrectly considered in the software logic for entering BTO or Normal mode.
	Brake/Stability Control Module	Moisture or other fluids from other vehicle systems (e.g., A/C condensation) could affect the brake/stability control module. This could affect the measurement of the vehicle speed.
	Connection between BPPS and ECM	Chafing or interference from other vehicle systems could affect the connection between the BPPS and ECM (e.g., wiring is cut). This could cause the ECM to receive no signal or an incorrect, intermittent, or delayed signal from the BPPS.

Table 22 shows three examples of CFs for a throttle adjustment related UCA:

- First CF describes a hardware failure in the engine RPM sensor, potentially causing the ECM to have the wrong engine speed information. The ECM may interpret the reduction in engine speed as a need to increase engine torque output.
- Second CF describes a software algorithm error in the ECM that potentially affects the calculation of the engine load. If the ECM incorrectly calculates the engine load from vehicle accessories, the ECM may increase the engine torque output by too much.
- Third CF describes a potential hardware failure in the connection between the APPS and the ECM. If the connection develops a short circuit, the ECM may have an incorrect understanding of the driver's torque request.

Table 22. Examples of Causal Factors for a Throttle Adjustment UCA

<table>
<tr><td>Hazard</td><td colspan="2">Potential uncontrolled vehicle propulsion</td></tr>
<tr><td>UCA (Example)</td><td colspan="2">The ECM issues the Increase Throttle Opening command when:
• the driver reduces or maintains the angular position of the AP, or is not pressing the AP.</td></tr>
<tr><td rowspan="4">Potential Causal Factors (Examples)</td><td>Component</td><td>Potential Causal Factor</td></tr>
<tr><td>Engine Rotational Speed Sensor</td><td>The engine rotational speed sensor may have an internal hardware failure.</td></tr>
<tr><td>ECM</td><td>A programming error or faulty software logic may cause the ECM to incorrectly calculate the engine load (e.g., from accessories such as A/C). If the ECM thinks the engine load increased, the ECM may increase the throttle opening or may not decrease the throttle opening enough.</td></tr>
<tr><td>Connection between APPS and ECM</td><td>The connection between the APPS and ECM could develop an open circuit, short to ground, short to battery, or short to other wires in the harness.</td></tr>
</table>

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.

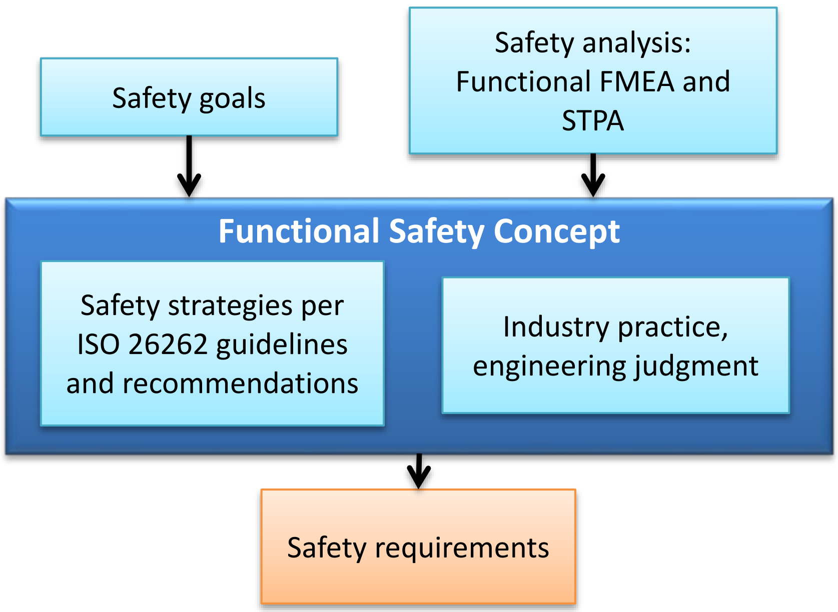


Figure 9. Functional Safety Concept Process

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 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[12] the health of the main controller (using an auxiliary processor).
4. Ensure the validity and correctness[13] 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[14]).
6. Validate the correctness of the throttle position (using redundant mechanism).
7. Ensure the health and sanity of the throttle position calculation algorithms.
8. Ensure the health and sanity of the BTO control algorithm.
9. Ensure that low-voltage power is available until the safe state is reached under all safety hazards conditions.
10. Mitigate the safety hazards when an unsafe condition is detected.
11. Ensure that the safe state is reached on time when a hazard is detected.
12. Ensure driver warnings are delivered when an unsafe condition is detected.
13. 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, a careful consideration is given to selecting the safe states in relation to the potential failure modes.

The safe states for the 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.

The safety analysis at the system level, the hardware level, and the software level may identify potential failure modes with the APPS, the BPPS, the ECM, the throttle actuator controller, throttle body, and other interfacing systems. In cases where a good but not confirmed APPS signal is available, the safe state may allow full torque but at a ramp rate slower than normal to give the driver more reaction time in case of unintended vehicle behavior. In case the APPS signal is completely non- reliable, or if the ECM faults, but the vehicle can still be controlled by

[12] "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.

[13] "Correctness" means that the value of a parameter is the correct one from the valid set.

[14] Quality factors refer to techniques for error detection in data transfer and communication including checksums, parity bits, cyclic redundancy checks, error correcting codes, etc.

the brakes and the throttle actuator controller, the vehicle may be allowed a torque level higher than creep torque. In case of APPS and BPPS malfunctions, no more than creep torque may be allowed. If the failure mode may result in uncontrolled torque production, then the system torque should be disabled.

Safe states may include, but not limited to, 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 (e.g., single APPS fault)
- Safe State 4: Torque produced without AP input; speed limited to TBD (> creep) mph (e.g., two APPS faults; an ECM fault with throttle actuator controller still able to control throttle)
- Safe State 5: Torque produced at zero AP input value of the torque map (e.g., two APPS faults plus BPPS fault)
- Safe State 6: Zero torque output (e.g., vehicle disabled; system is unable to mitigate the hazards or ensure Safe States 1-5).

The safe states listed above describe propulsion reduction (Safe States 2, and 4-6) or deviations from the specified speed decrease or increase profiles (Safe State 3). While these vehicle responses may be similar to the identified hazards H2 through H4, 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 are not 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 hazards H2 through H4 manifest.

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 probability 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; probability is high (e.g., AP Torque Map corruption, AP or BP communication/data transfer fault), or
  - Potential 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 at least with the red-light driver warning. The messages include instructions to the driver in case exiting or staying away from the vehicle is required.
- Haptic warning: Haptic warning 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 when the system is at the same time attempting to reach safe state and degraded operation.

9 APPLICATION OF THE FUNCTIONAL SAFETY CONCEPT

This study uses the example safety goals identified for the generic Gasoline engine ACS/ETC system introduced in this research and exercises the functional safety concept process depicted on Figure 9. Through this process, this study identifies 179 illustrative safety related engineering requirements for the concept ACS/ETC system and its components.[15]

These include 103 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 76 additional safety requirements related to the generic ACS/ETC system and components based on the use of STPA as well as the additional safety strategies suggested in MIL-STD-882E [2]. These 76 requirements are out of the scope of the Functional Safety Concept in ISO 26262 Part 3. 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 76 requirements.

9.1 Example Vehicle-Level Safety Requirements (Safety Goals)

Vehicle-level safety requirements for the generic ACS/ETC system correspond to the example safety goals presented in Table 17. 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 is to be mitigated in accordance to 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 to ASIL B classification.

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

- Insufficient vehicle propulsion is defined as the vehicle deviating from the correctly functioning speed increase profile when the driver increases the angular position of the accelerator pedal under any operating conditions by more than TBD sigma.

[15] 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 propulsion power loss/reduction resulting in vehicle deceleration exceeding the driver's intent by TBD m/s^2 or vehicle stalling is to be mitigated in accordance to ASIL D classification.

SG 4: Potential insufficient vehicle deceleration is to be mitigated in accordance to ASIL C classification.

- Insufficient vehicle deceleration is defined as vehicle deviating from the correctly functioning speed decrease profile when the driver decreases the angular position of the accelerator pedal under any operating conditions by more than TBD sigma.

SG 5: The ACS/ETC control algorithm is to choose the throttle command that has the highest priority for safety in accordance to ASIL D 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 all faults 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.
- If a failure that could lead to the vehicle-level hazards occurs, 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.
- If a failure that could lead to the vehicle-level hazards occurs, a warning is to be sent to the driver, and when necessary, the actions required by the driver are to be communicated to them.

9.2 Gasoline Engine ACS/ETC System and Components Functional Safety Requirements

Following the Concept Phase (Part 3) in ISO 26262, this study identifies 103 example functional safety requirements for the generic ACS/ETC system and its components. The distribution of these requirements is as follows.

1. General ACS/ETC System – 11 requirements
2. AP Assembly – 8 requirements
3. ECM – 64 requirements
4. Communication Signal – 8 requirements
5. Power Supply – 7 requirements
6. BP Assembly – 1 requirement
7. Interfacing System – 4 requirements

Table 23 shows examples of safety requirements associated with the ECM 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 ECM. The safety analysis identifies many ECM failure modes and CFs that could potentially lead to the violation of SG 1. Here, two ECM controller hardware failures are chosen as examples to illustrate the development process of safety requirements.

Table 23. Examples of ECM Safety Requirements

<table>
<tr><th>Safety Goal</th><td>SG 1: Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 to be mitigated in accordance to the identified ASIL level.</td></tr>
<tr><th>ASIL</th><td>D</td></tr>
<tr><th>Component</th><td>ECM</td></tr>
<tr><th>Safety Analysis (Examples)</th><td>• Hardware fault (sensors, ICs, etc.)
• Internal connection fault (short or open)</td></tr>
<tr><th>Safety Strategy</th><th>Potential Safety Requirements (Examples)</th></tr>
<tr><td>Detection</td><td rowspan="3">All single-point ECM 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.</td></tr>
<tr><td>Fault Tolerance</td></tr>
<tr><td>Safe State</td></tr>
<tr><td>Warning</td><td>The ECM 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 fault(s), including the time at which the fault was detected and the nature of the fault
• The time interval from the detection of the fault to reaching 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.</td></tr>
</table>

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 safe state in Table 23.

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/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 warning could be the one described in Table 23.

The rest of this section lists the 103 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 various levels of ASILs. The requirement may be implemented using different ASIL classification if independence among the implementation solutions can be demonstrated (Part 9 Clause 5.2 of ISO 26262).

9.2.1 General ACS/ETC System-Level Functional Safety Requirements

There are 11 general system-level functional safety requirements derived for the generic ACS/ETC system examined in this study, corresponding 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 C/D**).
    a. Critical parameters include those that are used to calculate the magnitude of the propulsion torque and throttle position, the low voltage power, the vehicle speed, engine RPM, and vehicle direction (forward or reverse).
    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 throttle valve actuator
        - The throttle valve position sensor
        - The communications channels between the APPS and the ECM, between the ECM and the throttle actuator controller, and between the throttle position sensor and the throttle actuator controller
        - A confirmation of the sanity and health of the ECM and throttle actuator controller 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[16]
    - State-of-health checks may include:
        - RAM/ ROM/ EEPROM tests,
        - Analog-to-digital converter test, and
        - 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 the event a failure is detected during the periodic self-tests, the ACS/ETC is to transition to the appropriate safe state within TBD ms.
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, in case of a failure of one element, 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 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 Diagnostic Trouble Codes (DTCs) are to be set (**ASIL QM/A/B**). The diagnostics approach is to cover:
   - Hardware: APPS, ECM, throttle actuator controller, and communication hardware.
   - Software Functions: APP calculations, torque command determination, throttle control, and BTO.
7. The ACS/ETC is to include diagnostics covering the following failure modes (**ASIL QM/A/B**).

---

[16] 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.

- APPS:
    - IC faults
    - Open/short I/Os
    - Stuck on the same reading
    - Out of range
    - Offset
    - State of Health
- TPS:
    - IC faults
    - Open/short I/Os
    - Stuck on the same reading
    - Out of range
    - Offset
- Throttle Motor
    - Circuit faults
    - Open/short I/Os
    - Stuck at the same position
- Harnesses and Connectors
    - Open/short circuits

8. The ACS/ETC system is to log and retain data that can be used to reconstruct the vehicle operating scenario prior to any faults that lead to a violation of a safety goal. The recording time is to be TBD seconds before and TBD seconds after the safety goal violation event. The data may include sensor data, human-machine interface data, communication signals, and values of critical parameters used in the propulsion torque and throttle position calculations **(ASIL QM)**. The following data may be considered.
    - Ignition switch status
    - Gear selector position
    - Vehicle speed
    - Vehicle direction
    - APPS value
    - ACC system settings
    - AEB system state
        - Object distance from vehicle
    - Driver assist safety systems status
    - Brake/stability control system status
        - ABS
        - TCS
        - ESC
    - 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 commending changes to propulsion torque
- Arbitration logic decisions by the ECM
- ECM propulsion torque request to throttle actuator controller (if used)
- Throttle actuator controller acknowledgement of propulsion torque request
- Throttle motor current command
- ECM received torque request from ACC
- ECM received torque request from AEB
- Steering torque sensor value
- Vehicle yaw rate

9. DTCs are to be set every time a safety goal may be violated (**ASIL QM**).
10. Diagnostics covering the safety related functionality of the ACS/ETC system components and connections (including ECM, throttle actuator controller, APPS, TPS, 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 A/B/QM**).
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 C/D**).

9.2.2 Accelerator Pedal Assembly Functional Safety Requirements

There are eight AP assembly functional safety requirements derived for the generic ACS/ETC system studied in this project, corresponding to all established safety goals.

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 C/D**).
2. The health and sanity of the APPS is to be monitored and confirmed under all operating vehicle conditions (**ASIL C/D**).
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. The value of the APP is to be communicated to the ECM (**ASIL B/C/D**):
    - The communication message or data transfer is to be qualified for validity (sent and received signals are the same), correctness (within range), and rationality (does not contradict with previous or other related signals/messages).
    - The updated value of the APP is to be received within TBD seconds. This time shall be specified to support the timely update of the throttle position to prevent the potential violation of any safety goal.

6. In case of a fault that violates a safety goal, the APPS is to communicate the fault to the ECM (**ASIL B/C/D**). Causes of faults may include:
    - Internal hardware failure,
    - Degradation over time,
    - Overheating due to increased resistance in a subcomponent or internal short, and
    - Reporting frequency too low.
7. The APPS is to have diagnostics for safety-relevant failures that could be caused by electromagnetic interference/electrostatic discharge, contamination, and other environmental condition (**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.
    - Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.

9.2.3 Engine Control Module Functional Safety Requirements

There are 64 ECM functional safety requirements that are derived in this project. Many of these requirements correspond to all established safety goals. In the writing below, these requirements do not have safety goals specifically stated in them. 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 ECM controller are to be ensured (**ASIL C/D**).
    - Power-on self-tests are to be implemented to check the health of the controller. These tests may include:
        - CPU and Register Tests to check the internal working of the CPU. All CPU registers associated with the propulsion torque and throttle position control functions are to be checked as part of this test.
        - Interrupt and Exception Tests to check the interrupt and exception processing of the controller.
        - EEPROM Checksum Test to check the EEPROM health.
        - Device Tests to check the peripheral devices connected to the controller.
2. The ECM's I/O pins are to be monitored for shorts or ground (**ASIL B/C/D**).
3. The ECM is to have diagnostics for potential safety relevant failures caused by EMI/ESD, contaminations, organic growths, single event effects, and other environmental conditions (**ASIL B/C/D**).
4. All single point ECM 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 ECM is to ensure the correct operation of the A/D conversion of sensor signals (**ASIL C/D**).
6. The ECM is to arbitrate between multiple requests for propulsion torque modifications from interfacing vehicle systems and the driver (**ASIL B/C/D**).
7. The arbitration strategy is to clearly define the action of the ACS/ETC system when there are conflicting propulsion torque requests from interfacing systems, the driver, and/or internal ACS/ETC functions (e.g., BTO) (**ASIL B/C/D**).
8. The ECM arbitration logic strategy and algorithm are to be checked for health and sanity periodically based on the FTTI (**ASIL D**).
    - In case of a failure in this arbitration strategy, the ACS/ETC system is to transition into Safe State 1 within a FTTI of TBD seconds and an amber light driver warning is to be issued.
9. The output of the ECM arbitration logic is to be qualified for validity and correctness (**ASIL D**).
10. The ECM is to calculate the propulsion torque based on inputs from the AP, vehicle speed sensor, vehicle direction sensor, and the inputs from the other vehicle systems that command propulsion or braking torque, such as ACC and AEB (**ASIL B/C/D**).
11. The propulsion torque command is to be controlled and updated with the correct magnitude and within the correct time duration (**ASIL B/C/D**).
12. The ECM's propulsion torque control algorithm is to include a speed increase/decrease profile. The torque calculation algorithm is to specify the parameters that form the basis for the ramp rate profile (e.g., vehicle speed) (**ASIL C/D**). **Safety Goals: 2 and 4.**
13. The time duration required to update the torque command is not to result in violation of a safety goal (**ASIL B/C/D**).
    - The time duration is to be reflected in the execution time of the relevant software functions.
14. Critical communications and data transfer between the ECM and other vehicle systems or components are to be qualified for validity and correctness (plausibility and rationality). This includes the transmission range sensors (**ASIL D**), vehicle directional sensor (**QM**), and all other inputs that are used by the ECM in the propulsion torque control algorithm.
15. All other critical parameters used by the torque control algorithm are to be checked periodically based on the FTTI requirements (**ASIL B/C/D**).
16. The ECM is to correctly adjust the propulsion torque when it receives a communication of a braking action by the braking system (**ASIL B/C/D**).
17. The ECM is to access the metrics that clearly define the limits of vehicle stability from the appropriate vehicle system (e.g., brake/stability control system) (**ASIL D**). **Safety Goals: 1 and 3**.

18. The ECM is to qualify the input(s) for stability metrics for validity and correctness (plausibility and rationality) (**ASIL D**). **Safety Goals: 1 and 3**.
19. The propulsion torque computed by the torque control algorithm is to be validated against the vehicle stability metrics before any propulsion torque command is issued (**ASIL D**). **Safety Goals: 1 and 3**.
    - If the calculated propulsion torque exceeds the vehicle stability limits, the ACS/ETC system is to transition into Safe State 2 within a FTTI of TBD seconds and an amber light driver warning is to be issued.
    - Appropriate driver notifications from affected interfacing systems are to be issued.
20. The ECM is to correctly adjust the propulsion torque in response to propulsion torque modification requests by other vehicle systems, such as AEB and ACC (**ASIL B/C/D**).
21. Critical communications and data transfer between the ECM 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**).
    - In case of the detection of a fault, the correct failure mode effect mitigation strategy is applied.
    - Critical communications and data transfer include communication signals that request propulsion torque modifications and diagnostics (failure) information of these systems.
    - This requirement also includes detecting erroneous torque commands issued by malicious intruders or aftermarket components.
22. The throttle position is to be controlled and updated in the correct direction within the correct time duration under all vehicle operating conditions. The time duration required to update the throttle position is not to result in uncontrolled propulsion condition (failure mode in software execution or execution time) (**ASIL D**). **Safety Goals: 1 and 5.**
23. The throttle position function is to qualify the communication and data transfer between the ECM and the APPS for validity and correctness (plausibility and rationality) (**ASIL B/C/D**).
    - In case of a fault, the correct failure mode effect mitigation strategy is to be applied.
    - The critical communications include the APP and the diagnostics of the APPS.
24. The throttle actuator controller is to have a throttle position drive and control (TPDC) algorithm for all engine speeds (**ASIL B/C/D**).
25. All electrical hardware and software elements associated with the delivery of the TPDC function are to comply with ASIL D classification for SG1 and SG3, ASIL C classification for SG2 and SG4, and ASIL B classification for SG1a unless otherwise specified (**ASIL B/C/D**). If independence of the elements (Part 9 Clause 5.2 of ISO 26262) cannot be demonstrated, the higher ASIL classification is to be adopted.

26. The throttle actuator controller is to drive the throttle to the position commanded by the ECM within TBD seconds (**ASIL B/C/D**).
27. The throttle actuator controller is to control the throttle position to within a pre-established tolerance band based on the vehicle operating situation that does not result in the potential violation of a safety goal (**ASIL B/C/D**).
28. The throttle actuator controller is to determine the throttle position at all times. The throttle position is to be qualified for validity and correctness (**ASIL B/C/D**).
29. All faults that result in a failure to determine the throttle position are to be detected. In case of a failure in detecting the throttle position, the system is to transition into Safe State 6 and a red-light driver warning is to be issued (**ASIL B/C/D**).
30. The health and sanity of the TPDC algorithm are to be checked periodically based on the correct FTTI to prevent potential violations of the safety goals (via an auxiliary processor or equivalent means), or a throttle position detection mechanism is to be employed (**ASIL B/C/D**).
    - Fault tolerant strategy is to be applied. The fault tolerant techniques may include redundancy, voting logic, or other techniques.
    - Control flow monitoring strategy is to be applied for the TPDC.
31. Critical communications and data transfer between the throttle actuator controller and other throttle body sub-system components is to be qualified for validity and correctness (plausibility and rationality) (**ASIL B/C/D**). The critical communications and data transfer include:
    - The actuator position and diagnostics associated with the actuator position determination/sensing mechanism
    - Actuator diagnostics
    - The throttle valve position sensor and its diagnostics if a sensor is used
32. All critical parameters used by the TPDC algorithm that may lead to potential violation of any safety goal when not correct is to be checked periodically based on the FTTI requirements (**ASIL B/C/D**).
33. The output of the TPDC algorithm is to be verified for validity and correctness (**ASIL B/C/D**).
34. In case of a fault, the throttle actuator controller is to communicate the fault to the ECM (**ASIL B/C/D**).
35. In case of a fault in the TPDC that results in a failure that could lead to potential violation of a safety goal, the system is to transition into Safe State 6, within TBD ms time (200 ms is considered in the industry for similar safety goals), and a red-light driver warning is to be issued. DTCs are to be set (**ASIL B/C/D**).
36. All single point throttle actuator controller hardware faults that may lead to potential violations of a safety goal are to be detected and mitigated within the FTTI. In case of a failure, the system is to transition to the corresponding safe state (**ASIL B/C/D**).

- Hardware faults include those occurring in the ICs, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.

37. All electrical hardware and software elements associated with the delivery of the TPDC function are to comply with ASIL D classification for SG1, SG3, and SG5, ASIL C classification for SG2 and SG4, and ASIL B classification for SG1a 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 (**ASIL B/C/D**).
38. The data, in addition to the APP, used in determining the requested propulsion torque is to be qualified for correctness and validity, including vehicle speed (**ASIL D**), engine speed (**ASIL D**), and altitude measurement **(QM)**. If torque maps or look up tables are used, their content is to be checked for validity and correctness at the correct frequency (**ASIL D**).
39. The ECM is to qualify the APP input for validity and correctness (plausibility and rationality) (**ASIL B/C/D**).
40. The ECM algorithm or method for calculating the throttle position is to be validated (**ASIL B/C/D**).
41. The throttle position corresponding to the propulsion torque requested by the driver or other vehicle systems is to be calculated correctly and the results is to be qualified for validity and correctness under all vehicle operating conditions (**ASIL B/C/D**).
42. The throttle position is to be controlled and updated in the correct direction within the correct time duration under all vehicle operating conditions (**ASIL B/C/D**).
43. The time duration required to update the throttle position is not to result in a potential violation of a safety goal. The time duration is to be reflected in the relevant software function execution time and the transient response of the throttle valve actuator (**ASIL B/C/D**).
44. The APP to propulsion torque rate of change mapping is to be monitored for correctness (**ASIL C**). **Safety Goals: 2, 4, and 5**.
45. The ECM throttle position control algorithm is to be checked periodically based on the correct FTTI to prevent the potential violation of safety goals (**ASIL C/D**).
    - Fault tolerant strategy is to be applied for the TPCA. The fault tolerant techniques may include redundancy, voting logic, or other techniques.
    - Control flow monitoring strategy is to be applied to the TPCA.
46. In case of a fault in the TPCA that leads the ECM unable to control the throttle position, the ACS/ETC is to transition into Safe State 6 within TBD ms. Some industry practices establish this TBD time at 200 ms. The red-light driver warning is to be issued (**ASIL B/C/D**).
    - For failures that prevent the ECM from controlling the throttle idle position, the FTTI at idle engine speed may be longer than the FTTI for operating speeds above idle engine speed.
    - DTCs are to be set.

47. The ECM is to communicate the correct throttle position to the throttle actuator controller under all vehicle operating situations within TBD time units (**ASIL B/C/D**).
48. Communications of the throttle position between the ECM and throttle actuator controller 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**).
49. Critical communications and data transfer between the ECM and other vehicle systems/components are to be qualified for validity and correctness (plausibility and rationality) including the BP sensor (**ASIL D**), vehicle speed sensor (**ASIL D**), engine RPM sensor (**ASIL D**), and all other inputs that are used by the TPCA including any external clock or other timing signals used by the ECM.
    - If the vehicle speed and engine speed are used redundantly, the ASIL classification may be applied based on a selected ASIL decomposition strategy.
50. All other critical parameters used by the TPCA are to be checked periodically based on the FTTI requirements (**ASIL B/C/D**).
51. 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 5**.
52. The ECM is to provide BTO control (**ASIL C**).
53. The ECM BTO control is to command a pre-determined throttle position 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**).
54. The ECM BTO control strategy is to include provisions, if necessary, for 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**).
55. The BTO control algorithm is to execute within TBD seconds (**ASIL C**).
56. The ECM BTO control algorithm is to be checked periodically based on the correct FTTI to prevent potential violation of the safety goals (**ASIL C**).
    - Fault tolerant strategy is to be applied, including redundancy, voting logic, or other techniques.
    - Control flow monitoring strategy is to be applied for the BTO.
    - 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.
57. 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**).
58. All requests or commands for change in the propulsion torque by other vehicle systems are to be ignored when BTO is activated (**ASIL C**).

59. In the event of ECM malfunction resulting in the loss of BTO control function, the ACS/ETC is to be able to reduce the throttle opening (**ASIL A/B/C**). **Safety Goals: 2 and 5**. Recommended implementation strategies include:
    - Enter Safe State, and
    - Implement a BTO control function that is subordinate to the ECM BTO control function.

    The ASIL classification to this requirement depends on whether it is a part of ASIL decomposition or if it is a safety mechanism to the ECM BTO function.
60. The ECM is to have a mechanism to prevent unauthorized access to the ECM software, including propulsion torque control calculations, throttle position control algorithms, and relevant command paths. (**ASIL B/C/D**).
61. All single point faults that result in a failure to prevent unauthorized access to the ECM are to be detected and mitigated (**ASIL B/C/D**).
    - In the event of unauthorized access to the ECM, 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.
62. Diagnostics covering the failures for the following parts of the ECM 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
        - central processing unit
        - processor memory
        - arithmetic logic unit
        - registers
        - A/D converter
        - 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
        - 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

63. Diagnostics covering the failures for the following parts of the throttle actuator controller are to be implemented (**ASIL QM/A/B**):
    - The list is the same as those in the requirement above.
64. The ECM 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 fault 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 Communication Signal Functional Safety Requirements

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

The critical communication signals include the following.

- APPS signal(s) from the APPS to ECM
- APPS fault diagnostics signal
- BPPS signal to ECM
- Communication channel "secure" signals between ECM and throttle actuator controller
- Communication channel “secure" signals between ECM and the following.
  - AEB
  - CC/ACC
  - Other systems that can request modification to the propulsion torque
  - Commands/requests for propulsion torque modifications from interfacing systems to ECM
  - Vehicle speed signal
  - Vehicle direction signal
  - Command for throttle position signal from the ECM to throttle actuator controller (if used)

- Throttle actuator controller fault diagnostics signal (if used)
- Throttle position sensor signal from the TPS to the throttle actuator controller (if used)
- Throttle position signal from the throttle actuator controller (if used) to the ECM
- TPS fault diagnostics signal
- Actuator rotor position signal from the actuator to the throttle actuator controller (if used)
- Driver warning signal
- Low voltage power loss from the low voltage power system to ECM signal
- CAN bus failure from the CAN bus to the ECM signal

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 ECM of the fault
    - Invoke the correct failure mode effect mitigation strategy
2. The CAN bus is to support the communication of the ACS/ETC with the rest of the vehicle systems to support the safe operation of the ACS/ETC (**ASIL B/C/D**).
3. The CAN bus is to be designed to avoid overload (**ASIL B/C/D**).
4. The CAN bus is to support the qualification of all critical CAN signals between the ACS/ETC and the interfacing vehicle systems (**ASIL B/C/D**).
5. The CAN bus is to prevent the corruption of the critical CAN signals during transmission between the ACS/ETC and the interfacing vehicle systems (**ASIL B/C/D**).
6. ACS/ETC system is to detect malicious intrusion of the signal on CAN bus, and prevent it from further harm (**ASIL B/C/D**).
7. In case of malfunction of the CAN bus or CAN module, the CAN communication system is to inform the ECM (**ASIL B/C/D**).
8. If the value of the APP is communicated to ECM through data bus, the APPS data is to have the highest level of signal priority (**ASIL B/C/D**).

9.2.5 Power Supply Functional Safety Requirements

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

1. The low voltage power supply is to provide the ACS/ETC and interfacing systems and sensors with the required low voltage power supply for operation (**ASIL D**).
2. The ACS/ETC is to have a redundant low voltage power supply. In case of a fault in the vehicle's low voltage power supply system, the redundant power supply is to activate

within TBD ms and sustain the low voltage power supply to the ACS/ETC for a duration greater than the longest FTTI of the ACS/ETC (**ASIL 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 low voltage power supply system operation (**ASIL B/C/D**).
5. All communications and data transfer sent by the low voltage power system to the ACS/ETC are to be qualified for validity and correctness (plausibility and rationality). This includes the low voltage power system diagnostics information (**ASIL D**).
6. 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 6 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**).
7. The APPS is to be able to detect the loss and abnormality (spike, intermittent failure, etc.) in its low voltage power supply, and inform the ECM that its reading may be affected (**ASIL C/D**).

9.2.6 Brake Pedal Assembly Functional Safety Requirements

There is one functional safety requirement for the BP assembly. It corresponds to all safety goals.

1. Critical communication and data transfer between the BPPS and the ECM 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**).

9.2.7 Interfacing Systems Functional Safety Requirements

There are four functional safety requirements for the interfacing systems, corresponding to all safety goals.

1. All requests or commands for propulsion torque modifications from vehicle interfacing systems are to be sent to the ECM (**ASIL B/C/D**). This includes the following.
    a. Request for torque increase or decrease from the CC/ACC system
    b. Request for torque reduction from the braking system including the AEB module (directly or indirectly through the braking system module)
    c. Request for torque modification from the TCS
    d. Request for torque modification from the ESC system
2. All communications and data transfer regarding requests or commands for propulsion torque modifications sent by the vehicle interfacing systems to the ECM are to be

qualified for validity and correctness (plausibility and rationality) by the sending system (**ASIL D**).
3. All interfacing systems are to inform the ECM in case of any failure that may cause the system, and the ECM is to transition into a degraded mode of operation (**ASIL B/C/D**).
4. In case of a fault in the transmitted information to the ECM from the interfacing system, the correct failure mode effect mitigation strategy is to be applied (**ASIL B/C/D**).

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 [2] 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 76 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 ACS/ETC System – 18 requirements
2. AP Assembly – 5 requirements
3. ECM – 35 requirements
4. Throttle Assembly – 1 requirement
5. BP Assembly – 5 requirements
6. Interfacing Systems – 12 requirements

9.3.1 <u>General ACS/ETC System-Level Safety Requirements</u>

This study identifies 18 general system-level safety requirements for ACS/ETC system outside the ISO 26262 Functional Safety Concept scope Part 3. These requirements correspond to all safety goals.

1. The packaging for 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 manufacturing process is to ensure the correct calibration of the critical interfacing sensors in the ECM (**ASIL B/C/D**).

5. The calibration of the safety critical sensors is to be checked and verified to be correct (**ASIL B/C/D**). Typical ACS/ETC safety critical sensors include the following.
    - TPS
    - APPS
    - BPPS
    - Engine RPM sensor
    - MAF/MAP
6. The calibration of the safety-critical actuators and their safety-critical characteristics (e.g., sizing) are to be checked and verified to be correct (**ASIL B/C/D**). Typical ACS/ETC safety-critical actuators include the following.
    - Throttle motor
    - Throttle valve
7. The ACS/ETC components are to meet the reliability and functional degradation requirements (**ASIL B/C/D**).
8. The APPS and TPS are to have TBD failure rate for 100,000 miles and under all normal vehicle operating conditions (to be specified including temperature, vibration, moisture, etc.) (**ASIL C/D**). Sensor failures may include, but are not limited to the following.
    - Hardware failure
    - Degradation over time
    - Internal short and increased resistance
9. The ACS/ETC components and connections are to meet the standards for EMI/EMC with the environment and the vehicle to prevent malfunctioning of the ECM, corruption of critical parameters including the torque maps, and corruption of software algorithms (**ASIL B/C/D**).
10. 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**).
11. The ACS/ETC components and connections are to meet the vibration and shock impact requirements (**ASIL B/C/D**).
12. 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**).
13. The ACS/ETC components and connections are to be designed to prevent organic growth from the external environment (e.g., fungi) that affects the safe functioning of the ACS/ETC (**ASIL B/C/D**).
14. 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**).

15. Active connection terminals are to be designed to prevent the ingress of moisture, corrosion, and contamination from the external environment or other systems in the vehicle (**ASIL B/C/D**).
16. 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**).
17. 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**).
18. 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**).

9.3.2 Accelerator Pedal Assembly Safety Requirements

This study identifies five 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. The APPS is to have TBD failure rate for 100,000 miles and under all normal (TBD) vehicle operating conditions (**ASIL C/D**). Sensor failures may include:
    - Hardware failure,
    - Degradation over time, and
    - Internal short and increased resistance.
2. The APPS is to have TBD reporting frequency so that the APP input is updated sufficiently (**ASIL C/D**).
3. AP assembly mechanical faults that result in incorrect measurement of the APP are to be detected and mitigated (**No ASIL—not within the scope of ISO 26262**).
    - Incorrect measurements include deviations from the correct APP value or being stuck at the same value permanently or intermittently.
4. The AP assembly critical mechanical components are to meet the life and durability requirements of TBD miles without any critical failures (**No ASIL—not within the scope of ISO 26262**).
5. 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 Engine Control Module (Including Throttle Actuator Control Function) Safety Requirements

This study identifies 35 ECM safety requirements outside the ISO 26262 functional Safety Concept scope (Part 3 of ISO 26262). Many of these requirements correspond to all vehicle-level safety goals. These requirements do not have safety goals specifically stated in them. However, some of the functional safety requirements correspond to only a subset of the safety goals. These requirements have the safety goals listed at the end.

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 ECM 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 ECM software algorithm is to correctly write to memory (**ASIL B/C/D**).
5. The ECM is to correctly calculate the engine load (e.g., additional load from accessories, such as A/C) and the results are to be qualified for validity and correctness under all vehicle operating conditions (**ASIL B/C/D**).
6. The ECM 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 ECM enters a degraded operating state (**ASIL B/C/D**).
7. The ECM software code is to be verified for correctness, including any automatically generated code (**ASIL B/C/D**).
8. The ECM is to verify the correctness of all clock or ECM internal timing signals (**ASIL B/C/D**).
9. Any unused circuits or pins in the ECM are to be properly managed to prevent unwanted signals or other interference with the ECM function (**ASIL B/C/D**).
10. The ECM IC board and its subcomponents are to have TBD reliability over the lifetime of the vehicle and under all vehicle operating conditions (to be specified including temperature, vibration, moisture, etc.) (**ASIL C/D**).
11. The ECM memory storage block is to have TBD quality and reliability over the lifetime of the vehicle and under all vehicle operating conditions (to be specified including temperature, vibration, moisture, etc.) (**ASIL C/D**).
12. The ECM is to command an increase in the throttle opening when another vehicle system requests an increase in torque and the driver is not issuing a conflicting command. If the driver is issuing a conflicting command, the conflict is to be resolved according to the ACS/ETC system's pre-established strategy for resolving conflicts among the commands from the driver and other vehicle systems (**ASIL B/C/D**).
13. The ECM is to command an increase in the throttle opening when the driver increases the angular position of the AP and the ECM is in normal mode or is transitioning from BTO to normal mode, unless another vehicle system with a higher priority than the AP input issues a conflicting torque request (**ASIL C/D**).

14. The ECM is not to command an increase in the throttle opening if the driver does not increase the AP angular position, unless another vehicle system with a higher priority than the AP input requests a torque increase and the ECM is in normal mode (**ASIL B/C/D**).
15. The ECM is not to command a decrease in the throttle opening if the driver is maintaining or increasing the AP angular position, unless another vehicle system with a higher priority than the AP input requests a torque decrease and the ECM is in normal mode (**ASIL B/C/D**).
16. The ECM is to command a decrease in the throttle opening if the driver reduces the APP while in normal mode, unless another vehicle system with a higher priority than the AP input issues a conflicting torque request (**ASIL B/C/D**).
17. The ECM is not to command a decrease in the throttle opening without a clear command to reduce torque from the driver or other vehicle systems. Any conflicting torque requests are to be resolved based on the system's prioritization strategy (**ASIL B/C/D**).
18. The ECM is to determine the idle position of the throttle based on the vehicle's current operating conditions. The idle throttle position is to be qualified for validity and correctness, and checked for plausibility (**ASIL B/C/D**).
19. When entering BTO mode, the ECM is to reduce the throttle opening to the idle position or other pre-set BTO throttle position (**ASIL C**).
20. The ECM is not to reduce the throttle opening below the idle position or other pre-set BTO throttle position while in BTO mode or when transitioning out of BTO mode (**ASIL C**).
21. The ECM 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 D**).
22. The ECM is to be able to detect when the throttle assembly does not respond properly to the ECM's command to enter or exit BTO mode. If the throttle assembly is not responding properly, the ACS/ETC is to still be capable of entering BTO mode (**ASIL C**).
23. If an activation delay time is incorporated into the control algorithms for entering or exiting BTO mode, the ECM is to have a specific activation delay time and shall monitor the activation delay timing (**ASIL C**).
24. In case of a fault in entering BTO mode or entering Normal mode, the ECM is to invoke the proper fault mitigation strategy, including transition to a safe state, if required, and alerting the driver (**ASIL C**).
25. The ECM 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 ECM is not to enter the BTO mode (**ASIL C**).

26. The ECM BTO and normal mode control algorithms are to have a specified vehicle speed threshold for entering BTO mode and the ECM is to monitor the vehicle speed (**ASIL C**).
27. The ECM is not to enter BTO mode when the BP is not pressed (**ASIL C**).
28. The ECM is not to exit BTO mode while both the AP and BP are still pressed (**ASIL C**).
29. The ECM BTO control model design is to be verified and validated for correctness, including pedals sequencing, critical process parameters, and timing (**ASIL C**).
30. When entering normal mode, the ECM is to resume responding to the driver's torque request via the AP (**ASIL B/C/D**).
31. The ECM is not to command an increase in the throttle opening while in BTO mode or while transitioning into BTO mode (**ASIL C**).
32. The ECM is not to command an increase in the throttle opening 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**).
33. Other vehicle systems are not to have the authority to command the ECM to exit BTO mode (**ASIL C**).
34. Incorporating additional requirements into the BTO algorithm beyond the APP, BPP, and vehicle speed are not to prevent the ECM from entering BTO mode when the driver's intention is to stop the vehicle. (**ASIL C/D**).
35. Incorporating additional requirements into the BTO algorithm beyond the APP and BPP, and vehicle speed are not to prevent the ECM from exiting BTO mode when the driver's intention is to resume acceleration. (**ASIL C**).

9.3.4 Throttle Assembly Safety Requirements

This study identifies one throttle assembly safety requirement outside the ISO 26262 Functional Safety Concept scope Part 3. This requirement corresponds to all safety goals.

1. The air intake stream is to be protected against any contamination or debris that could affect the movement of the throttle valve (**No ASIL—not within the scope of ISO 26262**).

9.3.5 Brake Pedal Assembly Safety Requirements

This study identifies five safety requirements for the BP assembly outside the ISO 26262 Functional Safety Concept scope Part 3 . These requirements trace back to all safety goals.

1. The BPP value is to be measured, and the value is to be valid and correct (**ASIL B/C/D**).
2. The BPPS is to have TBD reporting frequency so that the BPP is updated sufficiently (**ASIL B/C/D**).
3. 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**).

4. 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**).
5. BP mechanical assembly faults that result in incorrectly measurement of the BPP are to be detected and mitigated (**No ASIL—not within the scope of ISO 26262**).
    - Incorrect measurements include deviations from the correct BPP value or being stuck at the same value permanently or intermittently.

9.3.6 Interfacing Systems Safety Requirements

This study identifies 12 safety requirements for interfacing vehicle systems that are outside the ISO 26262 Functional Safety Concept scope Part 3. These requirements correspond to all safety goals.

1. Interfacing vehicle systems are to correctly identify themselves (according to the ECM prioritization strategy) when issuing torque requests to the ECM (**ASIL B/C/D**).
2. The interfacing system components are to meet the reliability and functional degradation requirements (**ASIL B/C/D**).
3. The packaging for interfacing system components and connections are to meet the standards for packaging clearances (**ASIL B/C/D**).
4. The interfacing system components and connections are to be protected from physical interference from foreign objects (e.g., road debris) (**ASIL B/C/D**).
5. The design and packaging for the interfacing system's critical sensors (e.g., engine RPM, mass airflow, wheel speed, etc.) are to consider the effect of the surrounding heat generation (**ASIL B/C/D**).
    - The temperatures of the interfacing system's critical sensors (e.g., engine RPM, MAF, wheel speed, etc.) is to be monitored.
6. The interfacing system assemblies are to be free from 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**).
7. The interfacing vehicle systems are to meet the standards for EMI/EMC with the environment and the vehicle (**ASIL B/C/D**).
8. The interfacing system 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**).
9. The interfacing system components and connections 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 meet the ambient temperature requirements considering the packaging location in the vehicle. The temperature of the components is to be monitored (**ASIL B/C/D**).

11. The interfacing system components and connections are to be designed to prevent organic growth from the external environment (e.g., fungi) that affects the safe functioning of the ACS/ETC (**ASIL B/C/D**).
12. The interfacing system components are to mitigate the effects of magnetic interference from other vehicle components, as well as the external environment (**ASIL B/C/D**).

10 OBSERVATIONS

This study follows the process in the ISO 26262 Concept Phase to develop safety requirements for the gasoline engine 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 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 subsystem 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 S 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 16).

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 10 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 10, 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 [13]. 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 S and E.

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 because objective data typically do not exist to support the assessment, and expert opinions are often used. This observation corroborates previous assessments of ISO 26262 [14] [15].

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 [16]. 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 [14] [15].

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 179 potential safety requirements for the ACS/ETC system following the Concept Phase process Part 3 of ISO 26262. 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 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 3of ISO 26262 to derive a list of potential safety requirements for a generic ACS/ETC system. Specifically, this research:

1. Identified five 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.	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.	B
SG 2	Potential insufficient vehicle propulsion[i] is to be mitigated in accordance to the identified ASIL.	C[ii]
SG 3	Potential propulsion power loss/reduction resulting in vehicle deceleration greater than TBD m/s^2 or vehicle stalling is to be mitigated in accordance to the identified ASIL.	D
SG 4	Potential insufficient vehicle deceleration[i] is to be mitigated in accordance to the identified ASIL.	C[ii]
SG 5	The ACS/ETC control algorithm is to choose the throttle command that has the highest priority for safety in accordance to the identified ASIL.	D

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 accelerator pedal.*
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 noted for SG 2 and SG 4 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 levels of 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 103 illustrative functional safety requirements by following the Concept Phase in ISO 26262, 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 ACS/ETC System – 11 requirements
- Accelerator Pedal (AP) Assembly – 8 requirements
- Engine Control Module – 64 requirements
- Communication Signal – 8 requirements
- Power Supply – 7 requirements
- Brake Pedal (BP) Assembly – 1 requirement
- Interfacing Systems – 4 requirements

3. Identified 76 additional 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 [2]. The breakdown of the number of requirements is as follows.

    - General ACS/ETC System – 18 requirements
    - AP Assembly – 5 requirements
    - ECM – 35 requirements
    - Throttle Assembly – 1 requirement
    - BP Assembly – 5 requirements
    - Interfacing Systems – 12 requirements

    These 76 requirements are out of the scope of the Functional Safety Concept phase in ISO 26262 Part 3. 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 76 requirements.

REFERENCES

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

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

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

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

[5] 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.

[6] 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.

[7] Coudert, O. (1994). Two-Level Logic Minimization: An Overview. *Integration, the VLSI Journal, 17-2*, p. 97-140.

[8] Van Eikema Hommes, Q. D., Becker, C., & Najm, W. (2018, June). Functional safety assessment of a generic accelerator control system with electronic throttle control in diesel-fueled vehicles (Report No. DOT HS 812 585). Washington, DC: National Highway Traffic Safety Administration.

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

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

[17] 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

Appendix A: STPA Causal Factor Guidewords and Guidewords Subcategories

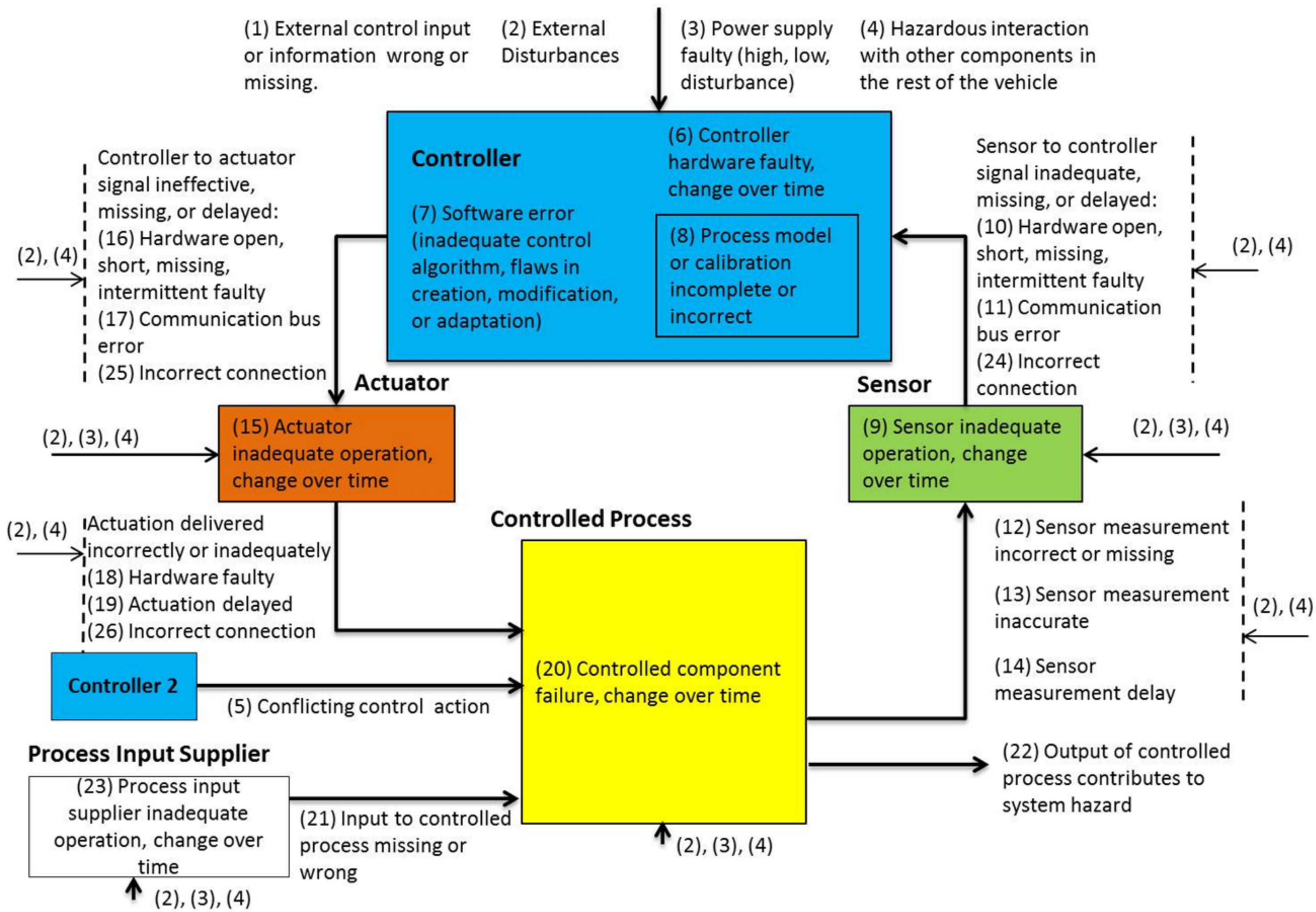


Figure A-1. Causal Factor Categories for Automotive Electronic Control Systems

Table A-1. Causal Factor Sub-Categories for Automotive Electronic Control Systems

The numbering in the table below corresponds to those in Figure A-1.

Components	
Controller	**(6) Controller hardware faulty, change over time** • Internal hardware failure • Overheating due to increased resistance in a subcomponent or internal shorting • Over temperature due to faulty cooling system • Degradation over time • Faulty memory storage or retrieval • Faulty internal timing clock • Faulty signal conditioning or converting (e.g., analog-to-digital converter, signal filters) • Unused circuits in the controller
	(7) Software error (inadequate control algorithm, flaws in creation, modification, or adaptation) • Inadequate control algorithm • Flaws in software code creation
	(8) Process model or calibration incomplete or incorrect • Sensor or actuator calibration, including degradation characteristics • Model of the controlled process, including its degradation characteristics
	(2) External control input or information wrong or missing • Timing-related input is incorrect or missing • Spurious input due to shorting or other electrical fault • Corrupted signal • Malicious Intruder
	(3) Power supply faulty (high, low, disturbance) • Loss of 12-volt power • Power supply faulty (high, low, disturbance)
	(2) External disturbances • EMI or ESD • Single event effects (e.g., cosmic rays, protons) • Vibration or shock impact • Manufacturing defects and assembly problems • Extreme external temperature or thermal cycling • Moisture, corrosion, or contamination • Organic growth • Physical interference (e.g., chafing)

	(4) Hazardous interaction with other components in the rest of the vehicle • EMI or ESD • Vibration or shock impact • Physical interference (e.g., chafing) • Moisture, corrosion, or contamination • Excessive heat from other components • Electrical arcing from neighboring components or exposed terminals • Corona effects from high voltage components
Sensor	**(9) Sensor inadequate operation, change over time** • Internal hardware failure • Overheating due to increased resistance in a subcomponent or internal shorting • Degradation over time • Over temperature due to faulty cooling system • Reporting frequency too low
	(3) Power supply faulty (high, low, disturbance) • Loss of 12-volt power • Reference voltage incorrect (e.g., too low, too high) • Power supply faulty (high, low, disturbance)
	(2) External disturbances • EMI or ESD • Single event effects (e.g., cosmic rays, protons) • Vibration or shock impact • Manufacturing defects and assembly problems • Extreme external temperature or thermal cycling • Moisture, corrosion, or contamination • Organic growth • Physical interference (e.g., chafing) • Magnetic interference
	(4) Hazardous interaction with other components in the rest of the vehicle • EMI or ESD • Vibration or shock impact • Physical interference (e.g., chafing) • Moisture, corrosion, or contamination • Excessive heat from other components • Magnetic interference • Electrical arcing from neighboring components or exposed terminals • Corona effects from high voltage components

<table>
<tr><td rowspan="8">Actuator</td><td>(15) Actuator inadequate operation, change over time</td></tr>
<tr><td>Internal hardware failure
Degradation over time
Over temperature due to faulty cooling system
Incorrectly sized actuator
Relay failure modes, including: 1) does not energize, 2) does not de-energize, and 3) welded contacts
Overheating due to increased resistance in a subcomponent or internal shorting</td></tr>
<tr><td>(3) Power supply faulty (high, low, disturbance)</td></tr>
<tr><td>Loss of 12-volt power
Power supply faulty (high, low, disturbance)</td></tr>
<tr><td>(2) External disturbances</td></tr>
<tr><td>EMI or ESD
Single event effects (e.g., cosmic rays, protons)
Vibration or shock impact
Manufacturing defects and assembly problems
Extreme external temperature or thermal cycling
Moisture, corrosion, or contamination
Organic growth
Physical interference (e.g., chafing)
Magnetic interference</td></tr>
<tr><td>(4) Hazardous interaction with other components in the rest of the vehicle</td></tr>
<tr><td>EMI or ESD
Vibration or shock impact
Physical interference (e.g., chafing)
Moisture, corrosion, or contamination
Excessive heat from other components
Magnetic interference
Electrical arcing from neighboring components or exposed terminals
Corona effects from high voltage components
Unable to meet demands from multiple components (e.g., inadequate torque)</td></tr>
<tr><td rowspan="4">Controlled Process</td><td>(20) Controlled component failure, change over time</td></tr>
<tr><td>Internal hardware failure
Degradation over time</td></tr>
<tr><td>(3) Power supply faulty (high, low, disturbance)</td></tr>
<tr><td>Loss of 12-volt power
Power supply faulty (high, low, disturbance)</td></tr>
</table>

Controlled Process	**(2) External disturbances** • EMI or ESD • Single event effects (e.g., cosmic rays, protons) • Vibration or shock impact • Manufacturing defects and assembly problems • Extreme external temperature or thermal cycling • Moisture, corrosion, or contamination • Organic growth • Physical interference (e.g., chafing) • Magnetic interference
	(4) Hazardous interaction with other components in the rest of the vehicle • EMI or ESD • Vibration or shock impact • Physical interference (e.g., chafing) • Moisture, corrosion, or contamination • Excessive heat from other components • Magnetic interference • Electrical arcing from neighboring components or exposed terminals • Corona effects from high voltage components • Unable to meet demands from multiple components (e.g., inadequate torque)
	(22) Output of controlled process contributing to system hazard
Process Input Supplier to Controlled Process	**(23) Process input supplier inadequate operation, change over time** • Process input supplier inadequate operation, change over time • Electrical noise other than EMI or ESD
	(3) Power supply faulty (high, low, disturbance) • Loss of 12-volt power • Power supply faulty (high, low, disturbance)
	(2) External disturbances • EMI or ESD • Single event effects (e.g., cosmic rays, protons) • Vibration or shock impact • Manufacturing defects and assembly problems • Extreme external temperature or thermal cycling • Moisture, corrosion, or contamination • Organic growth • Physical interference (e.g., chafing) • Magnetic interference

	(4) Hazardous interaction with other components in the rest of the vehicle • EMI or ESD • Vibration or shock impact • Physical interference (e.g., chafing) • Moisture, corrosion, or contamination • Excessive heat from other components • Magnetic interference • Electrical arcing from neighboring components or exposed terminals • Corona effects from high voltage components • Unable to meet demands from multiple components (e.g., inadequate torque)
Connections	
Sensor to Controller, Controller to Actuator	**(10) and (16) Hardware open, short, missing, intermittent faulty** • Connection is intermittent • Connection is open, short to ground, short to battery, or short to other wires in harness • Electrical noise other than EMI or ESD • Connector contact resistance is too high • Connector shorting between neighboring pins • Connector resistive drift between neighboring pins
	(11) and (17) Communication bus error • Bus overload or bus error • Signal priority too low • Failure of the message generator, transmitter, or receiver • Malicious intruder
	(24) and (25) Incorrect connection • Incorrect wiring connection • Incorrect pin assignment
	(2) External disturbances • EMI or ESD • Single event effects (e.g., cosmic rays, protons) • Vibration or shock impact • Manufacturing defects and assembly problems • Extreme external temperature or thermal cycling • Unused connection terminals affected by moisture, corrosion, or contamination • Organic growth • Physical interference (e.g., chafing) • Active connection terminals affected by moisture, corrosion, or contamination

	(4) Hazardous interaction with other components in the rest of the vehicle • EMI or ESD • Vibration or shock impact • Physical interference (e.g., chafing) • Unused connection terminals affected by moisture, corrosion, or contamination • Excessive heat from other components • Electrical arcing from neighboring components or exposed terminals • Corona effects from high voltage components • Active connection terminals affected by moisture, corrosion, or contamination • Mechanical connections affected by moisture, corrosion, or contamination
Actuator to Controlled Process	**(18) Actuation delivered incorrectly or inadequately: Hardware faulty**
	(19) Actuation delayed
	(20) Actuator to controlled process incorrect connection
	(2) External disturbances • EMI or ESD • Single event effects (e.g., cosmic rays, protons) • Vibration or shock impact • Manufacturing defects and assembly problems • Extreme external temperature or thermal cycling • Unused connection terminals affected by moisture, corrosion, or contamination • Organic growth • Physical interference (e.g., chafing) • Active connection terminals affected by moisture, corrosion, or contamination • Mechanical connections affected by moisture, corrosion, or contamination
	(4) Hazardous interaction with other components in the rest of the vehicle • EMI or ESD • Vibration or shock impact • Physical interference (e.g., chafing) • Unused connection terminals affected by moisture, corrosion, or contamination • Excessive heat from other components • Electrical arcing from neighboring components or exposed terminals • Corona effects from high voltage components • Active connection terminals affected by moisture, corrosion, or contamination • Mechanical connections affected by moisture, corrosion, or contamination

Controlled Process to Sensor	**(12) Sensor measurement incorrect or missing** Sensor incorrectly aligned/positioned
	(13) Sensor measurement inaccurate Sensor incorrectly aligned/positioned
	(14) Sensor measurement delay Sensor incorrectly aligned/positioned
	(2) External disturbances • EMI or ESD • Single event effects (e.g., cosmic rays, protons) • Vibration or shock impact • Manufacturing defects and assembly problems • Extreme external temperature or thermal cycling • Unused connection terminals affected by moisture, corrosion, or contamination • Organic growth • Physical interference (e.g., chafing) • Active connection terminals affected by moisture, corrosion, or contamination • Mechanical connections affected by moisture, corrosion, or contamination
	(4) Hazardous interaction with other components in the rest of the vehicle • EMI or ESD • Vibration or shock impact • Physical interference (e.g., chafing) • Unused connection terminals affected by moisture, corrosion, or contamination • Excessive heat from other components • Electrical arcing from neighboring components or exposed terminals • Corona effects from high voltage components • Active connection terminals affected by moisture, corrosion, or contamination • Mechanical connections affected by moisture, corrosion, or contamination
Other Controller to Controlled Process	**(5) Conflicting control action**
Process Input Supplier to Controlled Process	**(21) Input to controlled process missing or wrong**

APPENDIX B: HAZOP STUDY RESULTS

Table B-1. Function 1: Command Torque From the Propulsion System

I.D.	*Malfunction*	*Operating Mode*	*Potential Vehicle Level Hazard*
F1-1	Does not command torque	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
F1-2	Commands more torque 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
F1-3	Commands less torque than intended	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 insufficient vehicle propulsion
F1-4	Commands torque in the wrong direction	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	Not applicable.
F1-5	Commands torque intermittently	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
F1-6	Commands torque when not 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
F1-7	Does not update commanded torque Upward (stuck)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential insufficient vehicle propulsion 3, 4) Potential propulsion power reduction/loss or vehicle stalling
F1-8	Does not update commanded torque downward (stuck)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential insufficient vehicle deceleration

ON: Engine on
D: Drive
R: Reverse

Table B-2. Function 2: Provide Accelerator Pedal Position to the Engine Control Module

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F2-1	Does not provide the accelerator pedal (AP) position to the Engine Control Module	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
F2-2	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
F2-3	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
F2-4	Provides AP position 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
F2-5	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) Potential uncontrolled vehicle propulsion
F2-6	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 correct information.
F2-7	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 3, 4) Potential propulsion power reduction/loss or vehicle stalling

Table B-3. Function 3: Return AP to the Off (Un-Depressed) Position Within a Specified Time
(Note: ignore this section per ISO 26262 if the function is performed through mechanical means.)

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F3-1	Does not return AP to Off position within specified time	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential insufficient vehicle deceleration
F3-2	Returns AP to Off position too fast	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential propulsion power reduction/loss or vehicle stalling
F3-3	Returns AP to Off position within too long time	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential insufficient vehicle deceleration
F3-4	Returns AP past the OFF position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	Unknown
F3-5	Returns AP "short" of the Off position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion
F3-6	Returns AP to Off position intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion
F3-7	Moves the AP when released in the opposite direction of the OFF position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion
F3-8	Moves the AP when released to the Off position when not intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	Not a possible failure scenario
F3-9	Does not move AP from its position when un-depressed	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion

Table B-4. Function 4: Provide AP Request Rate Limiting

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F4-1	Does not limit the AP request rate	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F4-2	Over-limits the AP request rate	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential insufficient vehicle propulsion
F4-3	Under limits the AP request rate	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F4-4	Limits the AP request rate intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F4-5	Limits the AP request rate in the opposite direction (+ vs. -)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential insufficient vehicle propulsion
F4-6	Limits the AP request rate when not required	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential insufficient vehicle propulsion
F4-7	Limits the AP request rate using the same limit profile	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.

Table B-5. Function 5: Control the Throttle Position

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F5-1	Does not control the travel position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion Power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2, 3, 4) Potential insufficient vehicle propulsion
F5-2	Opens the throttle more 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
F5-3	Opens the throttle less 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
F5-4	Controls the throttle position intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2, 3, 4) Potential insufficient vehicle propulsion
F5-5	Moves the throttle opening in the wrong direction (open vs. close)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1,2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F5-6	Changes the throttle position when not intended	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 propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero

F5-7	Does not update the throttle position (throttle is 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, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2, 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero

Table B-6: Function 6: Communicate the Throttle Position to the ECM

Note: this function addresses communication system and management; F2 addresses the APP determination (sensing).

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F6-1	Does not communicate the throttle position to the ECM	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1,2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F6-2	Over-communicates the throttle position to the ECM	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F6-3	Under-communicates the throttle position to the ECM	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1,2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F6-4	Communicates the throttle position to the ECM intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1,2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F6-5	Communicates the throttle position when not required to the ECM	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F6-6	Communicates the same throttle position at all times to the ECM (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, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle propulsion

Table B-7. Function 7: Return Throttle to Idle Position within the Specified Time

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F7-1	Does not return the throttle to idle position within the specified time	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential insufficient vehicle deceleration
F7-2	Takes too long to return throttle to idle position within the specified time	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential insufficient vehicle deceleration
F7-3	Returns throttle to idle position too fast	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential insufficient vehicle deceleration
F7-4	Returns throttle past the idle position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F7-5	Returns throttle to above the idle position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F7-6	Return throttle to idle position intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential insufficient vehicle deceleration
F7-7	Moves throttle in the opposite direction of the idle position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F7-8	Moves throttle to the idle position when not intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential propulsion power reduction/loss or vehicle stalling
F7-9	Does not move the throttle from initial position toward idle 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, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2, 3, 4) Potential insufficient vehicle deceleration

Table B-8. Function 8: Establish Throttle Idle Position

I.D.	*Malfunction*	*Operating Mode*	*Potential Vehicle Level Hazard*
F8-1	Does not establish the throttle idle position	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling
F8-2	Sets the throttle idle position too high	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F8-3	Sets the throttle idle position too low	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F8-4	Establishes the throttle idle position intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling
F8-5	Does not update the throttle idle position set point	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling

Table B-9. Function 9: Provide Idle State Control

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F9-1	Does not control the idle state	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling
F9-2	Provides excessive control of the idle state	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F9-3	Provides in-sufficient control of the idle state	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling
F9-4	Provides idle state control intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling
F9-5	Provides idle state control in the opposite of the correct direction	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling
F9-6	Provides control of the idle state when not required	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F9-7	Maintains the idle state at the same position (stuck)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 3, 4) Potential propulsion power reduction/loss or vehicle stalling

Table B-10. Function 10. Provide Brake-Throttle Override Control - Engages at speed > 10 Miles per Hour (mph)

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F10-1	Does not provide BTO control	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped 5) ON; D or R: Moving <10 mph	1, 2) Potential uncontrolled vehicle propulsion 1, 2) Potential insufficient vehicle deceleration 3, 4) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F10-2	Provides excessive control of the BTO - Within a "grace time" period (very short overlap of AP and brake pedal (BP) at high speed)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped 5) ON; D or R: Moving <10 mph	None.
F10-3	Provides in-sufficient control of the BTO	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped 5) ON; D or R: Moving <10 mph	1, 2) Potential uncontrolled vehicle propulsion 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F10-4	Provides control in the opposite of the correct direction of the BTO	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped 5) ON; D or R: Moving <10 mph	1, 2) Potential uncontrolled vehicle propulsion 1, 2) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F10-5	Provides BTO control intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped 5) ON; D or R: Moving <10 mph	1, 2) Potential uncontrolled vehicle propulsion 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F10-6	Provides BTO control when not intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped 5) ON; D or R: Moving <10 mph	1, 2, 3, 4, 5) Potential propulsion power reduction/loss or vehicle stalling

I.D.	*Malfunction*	*Operating Mode*	*Potential Vehicle Level Hazard*
F10-7	Does not update the BTO control state (stuck)	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped 5) ON; D or R: Moving <10 mph	1, 2,5) Potential uncontrolled vehicle propulsion 1,2, 3, 4, 5) Potential propulsion power reduction/loss or vehicle stalling 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero

Table B-11. Function 11: Store the APP Torque Maps

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F11-1	Do not store the APP torque maps	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration 3,4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F11-2	Store values higher than the intended values of the maps	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 deceleration 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F11-3	Store values lower than the intended values in the maps	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) Potential insufficient vehicle acceleration
F11-4	Store values in the maps intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration
F11-5	Store values opposite in values than the intended values in the maps	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration
F11-6	Store values when no values are intended in the maps	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	Not a viable condition.

F11-7	Store the same values in all locations of the maps	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration

Table B-12. Function 12: Communicate with Internal Sub-systems and External Vehicle Systems

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F12-1	Does not communicate with interfacing sub-systems and systems	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration 3,4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F12-2	Over communicates with interfacing sub-systems and systems	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F12-3	Under communicates with interfacing sub-systems and systems	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration 3,4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F12-4	Communicates intermittently with interfacing sub-systems and systems	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration 3,4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F12-5	Communicates with interfacing sub-systems and systems when not intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.

F12-6	Communicates the same message(s) with interfacing sub-systems and systems	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration 3,4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero

Table B-13. Function 13: Provide Diagnostics and Diagnostics Trouble Codes

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F13-1	Does not provide diagnostics	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration 3,4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero
F13-2	Provides diagnostics more than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F13-3	Provides diagnostics less than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration
F13-4	Provides diagnostics intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration
F13-5	Provides diagnostics when not intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F13-6	Provides the same diagnostics (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, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) Potential insufficient vehicle deceleration 1, 2) Potential insufficient vehicle acceleration

Table B-14. Function 14: Provide Fault Detection and Failure Mitigation

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F14-1	Does not provide fault detection and failure mitigation		This function is not a part of the HAZOP; this function is a part of the design to mitigate the hazards resulting from the malfunctions.
F14-2	Provides fault detection and failure mitigation more than intended		Not applicable
F14-3	Provides fault detection and failure mitigation less than intended		Not applicable
F14-4	Provides fault detection and failure mitigation intermittently		Not applicable
F14-5	Provides fault detection and failure mitigation when not intended		Not applicable
F14-6	Provides the same fault detection and failure mitigation at all times		Not applicable

Table B-15. Function 15: Store Relevant Data

I.D.	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
F15-1	Does not store relevant data	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F15-2	Store more relevant data than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F15-3	Stores less relevant data than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F15-4	stores relevant data intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F15-5	Stores relevant data when not intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.
F15-6	Stores the same relevant data at all times	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	None.

APPENDIX C: UNSAFE CONTROL ACTION (UCA) ASSESSMENT TABLES

Table C-1: UCA Assessment for the "Enter Brake Throttle Override Mode" Control Action

Context Variables (Enter BTO Mode)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Accelerator Pedal Position	Brake Pedal Position	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		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Not Pressed	Not Pressed	≥ 10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Not Pressed	Pressed	< 10 mph			N/A	N/A	N/A	N/A			
Not Pressed	Pressed	≥ 10 mph			N/A	N/A	N/A	N/A			
Pressed	Not Pressed	< 10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Not Pressed	≥ 10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Pressed	< 10 mph		H3	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Pressed	≥ 10 mph	H1		N/A	N/A	N/A	N/A	H1	H3	H1

Vehicle Level Hazards:

- H1: Uncontrolled Vehicle Propulsion
- H3: Propulsion Power Reduction/Loss or Vehicle Stalling

* Vehicle speed values are based on the maximum vehicle speed threshold for activating BTO mode. Manufacturers may elect to have an activation speed less than 10 mph.

Table C-2: UCA Assessment for the "Enter Normal Mode" Control Action

Context Variables (Enter Normal Mode)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Accelerator Pedal Position	Brake Pedal Position	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			N/A	N/A	N/A	N/A		N/A	
Not Pressed	Not Pressed	≥ 10 mph			N/A	N/A	N/A	N/A		N/A	
Not Pressed	Pressed	< 10 mph			N/A	N/A	N/A	N/A		N/A	
Not Pressed	Pressed	≥ 10 mph			N/A	N/A	N/A	N/A		N/A	
Pressed	Not Pressed	< 10 mph	H2, H3		N/A	N/A	N/A	N/A	H3	N/A	H3
Pressed	Not Pressed	≥ 10 mph	H2, H3		N/A	N/A	N/A	N/A	H3	N/A	H3
Pressed	Pressed	< 10 mph		H1	N/A	N/A	N/A	N/A	Hazardous if Provided	N/A	Hazardous if Provided
Pressed	Pressed	≥ 10 mph		H1	N/A	N/A	N/A	N/A	Hazardous if Provided	N/A	Hazardous if Provided

Vehicle Level Hazards:

- H1: Uncontrolled Vehicle Propulsion
- H2: Insufficient Vehicle Propulsion
- H3: Propulsion Power Reduction/Loss or Vehicle Stalling

* Vehicle speed values are based on the maximum vehicle speed threshold for activating BTO mode. Manufacturers may elect to have an activation speed less than 10 mph.

Table C-3: UCA Assessment for the "Increase Throttle Opening" Control Action

Context Variables (Increase Throttle Opening)			**Guidewords for Assessing Whether the Control Action May Be Unsafe**								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
None	Not Pressed	Normal Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Not Pressed	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Not Pressed	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Not Pressed	BTO Switching to Normal		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Reduced	Normal Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Reduced	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Reduced	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Reduced	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Maintained	Normal Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Increase Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
None	Angular Position is Maintained	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Maintained	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Maintained	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Increased	Normal Mode	H2		H1	H2	H1	H2	H1, H2, H3	N/A	H2
None	Angular Position is Increased	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Increased	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Increased	BTO Switching to Normal	H2		H1	H2	H1	H2	H1, H2, H3	N/A	H2
Reduce	Not Pressed	Normal Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Not Pressed	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Not Pressed	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Increase Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce	Not Pressed	BTO Switching to Normal		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Reduced	Normal Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Reduced	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Reduced	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Reduced	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Maintained	Normal Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Maintained	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Maintained	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Maintained	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Increase Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce	Angular Position is Increased	Normal Mode	H2	H5	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Increased	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Increased	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Increased	BTO Switching to Normal	H2	H5	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Not Pressed	Normal Mode	H2	H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Not Pressed	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Not Pressed	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Not Pressed	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Reduced	Normal Mode	H5	H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Reduced	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Increase Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Increase	Angular Position is Reduced	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Reduced	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Maintained	Normal Mode	H5	H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Maintained	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Maintained	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Maintained	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Increased	Normal Mode	H2		H1	H2	H1	H2	H1, H2, H3	N/A	H2
Increase	Angular Position is Increased	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Increased	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Increase Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Increase	Angular Position is Increased	BTO Switching to Normal	H2		H1	H2	H1	H2	H1, H2, H3	N/A	H2
Reduce and Increase	Not Pressed	Normal Mode	H2	H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Not Pressed	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Not Pressed	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Not Pressed	BTO Switching to Normal		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Reduced	Normal Mode	H5	H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Reduced	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Reduced	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Reduced	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Increase Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce and Increase	Angular Position is Maintained	Normal Mode	H5	H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Maintained	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Maintained	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Maintained	BTO Switching to Normal		H1 *	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Increased	Normal Mode	H2	H5	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Increased	Normal Switching BTO		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Increased	BTO Mode		H1	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Increase Throttle Opening)			**Guidewords for Assessing Whether the Control Action May Be Unsafe**								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce and Increase	Angular Position is Increased	BTO Switching to Normal	H2	H5	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Vehicle Level Hazards:

- H1: Uncontrolled Vehicle Propulsion
- H2: Insufficient Vehicle Propulsion
- H3: Propulsion Power Reduction/Loss or Vehicle Stalling
- H5: Allowing Driver's Command to Override an Active Safety System

* This analysis is based on a brake override process flow diagram published by Toyota, which requires the driver to explicitly increase the accelerator pedal angle to exit BTO mode. Other manufacturers may have different strategies for exiting BTO mode.

Table C-4: UCA Assessment for the "Decrease Throttle Opening" Control Action

Context Variables (Decrease Throttle Opening)			**Guidewords for Assessing Whether the Control Action May Be Unsafe**								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
None	Not Pressed	Normal Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Not Pressed	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
None	Not Pressed	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Not Pressed	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Reduced	Normal Mode	H4		H3	H4	H3	H4	H1, H3, H4	N/A	H4
None	Angular Position is Reduced	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
None	Angular Position is Reduced	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Reduced	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Maintained	Normal Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Decrease Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
None	Angular Position is Maintained	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
None	Angular Position is Maintained	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Maintained	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Increased	Normal Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Increased	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
None	Angular Position is Increased	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
None	Angular Position is Increased	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Not Pressed	Normal Mode	H4		H3	H4	H3	H4	H1, H3, H4	N/A	H4
Reduce	Not Pressed	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce	Not Pressed	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Decrease Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce	Not Pressed	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Reduced	Normal Mode	H4		H3	H4	H3	H4	H1, H3, H4	N/A	H4
Reduce	Angular Position is Reduced	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce	Angular Position is Reduced	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Reduced	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Maintained	Normal Mode	H5	H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Maintained	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce	Angular Position is Maintained	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Maintained	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Decrease Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce	Angular Position is Increased	Normal Mode	H5	H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Increased	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce	Angular Position is Increased	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce	Angular Position is Increased	BTO Switching to Normal	H5	H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Not Pressed	Normal Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Not Pressed	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Increase	Not Pressed	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Not Pressed	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Reduced	Normal Mode	H4	H5	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Reduced	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4

Context Variables (Decrease Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Increase	Angular Position is Reduced	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Reduced	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Maintained	Normal Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Maintained	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Increase	Angular Position is Maintained	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Maintained	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Increased	Normal Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Increase	Angular Position is Increased	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Increase	Angular Position is Increased	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Decrease Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Increase	Angular Position is Increased	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Not Pressed	Normal Mode	H4	H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Not Pressed	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce and Increase	Not Pressed	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Not Pressed	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Reduced	Normal Mode	H4	H5	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Reduced	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce and Increase	Angular Position is Reduced	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Reduced	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Decrease Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce and Increase	Angular Position is Maintained	Normal Mode	H5	H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Maintained	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce and Increase	Angular Position is Maintained	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Maintained	BTO Switching to Normal		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Increased	Normal Mode	H5	H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided
Reduce and Increase	Angular Position is Increased	Normal Switching BTO	H4		H3	H4	H3	H4	H1, H3, H4	H3	H4
Reduce and Increase	Angular Position is Increased	BTO Mode		H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Context Variables (Decrease Throttle Opening)			Guidewords for Assessing Whether the Control Action May Be Unsafe								
Torque Request from Other Vehicle Systems	Driver action on accelerator pedal	ECM Operating Mode	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
Reduce and Increase	Angular Position is Increased	BTO Switching to Normal	H5	H3	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided	N/A	Hazardous if Provided

Vehicle Level Hazards:

- H1: Uncontrolled Vehicle Propulsion
- H3: Propulsion Power Reduction/Loss or Vehicle Stalling
- H4: Insufficient Vehicle Deceleration
- H5: Allowing Driver's Command to Override Active Safety Systems

APPENDIX D: STPA STEP 1: UCAS AND MAPPING TO HAZARDS

Table D-1: Unsafe Control Actions for the "Enter Brake Throttle Override Mode" Control Action

Vehicle Level Hazard	Unsafe Control Actions (Enter BTO Mode)
H1	The ECM correctly issues the Enter BTO Mode command, but the command is executed incorrectly.
H1	The ECM issues the Enter BTO Mode command when: • the accelerator pedal is pressed, • the brake pedal is pressed, and • the vehicle speed is 10 mph or greater, but the command is issued too late.
H1	The ECM does not issue the Enter BTO Mode command when: • the accelerator pedal is pressed, • the brake pedal is pressed, and • the vehicle speed is 10 mph or greater.
H3	The ECM issues the Enter BTO Mode command when: • the accelerator pedal is pressed, • the brake pedal is pressed, and • the vehicle speed is below 10 mph.
H3	The ECM issues the Enter BTO Mode command when: • the brake pedal is not pressed.
H3	The ECM issues the Enter BTO Mode command when: • the accelerator pedal is pressed, • the brake pedal is pressed, and • the vehicle speed is 10 mph or greater, but the command is issued too soon (i.e., before the end of the activation delay).

H1: Uncontrolled Vehicle Propulsion
H3: Propulsion Power Reduction/Loss or Vehicle Stalling

Table D-2: Unsafe Control Actions for the "Enter Normal Mode" Control Action

Vehicle Level Hazard(s)	Unsafe Control Actions (Enter Normal Mode)
H1	The ECM issues the Enter Normal Mode command when: • the accelerator pedal is pressed, and • the brake pedal is pressed.
H2, H3	The ECM does not issue the Enter Normal Mode command when: • the accelerator pedal is pressed, and • the brake pedal is not pressed.
H3	The ECM correctly issues the Enter Normal Mode command, but the command is executed incorrectly.
H3	The ECM issues the Enter Normal Mode command when: • the accelerator pedal is pressed, and • the brake pedal is not pressed, but the command is issued to late.

H1: Uncontrolled Vehicle Propulsion
H2: Insufficient Vehicle Propulsion
H3: Propulsion Power Reduction/Loss or Vehicle Stalling

Table D-3: Unsafe Control Actions for the "Increase Throttle Opening" Control Action

Vehicle Level Hazard(s)	**Unsafe Control Action (Increase Throttle Opening)**
H1	The ECM issues the Increase Throttle Opening command when: • the ECM is in BTO mode or is transitioning from normal mode into BTO mode.
H1, H2, H3	The ECM correctly issues the Increase Throttle Opening command, but the command is executed incorrectly.
H1	The ECM issues the Increase Throttle Opening command when: • the driver reduces or maintains the angular position of the accelerator pedal, or is not pressing the accelerator pedal.
H1	The ECM issues the Increase Throttle Opening command when: • other vehicle systems request an increase in engine torque, or are not requesting a change in engine torque, • the driver is increasing the angular position of the accelerator pedal, and • the ECM is in normal mode or is transitioning from BTO mode into normal mode, but too much of an increase in the throttle opening is commanded.
H1	The ECM issues the Increase Throttle Opening command when: • other vehicle systems request an increase in engine torque, or are not requesting a change in engine torque, • the driver is increasing the angular position of the accelerator pedal, and • the ECM is in normal mode or is transitioning from BTO mode into normal mode, but the command is issued for too long.
H2	The ECM issues the Increase Throttle Opening command when: • other vehicle systems do not request a change in engine torque, or request an increase in engine torque, • the driver increases the angular position of the accelerator pedal, and • the ECM is in normal mode or is transitioning from BTO mode into normal mode, but too little of an increase in the throttle opening is commanded.
H2	The ECM does not issue the Increase Throttle Opening command when: • the driver increases the angular position of the accelerator pedal and • the ECM is in normal mode or is transitioning from BTO mode into normal mode.
H2	The ECM does not issue the Increase Throttle Opening command when: • other vehicle systems request an increase in engine torque or request both an increase and reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode.
H2	The ECM issues the Increase Throttle Opening command when: • other vehicle systems do not request a change in engine torque, or request an increase in engine torque, • the driver increases the angular position of the accelerator pedal, and • the ECM is in normal mode or is transitioning from BTO mode into normal mode, but the command is issued for too short a period.

Vehicle Level Hazard(s)	Unsafe Control Action (Increase Throttle Opening)
H2	The ECM issues the Increase Throttle Opening command when: • other vehicle systems do not request a change in engine torque, or request an increase in engine torque, • the driver increases the angular position of the accelerator pedal, and • the ECM is in normal mode or is transitioning from BTO mode into normal mode, but the command is issued too late.
H5	The ECM issues the Increase Throttle Opening command when: • other vehicle systems request a reduction in engine torque or both a reduction and increase in engine torque, • the driver increases the angular position of the accelerator pedal, and • the ECM is in normal mode or is transitioning from BTO mode into normal mode.
H5	The ECM does not issue the Increase Throttle Opening command when: • other vehicle systems request an increase in engine torque or both a reduction and increase in engine torque, • the driver is maintaining or reducing the angular position of the accelerator pedal, and • the ECM is in normal mode.

H1: Uncontrolled Vehicle Propulsion
H2: Insufficient Vehicle Propulsion
H3: Propulsion Power Reduction/Loss or Vehicle Stalling
H5: Allowing the Driver's Command to Override Active Safety System

Table D-4: Unsafe Control Actions for the "Decrease Throttle Opening" Control Action

Vehicle Level Hazard	Unsafe Control Action (Decrease Throttle Opening)
H1, H3, H4	The ECM correctly issues the Decrease Throttle Opening command, but the command is executed incorrectly.
H3	The ECM issues the Decrease Throttle Opening command when: • the ECM is in BTO mode or is transitioning from BTO into normal mode.
H3	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems do not request a change in engine torque, request an increase in engine torque, or request both an increase and reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode.
H3	The ECM issues the Decrease Throttle Opening command when: • the driver maintains or increases the angular position of the accelerator pedal, and • the ECM is in normal mode.
H3	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems don't request a change in engine torque, or request a reduction in engine torque, • the driver is reducing the angular position of the accelerator pedal, and • the ECM is in normal mode, but too much of a decrease is commanded.
H3	The ECM issues the Decrease Throttle Opening command when: • the ECM is transitioning from normal into BTO mode, but too much of a decrease in the throttle opening is commanded.
H3	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems do not request a change, or request a reduction in engine torque, • the driver reduces the angular position of the accelerator pedal, and • the ECM is in normal mode, but the command is issued for too long a period.
H3	The ECM issues the Decrease Throttle Opening command when: • the ECM is transitioning from normal into BTO mode, but the command is issued for too long a period.
H3	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode, but too much of a decrease in the throttle opening is commanded.
H3	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode, but the command is issued for too long a period.
H3	The ECM issues the Decrease Throttle Opening command when: • the ECM is transitioning from normal into BTO mode, but the command is issued too soon.

Vehicle Level Hazard	Unsafe Control Action (Decrease Throttle Opening)
H4	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems do not request a change in engine torque, or request a reduction in engine torque, • the driver is reducing the angular position of the accelerator pedal, and • the ECM is in normal mode, but too little of a decrease is commanded.
H4	The ECM issues the Decrease Throttle Opening command when: • the ECM is transitioning from normal into BTO mode, but too little of a decrease in the throttle opening is commanded.
H4	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems do not request a change, or request a reduction in engine torque, • the driver is reducing the angular position of the accelerator pedal, and • the ECM is in normal mode, but the command is issued for too short a period.
H4	The ECM issues the Decrease Throttle Opening command when: • the ECM is transitioning from normal into BTO mode, but the command is issued for too short a period.
H4	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems do not request a change in engine torque, or request a reduction in engine torque, • the driver is reducing the angular position of the accelerator pedal, and • the ECM is in normal mode, but the command is issued too late.
H4	The ECM issues the Decrease Throttle Opening command when: • the ECM is transitioning from normal into BTO mode, but the command is issued too late.
H4	The ECM does not issue the Decrease Throttle Opening command when: • the driver reduces the angular position of the accelerator pedal, and • the ECM is in normal mode.
H4	The ECM does not issue the Decrease Throttle Opening command when: • the ECM is transitioning from normal mode into BTO mode.
H4	The ECM does not issue the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque or both an increase and reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode.
H4	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode, but too little of a decrease in the throttle opening is commanded.
H4	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode, but the command is issued for too short a period.

Vehicle Level Hazard	**Unsafe Control Action (Decrease Throttle Opening)**
H4	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque, • the driver is not pressing the accelerator pedal, and • the ECM is in normal mode, but the command is issued too late.
H5	The ECM does not issue the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque or both an increase and reduction in engine torque, • the driver is maintaining or increasing the angular position of the accelerator pedal, and • the ECM is in normal mode.
H5	The ECM issues the Decrease Throttle Opening command when: • other vehicle systems request an increase in engine torque, or request both an increase and reduction in engine torque, • the driver is reducing the angular position of the accelerator pedal, and • the ECM is in normal mode.
H5	The ECM does not issue the Decrease Throttle Opening command when: • other vehicle systems request a reduction in engine torque or both an increase and reduction in engine torque, • the driver is increasing the angular position of the accelerator pedal, and • the ECM is transitioning from BTO to normal mode.

H1: Uncontrolled Vehicle Propulsion
H3: Propulsion Power Reduction/Loss or Vehicle Stalling
H4: Insufficient Vehicle Deceleration
H5: Allowing the Driver's Command to Override Active Safety System

APPENDIX E: OPERATIONAL SITUATIONS

1. Vehicle in a parking lot or drive way and starting to move; good visibility with light pedestrian traffic.
2. Vehicle in a parking lot or drive way and starting to move; low visibility with light pedestrian traffic.
3. Vehicle in a parking lot or drive way and starting to move; good visibility with high pedestrian traffic (mall, supermarket)
4. Vehicle in a parking lot or drive way and starting to move; low visibility with high pedestrian traffic (mall, supermarket)
5. Vehicle going in reverse from a stopped condition at (relatively) low speed; low/good visibility; other vehicles present (stopped or moving at low speed); slippery/good road conditions; pedestrians present.
6. Driving inside the city with heavy traffic and pedestrians present, stop and go driving, good visibility, good road conditions.
7. Driving inside the city with heavy traffic and pedestrians present, stop and go driving, low visibility, slippery road conditions.
8. Driving inside the city with heavy traffic and negligible pedestrians present, stop and go driving, good visibility, and good road conditions.
9. Driving inside the city with heavy traffic and negligible pedestrians present, stop and go driving, bad visibility, and slippery road conditions.
10. Driving inside (< 40 kph) the city with heavy traffic and negligible pedestrians present, good visibility, and good road conditions.
11. Driving inside the city (< 40 kph) with heavy traffic and negligible pedestrians present, bad visibility, and slippery road conditions.
12. Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.
13. Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.
14. Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.
15. Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.
16. Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.
17. Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.
18. Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.

19. Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.
20. Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light/heavy traffic, low/good visibility, and good/slippery road conditions; pedestrian present.
21. Driving at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.
22. Driving at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.
23. Driving at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.
24. Driving at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.
25. Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, good visibility, and good road conditions.
26. Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, good visibility, and good road conditions.
27. Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, low visibility, and slippery road conditions.
28. Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.
29. Driving at very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.
30. Driving at very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.
31. Driving at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.
32. Driving at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.
33. Overtaking another vehicle at very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.
34. Overtaking another vehicle at very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.
35. Overtaking another vehicle at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.
36. Overtaking another vehicle at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.
37. Driving at high speed (100 kph < V < 130 kph), light traffic, low visibility, and slippery road conditions.

38. Overtaking another vehicle at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.
39. Overtaking another vehicle at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.
40. Overtaking another vehicle at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.
41. Overtaking another vehicle at high speed (100 kph < V < 130 kph), light traffic, low visibility, and slippery road conditions.
42. Driving at very high speed V > 130 kph), heavy traffic, good visibility, and good road conditions.
43. Vehicle in a parking lot or drive way and starting to move; good/low visibility, good/slippery road conditions.
44. Driving inside the city with heavy traffic, stop and go driving, good visibility, good road conditions.
45. Driving inside the city with heavy traffic, stop and go driving, low visibility, slippery road conditions.
46. Driving inside the city with light traffic, stop and go driving, good visibility, good road conditions.
47. Driving inside the city with light traffic, stop and go driving, low visibility, slippery road conditions.
48. Driving near rail road track, low/good visibility, good/slippery road conditions.
49. Driving at very high speed V > 130 kph), heavy traffic, low visibility, and slippery road conditions.
50. Vehicle in a Park or Neutral (P or N) position; good/low visibility with low/high pedestrian traffic.
51. Vehicle in a parking lot or drive way in a drive or reverse (D or R) and the brake is applied; good/slippery road conditions; good/low visibility; with low pedestrian traffic.
52. Vehicle in a parking lot or drive way in a drive or reverse (D or R) and the brake is applied; good/slippery road conditions; good/low visibility; with high pedestrian traffic.
53. Vehicle in a traffic stop and the brake is applied; good/slippery road conditions; good/low visibility; with light traffic.
54. Vehicle in a traffic stop and the brake is applied; good/slippery road conditions; good/low visibility; with heavy traffic.
55. Vehicle in hill-hold in drive position (D) with the brakes not applied
56. Vehicle in a parking lot or drive way and starting to move; good/low visibility, good/slippery road conditions, with light/heavy pedestrian traffic.
57. Driving inside the city with heavy traffic and pedestrians present, stop and go driving, good/low visibility, good/slippery road conditions.
58. Driving inside the city (< 40 kph) with heavy traffic and negligible pedestrians present, low visibility, and slippery road conditions.

59. Driving over a rail road track, low/good visibility, and good/slippery road conditions.
60. Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good/low visibility, and good/slippery road conditions.
61. Conducting an evasive maneuver deviating from desired path at medium speed (40 kph < V < 100 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.
62. Driving at high speed (100 kph < V < 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.
63. Conducting an evasive maneuver deviating from desired path at high speed (100 kph < V < 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.
64. Driving at very high speed (V > 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.
65. Conducting an evasive maneuver deviating from desired path at high speed (V > 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.
66. Overtaking another vehicle at very high speed (V > 130 kph) heavy traffic, low visibility, and slippery road conditions.
67. Driving inside the city with heavy traffic and pedestrians present, stop and go driving above 16 kph, good visibility, good road conditions.
68. Driving inside the city with heavy traffic and pedestrians present, stop and go driving above 16 kph, low visibility, slippery road conditions.
69. Driving inside the city with heavy traffic and negligible pedestrians present, stop and go driving above 16 kph, good visibility, and good road conditions.
70. Driving inside the city with heavy traffic and negligible pedestrians present, stop and go driving above 16 kph, bad visibility, and slippery road conditions.
71. Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.

APPENDIX F: ASIL ASSESSMENT

Table F-1: Unintended Vehicle Propulsion without Destabilization

(ASIL C)

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Vehicle in a parking lot or drive way and starting to move; good visibility with light pedestrian traffic.	The vehicle runs into a pedestrian at low speed.	E4	S2	C2	B
	Vehicle in a parking lot or drive way and starting to move; low visibility with light pedestrian traffic.	The vehicle runs into a pedestrian at low speed.	E3	S2	C2	A
	Vehicle in a parking lot or drive way and starting to move; good visibility with high pedestrian traffic (mall, supermarket)	The vehicle runs into a pedestrian; potential for running over the pedestrian also exists.	E3	S3	C2	A
	Vehicle in a parking lot or drive way and starting to move; low visibility with high pedestrian traffic (mall, supermarket)	The vehicle runs into a pedestrian; potential for running over the pedestrian also exists.	E2	S3	C2	A
	Vehicle going in reverse from a stopped condition at (relatively) low speed; low/good visibility; other vehicles present (stopped or moving at low speed); slippery/good road conditions; pedestrians present.	The vehicle runs into a pedestrian; potential for running over the pedestrian also exists.	E2	S3	C2	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Driving inside the city with heavy traffic and pedestrian presence, stop and go driving, good visibility, good road conditions.	The vehicle runs into another vehicle or a pedestrian; potential for running over the pedestrian also exists.	E3	S3	C2	B
	Driving inside the city with heavy traffic and pedestrian presence, stop and go driving, low visibility, slippery road conditions.	The vehicle runs into another vehicle or a pedestrian; potential for running over the pedestrian also exists.	E2	S3	C2	A
	Driving inside the city with heavy traffic and negligible pedestrian presence, stop and go driving, good visibility, and good road conditions.	The vehicle runs into another vehicle at low speed.	E4	S1	C2	A
	Driving inside the city with heavy traffic and negligible pedestrian presence, stop and go driving, bad visibility, and slippery road conditions.	The vehicle runs into another vehicle at low speed.	E3	S1	C2	QM
	Driving inside (< 40 kph) the city with heavy traffic and negligible pedestrian presence, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E4	S1	C2	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Driving inside the city (< 40 kph) with heavy traffic and negligible pedestrian presence, bad visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E3	S1	C2	QM
	Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E4	S3	C2	C
	Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E4	S3	C2	C
	Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C2	B
	Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light/heavy traffic, low/good visibility, and good/slippery road conditions; pedestrian present.	The vehicle runs into a person.	E2	S3	C2	A
	Driving at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle	E4	S3	C2	C
	Driving at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle	E4	S3	C2	C
	Driving at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle	E3	S3	C2	B
	Driving at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C1	A
	Driving at very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C2	B
	Driving at very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Driving at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E2	S3	C2	A
	Driving at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E2	S3	C2	A
	Overtaking another vehicle at a very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C2	B
	Overtaking another vehicle at a very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or barrier.	E3	S3	C2	B
	Overtaking another vehicle at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E2	S3	C2	A
	Overtaking another vehicle at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or barrier.	E2	S3	C2	A

Table F-2: Unintended Vehicle Propulsion with Destabilization

(ASIL D)

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion with Destabilization)			ASIL
			Exposure	Severity	Controllability	
Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E4	S3	C3	D
Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E4	S3	C3	D
Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C3	C
Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C3	C
Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion with Destabilization)			ASIL
			Exposure	Severity	Controllability	
Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C2	B
Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C2	B
Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C2	B
Hazard occurs with destabilization	Driving at very high speed V > 130 kph), heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C3	C
Hazard occurs with destabilization	Driving at very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C3	C
Hazard occurs with destabilization	Driving at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E2	S3	C3	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Unintended Vehicle Propulsion with Destabilization)			ASIL
			Exposure	Severity	Controllability	
Hazard occurs with destabilization	Driving at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E2	S3	C3	B
Hazard occurs with destabilization	Overtaking another vehicle at a very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C3	C
Hazard occurs with destabilization	Overtaking another vehicle at a very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	The vehicle runs into another vehicle or a barrier.	E3	S3	C3	B
Hazard occurs with destabilization	Overtaking another vehicle at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E2	S3	C3	B
Hazard occurs with destabilization	Overtaking another vehicle at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	The vehicle runs into another vehicle or a barrier.	E2	S3	C3	B

Table F-3: Unintended Vehicle Propulsion With Zero Starting Speed
(ASIL B)

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment Unintended Vehicle Propulsion With Zero Starting Speed			ASIL
			Exposure	Severity	Controllability	
	Vehicle in a Park or Neutral (P or N) position; good/low visibility with low/high pedestrian traffic.	None				
The failure produces enough torque to override the braking torque that is applied to counter the creep torque	Vehicle in a parking lot or drive way in a drive or reverse (D or R) and the brake is applied; good/slippery road conditions; good/low visibility; with low pedestrian traffic.	The vehicle moves and hits a pedestrian	E4	S2	C1	A
The failure produces enough torque to override the braking torque that is applied to counter the creep torque	Vehicle in a parking lot or drive way in a drive or reverse (D or R) and the brake is applied; good/slippery road conditions; good/low visibility; with high pedestrian traffic.	The vehicle moves and hits a pedestrian	E4	S2	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment Unintended Vehicle Propulsion With Zero Starting Speed			ASIL
			Exposure	Severity	Controllability	
The failure produces enough torque to override the braking torque that is applied to counter the creep torque	Vehicle in a traffic stop and the brake is applied; good/slippery road conditions; good/low visibility; with light traffic.	The vehicle moves and hits another vehicle.	E4	S1	C1	QM
The failure produces enough torque to override the braking torque that is applied to counter the creep torque	Vehicle in a traffic stop and the brake is applied; good/slippery road conditions; good/low visibility; with heavy traffic.	The vehicle moves and hits another vehicle.	E4	S1	C2	A
Failures cause reduction in propulsion torque.	Vehicle in hill-hold in drive position (D) with the brakes not applied	The vehicle rolls back	E2	S1	C0	None

Table F-4: Insufficient Vehicle Propulsion

(ASIL C)

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Vehicle in a parking lot or drive way and starting to move; good/low visibility, good/slippery road conditions, with light/heavy pedestrian traffic.	None	E4		C0	None
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Vehicle going in reverse from a stopped condition at (relatively) low speed; low/good visibility; other vehicles present (stopped or moving at low speed); slippery/good road conditions; pedestrians present.	None	E2	S0		None
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Driving inside the city with heavy traffic and pedestrian presence, stop and go driving, good/low visibility, good/slippery road conditions.	None	E3		C0	None

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Driving inside (< 40 kph) the city with heavy traffic and negligible pedestrian presence, good visibility, and good road conditions.	None	E4		C0	None
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Driving inside the city (< 40 kph) with heavy traffic and negligible pedestrian presence, low visibility, and slippery road conditions.	None	E3		C0	None
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Driving over a rail road track, low/good visibility, good/slippery road conditions.	Vehicle fails to achieve intended speed increase while driving across rail road track and gets hit by an incoming train.	E3	S3	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed, but there is no potential for accident scenario.	E4	S2	C1	QM
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Conducting an evasive maneuver deviating from desired path at medium speed (40 kph < V < 100 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into another the vehicle.	E2	S3	C1	QM
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C2	B
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C2	B
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light/heavy traffic, low/good visibility, and good/slippery road conditions; pedestrian present.	The vehicle runs into a person.	E2	S3	C3	B
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Driving at high speed (100 kph < V < 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed, but there is no potential for accident scenario.	E4		C0	None
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Conducting an evasive maneuver deviating from desired path at high speed (100 kph < V < 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into another the vehicle.	E2	S3	C2	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C3	C
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C3	C
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C3	C

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Driving at very high speed (V > 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed, but there is no potential for accident scenario.	E3		C0	None
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Conducting an evasive maneuver deviating from desired path at high speed (V > 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into another the vehicle.	E2	S3	C3	B
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at a very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C3	C

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Propulsion)			ASIL
			Exposure	Severity	Controllability	
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at a very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E3	S3	C3	C
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at very high speed (V > 130 kph) heavy traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E2	S3	C3	B
Failure causes the vehicle speed to increase at a slower rate than it is expected based on previous driving experience/feel	Overtaking another vehicle at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; another vehicle runs into the vehicle head on.	E2	S3	C3	B

Table F-5: Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization (ASIL C)

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Vehicle in a parking lot or drive way and starting to move; good/low visibility, good/slippery road conditions.	None	E3	S0		None
	Vehicle going in reverse from a stopped condition at (relatively) low speed; low/good visibility; other vehicles present (stopped or moving at low speed); slippery/good road conditions; pedestrians present.	None	E2	S0		None
	Driving inside the city with heavy traffic, stop and go driving, good visibility, good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind or on the side at low speed	E4	S1	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Driving inside the city with heavy traffic, stop and go driving, low visibility, slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind or on the side at low speed	E3	S1	C1	QM
	Driving inside the city with light traffic, stop and go driving, good visibility, good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind or on the side at low speed	E4	S1	C1	QM
	Driving inside the city with light traffic, stop and go driving, low visibility, slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind or on the side at low speed	E3	S1	C1	QM
	Driving near a rail road track, low/good visibility, good/slippery road conditions.	Vehicle stalls while stopping on rail road track and gets hit by an incoming train.	E1	S3	C3	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E4	S3	C2	C
	Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E4	S3	C2	C
	Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C2	B
	Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C2	B
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C2	B
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C2	B
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light/heavy traffic, low/good visibility, and good/slippery road conditions; pedestrian present.	The vehicle runs into a person.	E2	S3	C3	B
	Driving at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E4	S3	C2	C
	Driving at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E4	S3	C2	C
	Driving at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Driving at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C2	B
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
	Driving at very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C2	B
	Driving at very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C2	B
	Driving at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E2	S3	C2	A
	Driving at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E2	S3	C2	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
	Overtaking another vehicle at a very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
	Overtaking another vehicle at a very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
	Overtaking another vehicle at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E2	S3	C3	B
	Overtaking another vehicle at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E2	S3	C3	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light/heavy traffic, low/good visibility, and good/slippery road conditions; pedestrian present.	The vehicle runs into a person.	E2	S3	C2	A

Table F-6: Propulsion Power Reduction/Loss or Vehicle Stalling with Destabilization (ASIL D)

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling with Destabilization)			ASIL
			Exposure	Severity	Controllability	
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E4	S3	C3	D
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E4	S3	C3	D
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C3	C
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C3	C

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling with Destabilization)			ASIL
			Exposure	Severity	Controllability	
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling with Destabilization)			ASIL
			Exposure	Severity	Controllability	
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C3	C
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E3	S3	C3	C
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at very high speed V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E2	S3	C3	B
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Driving at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle from behind.	E2	S3	C3	B
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at a very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Propulsion Power Reduction/Loss or Vehicle Stalling with Destabilization)			ASIL
			Exposure	Severity	Controllability	
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at a very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E3	S3	C3	C
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E2	S3	C3	B
These scenarios are associated with rear-wheel drive vehicles. Hazard occurs with destabilization	Overtaking another vehicle at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	Vehicle loses acceleration. Another vehicle runs into the vehicle head on.	E2	S3	C3	B

Table F-7: Insufficient Vehicle Deceleration

(ASIL C)

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. The driver reduces the accelerator pedal angle (force); or 2. BTO is invoked. 3. Failure causes the vehicle speed to decrease at a slower rate than it is expected based on previous driving experience/feel	Vehicle in a parking lot or drive way and starting to move; good visibility with light pedestrian traffic.	The vehicle runs into a pedestrian at low speed.	E4	S2	C1	A
1. The driver reduces the accelerator pedal angle (force); or 2. BTO is invoked. 3. Failure causes the vehicle speed to decrease at a slower rate than it is expected based on previous driving experience/feel	Vehicle in a parking lot or drive way and starting to move; low visibility with light pedestrian traffic.	The vehicle runs into a pedestrian at low speed.	E3	S2	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. The driver reduces the accelerator pedal angle (force); or 2. BTO is invoked. 3. Failure causes the vehicle speed to decrease at a slower rate than it is expected based on previous driving experience/feel	Vehicle in a parking lot or drive way and starting to move; good visibility with high pedestrian traffic (mall, supermarket)	The vehicle runs into a pedestrian at low speed.	E4	S2	C1	A
1. The driver reduces the accelerator pedal angle (force); or 2. BTO is invoked. 3. Failure causes the vehicle speed to decrease at a slower rate than it is expected based on previous driving experience/feel	Vehicle in a parking lot or drive way and starting to move; low visibility with high pedestrian traffic (mall, supermarket)	The vehicle runs into a pedestrian at low speed.	E3	S2	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. The driver reduces the accelerator pedal angle (force); or 2. BTO is invoked. 3. Failure causes the vehicle speed to decrease at a slower rate than it is expected based on previous driving experience/feel	Vehicle going in reverse from a stopped condition at (relatively) low speed; low/good visibility; other vehicles present (stopped or moving at low speed); slippery/good road conditions; pedestrians present.	The vehicle runs into a pedestrian; potential for running over the pedestrian also exists.	E2	S3	C1	QM
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving inside the city with heavy traffic and pedestrian presence, stop and go driving above 16 kph, good visibility, good road conditions.	The vehicle runs into another vehicle or a pedestrian.	E4	S2	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving inside the city with heavy traffic and pedestrian presence, stop and go driving above 16 kph, low visibility, slippery road conditions.	The vehicle runs into another vehicle or a pedestrian.	E3	S2	C1	QM
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving inside the city with heavy traffic and negligible pedestrian presence, stop and go driving above 16 kph, good visibility, and good road conditions.	The vehicle runs into another vehicle at low speed.	E4	S1	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving inside the city with heavy traffic and negligible pedestrian presence, stop and go driving above 16 kph, bad visibility, and slippery road conditions.	The vehicle runs into another vehicle at low speed.	E3	S1	C1	QM
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E4	S2	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E4	S2	C1	A
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E3	S2	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E3	S2	C1	QM
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Conducting an evasive maneuver deviating from desired path at medium speed (40 kph < V < 100 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed reduction; vehicle runs into another the vehicle.	E2	S2	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S2	C1	QM
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S2	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S2	C1	QM
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at medium speed (40 kph < V < 100 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S2	C1	QM

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at high speed (100 kph < V < 130 kph), heavy traffic, good visibility, and good road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E4	S3	C2	C
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at high speed (100 kph < V < 130 kph), light traffic, good visibility, and good road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E4	S3	C2	C

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at high speed (100 kph < V < 130 kph), heavy traffic, low visibility, and slippery road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E3	S3	C2	B
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Conducting an evasive maneuver deviating from desired path at high speed (100 kph < V < 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed reduction; vehicle runs into another the vehicle.	E2	S3	C2	A
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S3	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S3	C1	A
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, heavy traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S3	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at high speed (100 kph < V < 130 kph), country road, light traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S3	C1	A
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E3	S3	C2	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E3	S3	C2	B
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E2	S3	C2	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Driving at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	The driver responds to traffic conditions by reducing speed, but vehicle speed is not reduced as intended, and the vehicle runs into another vehicle or barrier.	E2	S3	C2	A
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Conducting an evasive maneuver deviating from desired path at high speed (V > 130 kph), light/heavy traffic, good/low visibility, and good/slippery road conditions.	Vehicle does not achieve its intended speed reduction; vehicle runs into another the vehicle.	E2	S3	C3	B

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ASC/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at a very high speed (V > 130 kph), heavy traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S3	C1	A
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at a very high speed (V > 130 kph), light traffic, good visibility, and good road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E3	S3	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at very high speed (V > 130 kph), heavy traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E2	S3	C1	A
1. Under BTO condition 2. ACS/ETC is functioning properly. 3. AP and BP are pressed simultaneously. 4. The vehicle speed is getting reduced but not at the intended rate.	Overtaking another vehicle at very high speed (V > 130 kph), light traffic, low visibility, and slippery road conditions.	Vehicle does not achieve its intended speed; vehicle runs into another the vehicle.	E2	S3	C1	A

Assumptions	Operating Scenario Description	Potential Crash Scenario	ASIL Assessment (Insufficient Vehicle Deceleration)			ASIL
			Exposure	Severity	Controllability	
1. Under BTO condition 2. E/E part of ACS/ETC is functioning properly. 3. AP stuck due to a mechanical failure. 4. The vehicle speed is getting reduced but not at the intended rate.	All		Not covered by ISO 26262; however this shall be captured in the Failure Mode Analysis and assigned the appropriate severity (10 or 9 in a Design FMEA)			
1. Under BTO condition 2. E/E part of ACS/ETC is mal-functioning. 3. The vehicle speed is getting reduced but not at the intended rate.			This scenario is covered in the Unintended Vehicle Propulsion hazard. Regardless of whether BTO is functioning or not, the hazard may still occur due to failure in the ASC/ETC system. In this case BTO is a safety mechanism for ASIL D hazard and it should be developed with ASIL B classification per ISO 26262.			B

APPENDIX G: FMEA RESULTS

Table G-1. FMEA for H1: Uncontrolled Vehicle Propulsion

(Malfunction: Commands More Torque Than Requested)

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
Engine Control Module	Commands larger throttle opening than required by the requested torque by the driver	ECM fault:	Three levels monitoring		ECM Fault
		Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ECM I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Torque command calculation algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		Software parameters corrupted		Periodic Checks	
		Arbitration logic fault	Three Levels Monitoring		System Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
Engine Control Module	Commands larger throttle opening than required by the requested torque by the driver	Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	ECM Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	Misinterprets the APP	Hardware or Software Fault (covered above)			
	Commands Incorrect Throttle Position	Hardware or Software Fault (covered above)			
	BTO Control Fault	BTO algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		Software parameters corrupted		Periodic checks	
		BPPS Fault			
		Vehicle speed sensor fault			
		Engine RPM speed sensor fault			
	Torque Map Corrupted	Hardware fault (covered above)			
		Corrupted parameters (vehicle and/or environment)		Periodic checks	

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
Engine Control Module	Miscommunicates with internal subsystems	From: APPS	Critical messages/data transfer qualification		Communication Fault
		To: Electronic Throttle Control (ETC)	Critical messages/data transfer qualification		Communication Fault
		From: ETC	Critical messages/data transfer qualification		Communication Fault
	Miscommunicates with external systems	From: BPPS	Critical messages/data transfer qualification		Communication Fault
		From: Vehicle Speed Sensor	Critical messages/data transfer qualification		Communication Fault
		From: Engine Revolution per Minute (rpm) Sensor	Critical messages/data transfer qualification		Communication Fault
		From: Automatic Emergency Braking (AEB)	Critical messages/data transfer qualification		Communication Fault
		From: Cruise Control (CC)/Adaptive Cruise Control (ACC)	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
Engine Control Module	Miscommunicates with external systems	From: Atmospheric Pressure Sensor	Critical messages/data transfer qualification		Communication Fault
	Diagnostics fault	Considered only in mitigation of multiple point failure analysis (Fault Tree Analysis)	Out of Scope for Functional Safety Concept		
ETC	Drives the throttle to a larger opening than commanded by the ECM	ETC fault:	Fault tolerant redundancy		ETC fault
		Hardware fault (Sensors, Integrated Circuits (IC), Circuit Components, Circuit Boards…)		Hardware (Hardware) diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ETC Input/Output (I/O) connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ETC I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		Actuator (motor) fault		Hardware/Software (Software) diagnostics	System Fault
		Motor position sensor fault		Hardware/Software diagnostics	System Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ETC	Drives the throttle to a larger opening than commanded by the ECM	Throttle position sensor fault		Hardware/Software diagnostics	System Fault
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Throttle position command calculation algorithm fault		Software diagnostics	
		Software parameters corrupted			
		Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		Electromagnetic Compatibility (EMC)/Electromagnetic Interference (EMI) fault		Hardware/Software Diagnostics	System Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		Noise Vibration Harshness (NVH) fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	Misinterprets the communication message from the ECM	Hardware or Software fault (covered above)			

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ETC	Mechanical failure prevents throttle movement to correct position	Out of Scope	Out of Scope for Functional Safety Concept		
Brake Pedal Position (BPP) Sensor	Provides incorrect input to ECM	Communication Fault to ECM	Critical messages/data transfer qualification		Brake System Fault
		Out of Scope			
Accelerator Pedal Position (APP) Sensor	APP value interpreted/communicated higher than actual	Sensor fault:	Fault tolerant redundancy	Sensor diagnostics	APP Sensor Fault
		Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in APP sensor I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to another connection		Stuck Open/Short	
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
APP Sensor	APP value interpreted/communicated higher than actual	APP calculation algorithm fault		Software diagnostics	
		Software parameters corrupted		Periodic checks	
		Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	System Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	APP Communicates with ECM Incorrectly	Hardware or Software fault (covered above)			
	Accelerator Pedal (AP) Assembly-Mechanical	Out of Scope	Out of Scope for Functional Safety Concept		
Vehicle Speed Sensor	Provides incorrect vehicle speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
		Out of Scope			
Engine RPM Sensor	Provides incorrect engine speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
Engine RPM Sensor	Provides incorrect engine speed	Out of Scope			
Atmospheric Pressure Sensor	Provides incorrect pressure (elevation) value	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
		Out of Scope			
Vehicle Communication System (Communication Area Network (CAN) Bus)	Communication messages corrupted during transfer within the Accelerator Control System (ACS)/ETC, and from and to the ACS/ETC and interfacing vehicle modules	Out of Scope	Out of Scope for Functional Safety Concept		
Other (interfacing) vehicle systems	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
		Out of Scope			
AEB	Command/Request for braking from AEB to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
		Out of Scope			
CC/ACC	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
		Out of Scope			
CC/ACC	Command/Request for braking from CC/ACC to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
		Out of Scope			

Table G-2. FMEA for H1a: Uncontrolled Vehicle Propulsion With Zero Starting Speed (Malfunction: Commands More Torque Than Requested)

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion With Zero Starting Speed)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands larger throttle opening than required by the requested torque by the driver	ECM fault:	Three levels monitoring		ECM Fault
		Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ECM I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Torque command calculation algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		Software parameters corrupted		Periodic Checks	
		Arbitration logic fault	Three Levels Monitoring		System Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion With Zero Starting Speed)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands larger throttle opening than required by the requested torque by the driver	Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	ECM Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	Misinterprets the APP	Hardware or Software Fault (covered above)			
	Commands Incorrect Throttle Position	Hardware or Software Fault (covered above)			
	Incorrectly Establishes Idle Position	Hardware or Software fault (covered above)			
		Atmospheric Pressure Sensor fault			
	Torque Map Corrupted	Hardware fault (covered above)			
		Corrupted parameters (vehicle and/or environment)		Periodic Checks	
	Miscommunicates with internal subsystems	From: Accelerator Pedal Position Sensor (APPS)	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion With Zero Starting Speed)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Miscommunicates with internal subsystems	To: ETC	Critical messages/data transfer qualification		Communication Fault
		From: ETC	Critical messages/data transfer qualification		Communication Fault
	Miscommunicates with external systems	From: Brake Pedal Position Sensor (BPPS)	Critical messages/data transfer qualification		Communication Fault
		From: Vehicle Speed Sensor	Critical messages/data transfer qualification		Communication Fault
		From: Engine RPM Sensor	Critical messages/data transfer qualification		Communication Fault
		From: AEB	Critical messages/data transfer qualification		Communication Fault
		From: CC/ACC	Critical messages/data transfer qualification		Communication Fault
		From: Atmospheric Pressure Sensor	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion With Zero Starting Speed)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Diagnostics fault	Considered only in mitigation of multiple point failure analysis (FTA)	Out of Scope for Functional Safety Concept		
ETC	Drives the throttle to a larger opening than commanded by the ECM	ETC fault:	Fault tolerant redundancy		ETC fault
		Break in ETC I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ETC I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Actuator (motor) fault		Hardware/Software diagnostics	System Fault
		Motor position sensor fault		Hardware/Software diagnostics	System Fault
		Throttle position sensor fault		Hardware/Software diagnostics	System Fault
		Throttle position command calculation algorithm fault		Software diagnostics	
		Software parameters corrupted			
		EMC/EMI fault		Hardware/Software Diagnostics	System Fault
	Fails to Maintain Throttle Idle Position	Hardware or Software fault (covered above)			
	Misinterprets the communication message from the ECM	Hardware or Software fault (covered above)			

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion With Zero Starting Speed)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ETC	Mechanical failure prevents throttle movement to correct position	Out of Scope			
BPP Sensor	Provides incorrect input to ECM	Communication Fault to ECM	Critical messages/data transfer qualification		Brake System Fault
		Out of Scope			
APP Sensor	APP value interpreted/communicated higher than actual	Sensor fault:	Fault tolerant redundancy	Sensor diagnostics	APP Sensor Fault
		Break in APP sensor I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to another connection		Stuck Open/Short	
		APP calculation algorithm fault		Software diagnostics	
	APP Communicates with ECM Incorrectly	Hardware or Software fault (covered above)			
	AP Is Not Returned to Idle Position	AP-mechanical Failure-Out of Scope	Out of Scope for Functional Safety Concept		
	AP Assembly-Mechanical	Out of Scope	Out of Scope for Functional Safety Concept		

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion With Zero Starting Speed)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
Vehicle Speed Sensor	Provides incorrect vehicle speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Engine RPM Sensor	Provides incorrect engine speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Atmospheric Pressure Sensor	Provides incorrect pressure (elevation) value	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Vehicle Communication System (CAN Bus)	Communication messages corrupted during transfer within the ASC/ETC, and from and to the ACS/ETC and interfacing vehicle modules	Out of Scope	Out of Scope for Functional Safety Concept		
Other (Interfacing) vehicle systems	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
AEB	Command/Request for braking from AEB to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
CC/ACC	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Uncontrolled Vehicle Propulsion With Zero Starting Speed)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
CC/ACC	Command/Request for braking from CC/ACC to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

Table G-3. FMEA for H2: Insufficient Vehicle Propulsion

(Malfunction: Commands Less Torque Than Requested)

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands smaller throttle opening than required by the requested torque by the driver	ECM fault:	Three levels monitoring		ECM Fault
		Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ECM I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Torque command calculation algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		Software parameters corrupted		Periodic Checks	
		Arbitration logic fault	Three Levels Monitoring		System Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands smaller throttle opening than required by the requested torque by the driver	Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	ECM Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	Misinterprets the APP	Hardware or Software Fault (covered above)			
	APP Rate Limiting Fault (Over-Limiting)	Hardware or Software Fault (covered above)			
	Commands Incorrect Throttle Position	Hardware or Software Fault (covered above)			
	Brake Throttle Override Control Fault	BTO algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		BPPS Fault			
		Vehicle speed sensor fault			
		Engine RPM speed sensor fault			
	Torque Map Corrupted	Hardware fault (covered above)			
		Corrupted parameters (vehicle and/or environment)		Periodic checks	

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Miscommunicates with internal subsystems	From: APPS	Critical messages/data transfer qualification		Communication Fault
		To: ETC	Critical messages/data transfer qualification		Communication Fault
		From: ETC	Critical messages/data transfer qualification		Communication Fault
	Miscommunicates with external systems	From: BPPS	Critical messages/data transfer qualification		Communication Fault
		From: Vehicle Speed Sensor	Critical messages/data transfer qualification		Communication Fault
		From: Engine RPM Sensor	Critical messages/data transfer qualification		Communication Fault
		From: AEB	Critical messages/data transfer qualification		Communication Fault
		From: CC/ACC	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Miscommunicates with external systems	From: Atmospheric Pressure Sensor	Critical messages/data transfer qualification		Communication Fault
	Diagnostics fault	Considered only in mitigation of multiple point failure analysis (FTA)	Out of Scope for Functional Safety Concept		
ETC	Drives the throttle to a smaller opening than commanded by the ECM	ETC fault:	Fault tolerant redundancy		ETC fault
		Break in ETC I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ETC I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Actuator (motor) fault		Hardware/Software diagnostics	System Fault
		Motor position sensor fault		Hardware/Software diagnostics	System Fault
		Throttle position sensor fault		Hardware/Software diagnostics	System Fault
		Throttle position command calculation algorithm fault		Software diagnostics	
		Software parameters corrupted			
		EMC/EMI fault		Hardware/Software Diagnostics	System Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ETC	Misinterprets the communication message from the ECM	Hardware or Software fault (covered above)			
	Mechanical failure prevents throttle movement to correct position	Out of Scope	Out of Scope for Functional Safety Concept		
BPP Sensor	Provides incorrect input to ECM	Communication Fault to ECM	Critical messages/data transfer qualification		Brake System Fault
		Out of Scope			
APP Sensor	APP value interpreted/communicated lower than actual	Sensor fault:	Fault tolerant redundancy	Sensor diagnostics	APP Sensor Fault
		Break in APP sensor I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to another connection		Stuck Open/Short	
		APP calculation algorithm fault		Software diagnostics	
		Aging (durability)			
	APP Rate Limiting Fault (Over-Limiting)	AP-mechanical Failure-Out of Scope	Out of Scope for Functional Safety Concept		
	AP Assembly-Mechanical	Out of Scope	Out of Scope for Functional Safety Concept		

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
Vehicle Speed Sensor	Provides incorrect vehicle speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Vehicle Speed Sensor	Provides incorrect vehicle speed	Out of Scope			
Engine RPM Sensor	Provides incorrect engine speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Atmospheric Pressure Sensor	Provides incorrect pressure (elevation) value	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Vehicle Communication System (CAN Bus)	Communication messages corrupted during transfer within the ACS/ETC, and from and to the ACS/ETC and interfacing vehicle modules	Out of Scope	Out of Scope for Functional Safety Concept		
Other (Interfacing) vehicle systems	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
AEB	Command/Request for braking from AEB to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Propulsion)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
CC/ACC	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
CC/ACC	Command/Request for braking from CC/ACC to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

Table G-4. FMEA for H3: Propulsion Power Reduction/Loss or Vehicle Stalling
(Malfunction: Commands Less Torque Than Requested)

System/Subsystem	Potential Failure Mode (Propulsion Power Reduction/Loss or Vehicle Stalling)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands smaller throttle opening than required by the requested torque by the driver	ECM fault:	Three levels monitoring		ECM Fault
		Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ECM I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Torque command calculation algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		Software parameters corrupted		Periodic Checks	
		Arbitration logic fault	Three Levels Monitoring		System Fault

System/Subsystem	Potential Failure Mode (Propulsion Power Reduction/Loss or Vehicle Stalling)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands smaller throttle opening than required by the requested torque by the driver	Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	ECM Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	Misinterprets the APP	Hardware or Software Fault (covered above)			
	Commands Incorrect Throttle Position	Hardware or Software Fault (covered above)			
	Incorrectly Establishes Idle Position	Hardware or Software fault (covered above)			
		Atmospheric Pressure Sensor fault			
	BTO Control Fault	BTO algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		BPPS Fault			
		Vehicle speed sensor fault			
		Engine RPM speed sensor fault			
	Torque Map Corrupted	Hardware fault (covered above)			

System/Subsystem	Potential Failure Mode (Propulsion Power Reduction/Loss or Vehicle Stalling)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Torque Map Corrupted	Corrupted parameters (vehicle and/or environment)		Periodic checks	
	Miscommunicates with internal subsystems	From: APPS	Critical messages/data transfer qualification		Communication Fault
		To: ETC	Critical messages/data transfer qualification		Communication Fault
		From: ETC	Critical messages/data transfer qualification		Communication Fault
	Miscommunicates with external systems	From: BPPS	Critical messages/data transfer qualification		Communication Fault
		From: Vehicle Speed Sensor	Critical messages/data transfer qualification		Communication Fault
		From: Engine RPM Sensor	Critical messages/data transfer qualification		Communication Fault
		From: AEB	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Propulsion Power Reduction/Loss or Vehicle Stalling)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Miscommunicates with external systems	From: CC/ACC	Critical messages/data transfer qualification		Communication Fault
		From: Atmospheric Pressure Sensor	Critical messages/data transfer qualification		Communication Fault
	Diagnostics fault	Considered only in mitigation of multiple point failure analysis (FTA)	Out of Scope for Functional Safety Concept		
ETC	Drives the throttle to a smaller opening than commanded by the ECM	ETC fault:	Fault tolerant redundancy		ETC fault
		Break in ETC I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ETC I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Actuator (motor) fault		Hardware/Software diagnostics	System Fault
		Motor position sensor fault		Hardware/Software diagnostics	System Fault
		Throttle position sensor fault		Hardware/Software diagnostics	System Fault
		Throttle position command calculation algorithm fault		Software diagnostics	
		Software parameters corrupted			

System/Subsystem	Potential Failure Mode (Propulsion Power Reduction/Loss or Vehicle Stalling)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ETC	Drives the throttle to a smaller opening than commanded by the ECM	EMC/EMI fault		Hardware/Software Diagnostics	System Fault
	Fails to Maintain Throttle Idle Position	Hardware or Software fault (covered above)			
	Misinterprets the communication message from the ECM	Hardware or Software fault (covered above)			
	Mechanical failure prevents throttle movement to correct position	Out of Scope	Out of Scope for Functional Safety Concept		
BPP Sensor	Provides incorrect input to ECM	Communication Fault to ECM	Critical messages/data transfer qualification		Brake System Fault
		Out of Scope			
APP Sensor	APP value interpreted lower than actual	Sensor fault:	Fault tolerant redundancy	Sensor diagnostics	APP Sensor Fault
		Break in APP sensor I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to another connection		Stuck Open/Short	
		APP calculation algorithm fault		Software diagnostics	
		Aging (durability)			

System/Subsystem	Potential Failure Mode (Propulsion Power Reduction/Loss or Vehicle Stalling)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
APP Sensor	APP value interpreted lower than actual	Manufacturing variability			
	AP Is Not Returned to Idle Position Correctly	AP-mechanical Failure-Out of Scope	Out of Scope for Functional Safety Concept		
	APP Communicates with ECM Incorrectly	Hardware or Software fault (covered above)			
	AP Assembly-Mechanical	Out of scope	Out of Scope for Functional Safety Concept		
Vehicle Speed Sensor	Provides incorrect vehicle speed to ECM	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Engine RPM Sensor	Provides incorrect engine speed to ECM	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Atmospheric Pressure Sensor	Provides incorrect pressure (elevation) value to ECM	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Vehicle Communication System (CAN Bus)	Communication messages corrupted during transfer within the ASC/ETC, and from and to the ACS/ETC and interfacing vehicle modules	Out of Scope	Out of Scope for Functional Safety Concept		
Other (Interfacing) vehicle systems	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
AEB	Command/Request for braking from AEB to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Propulsion Power Reduction/Loss or Vehicle Stalling)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
CC/ACC	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
	Command/Request for braking from CC/ACC to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

Table G-5. FMEA for H4: Insufficient Vehicle Deceleration

(Malfunction: Commands More Torque Than Requested)

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands smaller throttle opening than required by the requested torque by the driver	ECM fault:	Three levels monitoring		ECM Fault
		Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ECM I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Torque command calculation algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault
		Software parameters corrupted		Periodic Checks	

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Commands smaller throttle opening than required by the requested torque by the driver	Arbitration logic fault	Three Levels Monitoring		System Fault
		Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	ECM Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	Misinterprets the APP	Hardware or Software Fault (covered above)			
	APP Rate Limiting Fault (Over-Limiting)	Hardware or Software Fault (covered above)			
	Commands Incorrect Throttle Position	Hardware or Software Fault (covered above)			
	Incorrectly Establishes Idle Position	Hardware or Software fault (covered above)			
		Software parameters corrupted		Periodic checks	
		Atmospheric Pressure Sensor fault			
	BTO Control Fault	BTO algorithm fault	Three Levels Monitoring	Software diagnostics	System Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	BTO Control Fault	Software parameters corrupted		Periodic checks	
		BPPS Fault			
		Vehicle speed sensor fault			
		Engine RPM speed sensor fault			
	Torque Map Corrupted	Hardware fault (covered above)			
		Corrupted parameters (vehicle and/or environment)		Periodic checks	
	Miscommunicates with internal subsystems	From: APPS	Critical messages/data transfer qualification		Communication Fault
		To: ETC	Critical messages/data transfer qualification		Communication Fault
		From: ETC	Critical messages/data transfer qualification		Communication Fault
	Miscommunicates with external systems	From: BPPS	Critical messages/data transfer qualification		Communication Fault
		From: Vehicle Speed Sensor	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ECM	Miscommunicates with external systems	From: Engine RPM Sensor	Critical messages/data transfer qualification		Communication Fault
		From: AEB	Critical messages/data transfer qualification		Communication Fault
		From: CC/ACC	Critical messages/data transfer qualification		Communication Fault
		From: Atmospheric Pressure Sensor	Critical messages/data transfer qualification		Communication Fault
	Diagnostics fault	Considered only in mitigation of multiple point failure analysis (FTA)	Out of Scope for Functional Safety Concept		
ETC	Drives the throttle to a larger opening than commanded by the ECM	ETC fault:	Fault tolerant redundancy		ETC fault
		Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)		Hardware diagnostics	
		Internal connection fault (short or open)		Hardware diagnostics	
		Break in ETC I/O connections	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
ETC	Drives the throttle to a larger opening than commanded by the ECM	Short in ETC I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in ECM I/O connections to another connection		Stuck Open/Short	
		Actuator (motor) fault		Hardware/Software diagnostics	System Fault
		Motor position sensor fault		Hardware/Software diagnostics	System Fault
		Throttle position sensor fault		Hardware/Software diagnostics	System Fault
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		Throttle position command calculation algorithm fault		Software diagnostics	
		Software parameters corrupted			
		Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	System Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		

<table>
<tr><th rowspan="2">System/Subsystem</th><th rowspan="2">Potential Failure Mode (Insufficient Vehicle Deceleration)</th><th rowspan="2">Potential Cause/Mechanism of Failure</th><th colspan="3">Current Process Controls</th></tr>
<tr><th>Safety Mechanism</th><th>Diagnostics</th><th>Diagnostic Trouble Code</th></tr>
<tr><td rowspan="7">ETC</td><td rowspan="4">Drives the throttle to a larger opening than commanded by the ECM</td><td>Aging (durability)</td><td colspan="3">Out of Scope for Functional Safety Concept</td></tr>
<tr><td>Manufacturing defect</td><td colspan="3">Out of Scope for Functional Safety Concept</td></tr>
<tr><td>Manufacturing variability</td><td colspan="3">Out of Scope for Functional Safety Concept</td></tr>
<tr><td>Service/Maintenance</td><td colspan="3">Out of Scope for Functional Safety Concept</td></tr>
<tr><td>Fails to Maintain Throttle Idle Position</td><td>Hardware or Software fault (covered above)</td><td></td><td></td><td></td></tr>
<tr><td>Misinterprets the communication message from the ECM</td><td>Hardware or Software fault (covered above)</td><td></td><td></td><td></td></tr>
<tr><td>Mechanical failure prevents throttle movement to correct position</td><td>Out of Scope</td><td colspan="3">Out of Scope for Functional Safety Concept</td></tr>
<tr><td rowspan="2">BPP Sensor</td><td rowspan="2">Provides incorrect input to ECM</td><td>Communication Fault to ECM</td><td>Critical messages/data transfer qualification</td><td></td><td>Brake System Fault</td></tr>
<tr><td>Out of Scope</td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">APP Sensor</td><td rowspan="4">APP value interpreted/communicated higher than actual</td><td>Sensor fault:</td><td>Fault tolerant redundancy</td><td>Sensor diagnostics</td><td>APP Sensor Fault</td></tr>
<tr><td>Hardware fault (Sensors, ICs, Circuit Components, Circuit Boards…)</td><td></td><td>Hardware diagnostics</td><td></td></tr>
<tr><td>Internal connection fault (short or open)</td><td></td><td>Hardware diagnostics</td><td></td></tr>
<tr><td>Break in APP sensor I/O connections</td><td>Critical messages/data transfer qualification</td><td>Stuck Open/Short</td><td>I/O Fault</td></tr>
</table>

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
APP Sensor	APP value interpreted/communicated higher than actual	Short in APP sensor I/O connections to Ground or Voltage	Critical messages/data transfer qualification	Stuck Open/Short	I/O Fault
		Short in APP sensor I/O connections to another connection		Stuck Open/Short	
		Signal connector connection failure		Hardware diagnostics	
		Power connector connection failure		Hardware diagnostics	
		APP calculation algorithm fault		Software diagnostics	
		Software parameters corrupted		Periodic checks	
		Supply power out of range		Supply power value	Loss of Power
		Supply power quality failure		Supply power quality	Loss of Power
		EMC/EMI fault		Hardware/Software Diagnostics	System Fault
		Contamination/Corrosion	Out of Scope for Functional Safety Concept		
		NVH fault	Out of Scope for Functional Safety Concept		
		Environmental temperature exposure failure	Out of Scope for Functional Safety Concept		
		Aging (durability)	Out of Scope for Functional Safety Concept		
		Manufacturing defect	Out of Scope for Functional Safety Concept		
		Manufacturing variability	Out of Scope for Functional Safety Concept		
		Service/Maintenance	Out of Scope for Functional Safety Concept		
	AP Returned to Idle Position Incorrectly	AP-mechanical Failure-Out of Scope	Out of Scope for Functional Safety Concept		

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
APP Sensor	APP Rate Limiting Fault (Over-Limiting)	AP-mechanical Failure-Out of Scope	Out of Scope for Functional Safety Concept		
	AP Assembly-Mechanical	Out of Scope	Out of Scope for Functional Safety Concept		
Vehicle Speed Sensor	Provides incorrect vehicle speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Engine RPM Sensor	Provides incorrect engine speed	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Atmospheric Pressure Sensor	Provides incorrect pressure (elevation) value	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
Vehicle Communication System (CAN Bus)	Communication messages corrupted during transfer within the ASC/ETC, and from and to the ACS/ETC and interfacing vehicle modules	Out of Scope	Out of Scope for Functional Safety Concept		
Other (Interfacing) vehicle systems	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
AEB	Command/Request for braking from AEB to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

System/Subsystem	Potential Failure Mode (Insufficient Vehicle Deceleration)	Potential Cause/Mechanism of Failure	Current Process Controls		
			Safety Mechanism	Diagnostics	Diagnostic Trouble Code
CC/ACC	Provides request for incorrect (more) propulsion torque	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault
CC/ACC	Command/Request for braking from CC/ACC to ECM failure	Communication Fault to ECM	Critical messages/data transfer qualification		Communication Fault

APPENDIX H: STPA STEP 2: CAUSAL FACTORS

Table H-1: Accelerator Pedal Mechanical Assembly

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Mechanical Assembly)
249	Actuator inadequate operation, change over time	Degradation over time	The accelerator pedal assembly hardware may degrade over time (e.g., increased friction), preventing the accelerator pedal from properly activating the accelerator pedal position sensor. Possible effects of this hardware failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal - becoming stuck at a position. The Engine Control Module may have the wrong accelerator pedal position information or may think the accelerator pedal is not pressed.
541	Actuator inadequate operation, change over time	Internal hardware failure	A hardware failure in the accelerator pedal assembly (e.g., pedal comes loose, return spring failure) could prevent the accelerator pedal from properly activating the accelerator pedal position sensor. Possible effects of this hardware failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal - becoming stuck at a position. The ECM may have the wrong accelerator pedal position information or may think the accelerator pedal is not pressed.
250	External disturbances	Physical interference (e.g., chafing)	Foreign objects in the driver's foot well could affect the accelerator pedal movement and positioning. Possible effects of this failure may include: - loss of function - incorrect or intermittent positioning of the accelerator pedal, - becoming stuck at a position.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Mechanical Assembly)
256	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects and assembly problems could affect the movement of the accelerator pedal (e.g., slow return). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
283	External disturbances	Vibration or shock impact	Vibration and shock impact may cause the accelerator pedal assembly hardware to move (e.g., vibration of the pedal). Possible effects of this failure may include: - loss of function - incorrect or intermittent movement of the accelerator pedal. In regard to mode switching: If the mode switching algorithm has a minimum pedal angle that signifies "pressed", vibration may cause the pedal angle to fall below this threshold. This may cause the ECM to think the pedal conflict is removed and exit Brake Throttle Override mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
583	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion or contamination from the external environment (e.g., dirt, rust) may affect the movement of the accelerator pedal. Possible effects of this pedal failure may include: - loss of function - incorrect or intermittent movement of the accelerator pedal, - a delay in movement, or - becoming stuck at a position.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Mechanical Assembly)
251	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components may interfere with the accelerator pedal (e.g., floor mats), preventing the pedal from moving when the driver tries to change the angular position of the pedal. Possible effects of this failure may include: - loss of function, - incorrect or intermittent positioning of the accelerator pedal, or - becoming stuck at a position.

Table H-2: Accelerator Pedal Position Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
252	Sensor inadequate operation, change over time	Internal hardware failure	A hardware failure in the accelerator pedal position sensor could result in an open circuit or an intermittent open circuit. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If the signal from the Accelerator Pedal Position Sensor (APPS) becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
286	Sensor inadequate operation, change over time	Degradation over time	The APPS may degrade over time, resulting in a short circuit, change in the sensor's measurement properties, or an intermittent signal to the ECM. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement/reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If the signal from the APPS becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
316	Sensor inadequate operation, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) may cause the APPS to overheat, affecting its function. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. This may cause the ECM to have the wrong accelerator pedal position information. In regard to mode switching: If this results in an intermittent signal to the ECM, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
589	Sensor inadequate operation, change over time	Reporting frequency too low	If the APPS reading frequency is too low, there may be a delay before the ECM realizes the accelerator pedal position has changed.
254	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) may affect the accelerator pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If the signal from the APPS becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
255	External disturbances	Electromagnetic Interference (EMI) or Electrostatic Discharge (ESD)	EMI or ESD from the external environment may affect the accelerator pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
288	External disturbances	Vibration or shock impact	Vibration and shock impact from the external environment may affect the accelerator pedal position sensor (e.g., the sensor makes intermittent contact). Possible effects of this signal may include: - loss of function, - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: This may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
315	External disturbances	Extreme external temperature or thermal cycling	Extreme external temperature or temperature cycling (e.g., heat or cold) may damage the APPS or cause the APPS to overheat, affecting its function. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If this results in an intermittent signal to the ECM, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
604	External disturbances	Organic growth	Organic growth from the external environment (e.g., fungi) may affect the accelerator pedal position sensor, causing shorting or damage to the electrical subcomponents. Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
605	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the function of the accelerator pedal position sensor. Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measurement or reporting of the accelerator pedal position, or - becoming stuck at a value (e.g., the accelerator pedal position measurement does not update).
610	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects may damage the accelerator pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If this results in an intermittent signal to the ECM, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
611	External disturbances	Magnetic interference	Magnetic interference from the external environment could affect the accelerator pedal position sensor measurement (e.g., if it is a hall effect sensor). Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measuring or reporting of the accelerator pedal position, or - becoming stuck at a value (e.g., reporting a constant accelerator pedal position).
257	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components may affect the accelerator pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
258	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., Air Conditioning (A/C) condensation) may affect the accelerator pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
289	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components (e.g., deformation of the sensor due to inadequate clearance) may damage the accelerator pedal position sensor. Possible effects of this sensor failure may include - loss of function, - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If this results in an intermittent signal to the ECM, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
608	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the accelerator pedal position sensor. Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measuring or reporting of the accelerator pedal position, or - becoming stuck at a value (e.g., reporting a constant accelerator pedal position).
609	Hazardous interaction with other components in the rest of the vehicle	Magnetic interference	Magnetic interference from other vehicle components could affect the accelerator pedal position sensor measurement (e.g., if it is a hall effect sensor). Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measuring or reporting of the accelerator pedal position, or - becoming stuck at a value (e.g., reporting a constant accelerator pedal position).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
612	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive temperatures from other vehicle components may affect the accelerator pedal position sensor. Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measuring or reporting of the accelerator pedal position, - a delay in reporting the accelerator pedal position, or - becoming stuck at a value. In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
259	Power supply faulty (high, low, disturbance)	Loss of 12-volt power	If the accelerator pedal position sensor loses 12-volt power, it will not be able to transmit a signal to the ECM. The ECM may think the pedal is released.
287	Power supply faulty (high, low, disturbance)	Power supply faulty (high, low, disturbance)	If there is a disruption in the 12-volt power supply, the accelerator pedal position sensor may issue an intermittent signal to the ECM. Possible effects of this disruption may include: - loss of function - incorrect or intermittent measurement/reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. This may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
543	Power supply faulty (high, low, disturbance)	Reference voltage incorrect (e.g., too low, too high)	A decrease in the supply voltage to the accelerator pedal position sensor may cause the ECM to think that the accelerator pedal angular position is decreasing or is less than the actual pedal position.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor)
813	Power supply faulty (high, low, disturbance)	Reference voltage incorrect (e.g., too low, too high)	An increase in the supply voltage to the accelerator pedal position sensor may cause the ECM to think that the accelerator pedal angular position is increasing or is greater than the actual pedal position.

Table H-3: Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
3	Controller hardware faulty, change over time	Internal hardware failure	The ECM may be affected by a faulty electronic subcomponent or electrical connection within the ECM (e.g., a transistor is not switched off or soldering breaks).
4	Controller hardware faulty, change over time	Faulty memory storage or retrieval	The memory block in the ECM that stores the current throttle position may have a fault, or an error may occur when storing or retrieving data from memory. This could cause the ECM to have incorrect information about the throttle position (e.g., ECM may think the throttle is at idle when it's not).
188	Controller hardware faulty, change over time	Degradation over time	Internal subcomponents in the ECM may degrade over time, affecting the function of the ECM.
211	Controller hardware faulty, change over time	Faulty memory storage or retrieval	If the vehicle speed is written to memory, the memory block in the ECM storing the vehicle speed may have a fault, or an error may occur when storing or retrieving data from memory. This could cause the ECM to have the incorrect vehicle speed.
216	Controller hardware faulty, change over time	Faulty memory storage or retrieval	The memory block in the ECM storing the operating mode may have a fault, or an error may occur when storing or retrieving data from memory. This could prevent the ECM from switching operating modes or may cause the ECM to incorrectly switch operating modes.
219	Controller hardware faulty, change over time	Faulty internal timing clock	If the ECM uses internal timing for determining when to issue a control action (e.g., engage BTO), faulty electronic subcomponents in the timing module could cause the control action to be issued too soon or too late.
236	Controller hardware faulty, change over time	Faulty memory storage or retrieval	If the brake pedal position is written to memory, the memory block in the ECM storing the brake pedal position may have a fault, or an error may occur when storing or retrieving data from memory.
308	Controller hardware faulty, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) may cause the ECM to overheat, affecting its function.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
360	Controller hardware faulty, change over time	Faulty memory storage or retrieval	The memory block in the ECM that stores the idle throttle position may have a fault, or an error may occur when storing or retrieving data from memory. This could cause the ECM to have incorrect information about where the throttle should be at idle.
452	Controller hardware faulty, change over time	Faulty signal conditioning or converting (e.g., analog-to-digital converter, signal filters)	A fault in interpreting an analogue signal from a system sensor (e.g., analogue-to-digital converter, signal filters) could affect the ECM's ability to determine the correct throttle position.
468	Controller hardware faulty, change over time	Faulty memory storage or retrieval	The memory block in the ECM storing the throttle position for BTO mode (i.e., if different from the idle position) may have a fault, or an error may occur when storing or retrieving data from memory. This could cause the ECM to use the wrong throttle position for BTO mode.
767	Controller hardware faulty, change over time	Over temperature due to faulty cooling system	A hardware failure in the cooling system (e.g., damage to cooling fins) could cause the ECM to overheat, affecting its function.
798	Controller hardware faulty, change over time	Unused circuits in the controller	A signal could jump to an unused circuit built into the microcontroller and cause it to fail. This failure could affect the functioning of the ECM.
218	External control input or information wrong or missing	Timing related input is incorrect or missing	If the ECM requires a timing signal from an external source (e.g., a central timing module), this signal may be incorrect or missing.
444	External control input or information wrong or missing	Corrupted input signal	A failure in an active vehicle safety system, cruise control system, or other systems that can request a throttle change may affect the throttle requests. Possible effects of this system failure may include: - an incorrect throttle request, - a throttle reduction that is not needed.
542	External control input or information wrong or missing	Spurious input due to shorting or other electrical fault	The ECM may receive a signal that mimics a torque request from another vehicle system when no such request was made (e.g., a communication bus error, or a short in a wired connection to the ECM).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
766	External control input or information wrong or missing	Malicious Intruder	A malicious intruder may send a signal to the ECM that mimics a torque request from another vehicle system when no such request was made.
91	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the ECM, causing internal short or open circuits, or other failures of the control module.
92	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the ECM.
106	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the function of the ECM.
178	External disturbances	Vibration or shock impact	Vibration or shock impact may affect the ECM, causing damage to internal subcomponents (e.g., soldering breaks).
307	External disturbances	Extreme external temperature or thermal cycling	Extreme external temperature or temperature cycling (e.g., heat or cold) may damage the ECM or cause the ECM to overheat.
762	External disturbances	Single event effects (e.g., cosmic rays, protons)	A Single Event Effect (SEE) caused by high-energy particles could affect the ECM (e.g., cause temporary faults in software logic or memory corruption).
763	External disturbances	Organic growth	Organisms may grow in the ECM (e.g., fungi), resulting in internal shorting or damage of electrical subcomponents.
793	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects from the external environment could affect the ECM (e.g., damaging internal subcomponents).
2	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the ECM.
93	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the ECM, causing internal short or open circuits, or other failures of the control module.
177	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components may affect the ECM (e.g., damaging internal subcomponents).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
764	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the ECM (e.g., damaging internal subcomponents).
765	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the ECM (e.g., damaging internal subcomponents).
94	Power supply faulty (high, low, disturbance)	Loss of 12-volt power	If the ECM loses 12-volt power, it will be unable to issue a required control action.
223	Power supply faulty (high, low, disturbance)	Power supply faulty (high, low, disturbance)	A power supply voltage fluctuation, including power spikes in the 12-volt power supply may damage the ECM, cause the ECM to erase information stored in volatile memory (e.g., sensor data or operating mode), or cause the ECM to delay issuing a control action (e.g., switching operating modes), or cause the ECM to incorrectly issue a control action (e.g. switching modes before the conditions are met).
10	Process model or calibration incomplete or incorrect	Sensor or actuator calibration, including degradation characteristics	The throttle position sensor calibration in the ECM may be incorrect. This would cause the ECM to have incorrect information about the throttle position.
95	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	If the ECM process model considers variables beyond the accelerator pedal position, brake pedal position, and the vehicle speed, this may make the conditions for entering BTO mode too stringent.
150	Process model or calibration incomplete or incorrect	Sensor or actuator calibration, including degradation characteristics	The brake pedal position sensor calibration in the ECM may be incorrect. This could cause the ECM to misinterpret the travel distance of the brake pedal.
195	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	The ECM process model may have an incorrect value for determining the pedal application sequence.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
214	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	If the ECM process model does not consider vehicle speed or considers a vehicle speed below 10 Miles per Hour (mph), the ECM may switch into BTO when the driver presses both pedals and the vehicle speed is below 10 mph.
222	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	The ECM process model may have an incorrect value for the BTO activation delay (e.g., 0.05 seconds instead of 0.5 seconds or vice versa).
264	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	If the ECM process model considers variables beyond the accelerator pedal position and brake pedal position this may make the conditions for entering Normal mode too stringent.
265	Process model or calibration incomplete or incorrect	Sensor or actuator calibration, including degradation characteristics	The accelerator pedal position sensor calibration in the ECM may be incorrect. This could cause the ECM to have the wrong pedal position information.
293	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	If the ECM process model considers conditions other than the brake and accelerator pedal positions for exiting BTO mode (e.g., drive power or engine speed), then the ECM may prematurely exit BTO mode.
357	Process model or calibration incomplete or incorrect	Sensor or actuator calibration, including degradation characteristics	The engine Revolution per Minute (rpm) sensor calibration in the ECM may be incorrect. This could cause the ECM to misinterpret the engine speed information and the ECM may adjust the throttle to maintain the appropriate idle engine speed.
358	Process model or calibration incomplete or incorrect	Sensor or actuator calibration, including degradation characteristics	The MAF/ MAP sensor calibration in the ECM may be incorrect. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
448	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	The ECM model for the throttle position accumulates errors (e.g., numerical errors, integral windup), causing the ECM to incorrectly adjust the throttle position.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
457	Process model or calibration incomplete or incorrect	Model of the controlled process, including degradation characteristics	The ECM may learn an incorrect idle throttle position due to faulty inputs to the controller (e.g., the accelerator pedal position sensor shaft may have resonance with vibrations, causing the ECM to falsely recalibrate the idle position of the accelerator pedal).
814	Process model or calibration incomplete or incorrect	Sensor or actuator calibration, including degradation characteristics	The throttle motor calibration in the ECM may be incorrect. This may cause the ECM to request too much or too little of a throttle opening.
5	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to decrease the throttle opening when transitioning into normal mode (i.e., instead of increasing the throttle opening).
8	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic allows the ECM to decrease the throttle opening when the driver reduces the angular position of the accelerator pedal when in BTO mode (e.g., the throttle opening was already reduced to idle upon entering BTO mode).
90	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic prevents the ECM from switching into BTO mode when the driver presses both pedals and the vehicle speed is over 10 mph.
179	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The sequence of pedal application is not considered or is incorrectly considered in the software logic for entering BTO or Normal mode.
213	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to switch into BTO mode when the driver presses both pedals, but the vehicle speed is below 10 mph.
217	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic may prevent storing the current ECM mode (e.g., writing to memory) after the ECM issues the command to switch.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
220	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The timing delay before activating BTO is not considered or is incorrectly considered in the software logic for entering BTO mode.
237	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to switch into BTO mode when the brake pedal is not pressed.
290	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to switch into Normal mode while the driver presses both the accelerator pedal and brake pedal.
291	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The software algorithm allows the ECM to exit BTO mode when one pedal drops below an angular position threshold (e.g., below 25%), and does not require BTO mode to persist until the pedal conflict is removed (i.e., one pedal is released).
292	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The software algorithm may allow other vehicle systems to command the ECM to exit BTO mode while a pedal conflict still exists.
305	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The software algorithm may incorporate a delay before exiting BTO mode.
355	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A faulty control algorithm affects how much the ECM decreases the throttle opening when the driver reduces the angular position of the accelerator pedal and the ECM is in normal mode.
356	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The ECM software algorithm gives precedence to another vehicle system's request to adjust the throttle position (e.g., increase throttle), rather than the driver's request via the accelerator pedal.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
370	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to incorrectly reconcile the magnitude of multiple torque requests in opposite directions, causing the ECM not to issue a control action (i.e., inaction) or to issue an unsafe control action (e.g., increasing instead of reducing the throttle opening).
414	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic allows the ECM to execute another vehicle system's request to decrease or increase the throttle opening when the ECM is in BTO mode or transitioning into BTO mode (e.g., a throttle reduction request for traction control).
441	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A faulty control algorithm causes the ECM to incorrectly translate the torque requests from other vehicle systems to throttle opening command (e.g., produce too much or too little throttle opening).
445	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to decrease the throttle opening when the driver increases the angular position of the accelerator pedal.
446	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic may cause the ECM to incorrectly calculate the engine load. If the ECM thinks the engine load decreased, the ECM may decrease the throttle opening or may not increase the throttle opening enough. If the ECM thinks the engine load increased, the ECM may increase the throttle opening or may not decrease the throttle opening enough.
447	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic may cause the ECM to incorrectly enter a "limp-home" mode when the driver reduces the angular position of the accelerator pedal.
449	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to incorrectly reconcile the magnitude of multiple torque requests in the same direction (e.g., it may add the magnitude of torque reductions).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
451	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The control algorithm or transfer function is incorrect, leading to a large steady state error in the throttle position.
455	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic may cause the ECM to incorrectly calculate the idle throttle position.
469	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic affects how much the ECM decreases the throttle opening when transitioning into BTO mode.
474	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic introduces a delay into decreasing the throttle position when transitioning into BTO mode.
476	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to give precedence to the driver's input via the accelerator pedal instead of torque requests from other vehicle systems.
477	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM not to recognize that a torque request is from an active safety system.
527	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes a delay when the ECM tries to reconcile the magnitude of multiple torque requests.
536	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to match the throttle position to the accelerator pedal angular position when transitioning into normal mode, without the driver increasing the angular position of the accelerator pedal.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
539	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to increase the throttle opening when the driver decreases the angular position of the accelerator pedal.
540	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to execute another vehicle system's request to increase the throttle opening when transitioning into normal mode, without the driver increasing the angular position of the accelerator pedal.
544	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic may cause the ECM to incorrectly enter a "limp-home" mode when transitioning from BTO mode to normal mode or when transitioning from normal mode into BTO mode.
545	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A faulty control algorithm affects how the ECM increases the throttle opening when transitioning into normal mode (e.g., the throttle opening value is incorrect).
548	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic prevents the ECM from increasing the throttle opening when transitioning into normal mode when the driver increases the angular position of the accelerator pedal.
549	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic may cause the ECM to incorrectly enter a "limp-home" mode when other vehicle systems request an increase in engine torque or when the driver increases the angular position of the accelerator pedal.
550	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic prevents the ECM from overriding the accelerator pedal input when the ECM is in BTO mode or is transitioning into BTO mode.
586	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The ECM software algorithm does not check for consistency between the engine speed, vehicle speed, and throttle opening states.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module)
587	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	A programming error or faulty software logic causes the ECM to command the throttle to increase or decrease for too long or too short of a period (e.g., wrong parameter value).
761	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Flaws in software code creation	An error in the ECM software code may be introduced when the code is created (e.g., a flaw in automatic code generation).

Table H-4: Throttle Motor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor)
479	Actuator inadequate operation, change over time	Incorrectly sized actuator	If the throttle motor is the wrong size, it will have a different torque output than expected by the ECM. This could result in a different throttle opening than requested by the ECM.
481	Actuator inadequate operation, change over time	Internal hardware failure	A hardware failure in the throttle motor could affect its torque output (e.g., loose shaft, faulty H-bridge circuit). Possible effects of this hardware failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output value. This could result in a different throttle opening than requested by the ECM.
482	Actuator inadequate operation, change over time	Degradation over time	The throttle motor may degrade over time (e.g., wear of commutator brushes), which could affect its torque output. Possible effects of this hardware failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output value. This could result in a different throttle opening than requested by the ECM.
483	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the throttle motor. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output value. This could result in a different throttle opening than requested by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor)
484	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, dirt) could affect the throttle motor. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.
485	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could damage the throttle motor (e.g., solder cracking), affecting its torque output. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.
486	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the throttle motor. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor)
487	External disturbances	Extreme external temperature or thermal cycling	Extreme external temperatures or temperature cycling could affect the throttle motor (e.g., overheating). Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.
717	External disturbances	Organic growth	Organisms may grow in the throttle motor (e.g., fungi), causing internal shorting or damage to subcomponents. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output value. This could result in a different throttle opening than requested by the ECM.
786	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could damage the throttle motor (e.g., solder cracking), affecting its torque output. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor)
490	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the throttle motor. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.
491	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components could affect the throttle motor (e.g., causing misalignment of the motor). Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.
492	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components could affect the throttle motor (e.g., causing a short circuit). Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor)
718	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive temperatures from other vehicle components may affect the throttle motor. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.
728	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the throttle motor. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.
488	Power supply faulty (high, low, disturbance)	Loss of 12-volt power	If the throttle motor loses 12-volt power, it would be unable to adjust the throttle opening.
815	Power supply faulty (high, low, disturbance)	Power supply faulty (high, low, disturbance)	A power surge could damage the throttle motor, affecting its torque output. Possible effects of this motor failure may include: - loss of function - incorrect or intermittent torque output from the throttle motor, - a delay in torque output, or - becoming stuck at a constant torque output. This could result in a different throttle opening than requested by the ECM.

Table H-5: Throttle Position Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor)
18	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the TPS. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
88	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the TPS. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
107	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment may affect the throttle position sensor, causing damage to internal subcomponents (e.g., soldering breaks). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
181	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the function of the throttle position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor)
321	External disturbances	Extreme external temperature or thermal cycling	An extreme external temperature or temperature cycling (e.g., heat or cold) could damage the throttle position sensor. Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
719	External disturbances	Organic growth	Organisms may grow in the TPS (e.g., fungi), causing internal shorting or damage to electrical subcomponents. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
21	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the TPS. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
89	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the TPS. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
180	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components (e.g., inadequate clearance) could affect the TPS. This could cause the TPS to incorrectly measure the throttle position.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor)
720	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive temperatures from other vehicle components could affect the TPS. This could cause the TPS to incorrectly measure the throttle position.
721	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the TPS. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
87	Power supply faulty (high, low, disturbance)	Loss of 12-volt power	If the TPS loses 12-volt power, this could affect the signal to the ECM. Possible effects of this loss may include: - loss of function - becoming stuck at a value, - ECM may think the throttle is in the closed position.
471	Power supply faulty (high, low, disturbance)	Reference voltage incorrect (e.g., too low, too high)	A reduction in the supply voltage to the TPS may cause the ECM to think the throttle opening is smaller than the actual throttle opening.
811	Power supply faulty (high, low, disturbance)	Reference voltage incorrect (e.g., too low, too high)	An increase in the supply voltage to the TPS may cause the ECM to think the throttle opening is larger than the actual throttle opening.
17	Sensor inadequate operation, change over time	Internal hardware failure	The TPS may have an internal hardware failure (e.g., short circuit). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor)
103	Sensor inadequate operation, change over time	Degradation over time	The TPS could degrade over time (e.g., wear of a potentiometer brush), which could change its measurement properties or cause the sensor to stop functioning. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
322	Sensor inadequate operation, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) could cause the throttle position sensor to overheat, affecting its function. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the TPS to incorrectly measure the throttle position.
591	Sensor inadequate operation, change over time	Reporting frequency too low	If the throttle position sensor reading frequency is too low, there may be a delay before the ECM realizes the throttle valve position has changed.

Table H-6: Throttle Valve

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Valve)
493	Conflicting control action	Other	If the cruise control system directly interfaces with the throttle valve (e.g., using a servo), then a conflicting command from the cruise control system could prevent the throttle valve from moving to the position commanded by the ECM.
494	Controlled component failure, change over time	Degradation over time	The throttle valve may degrade over time (e.g., mechanical wear). Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
495	Controlled component failure, change over time	Internal hardware failure	A hardware failure of the throttle valve (e.g., a loose bearing) could prevent the throttle valve from moving to the position commanded by the ECM. Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position.
496	Controlled component failure, change over time	Other	The throttle valve may be incorrectly sized (e.g., the wrong valve). Possible effects of this valve failure may include: - incorrect positioning of the throttle valve. This could cause the throttle valve to allow more or less air into the engine than expected by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Valve)
497	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., throttle icing) could affect the throttle valve. Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - becoming stuck at a constant open throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
498	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could affect the throttle valve (e.g., causing a loose bearing). Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
499	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the throttle valve (e.g., exceeded tolerances). Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Valve)
500	External disturbances	Extreme external temperature or thermal cycling	Extreme external temperature or temperature cycling could affect the throttle valve (e.g., expansion/contraction of the valve). Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
525	External disturbances	Physical interference (e.g., chafing)	Foreign objects in the air intake stream could cause the throttle valve to bind. Possible effects of this failure may include: - loss of function, - incorrect or intermittent commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
738	External disturbances	Magnetic interference	Magnetic interference from the external environment could affect the throttle valve. Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - becoming stuck at a constant open throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Valve)
501	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components could affect the throttle valve. Possible effects of this valve failure may include: - loss of function, - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
502	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the throttle valve. Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
739	Hazardous interaction with other components in the rest of the vehicle	Magnetic interference	Magnetic interference from other vehicle components could affect the throttle valve. Possible effects of this valve failure may include: - loss of function - incorrect or intermittent positioning of the throttle valve, - a delay in throttle valve positioning, or - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.

Table H-7: Brake/Stability Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
14	Controller hardware faulty, change over time	Degradation over time	Degradation of internal subcomponents could affect the Brake/Stability Control Module. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
310	Controller hardware faulty, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) may cause the Brake/Stability Control Module to overheat, affecting its function. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
625	Controller hardware faulty, change over time	Faulty memory storage or retrieval	If individual wheel speeds are stored in memory, an error may occur during storage or retrieval of the wheel speed measurement. Possible effects of this failure include: - loss of function, - incorrect calculation or reporting of the vehicle speed, or - becoming stuck at a value (e.g., reporting a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
626	Controller hardware faulty, change over time	Over temperature due to faulty cooling system	The Brake/Stability Control Module may overheat due to a faulty cooling system, affecting its function. Possible effects of this failure include: - loss of function, - incorrect or intermittent calculation or reporting of the vehicle speed, - a delay in reporting the vehicle speed, or - becoming stuck at a value (e.g., reporting a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
627	Controller hardware faulty, change over time	Faulty signal conditioning or converting (e.g., analog-to-digital converter, signal filters)	The Brake/Stability Control Module may incorrectly process the individual wheel speed measurements (e.g., faulty analog to digital conversion). Possible effects of this failure include: - loss of function, - incorrect calculation of the vehicle speed, or - becoming stuck at a value (e.g., calculating a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
12	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) can affect the Brake/Stability Control Module, causing internal short or open circuits, or other failure of the control module. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
72	External disturbances	EMI or ESD	EMI or ESD from the external environment can affect the Brake/Stability Control Module. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
75	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects and assembly problems could affect the function of the Brake/Stability Control Module. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
194	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could damage internal subcomponents in the Brake/Stability Control Module (e.g., solder breaks). Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - becoming stuck at a value. This could result in an incorrect vehicle speed calculation. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
309	External disturbances	Extreme external temperature or thermal cycling	Extreme external temperature or thermal cycling (e.g., heat or cold) may damage the Brake/Stability Control Module or cause the Brake/Stability Control Module to overheat, affecting its function. Possible effects of this failure may include: - loss of function, - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
621	External disturbances	Single event effects (e.g., cosmic rays, protons)	A Single Event Effect (SEE) caused by high-energy particles could affect the Brake/Stability Control Module (e.g., cause temporary faults in software logic or memory corruption). Possible effects of this failure include: - loss of function, - incorrect or intermittent calculation or reporting of the vehicle speed, - a delay in reporting the vehicle speed, or - becoming stuck at a value (e.g., reporting a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
622	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the Brake/Stability Control Module, causing internal shorting or damage to electrical subcomponents. Possible effects of this failure include: - loss of function, - incorrect or intermittent calculation or reporting of the vehicle speed, - a delay in reporting the vehicle speed, or - becoming stuck at a value (e.g., reporting a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
769	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the function of the Brake/Stability Control Module. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
20	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the Brake/Stability Control Module. Possible effects of this failure may include: - loss of function - incorrect or intermittent calculation of the vehicle speed, - a delay in reporting a calculation, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
74	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components may affect the Brake/Stability Control Module (e.g., A/C condensation), causing internal short or open circuits, or other failure of the control module. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
187	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components may affect the Brake/Stability Control Module, causing internal short or open circuits, or other failures of the control module. This could result in an incorrect vehicle speed calculation. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
623	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could damage internal subcomponents in the Brake/Stability Control Module (e.g., solder breaks). Possible effects of this failure include: - loss of function, - incorrect or intermittent calculation or reporting of the vehicle speed, or - becoming stuck at a value (e.g., reporting a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
624	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components may damage the Brake/Stability Control Module (e.g., damaging electronic subcomponents) or cause the Brake/Stability Control Module to overheat. Possible effects of this failure include: - loss of function, - incorrect or intermittent calculation or reporting of the vehicle speed, - a delay in reporting the vehicle speed, or - becoming stuck at a value (e.g., reporting a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
73	Power supply faulty (high, low, disturbance)	Loss of 12-volt power	If the Brake/Stability Control Module loses 12-volt power, it would be unable to compute and report a vehicle speed measurement. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. The ECM may operate with outdated vehicle speed information or may assume the vehicle speed is zero. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
629	Power supply faulty (high, low, disturbance)	Power supply faulty (high, low, disturbance)	A fluctuation in the 12-volt power supply may damage the Brake/Stability Control Module or cause the Brake/Stability Control Module to erase information stored in volatile memory (e.g., sensor data). Possible effects of this failure include: - loss of function, - incorrect or intermittent calculation or reporting of the vehicle speed, - a delay in reporting the vehicle speed, or - becoming stuck at a value (e.g., the vehicle speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module)
588	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The Brake/Stability Control Module may have software programming errors or faulty logic, which could result in incorrectly determining the individual wheel speed. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the average wheel speed/ vehicle speed calculation - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
628	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	Inadequate control algorithm	The Brake/Stability Control Module may have software programming errors or faulty logic related to determining the vehicle speed. Possible effects of this failure may include: - loss of function, - incorrect or intermittent calculating or reporting of the vehicle speed, - a delay in reporting the vehicle speed, or - becoming stuck at a value (e.g., reporting a constant vehicle speed). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module computes an average vehicle speed from the wheel speed, and provides the average vehicle speed to the ECM. Other vehicle configurations may use other components to compute the vehicle speed.

Table H-8: Brake Pedal Mechanical Assembly

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Mechanical Assembly)
84	Actuator inadequate operation, change over time	Internal hardware failure	Failure of the brake pedal assembly hardware could cause the brake pedal to become dislodged. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position by the pedal position sensor, - a delay in reporting a measurement, or - becoming stuck at a value.
232	Actuator inadequate operation, change over time	Degradation over time	The return spring in the brake pedal assembly may fail or degrade over time. Possible effects of this failure may include: - loss of function - incorrect or intermittent positioning of the brake pedal - becoming stuck at a position, - difficulties actuating the brake pedal.
645	Actuator inadequate operation, change over time	Incorrectly sized actuator	Incorrectly sized return springs in the brake pedal assembly could affect the motion of the brake pedal (e.g., slow return). Possible effects of this actuator failure may include: - a delay in movement of the brake pedal, or - becoming stuck in a position (e.g., pedal does not return).
85	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects in the driver's foot well could affect the motion of the brake pedal. Possible effects of this interference may include: - loss of function - incorrect or intermittent measurement of the brake pedal position by the pedal position sensor, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Mechanical Assembly)
108	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems (e.g., exceeding tolerances) could affect the brake pedal assembly. Possible effects of this failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
641	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment could affect the motion of the brake pedal (e.g., increasing friction). Possible effects of this actuator failure may include: - a delay in movement of the brake pedal, or - becoming stuck in a position (e.g., pedal does not return).
642	External disturbances	Vibration or shock impact	Vibration may affect the brake pedal assembly. Possible effects of this failure include: - intermittent movement of the brake pedal, or - unintended movement of the brake pedal. The ECM may remain in BTO mode without a consistent signal that the brake pedal is released (e.g., if the brake must be pressed for a certain period of time before exiting BTO mode).
86	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference with other vehicle components may interfere with the brake pedal assembly (e.g., floor mats). Possible effects of this interference may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Mechanical Assembly)
643	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration from other vehicle components may affect the brake pedal assembly. Possible effects of this failure include: - intermittent movement of the brake pedal, or - unintended movement of the brake pedal. The ECM may remain in BTO mode without a consistent signal that the brake pedal is released (e.g., if the brake must be pressed for a certain period of time before exiting BTO mode).
644	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components could affect the motion of the brake pedal (e.g., increasing friction). Possible effects of this actuator failure may include: - a delay in movement of the brake pedal, or - becoming stuck in a position (e.g., pedal does not return).

Table H-9: Brake Pedal Position Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor)
77	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems (e.g., improper installation) could affect the brake pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
79	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, dirt, and salt corrosion) could affect the brake pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
80	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the brake pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
182	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could cause the brake pedal position sensor to become misaligned. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor)
313	External disturbances	Extreme external temperature or thermal cycling	An extreme external temperature or thermal cycling (e.g., heat or cold) may cause the brake pedal position sensor to overheat, affecting its function. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
654	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects may affect the brake pedal position sensor. Possible effects of this failure include: - loss of function, - incorrect or intermittent measuring of the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).
655	External disturbances	Organic growth	Organisms may grow in the brake pedal position sensor (e.g., fungi), causing internal shorting or damage to electrical subcomponents. Possible effects of this failure include: - loss of function, - incorrect or intermittent measuring or reporting of the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).
81	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components (e.g., inadequate clearance) could damage the brake pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
82	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the brake pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor)
83	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the brake pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
656	Hazardous interaction with other components in the rest of the vehicle	Magnetic interference	Magnetic interference from other vehicle components could affect the brake pedal position sensor (e.g., a hall-effect type sensor). Possible effects of this failure include: - loss of function, - incorrect or intermittent measuring or reporting of the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).
657	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the brake pedal position sensor. Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measuring or reporting of the brake pedal position, - a delay in reporting the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).
658	Hazardous interaction with other components in the rest of the vehicle	Electrical arcing from neighboring components or exposed terminals	If the brake pedal position sensor is a plunger-type switch, electrical arcing from neighboring components or across exposed terminals could affect the measurement. Possible effects of this failure include: - loss of function, - incorrect measuring of the brake pedal position.
659	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the brake pedal position sensor. Possible effects of this sensor failure include: - intermittent measuring or reporting of the brake pedal position.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor)
78	Power supply faulty (high, low, disturbance)	Loss of 12-volt power	If the brake pedal position sensor loses 12-volt power, it would be unable to issue a signal when the brake pedal has been pressed. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
810	Power supply faulty (high, low, disturbance)	Reference voltage incorrect (e.g., too low, too high)	An increase in the supply voltage could affect the brake pedal position sensor measurement. This could cause the sensor to stop functioning or activate when the brake is not pressed.
76	Sensor inadequate operation, change over time	Degradation over time	The brake pedal position sensor hardware could degrade over time (e.g., carbonization of electrical contacts). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
105	Sensor inadequate operation, change over time	Internal hardware failure	The brake pedal position sensor could have an internal hardware failure (e.g., flawed design, plunger breaks). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
314	Sensor inadequate operation, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) may cause the brake pedal position sensor to overheat, affecting internal subcomponents. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor)
590	Sensor inadequate operation, change over time	Reporting frequency too low	If the brake pedal position sensor reading frequency is too low, there may be a delay before the ECM realizes the brake pedal position has changed.

Table H-10: Engine Speed (rpm) Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
16	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the engine RPM sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
96	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the engine RPM sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
110	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the function of the engine RPM sensor. This could affect engine crankshaft speed measurements. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
192	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could affect the engine RPM sensor (e.g., dislodge the sensor). This could affect engine crankshaft speed measurements. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
320	External disturbances	Extreme external temperature or thermal cycling	An extreme external temperature or temperature cycling (e.g., heat or cold) could damage the engine RPM sensor. This could affect engine crankshaft speed measurements. Possible effects of this sensor failure may include - loss of function, - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
680	External disturbances	Organic growth	Organisms may grow in the engine RPM sensor (e.g., fungi), causing internal shorting or damage to electrical subcomponents. Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measuring or reporting of the engine crankshaft speed, or - becoming stuck at a value (e.g., reporting a constant engine crankshaft speed).
779	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the engine RPM sensor (e.g., dislodge the sensor). This could affect engine crankshaft speed measurements. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
809	External disturbances	Magnetic interference	Magnetic interference from the external environment could affect the function of the engine RPM sensor. This could affect engine crankshaft speed measurements. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
97	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the engine RPM sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
98	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the engine RPM sensor. This could affect the measurement of the engine crankshaft speed. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
104	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	The engine RPM sensor could be affected by excessive heat from other vehicle components (e.g., engine). This could affect the measurement of the engine crankshaft speed. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
185	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components could affect the engine RPM sensor (e.g., dislodge the sensor). This could affect the measurement of the engine crankshaft speed. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
681	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the positioning of the engine RPM sensor. Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measuring or reporting of the engine crankshaft speed, or - becoming stuck at a value (e.g., the engine crankshaft speed measurement does not update).
682	Hazardous interaction with other components in the rest of the vehicle	Magnetic interference	Magnetic interference from other vehicle components could affect the engine RPM sensor. Possible effects of this sensor failure include: - loss of function, - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting the engine crankshaft speed, or - becoming stuck at a value (e.g., a constant crankshaft speed measurement).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
191	Power supply faulty (high, low, disturbance)	Loss of 12-volt power	The engine RPM sensor could lose 12-volt power. Possible effects of this power failure may include: - loss of function - incorrect or intermittent measurement of the engine RPM, - becoming stuck at a value. This would prevent the sensor from reporting the engine speed to the ECM. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
459	Power supply faulty (high, low, disturbance)	Reference voltage incorrect (e.g., too low, too high)	A reduction in the supply voltage to the engine RPM sensor could cause the ECM to think the engine speed was lower than the actual engine speed (i.e., increase in engine load). This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
812	Power supply faulty (high, low, disturbance)	Reference voltage incorrect (e.g., too low, too high)	An increase in the supply voltage to the engine RPM sensor could cause the ECM to think the engine speed was higher than the actual engine speed (i.e., reduction in engine load). This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
15	Sensor inadequate operation, change over time	Internal hardware failure	The engine RPM sensor may have an internal hardware failure. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
184	Sensor inadequate operation, change over time	Degradation over time	The engine RPM sensor may degrade over time. This could affect engine crankshaft speed measurements. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor)
319	Sensor inadequate operation, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) could cause the engine RPM sensor to overheat, affecting its function. This could affect engine crankshaft speed measurement Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
584	Sensor inadequate operation, change over time	Other	The sensor has a high reading error (e.g., magnetic vs. hall effect sensor). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
794	Sensor inadequate operation, change over time	Reporting frequency too low	If the engine RPM sensor reporting frequency is too low, there may be a delay before the ECM realizes the engine RPM has changed.

Table H-11: Engine Temperature Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor)
555	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the engine temperature sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
556	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the engine temperature sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
557	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the function of the engine temperature sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor)
558	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could affect the engine temperature sensor (e.g., dislodge the sensor). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
559	External disturbances	Extreme external temperature or thermal cycling	An extreme external temperature or thermal cycling (e.g., heat or cold) could affect the measurement of the engine temperature sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).
689	External disturbances	Vibration or shock impact	Organisms may grow in the engine temperature sensor (e.g., fungi), causing internal shorting or damage to electrical subcomponents. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor)
781	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the engine temperature sensor (e.g., dislodge the sensor). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
561	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the engine temperature sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
562	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the engine temperature sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor)
563	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	The engine temperature sensor could be affected by excessive temperatures from other vehicle components aside from the engine. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
564	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components could affect the engine temperature sensor (e.g., dislodge the sensor). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
690	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the positioning of the engine temperature sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor)
560	Power supply faulty (high, low, disturbance)	Power supply faulty (high, low, disturbance)	A disturbance in the 12-volt power supply could affect the measurement of the engine temperature sensor. Possible effects of this power failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).
552	Sensor inadequate operation, change over time	Internal hardware failure	The engine temperature sensor may have an internal hardware failure. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
553	Sensor inadequate operation, change over time	Degradation over time	The engine temperature sensor may degrade over time. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor)
554	Sensor inadequate operation, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) could cause the engine temperature sensor to overheat. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the engine temperature, - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
795	Sensor inadequate operation, change over time	Reporting frequency too low	If the engine temperature sensor reporting frequency is too low, there may be a delay before the ECM realizes the engine temperature has changed.

Table H-12: Ignition Key

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Ignition Key)
461	Actuator inadequate operation, change over time	Internal hardware failure	An internal hardware failure in the ignition key assembly (e.g., key breaks contact, excessive switch bouncing) could cause the vehicle to lose 12-volt power including the ECM, or may cause an intermittent connection leading to a disruption in the 12-volt power supply.
698	Actuator inadequate operation, change over time	Degradation over time	The ignition key assembly may degrade over time, causing intermittent or loss of 12-volt power to vehicle systems.
463	External disturbances	Physical interference (e.g., chafing)	Foreign objects may interfere with the ignition key assembly causing intermittent or loss of 12-volt power to vehicle systems (e.g., driver making contact with ignition key).
464	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination of the ignition key assembly (e.g., moisture, dirt) may cause intermittent or loss of 12-volt power to vehicle systems.
466	External disturbances	EMI or ESD	EMI or ESD from the external environment may interfere with the ignition key assembly (e.g., wireless key and start/stop switches) causing intermittent or loss of 12-volt power to vehicle systems.
699	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the ignition key assembly, causing intermittent or loss of 12-volt power to vehicle systems.
700	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could affect the ignition key assembly, causing intermittent or loss of 12-volt power to vehicle systems.
465	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components could affect the ignition key assembly, causing intermittent or loss of 12-volt power to vehicle systems.
467	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components may interfere with the ignition key assembly (e.g., wireless key and start/stop switches) causing intermittent or loss of 12-volt power to vehicle systems.
701	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the ignition key assembly, causing intermittent or loss of 12-volt power to vehicle systems.

Table H-13: Mass Air Flow/Manifold Absolute Pressure Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor)
418	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems (e.g., exceeded tolerance) may cause the MAF/MAP sensor to incorrectly measure the air flow. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
419	External disturbances	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, dirt, salt corrosion) may cause the MAF/MAP sensor to incorrectly measure the air flow. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
420	External disturbances	EMI or ESD	EMI or ESD from the external environment may cause the MAF/MAP sensor to incorrectly measure the air flow. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. That could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor)
421	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could affect the positioning of the MAF/MAP sensor. This could affect the air flow measurement. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
422	External disturbances	Extreme external temperature or thermal cycling	An extreme external temperature or temperature cycling (e.g., heat or cold) may damage the MAF/MAP sensor. Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
702	External disturbances	Organic growth	Organisms may grow in the MAF/MAP sensor (e.g., fungi), resulting in internal shorting or damage of electrical subcomponents. This could affect the air flow measurement. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor)
783	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the positioning of the MAF/MAP sensor. This could affect the air flow measurement. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
24	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the MAF/MAP sensor. Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. The ECM may adjust the throttle position based on an incorrect ambient pressure measurement.
424	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components (e.g., inadequate clearance) could affect the MAF/MAP sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor)
425	Hazardous interaction with other components in the rest of the vehicle	Moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the MAF/MAP sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
703	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the MAF/MAP sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
704	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the positioning of the MAF/MAP sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor)
423	Power supply faulty (high, low, disturbance)	Power supply faulty (high, low, disturbance)	A disruption in the 12-volt power supply to the MAF/MAP sensor could affect the temperature of heated elements (e.g., hot wire MAF). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
22	Sensor inadequate operation, change over time	Internal hardware failure	The MAF/MAP sensor could have an internal hardware failure (e.g., a resistor fails). Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. The ECM may adjust the throttle position based on an incorrect ambient pressure measurement.
416	Sensor inadequate operation, change over time	Degradation over time	The MAF/MAP sensor could degrade over time (e.g., wear of the sensing element). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor)
417	Sensor inadequate operation, change over time	Overheating due to increased resistance in a subcomponent or internal shorting	A hardware failure (e.g., increased resistance in a subcomponent, internal shorting) may cause the MAF/MAP sensor to overheat. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
796	Sensor inadequate operation, change over time	Reporting frequency too low	If the MAF/MAP sensor reporting frequency is too low, there may be a delay before the ECM realizes the mass air flow has changed.

Table H-14: Accelerator Pedal Mechanical Assembly to Accelerator Pedal Position Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Mechanical Assembly to Accelerator Pedal Position Sensor)
600	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects and assembly problems (e.g., exceeded tolerance) could affect the connection between the accelerator pedal and accelerator pedal position sensor. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position - becoming stuck at a value. If the accelerator pedal intermittently activates the pedal position sensor, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
601	External disturbances	Mechanical connections affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could cause the mechanical connection between the accelerator pedal and accelerator pedal position sensor to degrade. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position - becoming stuck at a value. If the accelerator pedal intermittently activates the pedal position sensor, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
607	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could affect the connection between the accelerator pedal and accelerator pedal position sensor (e.g., misalignment of the sensor). Possible effects of this failure include: - loss of function, - incorrect or intermittent measurement of the accelerator pedal position, or - becoming stuck at a value (e.g., reporting a constant accelerator pedal position).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Mechanical Assembly to Accelerator Pedal Position Sensor)
768	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects may affect the connection between the acceleration pedal and the accelerator pedal position sensor (e.g., misalignment of the sensor). Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the accelerator pedal position, or - becoming stuck at a value. If the accelerator pedal intermittently activates the pedal position sensor, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
602	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference from other vehicle components (e.g., insufficient clearance) could cause the accelerator pedal and accelerator pedal position sensor to become misaligned. Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the accelerator pedal position, or - becoming stuck at a value. If the accelerator pedal intermittently activates the pedal position sensor, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
606	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the connection between the accelerator pedal and accelerator pedal position sensor (e.g., misalignment of the sensor). Possible effects of this failure include: - loss of function, - incorrect or intermittent measurement of the accelerator pedal position, or - becoming stuck at a value (e.g., reporting a constant accelerator pedal position).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Mechanical Assembly to Accelerator Pedal Position Sensor)
603	Sensor measurement delay	Other	The connection between the accelerator pedal and accelerator pedal position sensor (e.g., shaft) could have a hardware failure. Possible effects of this hardware failure may include: - loss of function - incorrect or intermittent activation of the accelerator pedal sensor - delayed activation of the sensor (e.g., the shaft slips before engaging the potentiometer). - becoming stuck at a value.
599	Sensor measurement inaccurate	Sensor incorrectly aligned or positioned	If the accelerator pedal and accelerator pedal position sensor are misaligned, the sensor may incorrectly measure the pedal position. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position - becoming stuck at a value.
598	Sensor measurement incorrect or missing	Other	The connection between the accelerator pedal and accelerator pedal position sensor (e.g., shaft) could become damaged or may degrade over time. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position - a delay in reporting a measurement, or - becoming stuck at a value. If the accelerator pedal intermittently activates the pedal position sensor, this may cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Table H-15: Accelerator Pedal Position Sensor to Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
272	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the accelerator pedal position sensor (APPS) or ECM, causing shorting to other pins. Possible effects of this communication failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
274	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection between the accelerator pedal position sensor (APPS) and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
276	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could cause the connection terminals of the accelerator pedal position sensor (APPS) or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include - loss of function, - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
277	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect unused terminals on the wiring harness connecting the accelerator pedal position sensor (APPS) and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
613	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the connection terminals of the accelerator pedal position sensor or ECM, causing shorting between pins. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the accelerator pedal position, or - becoming stuck at a value (i.e., reporting a constant accelerator pedal position). In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
614	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems may affect the connection between the accelerator pedal position sensor and ECM. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the accelerator pedal position, or - becoming stuck at a value (i.e., reporting a constant accelerator pedal position). In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
615	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could cause the connection between the accelerator pedal position sensor (APPS) and ECM to develop an open connection, short to ground, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
273	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the active connection terminals of the accelerator pedal position sensor (APPS) or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
275	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection between the accelerator pedal position sensor (APPS) and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
278	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion or contamination from other vehicle components (e.g., A/C condensation) could affect unused terminals on the wiring harness connecting the accelerator pedal position sensor (APPS) and ECM. The ECM may not receive a pedal position measurement, may receive an incorrect or intermittent pedal position measurement, or the pedal position measurement may not update (i.e., stuck at value). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
279	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other components could cause the connection between the accelerator pedal position sensor (APPS) and ECM to develop an open connection, short to ground, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
616	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the accelerator pedal position sensor or ECM to wear (e.g., fretting) or become loose. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting the accelerator pedal position, or - becoming stuck at a value (i.e., reporting a constant accelerator pedal position). In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
269	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Bus overload or bus error	If the signal from the accelerator pedal position sensor (APPS) to the ECM is transmitted over the communication bus, a communication bus error or overload could affect the accelerator pedal position signal. Possible effects of this communication failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If the signal from the APPS becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
270	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the signal from the accelerator pedal position sensor to the ECM is transmitted over the communication bus, a failure of the message generator, transmitter, or receiver could affect the accelerator pedal position signal. Possible effects of this communication failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If the signal from the APPS becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
331	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Malicious Intruder	If the signal from the accelerator pedal position sensor to the ECM is transmitted over the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics the accelerator pedal position. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
597	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Signal priority too low	If the signal from the accelerator pedal position sensor to the ECM is transmitted over the communication bus, the accelerator pedal position signal priority on the communication bus may not be high enough. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. The ECM may not receive a pedal position measurement or the pedal position measurement may not update (i.e., stuck at value).
268	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the accelerator pedal position sensor and ECM could develop an open circuit, short to ground, short to battery, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
294	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the accelerator pedal position sensor and ECM may degrade over time (e.g., worn insulation). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value. In regard to mode switching: If the signal from the APPS becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
326	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI/ESD, could affect the signal from the accelerator pedal position sensor to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
619	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connector terminals of the accelerator pedal position sensor or ECM may have shorting between pins. Possible effects of this failure include: - loss of function, - incorrect reporting of the accelerator pedal position, or - becoming stuck at a value (e.g., the accelerator pedal position measurement does not update). In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Accelerator Pedal Position Sensor to Engine Control Module)
620	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector contact resistance is too high	The contact resistance in the connector terminals of the accelerator pedal position sensor or ECM may be too high. Possible effects of this failure include: - loss of function, - incorrect reporting of the accelerator pedal position, or - becoming stuck at a value (e.g., the accelerator pedal position measurement does not update). In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.
271	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect pin assignment	An incorrect pin assignment in the connection between the accelerator pedal position sensor and ECM could cause the ECM to have the wrong accelerator pedal position information. Possible effects of this communication failure may include: - loss of function - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
618	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect wiring connection	The connection between the accelerator pedal position sensor and ECM could be incorrectly wired (e.g., reversed wires). Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the accelerator pedal position, or - becoming stuck at a value (e.g., the accelerator pedal position measurement does not update). In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Table H-16: Engine Control Module to Throttle Motor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
516	Controller to actuator signal ineffective, missing, or delayed: Communication bus error	Bus overload or bus error	If the signal from the ECM to the throttle motor is transmitted over the communication bus, a communication bus overload or error could affect the signal from the ECM to the throttle motor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value.
517	Controller to actuator signal ineffective, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the signal from the ECM to the throttle motor is transmitted over the communication bus, a failure of the message generator, transmitter, or receiver could affect transmission of the signal from the ECM to the throttle motor. Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value.
518	Controller to actuator signal ineffective, missing, or delayed: Communication bus error	Malicious Intruder	If the signal from the ECM to the throttle motor is transmitted over the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics the signal from the ECM. Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
731	Controller to actuator signal ineffective, missing, or delayed: Communication bus error	Signal priority too low	If the signal from the ECM to the throttle motor is transmitted over the communication bus, the throttle motor signal priority on the communication bus may not be high enough. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value.
504	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the ECM and throttle motor could develop an open circuit, short to ground, short to battery, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This would cause the throttle motor to receive the incorrect command from the ECM.
732	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI or ESD, could affect the signal from the ECM to the throttle motor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This would cause the throttle motor to receive the incorrect command from the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
733	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector contact resistance is too high	The contact resistance in the connector terminals of the throttle motor or ECM may be too high. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This would cause the throttle motor to receive the incorrect command from the ECM.
734	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connector terminals of the throttle motor or ECM may have shorting between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This would cause the throttle motor to receive the incorrect command from the ECM.
737	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	The connection between the throttle motor and ECM could become intermittent. Possible effects of this connection failure may include: - intermittent commands to the throttle motor. This would cause the throttle motor to receive the incorrect command from the ECM.
505	Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	Incorrect wiring connection	If the connection from the ECM to the throttle motor is incorrectly wired (e.g., wiring is reversed), the throttle motor would not operate in the way the ECM expects. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
506	Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	Incorrect pin assignment	If the connection from the ECM to the throttle motor has an incorrect pin assignment, the throttle motor would not operate in the way the ECM expects. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value.
508	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection from the ECM to the throttle motor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
509	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the ECM or throttle motor, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
510	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect unused connection terminals in the wiring harness connecting the ECM and throttle motor, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
511	External disturbances	Vibration or shock impact	Vibration or shock could cause the connection terminals of the ECM or throttle motor to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent commands to the throttle motor, or - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
735	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the connection terminals of the throttle motor or ECM, causing shorting between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
736	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems may affect the connection between the throttle motor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
778	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the connection from the ECM to the throttle motor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
512	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection from the ECM to the throttle motor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
513	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the active connection terminals of the ECM or throttle motor, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
514	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect unused connection terminals in the wiring harness connecting the ECM and throttle motor, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
515	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components (e.g., wiring is cut) could cause the connection between the ECM and the throttle motor to develop an open circuit, short to ground or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Control Module to Throttle Motor)
729	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the connection between the throttle motor and the ECM (e.g., wiring melts). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.
730	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the throttle motor or ECM to wear (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent commands to the throttle motor, - a delay in a command to the throttle motor, or - becoming stuck at a constant throttle motor value. This could cause the throttle motor to receive the incorrect command from the ECM.

Table H-17: Throttle Motor to Throttle Valve

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor to Throttle Valve)
519	Actuation delivered incorrectly or inadequately: Hardware faulty	Other	The connection from the throttle motor to throttle valve could break (e.g., shaft breaks). Possible effects of this connection failure may include: - loss of function, - incorrect commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
520	Actuation delivered incorrectly or inadequately: Hardware faulty	Other	The connection from the throttle motor to throttle valve could degrade over time (e.g., mechanical wear of the shaft). Possible effects of this connection failure may include: - loss of function, - incorrect commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
521	External disturbances	Mechanical connections affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, dirt) could affect the mechanical connection from the throttle motor to the throttle valve. Possible effects of this connection failure may include: - loss of function, - incorrect commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor to Throttle Valve)
522	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could affect the connection from the throttle motor to the throttle valve. Possible effects of this connection failure may include: - loss of function, - incorrect commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
523	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects and assembly problems could affect the connection from the throttle motor to the throttle valve. Possible effects of this connection failure may include: - loss of function, - incorrect commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
787	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the connection from the throttle motor to the throttle valve. Possible effects of this connection failure may include: - loss of function, - incorrect commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Motor to Throttle Valve)
524	Hazardous interaction with other components in the rest of the vehicle	Mechanical connections affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination other vehicle components (e.g., A/C condensation) could affect the connection from the throttle motor to the throttle valve. Possible effects of this connection failure may include: - loss of function, - incorrect commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.
526	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components could affect the connection from the throttle motor to the throttle valve. Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent commands to the throttle valve, - becoming stuck at a constant throttle valve position. This could prevent the throttle valve from moving to the position commanded by the ECM.

Table H-18: Throttle Position Sensor to Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor to Engine Control Module)
154	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection between the throttle position sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
156	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect unused connection terminals in the wiring harness connecting the throttle position sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
157	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the throttle position sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value. This applies if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. (Note: Since Federal Motor Vehicle Safety Standards (FMVSS) does not specify a BTO design, Original Equipment Manufacturers (OEMs) may use different sensors for developing a BTO strategy.)

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor to Engine Control Module)
158	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could cause the connection terminals of the throttle position sensor or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
722	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the connection terminals of the throttle position sensor or ECM, causing shorting between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
723	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems may affect the connection between the throttle position sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
788	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the connection between the throttle position sensor and the engine control module (e.g., wire chafing). Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor to Engine Control Module)
155	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection between the throttle position sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
159	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle systems could cause an open circuit, short to ground, or short to other wires in the harness to develop in the connection between the throttle position sensor and ECM (e.g., wiring is cut). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
160	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the active connection terminals of the throttle position sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
162	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect unused connection terminals of the wiring harness connecting the throttle position sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor to Engine Control Module)
726	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the throttle position sensor or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
727	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the connection between the throttle position sensor and ECM (e.g., melt the wiring). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
333	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Malicious Intruder	If the signal from the throttle position sensor to the ECM is transmitted over the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics the throttle position. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
409	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Bus overload or bus error	If the signal from the throttle position sensor to the ECM is transmitted over the communication bus, a communication bus error or overload could affect the signal to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor to Engine Control Module)
410	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the signal from the throttle position sensor to the ECM is transmitted over the communication bus, a failure of the message generator, transmitter, or receiver could affect the signal to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
593	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Signal priority too low	If the signal from the throttle position sensor to the ECM is transmitted over the communication bus, the throttle position signal priority on the communication bus may not be high enough. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
407	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the throttle position sensor and ECM could develop an open circuit, short to ground, short to battery, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
408	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI/ESD, could affect the signal from the throttle position sensor to the ECM. The ECM may not receive a measurement, or may receive an incorrect or delayed measurement of the throttle position. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Position Sensor to Engine Control Module)
724	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector contact resistance is too high	The contact resistance in the connector terminals of the throttle position sensor or ECM may be too high. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
725	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connector terminals of the throttle position sensor or ECM may have shorting between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - a delay in reporting a measurement, or - becoming stuck at a value.
802	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	The connection between the throttle position sensor and ECM could become intermittent. Possible effects of this failure include: - intermittent reporting of the throttle position.
201	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect pin assignment	The throttle position sensor or ECM connection terminals could have an incorrect pin assignment. This could cause the ECM to receive an incorrect throttle position signal. Possible effects of this incorrect pin assignment may include: - loss of function - incorrect or intermittent measurement of the throttle position, - becoming stuck at a value.
412	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect wiring connection	The wiring from the throttle position sensor to the ECM could be reversed. Possible effects of this wiring failure may include: - loss of function - incorrect reporting of the throttle position, - becoming stuck reporting a value.

Table H-19: Throttle Valve to Throttle Position Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Valve to Throttle Position Sensor)
531	External disturbances	Mechanical connections affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment may affect the connection between the throttle valve and throttle position sensor (e.g., rust, dirt). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - becoming stuck at a value.
532	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment may affect the connection between the throttle valve and throttle position sensor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - becoming stuck at a value.
741	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects (e.g., exceeded tolerance) or assembly problems could affect the connection between the throttle valve and throttle position sensor (e.g., rust, dirt). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - becoming stuck at a value.
789	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects may affect the connection between the throttle valve and throttle position sensor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - becoming stuck at a value.
533	Hazardous interaction with other components in the rest of the vehicle	Mechanical connections affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) may affect the connection between the throttle valve and throttle position sensor. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Throttle Valve to Throttle Position Sensor)
534	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components may affect the connection between the throttle valve and throttle position sensor (e.g., displace the sensor). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - becoming stuck at a value.
740	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could affect the connection between the throttle valve and throttle position sensor (e.g., misalignment of the sensor). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the throttle position, - becoming stuck at a value.
529	Sensor measurement inaccurate	Sensor incorrectly aligned or positioned	If the TPS is incorrectly mounted on the throttle valve, the measurement of the throttle position may be incorrect or delayed (e.g., the TPS may not move linearly with the throttle valve). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the throttle position, - becoming stuck at a value.
528	Sensor measurement incorrect or missing	Other	If the throttle valve becomes disconnected from the TPS, the TPS would be unable to measure the throttle position.

Table H-20: Brake/Stability Control Module to Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
115	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection from the Brake/Stability Control Module to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
117	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the Brake/Stability Control Module or ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
118	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion), could affect unused connection terminals on the wiring harness connecting the Brake/Stability Control Module and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
119	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could cause the connection terminals of the Brake/Stability Control Module or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
632	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the connection between the Brake/Stability Control Module and ECM. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the vehicle speed, or - becoming stuck at a value (e.g., the vehicle speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
633	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the connection terminals of the Brake/Stability Control Module or ECM, causing shorting between pins. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the vehicle speed, or - becoming stuck at a value (e.g., the vehicle speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
770	External disturbances	Physical interference (e.g., chafing)	Physical interference from foreign objects could affect the connection from the Brake/Stability Control Module to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
116	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection from the Brake/Stability Control Module to the ECM. Possible effects of this communication failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
120	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components could cause an open circuit, short circuit, or short to other wires in the harness to develop in the connection between the Brake/Stability Control Module and ECM (e.g., wiring is cut). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
121	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the active connection terminals of the Brake/Stability Control Module or ECM. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
122	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the unused connection terminals in the wiring harness connecting the Brake/Stability Control Module and ECM, causing shorts between pins. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
803	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the Brake/Stability Control Module or ECM to wear over time (e.g., fretting) or becoming loose. Possible effects of this connection failure may include - loss of function, - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
199	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the signal from the Brake/Stability Control Module to ECM is transmitted over the communication bus, a failure of the message generator, transmitter, or receiver could affect the vehicle speed signal. Possible effects of this communication bus failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
200	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Bus overload or bus error	If the signal from the Brake/Stability Control Module to ECM is transmitted over the communication bus, a bus overload or error could affect the vehicle speed signal. Possible effects of this communication bus failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
329	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Malicious Intruder	If the signal from the Brake/Stability Control Module to the ECM is transmitted over the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics a vehicle speed measurement. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
592	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Signal priority too low	If the signal from the Brake/Stability Control Module to ECM is transmitted over the communication bus, the vehicle speed signal priority on the communication bus may not be high enough. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
215	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the Brake/Stability Control Module and ECM could develop an open circuit, short to ground, short to battery, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to think the vehicle speed is higher than the actual vehicle speed. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
303	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	An intermittent fault could develop in the wiring or connectors between the Brake/Stability Control Module and the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
323	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI/ESD, could affect the signal from the Brake/Stability Control Module to the ECM. This could cause the ECM to receive an incorrect vehicle speed measurement. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the vehicle speed, - a delay in reporting a measurement, or - becoming stuck at a value. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
634	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connection between the Brake/Stability Control Module and ECM could develop shorting between pins. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the vehicle speed, or - becoming stuck at a value (e.g., the vehicle speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
635	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	The connection between the Brake/Stability Control Module and ECM could become intermittent. Possible effects of this failure include: - loss of function, or - intermittent reporting of the vehicle speed. This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
630	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect pin assignment	The Brake/Stability Control Module or ECM may have an incorrect pin assignment. Possible effects of this failure include: - loss of function, - incorrect reporting of the vehicle speed, or - becoming stuck at a value (e.g., the vehicle speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake/Stability Control Module to Engine Control Module)
631	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect wiring connection	The Brake/Stability Control Module or ECM may be incorrectly wired. Possible effects of this failure include: - loss of function, - incorrect reporting of the vehicle speed, or - becoming stuck at a value (e.g., the vehicle speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the average vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Table H-21: Brake Pedal Mechanical Assembly to Brake Pedal Position Sensor

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Mechanical Assembly to Brake Pedal Position Sensor)
127	External disturbances	Physical interference (e.g., chafing)	Foreign objects in the driver's foot well could cause the brake pedal and brake pedal position sensor to become misaligned. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - becoming stuck at a value.
650	External disturbances	Mechanical connections affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., salt corrosion) could cause the connection between the brake pedal and brake pedal position sensor to degrade. Possible effects of this failure include: - loss of function (e.g., the brake pedal does not activate the pedal position sensor), - incorrect or intermittent activation of the pedal position sensor, or - the brake pedal position sensor becoming stuck at a value (e.g., in the "pressed" position).
651	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems (e.g., exceeded tolerance) could cause the brake pedal and brake pedal position sensor to be misaligned. Possible effects of this failure include: - loss of function (e.g., the brake pedal does not activate the pedal position sensor), - incorrect or intermittent activation of the pedal position sensor, or - the brake pedal position sensor becoming stuck at a value (e.g., in the "pressed" position).
652	External disturbances	Vibration or shock impact	Vibration or shock impact could cause the brake pedal and brake pedal position sensor to become misaligned. Possible effects of this failure include: - loss of function (e.g., the brake pedal does not activate the pedal position sensor), - incorrect or intermittent activation of the pedal position sensor, or - the brake pedal position sensor becoming stuck at a value (e.g., in the "pressed" position).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Mechanical Assembly to Brake Pedal Position Sensor)
773	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could cause the brake pedal and brake pedal position sensor to be misaligned. Possible effects of this failure include: - loss of function (e.g., the brake pedal does not activate the pedal position sensor), - incorrect or intermittent activation of the pedal position sensor, or - the brake pedal position sensor becoming stuck at a value (e.g., in the "pressed" position).
126	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference with other vehicle components could cause the brake pedal and brake pedal position sensor to become misaligned. Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the brake pedal position, or - becoming stuck at a value.
653	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the brake pedal and brake pedal position sensor to become misaligned. Possible effects of this failure include: - loss of function (e.g., the brake pedal does not activate the pedal position sensor), - incorrect or intermittent activation of the pedal position sensor, or - the brake pedal position sensor becoming stuck at a value (e.g., in the "pressed" position).
804	Hazardous interaction with other components in the rest of the vehicle	Mechanical connections affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components could cause the mechanical connection between the brake pedal and brake pedal position sensor to degrade. Possible effects of this failure include: - loss of function (e.g., the brake pedal does not activate the pedal position sensor), - incorrect or intermittent activation of the pedal position sensor, or - the brake pedal position sensor becoming stuck at a value (e.g., in the "pressed" position).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Mechanical Assembly to Brake Pedal Position Sensor)
649	Sensor measurement inaccurate	Sensor incorrectly aligned or positioned	The connection between the brake pedal and brake pedal position sensor (e.g., shaft) could become damaged or may degrade over time, resulting in misalignment. Possible effects of this failure include - loss of function (e.g., the brake pedal does not activate the pedal position sensor), - incorrect or intermittent activation of the pedal position sensor, or - the brake pedal position sensor becoming stuck at a value (e.g., in the "pressed" position).
124	Sensor measurement incorrect or missing	Sensor incorrectly aligned or positioned	The brake pedal and brake pedal position sensor could become misaligned (e.g., driver pulls upward on the brake pedal). Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - becoming stuck at a value.

Table H-22: Brake Pedal Position Sensor to Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor to Engine Control Module)
131	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the brake pedal position sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
132	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect unused connection terminals in the wiring harness connecting the brake pedal position sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
133	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection between the brake pedal position sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
163	External disturbances	Vibration or shock impact	Vibration or shock impact could cause the connection terminals of the brake pedal position sensor or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor to Engine Control Module)
662	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the connection between the brake pedal position sensor and ECM. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).
663	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the connection terminals of the brake pedal position sensor or ECM, causing shorting between pins. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).
774	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the connection between the brake pedal position sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
134	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection between the brake pedal position sensor and ECM. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor to Engine Control Module)
135	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle systems could affect the connection between the brake pedal position sensor and ECM (e.g., wiring is cut). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
136	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle systems (e.g., A/C condensation) could affect the active connection terminals of the brake pedal position sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
145	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect unused connection terminals on the wiring harness connecting the brake pedal position sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
664	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the connection from the brake pedal position sensor and ECM (e.g., melt the wiring). Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor to Engine Control Module)
665	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the brake pedal position sensor or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the brake pedal position, or - becoming stuck at a value (e.g., reporting a constant brake pedal position).
197	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Bus overload or bus error	If the signal from the brake pedal position sensor to ECM is transmitted over the communication bus, a bus overload or error could affect the sensor signal . Possible effects of this communication bus failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
198	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the signal from the brake pedal position sensor to ECM is transmitted over the communication bus, a failure of the message generator, transmitter, or receiver could affect the sensor signal. Possible effects of this communication bus failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.
267	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Malicious Intruder	If the signal from the brake pedal position sensor to the ECM is transmitted over the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics the brake pedal position sensor signal. Possible effects of this signal may include: - loss of function - incorrect or intermittent reporting of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor to Engine Control Module)
666	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Signal priority too low	If the signal from the brake pedal position sensor to ECM is transmitted over the communication bus, the brake pedal position signal priority on the communication bus may not be high enough. Possible effects of this failure include: - loss of function, - intermittent reporting of the brake pedal position, - a delay in reporting the brake pedal position, or - becoming stuck at a value (e.g., the brake pedal position measurement does not update).
128	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the brake pedal position sensor and ECM could develop a short to ground, short to battery, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the brake pedal position, - becoming stuck at a value.
129	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	If an intermittent connection failure develops between the brake pedal position sensor and ECM, the signal from the brake pedal position sensor may not persist long enough to engage BTO (i.e., the switching algorithm may require a minimum period of brake activation). Alternatively, an intermittent connection failure may cause the ECM to think the pedal conflict has cleared. The ECM may not re-engage BTO if the pedal application sequence requires the brake pedal to be pressed first.
324	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI/ESD, could affect the signal from the brake pedal position sensor to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the brake pedal position, - a delay in reporting a measurement, or - becoming stuck at a value.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Brake Pedal Position Sensor to Engine Control Module)
660	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connection terminals of the brake pedal position sensor or ECM may develop shorts between pins. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the brake pedal position, or - becoming stuck at a value (e.g., the brake pedal position measurement does not update).
661	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector contact resistance is too high	The contact resistance in the connector terminals of the brake pedal position sensor and ECM may be too high. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the brake pedal position, or - becoming stuck at a value (e.g., the brake pedal position measurement does not update).
130	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect wiring connection	If the connection from the brake pedal position sensor to the ECM is incorrectly wired, the signal to the ECM may be affected. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the brake pedal position, - becoming stuck at a value.
196	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect pin assignment	The brake pedal position sensor or ECM connection terminals could have an incorrect pin assignment. Possible effects of this incorrect pin assignment may include: - loss of function - incorrect or intermittent measurement of the wheel speed, or - becoming stuck at a value. This could cause the ECM to receive an incorrect signal.

Table H-23: Engine Speed (rpm) Sensor to Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
138	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection between the engine RPM sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
140	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the engine RPM sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
141	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect unused connection terminals in the wiring harness connecting the engine RPM sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
142	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could cause the connection terminals of the engine RPM sensor or ECM to wear over time, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
686	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the connection terminals of the engine RPM sensor or ECM, causing shorting between pins. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the engine crankshaft speed, or - becoming stuck at a value (e.g., engine crankshaft speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
687	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the connection between the engine RPM sensor and ECM. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the engine crankshaft speed, or - becoming stuck at a value (e.g., the engine crankshaft speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
780	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the connection between the engine RPM sensor and ECM. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the engine crankshaft speed, or - becoming stuck at a value (e.g., the engine crankshaft speed measurement does not update). This causal factor applies if the vehicle speed is used to determine whether to engage BTO or to determine the appropriate fuel delivery rate when in BTO Mode. This analysis assumes the Brake/Stability Control Module provides the vehicle speed to the ECM; other vehicle configurations may use other components to compute the vehicle speed.
139	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection between the engine RPM sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
143	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle systems could cause an open circuit, short circuit, or short to other wires in the harness to develop in the connection between the engine RPM sensor and ECM (e.g., wiring is cut). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
144	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the active connection terminals of the engine RPM sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
161	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect unused connection terminals of the wiring harness connecting the engine RPM sensor and ECM, causing shorts between pins. This could cause an incorrect engine speed to be reported to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
688	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the engine RPM sensor or ECM to wear (e.g., fretting) or become loose. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the accelerator pedal position, - a delay in reporting the accelerator pedal position, or - becoming stuck at a value (i.e., reporting a constant accelerator pedal position). In regard to mode switching: If the signal from the accelerator pedal position sensor becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode; the ECM may not re-enter BTO mode because the brake pedal will appear to have been pressed first.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
209	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Bus overload or bus error	If the engine RPM sensor is connected to the ECM with the communication bus, a bus overload or error could prevent or incorrectly transmit the engine speed to the ECM. Possible effects of this communication bus failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
210	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the engine RPM sensor is connected to the ECM with the communication bus, a failure of the message generator, transmitter, or receiver could prevent or incorrectly transmit the engine speed to the ECM. Possible effects of this communication bus failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
332	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Malicious Intruder	If the signal from the engine RPM sensor to the ECM is transmitted over the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics the engine speed. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
585	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Signal priority too low	If the engine RPM sensor is connected to the ECM with the communication bus, the engine speed signal priority on the communication bus may not be high enough. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
31	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the engine RPM sensor and the ECM could develop an open circuit, short to ground, short to battery or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to receive an incorrect engine speed measurement. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
327	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI/ESD, could affect the signal from the engine RPM sensor to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine speed, - a delay in reporting a measurement, or - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.
683	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connection terminals of the engine RPM sensor or ECM may have shorting between pins. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the engine crankshaft speed, or - becoming stuck at a value (e.g., the engine crankshaft speed measurement does not update).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
684	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector contact resistance is too high	The contact resistance in the connector terminals of the engine RPM sensor or ECM may be too high. Possible effects of this failure include: - loss of function, - incorrect or intermittent reporting of the engine crankshaft speed, or - becoming stuck at a value (e.g., the engine crankshaft speed measurement does not update).
685	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	The connection between the engine RPM sensor and ECM could become intermittent. Possible effects of this failure include: - intermittent reporting of the engine crankshaft speed.
208	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect pin assignment	If the engine RPM sensor or ECM has an incorrect pin assignment, this could cause the wrong engine speed to be transmitted to the ECM. Possible effects of this incorrect pin assignment may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Speed (rpm) Sensor to Engine Control Module)
799	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect wiring connection	If the connection from the engine RPM sensor to the ECM is incorrectly wired (e.g., wiring is reversed), the ECM may receive the wrong signal from the engine RPM sensor. Possible effects of this incorrect pin assignment may include: - loss of function - incorrect or intermittent measurement of the engine crankshaft speed, - becoming stuck at a value. This affects engine load calculations. This applies to throttle adjustment and may apply to mode switching if the engine speed is used to determine whether to engage BTO or to determine the appropriate throttle position when in BTO Mode.

Table H-24: Engine Temperature Sensor to Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
575	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection between the engine temperature sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
576	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the engine temperature sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
577	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect unused connection terminals in the wiring harness connecting the engine temperature sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
578	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could cause the connection terminals of the engine temperature sensor or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include - loss of function, - incorrect or intermittent reporting of the engine temperature, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
694	External disturbances	Organic growth	Organisms (e.g., fungi) may grow in the connection terminals of the engine temperature sensor or ECM, causing shorting between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
695	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems may affect the connection between the engine temperature sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
782	External disturbances	Physical interference (e.g., chafing)	Physical interference with foreign objects could affect the connection between the engine temperature sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
579	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection between the engine temperature sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
580	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the active connection terminals of the engine temperature sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
581	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect unused connection terminals in the wiring harness connecting the engine temperature sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
582	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components (e.g., wiring is cut) could cause the connection between the engine temperature sensor and ECM to develop an open circuit, short to ground or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
696	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the engine temperature sensor or ECM to wear (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
697	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the connection between the engine temperature sensor and the ECM (e.g., wiring melts). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the incorrect engine temperature to be reported to the ECM.
571	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Bus overload or bus error	If the engine temperature sensor is connected to the ECM with the communication bus, a communication bus overload or error could prevent or incorrectly transmit the engine temperature to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).
572	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the engine temperature sensor is connected to the ECM with the communication bus, a failure of the message generator, transmitter, or receiver could prevent or incorrectly transmit the engine temperature to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
573	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Malicious Intruder	If the engine temperature sensor is connected to the ECM with the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics the engine temperature measurement. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).
596	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Signal priority too low	If the engine temperature sensor is connected to the ECM with the communication bus, the engine temperature signal priority on the communication bus may not be high enough. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).
569	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the engine temperature sensor and the ECM could develop an open circuit, short to ground, short to battery, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
570	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI/ESD, could affect the signal from the engine temperature sensor to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
691	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	The connection between the engine temperature sensor and ECM could become intermittent. Possible effects of this failure include: - intermittent reporting of the engine temperature speed.
692	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector contact resistance is too high	The contact resistance in the connector terminals of the engine temperature sensor or ECM may be too high. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Engine Temperature Sensor to Engine Control Module)
693	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connection terminals of the engine temperature sensor or ECM may have shorting between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - a delay in reporting a measurement, or - becoming stuck at a value. This could affect the engine temperature measurement, causing the ECM to adjust the throttle position (e.g., to compensate for a cold start).
574	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect pin assignment	If the engine temperature sensor or ECM has an incorrect pin assignment, this could cause the wrong engine temperature to be reported to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).
800	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect wiring connection	If the connection between the engine temperature sensor and the ECM is incorrectly wired, this could cause the wrong engine temperature to be reported to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the engine temperature, - becoming stuck at a value. This could cause the ECM to adjust the throttle position (e.g., to compensate for a cold start).

Table H-25: Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
431	External disturbances	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect the active connection terminals of the MAF/MAP sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
432	External disturbances	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from the external environment (e.g., moisture, salt corrosion) could affect unused connection terminals in the wiring harness connecting the MAF/MAP sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
433	External disturbances	EMI or ESD	EMI or ESD from the external environment could affect the connection between the MAF/MAP sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
434	External disturbances	Vibration or shock impact	Vibration or shock impact from the external environment could cause the connection terminals of the MAF/MAP sensor or ECM to wear over time (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent reporting of the air flow, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
705	External disturbances	Organic growth	Organisms may grow in the connection terminals of the MAF/MAP sensor or ECM (e.g., fungi), causing shorting between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
706	External disturbances	Manufacturing defects and assembly problems	Manufacturing defects or assembly problems could affect the connection between the MAF/MAP sensor and the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
784	External disturbances	Physical interference (e.g., chafing)	Physical interference from foreign objects could affect the connection between the MAF/MAP sensor and ECM (e.g., chafed wiring). Possible effects of this connection failure may include: - loss of function, - incorrect or intermittent reporting of the air flow, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
435	Hazardous interaction with other components in the rest of the vehicle	EMI or ESD	EMI or ESD from other vehicle components could affect the connection between the MAF/MAP sensor and ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
436	Hazardous interaction with other components in the rest of the vehicle	Physical interference (e.g., chafing)	Physical interference or chafing from other vehicle components (e.g., abraded wiring) could cause the connection between the MAF/MAP sensor and ECM to develop an open circuit, short to ground, or short to other wires in the harness. Possible effects of this sensor failure may include: - loss of function, - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
437	Hazardous interaction with other components in the rest of the vehicle	Active connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect the active connection terminals of the MAF/MAP sensor or ECM, causing shorting to other pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
438	Hazardous interaction with other components in the rest of the vehicle	Unused connection terminals affected by moisture, corrosion, or contamination	Moisture, corrosion, or contamination from other vehicle components (e.g., A/C condensation) could affect unused connection terminals in the wiring harness connecting the MAF/MAP sensor and ECM, causing shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
707	Hazardous interaction with other components in the rest of the vehicle	Vibration or shock impact	Vibration or shock impact from other vehicle components could cause the connection terminals of the MAF/MAP sensor or the ECM to wear (e.g., fretting) or become loose. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
708	Hazardous interaction with other components in the rest of the vehicle	Excessive heat from other components	Excessive heat from other vehicle components could affect the connection between the MAF/MAP sensor and ECM (e.g., melt the wiring). Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
427	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Bus overload or bus error	If the signal from the MAF/MAP sensor to the ECM is transmitted over the communication bus, a communication bus overload or error could prevent or delay transmission of the air flow measurement to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
428	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Malicious Intruder	If the signal from the MAF/MAP sensor to the ECM is transmitted over the communication bus, a malicious intruder or aftermarket component may write a signal to the communication bus that mimics the air flow measurement. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
443	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure of the message generator, transmitter, or receiver	If the signal from the MAF/MAP sensor to the ECM is transmitted over the communication bus, a failure of the message generator, transmitter, or receiver could prevent or delay transmission of the air flow measurement to the ECM. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
595	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Signal priority too low	If the signal from the MAF/MAP sensor to the ECM is transmitted over the communication bus, the air flow measurement priority on the communication bus may not be high enough. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
36	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is open, short to ground, short to battery, or short to other wires in harness	The connection between the MAF/MAP sensor and ECM could develop an open circuit, short to ground, short to battery, or short to other wires in the harness. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. The ECM may adjust the throttle position based on an incorrect ambient pressure measurement.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
426	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Electrical noise other than EMI or ESD	Electrical noise, in addition to EMI/ESD, could affect the signal from the MAF/MAP sensor to the ECM. Possible effects of this sensor failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
709	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector contact resistance is too high	The contact resistance in the connection terminals of the MAF/MAP sensor or ECM may be too high. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. The ECM may adjust the throttle position based on an incorrect ambient pressure measurement.
710	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connector shorting between neighboring pins	The connection terminals of the MAF/MAP sensor or ECM may develop shorts between pins. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent measurement of the air flow, - a delay in reporting a measurement, or - becoming stuck at a value. The ECM may adjust the throttle position based on an incorrect ambient pressure measurement.

Causal Factor ID Number	Causal Factor Guide Phrase	Causal Factor Subcategory	Causal Factor (Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module)
801	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Connection is intermittent	The connection between the MAF/MAP sensor and ECM could become intermittent. Possible effects of this failure include: - intermittent reporting of the air flow.
429	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect wiring connection	If the connection from the MAF/MAP sensor to the ECM is incorrectly wired, the ECM may receive an incorrect air flow measurement. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.
430	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Incorrect pin assignment	The MAF/MAP sensor or ECM connection terminals could have an incorrect pin assignment. Possible effects of this connection failure may include: - loss of function - incorrect or intermittent reporting of the air flow, - becoming stuck at a value. This could cause the ECM to adjust the throttle position based on the wrong ambient pressure curve.

DOT HS 812 557
July 2018

U.S. Department
of Transportation

National Highway
Traffic Safety
Administration

NHTSA

13637-072418-v1b