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

NHTSA

DOT HS 812 657

August 2019

Functional Safety Assessment Of a Generic Accelerator Control System with Electronic Throttle Control in Hybrid Electric Vehicles with Gasoline Internal Combustion Engines

DISCLAIMER

This publication is distributed by the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation or the National Highway Traffic Safety Administration. The United States Government assumes no liability for its contents or use thereof. If trade names, manufacturers' names, or specific products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Suggested APA Format Citation:

Becker, C., Nasser, A., & Attioui, F. (2019, August). *Functional safety assessment of a generic accelerator control system with electronic throttle control in hybrid electric vehicles with a gasoline internal combustion engine*. (Report No. DOT HS 812 657). Washington, DC: National Highway Traffic Safety Administration.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No.0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	August 2019	

4. TITLE AND SUBTITLE
Functional Safety Assessment of a Generic Accelerator Control System with Electronic Throttle Control in Hybrid Electric Vehicles with a Gasoline Internal Combustion Engine

5. FUNDING NUMBERS
Intra-Agency Agreement
DTNH22-13-V-00114/
DTNH22-15-V-00010
51HS7BA100/51HS7BA200

6. AUTHOR(S)
Christopher Becker, Ahmad Nasser, and Fouad Attioui

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

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-NHTSA-16-05

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
David Freeman
U.S. Department of Transportation
National Highway Traffic Safety Administration
1200 New Jersey Avenue SE.
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
DOT HS 812 657

11. SUPPLEMENTARY NOTES

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

12b. DISTRIBUTION CODE

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 hybrid electric vehicles (HEVs) that combine an electric powertrain subsystem with a gasoline internal combustion engine. Three common HEV architectures are considered, the series HEV, parallel HEV, and series-parallel HEV. 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 derives 8 vehicle-level safety goals and 260 safety requirements (an output of the ISO 26262 and STPA processes). This study uses the results of the analysis to identify potential opportunities to improve the risk assessment approach in the ISO 26262 standard.

14. SUBJECT TERMS
Accelerator control system, electronic throttle control, hybrid electric vehicle, 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
465

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

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

This Report

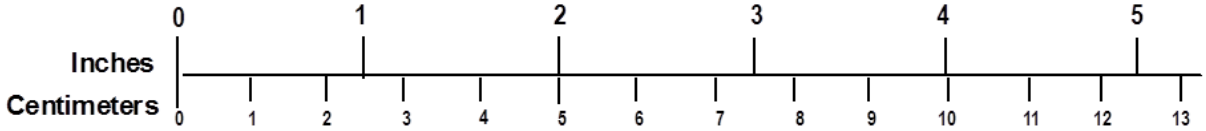
This report describes the research effort to assess the functional safety of accelerator control systems with electronic faults, such as errant electronic throttle control signals, following an industry process standard. This study focuses specifically on errant signals in hybrid electric vehicles (HEVs) that combine an electric powertrain subsystem with a gasoline internal combustion engine. Three common HEV architectures are considered, the series HEV, parallel HEV, and series-parallel HEV. 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 derives 8 vehicle-level safety goals and 260 safety requirements (an output of the ISO 26262 and STPA processes). This study uses the results of the analysis to identify potential opportunities to improve the risk assessment approach in the ISO 26262 standard.

This publication is part of a series of reports that describe NHTSA's initial work in the automotive electronics reliability program. This research specifically supports the first, second, fourth, and fifth goals of NHTSA's electronics reliability research program by gaining understanding on both the functional safety requirements for ACS/ETC systems and how the ISO 26262 industry standard may enhance safety.

METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC	METRIC TO ENGLISH
LENGTH (APPROXIMATE)	**LENGTH** (APPROXIMATE)
1 inch (in) = 2.5 centimeters (cm)	1 millimeter (mm) = 0.04 inch (in)
1 foot (ft) = 30 centimeters (cm)	1 centimeter (cm) = 0.4 inch (in)
1 yard (yd) = 0.9 meter (m)	1 meter (m) = 3.3 feet (ft)
1 mile (mi) = 1.6 kilometers (km)	1 meter (m) = 1.1 yards (yd)
	1 kilometer (km) = 0.6 mile (mi)
AREA (APPROXIMATE)	**AREA** (APPROXIMATE)
1 square inch (sq in, in^2) = 6.5 square centimeters (cm^2)	1 square centimeter (cm^2) = 0.16 square inch (sq in, in^2)
1 square foot (sq ft, ft^2) = 0.09 square meter (m^2)	1 square meter (m^2) = 1.2 square yards (sq yd, yd^2)
1 square yard (sq yd, yd^2) = 0.8 square meter (m^2)	1 square kilometer (km^2) = 0.4 square mile (sq mi, mi^2)
1 square mile (sq mi, mi^2) = 2.6 square kilometers (km^2)	10,000 square meters (m^2) = 1 hectare (ha) = 2.5 acres
1 acre = 0.4 hectare (he) = 4,000 square meters (m^2)	
MASS - WEIGHT (APPROXIMATE)	**MASS - WEIGHT** (APPROXIMATE)
1 ounce (oz) = 28 grams (gm)	1 gram (gm) = 0.036 ounce (oz)
1 pound (lb) = 0.45 kilogram (kg)	1 kilogram (kg) = 2.2 pounds (lb)
1 short ton = 2,000 pounds (lb) = 0.9 tonne (t)	1 tonne (t) = 1,000 kilograms (kg) = 1.1 short tons
VOLUME (APPROXIMATE)	**VOLUME** (APPROXIMATE)
1 teaspoon (tsp) = 5 milliliters (ml)	1 milliliter (ml) = 0.03 fluid ounce (fl oz)
1 tablespoon (tbsp) = 15 milliliters (ml)	1 liter (l) = 2.1 pints (pt)
1 fluid ounce (fl oz) = 30 milliliters (ml)	1 liter (l) = 1.06 quarts (qt)
1 cup (c) = 0.24 liter (l)	1 liter (l) = 0.26 gallon (gal)
1 pint (pt) = 0.47 liter (l)	
1 quart (qt) = 0.96 liter (l)	
1 gallon (gal) = 3.8 liters (l)	
1 cubic foot (cu ft, ft^3) = 0.03 cubic meter (m^3)	1 cubic meter (m^3) = 36 cubic feet (cu ft, ft^3)
1 cubic yard (cu yd, yd^3) = 0.76 cubic meter (m^3)	1 cubic meter (m^3) = 1.3 cubic yards (cu yd, yd^3)
TEMPERATURE (EXACT)	**TEMPERATURE** (EXACT)
[(x-32)(5/9)] °F = y °C	[(9/5) y + 32] °C = x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSION

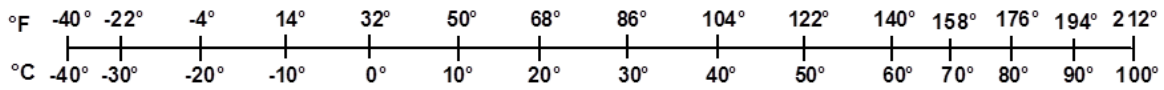


TABLE OF CONTENTS

EXECUTIVE SUMMARY xiii
1 INTRODUCTION 1
1.1 Research Objectives 1
1.2 Report Outline 2
2 ANALYSIS APPROACH 3
2.1 Analysis Steps 5
2.2 Hazard and Safety Analysis Methods 5
2.2.1 Hazard and Operability Study 5
2.2.2 Functional Failure Modes and Effects Analysis 7
2.2.3 Systems-Theoretic Process Analysis 7
3 SYSTEM DEFINITION 11
3.1 System Analysis Scope 11
3.2 Analysis Assumptions 13
3.2.1 Assumptions Applicable to All Three HEV Architectures 13
3.2.2 Series HEV Specific Assumptions 14
3.2.3 Parallel HEV Specific Assumptions 14
3.2.4 Series-Parallel HEV Specific Assumptions 15
3.3 System Block Diagram 15
3.4 System Description 19
3.4.1 Series HEV System Description 19
3.4.2 Parallel HEV System Description 22
3.4.3 Series-Parallel HEV System Description 27
3.4.4 Comparison of Key ACS/ETC Features Across All Three HEV Architectures 30
4 VEHICLE-LEVEL HAZARD ANALYSIS 32
4.1 Vehicle-Level Hazards 32
4.2 Hazard and Operability Study 34
4.2.1 Series HEV HAZOP Study 34
4.2.2 Parallel HEV HAZOP Study 39
4.2.3 Series-Parallel HEV HAZOP Study 42
4.3 Systems-Theoretic Process Analysis: Step 1 47

4.3.1 Series HEV STPA Step 1 Results 47
4.3.2 Parallel HEV STPA Step 1 Results 56
4.3.3 Series-Parallel HEV STPA Step 1 Results 61
5 RISK ASSESSMENT 66
5.1 Automotive Safety Integrity Level Assessment Steps 66
5.1.1 Vehicle Operational Situations 66
5.1.2 Automotive Safety Integrity Level Assessment 67
5.2 Automotive Safety Integrity Level Assignment for Each Hazard 70
6 VEHICLE-LEVEL SAFETY GOALS 72
7 SAFETY ANALYSIS 73
7.1 Functional Failure Modes and Effects Analysis 73
7.1.1 Series HEV Functional FMEA 73
7.1.2 Parallel HEV Functional FMEA 76
7.1.3 Series-Parallel HEV Functional FMEA 77
7.2 Systems-Theoretic Process Analysis: Step 2 79
7.2.1 Series HEV STPA Step 2 Results 80
7.2.2 Parallel HEV STPA Step 2 Results 82
7.2.3 Series-Parallel HEV STPA Step 2 Results 84
8 FUNCTIONAL SAFETY CONCEPT 86
8.1 Safety Strategies 86
8.2 Example Safe States 87
8.3 Example Driver Warning Strategies 89
9 APPLICATION OF THE FUNCTIONAL SAFETY CONCEPT 90
9.1 Example Vehicle-Level Safety Requirements (Safety Goals) 91
9.2 HEV ACS/ETC System and Components Functional Safety Requirements 93
9.2.1 General HEV ACS/ETC System-Level Functional Safety Requirements 95
9.2.2 Accelerator Pedal Assembly Functional Safety Requirements 98
9.2.3 HEV Powertrain Control Module Functional Safety Requirements 99
9.2.4 Electric Powertrain Subsystem Functional Safety Requirements 106
9.2.5 Gasoline ICE Powertrain Subsystem Functional Safety Requirements 110
9.2.6 Power Split Device Functional Safety Requirements 114

9.2.7 Communication Signals Functional Safety Requirements 115
9.2.8 Power Supply Functional Safety Requirements 116
9.2.9 Interfacing Systems Functional Safety Requirements 117
9.3 Additional Safety Requirements beyond the Scope of the ISO 26262 Functional Safety Concept 118
9.3.1 Additional General HEV ACS/ETC System-Level Safety Requirements 119
9.3.2 Accelerator Pedal Assembly Additional Safety Requirements 121
9.3.3 HEV Powertrain Control Module Additional Safety Requirements 121
9.3.4 Electric Powertrain Subsystem Additional Safety Requirements 123
9.3.5 Gasoline ICE Powertrain Subsystem Additional Safety Requirements 124
9.3.6 Power Split Device Additional Safety Requirements 125
9.3.7 Communication Signals Additional Safety Requirements 125
9.3.8 Power Supply Additional Safety Requirements 126
9.3.9 Interfacing Systems Additional Safety Requirements 127
10 OBSERVATIONS 130
10.1 ASIL Dependence on a Feature's Operational Situations 130
10.2 Generation of Operational Situations 130
10.3 Variations in the Automotive Safety Integrity Level Assessment 131
11 POTENTIAL USE OF STUDY RESULTS 132
12 CONCLUSIONS 133

APPENDIX A: STPA Causal Factor Guidewords and Guidewords Subcategories A-1
APPENDIX B: HAZOP Study Results B-1
APPENDIX C: Unsafe Control Action (UCA) Assessment Tables C-1
APPENDIX D: STPA Step 1: UCAs and MAPPing to Hazards D-1
APPENDIX E: Operational Situations E-1
APPENDIX F: ASIL Assessment F-1
APPENDIX G: FMEA Results G-1
APPENDIX H: STPA Step 2: Causal Factors H-1

LIST OF FIGURES

Figure 1. Safety Analysis and Requirements Development Process 4
Figure 2. HAZOP Study Process 6
Figure 3. STPA Process 8
Figure 4. Guidewords for UCAs 9
Figure 5. Block Diagram of a Generic ACS/ETC for a Series Hybrid Electric Vehicle 16
Figure 6. Block Diagram of a Generic ACS/ETC for a Parallel Hybrid Electric Vehicle 17
Figure 7. Block Diagram of a Generic ACS/ETC for a Series-Parallel Hybrid Electric Vehicle 18
Figure 8. HAZOP Block Diagram for the Series HEV ACS/ETC System 34
Figure 9. HAZOP Block Diagram of the Parallel HEV ACS/ETC System 39
Figure 10. HAZOP Block Diagram of the Series-Parallel HEV ACS/ETC System 43
Figure 11. Detailed Control Structure Diagram for the Series HEV ACS/ETC System 48
Figure 12. Detailed Control Structure Diagram for the Parallel HEV ACS/ETC System 57
Figure 13. Detailed Control Structure Diagram for the Series-Parallel HEV ACS/ETC System 62
Figure 14. Traceability in STPA Results 79
Figure 15. Functional Safety Concept Process 86
Figure 16. Commonality of Safety Requirements between HEV ACS/ETC Architecture Types 91

LIST OF TABLES

Table 1. Example Power Assignments for Typical Driving Scenarios in a Parallel HEV 23
Table 2. Example Power Assignments for Typical Driving Scenarios in a Series-Parallel HEV 28
Table 3. Key Differences between the Three HEV ACS/ETC Architectures 31
Table 4. Vehicle-Level Hazards and Definitions 32
Table 5. Allocation of Vehicle-Level Hazards to the Three HEV ACS/ETC Architectures 33
Table 6. Derivation of Malfunctions and Hazards Using the HAZOP Study (Example) 37
Table 7. Number of Identified Malfunctions for Each HAZOP Function in the Series HEV 38
Table 8. Number of Identified Malfunctions for Each HAZOP Function in the Parallel HEV ... 42
Table 9. Number of Identified Malfunctions for Each HAZOP Function in the Series-Parallel HEV 46
Table 10. Series HEV STPA Context Variables for Mode Switching 49
Table 11. Series HEV STPA Context Variables for Commanding Torque (Magnitude) 50
Table 12. Series HEV STPA Context Variables for the Commanding Torque (Direction) 51
Table 13. Series HEV STPA Context Variables for Inverter/Converter Cooling 51
Table 14. Series HEV STPA Context Variables for Discharging the HV Bus 52
Table 15. Series HEV STPA Context Variables for Opening the Contactor 52
Table 16. Series HEV STPA Context Variables for Requesting DC Power 52
Table 17. Series HEV STPA Context Variables for Regulating Current Supply 53
Table 18. UCA Assessment Table (Example) 54
Table 19. Number of Identified UCAs for Each Series HEV STPA Control Action 55

Table 20. Example STPA UCA Statement for Electric Motor Torque Control (Magnitude) 55
Table 21. Example STPA UCA Statement for the Direction of Torque Output Control 56
Table 22. Example STPA UCA Statement for Electric Motor Current Control 56
Table 23. Parallel HEV STPA Context Variables for Commanding the Net Power Output..... 59
Table 24. Parallel HEV STPA Context Variables for Adjusting the Throttle Position..... 60
Table 25. Number of Identified UCAs for Each Parallel HEV STPA Control Action 60
Table 26. Series-Parallel HEV STPA Context Variables for Regulating Current Supply to the Second Electric Motor 65
Table 27. Number of Identified UCAs for Each Series-Parallel HEV STPA Control Action 65
Table 28. Variables and States for Description of Vehicle Operational Situations..... 67
Table 29. Exposure Assessment 68
Table 30. Severity Assessment 68
Table 31. Acceptable Approach to Assess Severity 68
Table 32. Controllability Assessment..... 69
Table 33. ASIL Assessment..... 69
Table 34. Vehicle-Level Hazards and Corresponding ASIL 71
Table 35. Safety Goals with ASIL..... 72
Table 36. Number of Identified Faults by Failure Mode for the Series HEV 73
Table 37. Sample Functional FMEA for Potential Uncontrolled Vehicle Propulsion (H1) (Not Complete)..... 75
Table 38. Number of Identified Faults by Failure Mode for the Parallel HEV 76
Table 39. Number of Identified Faults by Failure Mode for the Series-Parallel HEV..... 77
Table 40. Number of Identified Causal Factors by Causal Factor Category for the Series HEV 80
Table 41. Examples of Causal Factors for a Torque Increase UCA..... 81
Table 42. Examples of Causal Factors for a UCA for Decreasing the Current Supply..... 81
Table 43. Number of Identified Causal Factors by Causal Factor Category for the Parallel HEV 82
Table 44. Examples of Causal Factors for a UCA for Decreasing the Throttle Opening..... 83
Table 45. Number of Identified Causal Factors by Causal Factor Category for the Series-Parallel HEV 84
Table 46. Examples of HEV PCM Safety Requirements 94
Table 47. General HEV ACS/ETC System Level Functional Safety Requirements..... 96
Table 48. Accelerator Pedal Assembly Functional Safety Requirements 99
Table 49. HEV PCM Functional Safety Requirements 100
Table 50. EPS Functional Safety Requirements..... 106
Table 51. Gasoline ICE Powertrain Subsystem Functional Safety Requirements 110
Table 52. PSD Functional Safety Requirements..... 114
Table 53. Communication Signal Functional Safety Requirements..... 116
Table 54. Power Supply Functional Safety Requirements 116
Table 55. Interfacing Systems Functional Safety Requirements..... 117

Table 56. Additional General HEV ACS/ETC Safety Requirements 119
Table 57. Accelerator Pedal Assembly Additional Safety Requirements 121
Table 58. HEV PCM Additional Safety Requirements 122
Table 59. EPS Additional Safety Requirements 123
Table 60. Gasoline ICE Powertrain Subsystem Additional Safety Requirements 124
Table 61. PSD Additional Safety Requirements 125
Table 62. Communication Signal Additional Safety Requirements 125
Table 63. Power Supply Additional Safety Requirements 126
Table 64. Interfacing Systems Additional Safety Requirements 127

LIST OF ACRONYMS

A/D	Analog-to-Digital
AC	Alternating Current
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
CAN	Controller Area Network
CC	Cruise Control
CF	Causal Factor
CPU	Central Processing Unit
DC	Direct Current
DTC	Diagnostic Trouble Code
ECM	Engine Control Module
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPS	Electric Powertrain Subsystem
ESD	Electrostatic Discharge
ETC	Electronic Throttle Control
EV	Electric Vehicle
FMEA	Failure Modes and Effects Analysis
FMVSS	Federal Motor Vehicle Safety Standard
FTTI	Fault Tolerant Time Interval
HAZOP	Hazard and Operability Study
HEGO	Heated Exhaust Gas Oxygen
HEV	Hybrid Electric Vehicle
HV	High Voltage
HVIL	High Voltage Interlock Loop
I/O	Input/Output
IC	Integrated Circuit
ICE	Internal Combustion Engine
IEC	International Electrotechnical Commission

ISO	International Standards Organization
KPH	Kilometers per Hour
M/G	Motor/Generator
MISRA	Motor Industry Software Reliability Association
MPH	Miles Per Hour
NHTSA	National Highway Traffic Safety Administration
PCM	Powertrain Control Module
PSD	Power Split Device
QM	Quality Management
RESS	Rechargeable Energy Storage System
SAE	SAE International
SG	Safety Goal
SOC	State-of-Charge
STPA	Systems Theoretic Process Analysis
TBD	To-Be-Determined
TCS	Traction Control System
TICM	Traction Inverter Control Module
TPS	Throttle Position Sensor
U.S.	United States
UCA	Unsafe Control Action

EXECUTIVE SUMMARY

This report describes a research effort by the Volpe National Transportation Systems Center (Volpe), in conjunction with the National Highway Traffic Safety Administration (NHTSA), to identify example safety requirements[1] related to the failures and countermeasures of the Accelerator Control System (ACS) with electronic faults, such as errant Electronic Throttle Control (ETC) signals. ACS/ETC systems are the subset of ACS architectures where the throttle is controlled electronically, rather than through a mechanical connection to the driver-operated control. Specifically, this report focuses on the identification of example safety requirements for the ACS/ETC systems in hybrid electric vehicles (HEVs) with gasoline internal combustion engines (ICEs).[2] In ACS the throttle for EVs is defined as the electric power delivery to the traction motor.

This report considers three HEV architectures:

- The *series HEV* operates similar to an electric vehicle (EV) and may also be referred to as a range-extended EV. An electric motor is the sole source of propulsion for the drivetrain. The gasoline ICE supplies mechanical energy to a generator, which in turn supplies electrical power to the Rechargeable Energy Storage System (RESS). Since the gasoline ICE does not directly contribute to the vehicle's propulsion, it is not considered part of the ACS/ETC for this project.
- The *parallel HEV* uses a mechanical coupling to combine the power output from the gasoline ICE and an electric motor. The net power output from the mechanical coupling provides propulsion to the drivetrain. The parallel HEV contains a single electric motor, which can switch between supplying propulsion and generating electrical power to recharge the battery. The driver-operated control regulates the net power output from the mechanical coupling, while the ACS/ETC determines the optimal split between the electric motor and gasoline ICE.
- The *series-parallel HEV* uses a power split device to combine the power output from the gasoline ICE and two electric motors. The net power output from the power split device provides propulsion to the drivetrain. In the series-parallel HEV, the electric motors may either supply propulsion or generate electrical power. The driver-operated control regulates the net power output from the power split device, while the ACS/ETC determines the optimal split between the electric motors and gasoline ICE.

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

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

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 then follows the International Organization for Standardization (ISO) 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 ASIL levels, 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 ASIL levels that effectively mitigate the underlying safety risks.

This research follows the Concept Phase process (Part 3) in ISO 26262 [2] to derive a list of potential safety requirements. Specifically, this research:

1. Defines the scope and functions of a generic series HEV ACS/ETC, parallel HEV ACS/ETC, and series-parallel HEV ACS/ETC. Each generic system is represented in block diagrams.

2. Performs a vehicle-level hazard analysis using both the Hazard and Operability (HAZOP) study and the Systems Theoretic Process Analysis (STPA) method. By integrating the hazards identified in both the HAZOP study and STPA, the process identifies eight vehicle-level hazards (Table ES-1).
    a. The following is a breakdown of the HAZOP study results by HEV architecture:
        - Series HEV: 139 malfunctions from analysis of the 20 ACS/ETC functions (see Section 4.2.1.3, Table 7 for details.);
        - Parallel HEV: 224 malfunctions from analysis of the 31 ACS/ETC functions (see Section 4.2.2.3, Table 8 for details.); and
        - Series-Parallel HEV: 252 malfunctions from analysis of the 35 ACS/ETC functions (see Section 4.2.3.3, Table 9 for details).
    b. The following is a breakdown of the STPA results by HEV architecture:
        - Series HEV: 95 unsafe control actions (UCAs) from analysis of 13 ACS/ETC control actions (see Section 4.3.1.4, Table 19 for details);
        - Parallel HEV: 123 UCAs from analysis of 17 ACS/ETC control actions (see Section 4.3.2.4, Table 25 for details); and
        - Series-Parallel HEV: 140 UCAs from analysis of 19 ACS/ETC control actions (see Section 4.3.3.4, Table 27 for details).

3. Applies the ASIL assessment[3] approach in the ISO 26262 standard to evaluate the risks associated with each of the identified hazards. In total, 69 operational situations were developed to assess the seven vehicle-level hazards common to all three HEV ACS/ETC architectures. In addition, eight operational situations were developed to assess an eighth vehicle-level hazard, which is common to the parallel HEV and series-parallel HEV ACS/ETC architectures.

   Following the practice in the ISO 26262 process, the most severe ASIL is chosen for each vehicle-level hazard. Table ES-1 summarizes the outcome of the ASIL assessment. Table ES-1 also indicates which of the potential vehicle level hazards is associated with each of the three HEV architectures.

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

	Hazards	**ASIL**	**S HEV**	**P HEV**	**S-P HEV**
H1	Potential uncontrolled vehicle propulsion	D	●	●	●
H1a	Potential uncontrolled vehicle propulsion when the vehicle speed is zero	B[i]	●	●	●
H2	Potential insufficient vehicle propulsion	C[ii]	●	●	●
H3	Potential vehicle movement in an unintended direction	C	●	●	●
H4	Potential propulsion power reduction/loss or vehicle stalling	D	●	●	●
H5	Potential insufficient vehicle deceleration	C[ii]	●	●	●
H6	Potentially allowing driver's command to override active safety systems[iv]	D[iii]	●	●	●
H7	Potential electric shock	B[v]	●	●	●
H8	Potential RESS thermal event[vi]	C		●	●

i. For certain control system features that only operate when the 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 feature 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 assessment for this hazard varied among safety analysts in the absence of objective data. This research finds that objective data are not readily available for the assessment of the three dimensions used to determine the ASIL--severity, exposure, and controllability.

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

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

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

vi. This study only considers the potential for this hazard to result from malfunctions in the ACS/ETC system.

[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.

4. Performs a safety analysis using both the Functional Failure Modes and Effects Analysis (FMEA) and the STPA method.
   a. The following is a breakdown of the Functional FMEA results by HEV architecture:
      - Series HEV: 30 failure modes and 90 potential causes (see Section 7.1.1, Table 36 for details);
      - Parallel HEV: 44 failure modes and 129 potential causes (see Section 7.1.2, Table 38 for details); and
      - Series-parallel HEV: 47 failure modes and 133 potential causes (see Section 7.1.3, Table 39 for details).
   b. The following is a breakdown of the STPA results by HEV architecture:
      - Series HEV: 1,104 causal factors that may lead to the 95 UCAs (see Section 7.2.1, Table 40 for details);
      - Parallel HEV: 1,635 causal factors that may lead to the 123 UCAs (see Section 7.2.2, Table 43 for details); and
      - Series-parallel HEV: 1,785 causal factors that may lead to the 140 UCAs (see Section 7.2.3, Table 45 for details).

5. Derives 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. The functional safety requirements are derived by following the Concept Phase in the ISO 26262 standard. Examples of additional safety requirements are also derived by following additional safety strategies, such as those outlined in the military standard MIL-STD-882E [3]. These requirements are out of the scope of the Functional Safety Concept phase in ISO 26262 (Part 3 of the ISO 26262 standard). 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 result in derivation of similar requirements. The study derived:
   a. 171 example functional safety requirements.
   b. 89 examples of additional safety requirements.

   Of the 260 example safety requirements derived in this study, 194 safety requirements are common to all three HEV ACS/ETC architectures. The remaining 66 safety requirements only apply to one or two HEV architectures. Table ES-2 provides a breakdown of the example functional safety requirements and 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	2
Hybrid Electric Vehicle Powertrain Control Module (HEV PCM)	55	24
Electric Powertrain Subsystem (EPS)	39	9
Gasoline ICE Subsystem	33	7
Power Split Device (PSD)	9	1
Communication Signals	5	4
Power Supply (Low and High Voltage)	6	2
Interfacing Systems	5	22

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 HEV ACS/ETC systems.
- 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 (NHTSA), the Volpe National Transportation Systems Center (Volpe) 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 (ACS) with electronic faults, such as errant Electronic Throttle Control (ETC) signals. This project focuses on the ACS/ETC, which is the subset of ACS architectures where the throttle 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 the International organization for Standardization (ISO) 26262 Concept Phase (Part 3, [2]) and other system safety standards, such as MIL-STD-882E [3].

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

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

This report covers the study of the three HEV ACS/ETC architectures with gasoline ICEs in light motor vehicles (i.e., passenger cars, vans, minivans, sport utility vehicles, and pickup trucks with a gross vehicle weight rating of 10,000 pounds or less). This report documents the approach and the findings of the analysis.

[4] All requirements presented in this section are not actual compliance requirements currently in 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 generic ACS/ETC systems for each of the three HEV architectures. It also defines the analysis scope and assumptions used in this study.
- Section Four: details the vehicle-level hazard analysis approaches and results.
- Section Five: documents the risk assessment on the identified vehicle-level hazards.
- Section Six: summarizes the vehicle-level safety goals as the result of the hazard analysis and risk assessment.
- Section Seven: details the safety analysis that supports the functional safety concept and the safety requirements.
- Section Eight: describes the functional safety concept.
- Section Nine: lists the safety requirements.
- Section Ten: discusses observations on the application of the ISO 26262 standard.
- Section Eleven: considers potential uses of the results of this study.

Sections two, ten, and eleven of this report are essentially unchanged from a previous report published as part of this project entitled *Functional Safety Assessment of a Generic Accelerator Control System with Electronic Throttle Control in Gasoline Internal Combustion Engine Vehicles* (Volpe Report DOT-VNTSC-NHTSA-15-06). These sections are reproduced here so that this report can serve as a stand-alone document.

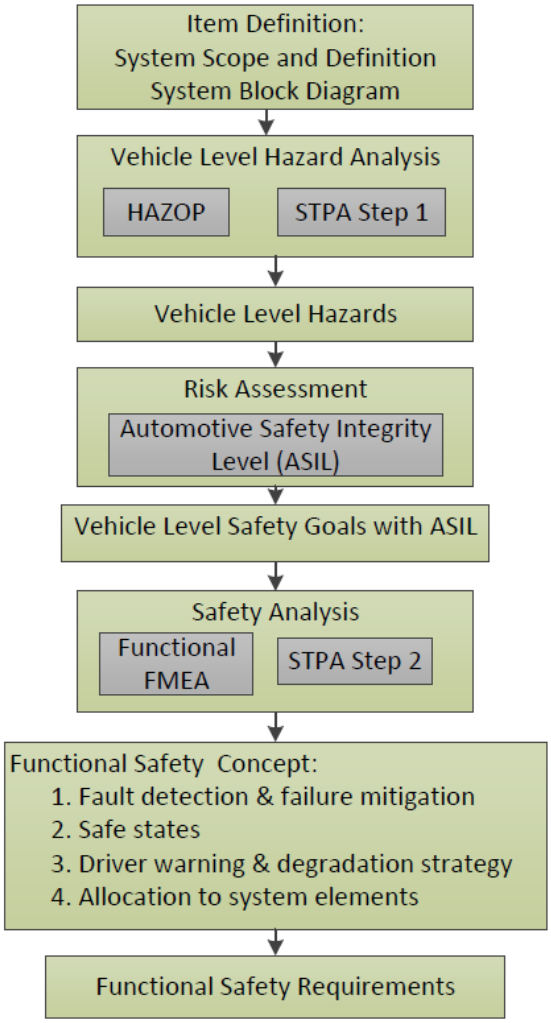
2 ANALYSIS APPROACH

The primary purpose of this work is to study and analyze the potential hazards that could result from cases of electrical or electronic failures impacting the functions of vehicular control systems. The study follows the ISO 26262 process to identify the integrity requirements of these functions at the concept level, independent of implementation variations. ISO 26262 is a functional safety standard adapted from the International Electrotechnical Commission (IEC) Standard 61508, and is intended for application to electrical and electronic systems in motor vehicles (Introduction in Part 1 of ISO 26262 [2]). 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 (ASIL) of the item under consideration. While this study does not go into implementation strategies to achieve these ASIL levels, 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 ASIL levels 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 [2]. The process shown in Figure 1 was developed in part based on learnings from applying Part 3 of the ISO 26262 standard in a previous study.[5]

[5] *Safety Management of Automotive Rechargeable Energy Storage Systems*, Volpe report number DOT-VNTSC-NHTSA-15-01.



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

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

FMEA: Failure 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 analysts in the rest of the process.
2. Carry out the hazard analysis using both the Hazard and Operability (HAZOP) study [4] and the Systems-Theoretic Process Analysis (STPA) method [5]. The output of the hazard analysis is a list of vehicle-level hazards.
3. Apply the ISO 26262 risk assessment approach to the identified vehicle-level hazards, and assign an ASIL to each hazard as defined in ISO 26262.
4. Generate vehicle-level safety goals, which are vehicle-level safety requirements based on the identified vehicle-level hazards. The ASIL associated with each hazard is also transferred directly to the vehicle-level safety goal.
5. Perform safety analyses on the relevant system components and interactions as defined in the first step of this process. This project applies both a Functional Failure Modes and Effects Analysis (FMEA) [6] and STPA in the safety analysis.
6. Develop a functional safety concept and functional safety requirements for the three HEV ACS/ETC architectures at the system and component levels by following the ISO 26262 process. The functional safety concept and safety requirements are based on results from the hazard and safety analyses, ISO 26262 guidelines, and industry practice experiences.

2.2 Hazard and Safety Analysis Methods

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

2.2.1 Hazard and Operability Study

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

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

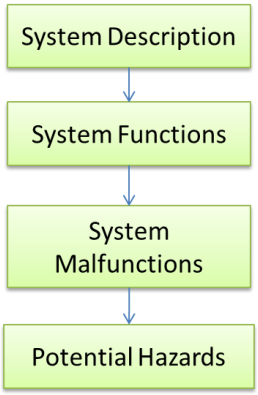


Figure 2. HAZOP Study Process

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

1. Define the system of study and the scope of the analysis. Draw a block diagram to illustrate the system components, system boundary, and interfaces. This step is accomplished in the first step of the overall project (Figure 1).
2. List all of the functions that the system is designed to perform. This step is also accomplished in the first step of the overall project (Figure 1).
3. Apply a set of guidewords to each of the identified functions to describe the various ways in which the function may deviate from its design intent. IEC 61882[8] lists 11 suggested guidewords, but notes that the guidewords can be tailored to the particular system being analyzed [4]. The HAZOP study implemented in this project uses the following seven malfunction guidewords:
    - Loss of function
    - More than intended
    - Less than intended
    - Intermittent
    - Incorrect direction
    - Not requested
    - Locked function
4. Assess the effect of these functional deviations at the vehicle level. If a deviation from an intended function may result in a vehicle-level hazard, the hazard is then documented.

[8] IEC 61882:2001, *Hazard and operability studies (HAZOP studies) - Application guide*, provides a guide for HAZOP studies of systems 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 the safety analysis to identify failure modes at the function level that could potentially lead to the vehicle-level hazards. The failure modes and potential faults identified by the Functional FMEA are used to derive the safety requirements.

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

1. List each function of the item on a FMEA worksheet.
2. Identify potential failure modes for each item and item function.
3. Describe potential effects of each specific failure mode and assign a severity to each effect.
4. Identify potential failure causes or mechanisms.
5. Assign a likelihood of occurrence to each failure cause or mechanism.
6. Identify current design controls that detect or prevent the cause, mechanism, or mode of the failure.
7. Assign a likelihood of failure detection to the design control.

This study applies the first four steps listed above for the Functional FMEA. Since this study is performed during the Concept Phase of ISO 26262, the analysis is not based on a specific design and does not assume controls or mitigation measures are present; there are not enough data to support Steps 5 through 7. The completed Functional FMEA worksheet is intended to be a living document that is continually updated throughout the development process.

2.2.3 Systems-Theoretic Process Analysis

STPA is a top-down systems engineering approach to system safety [5]. In STPA, the system is modelled as a dynamic control problem, where proper controls and communications in the system ensure the desired outcome for emergent properties, such as safety. In the STPA framework, a system will not enter a hazardous state unless an unsafe control action (UCA) 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.

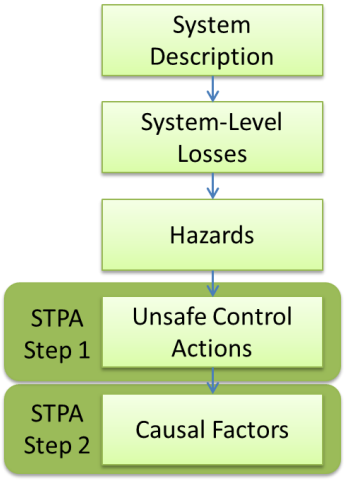


Figure 3. STPA Process

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 (controllers, sensors, actuators, controlled processes, and communications links). This control structure is a generic representation of the functions for a typical system.
    b. Identify the system boundary and interfaces with other vehicle systems and the external environment.

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

2. Define the losses at the system level that should be mitigated. STPA defines system-level losses as undesired and unplanned events that result in the loss of human life or injury, property damage, environmental pollution, etc. [5]. For this project, the potential losses include the occurrence of a vehicle crash, electrocution, and a battery fire/explosion.
3. Identify a preliminary list of vehicle-level hazards. STPA defines a hazard as a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a system-level loss [5]. Initially, based on engineering experience and a literature search, a preliminary hazard list is generated. This list is further refined through iterations in STPA Steps 1 and 2 — UCA and causal factor (CF) identification.
4. **STPA Step 1**: Identify potential UCAs issued by each of the system controllers that could lead to vehicle-level hazards. Four sub-steps are involved:

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

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

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

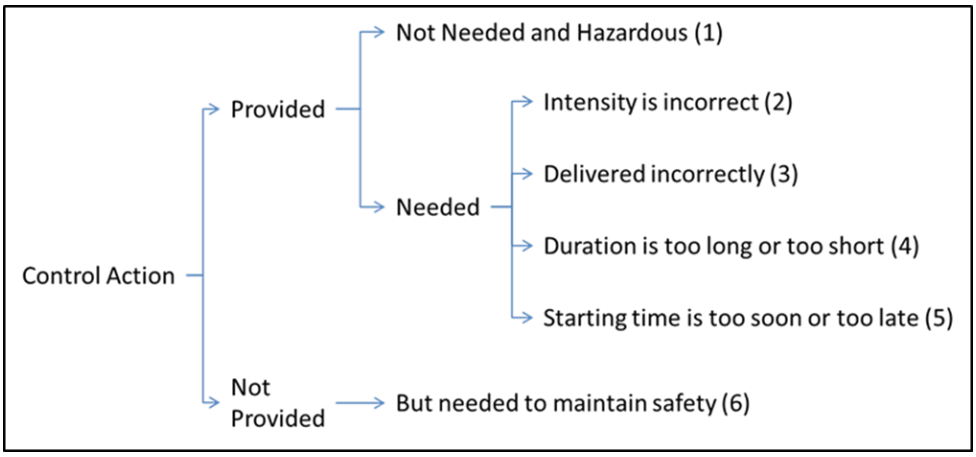


Figure 4. Guidewords for UCAs

For each control action, assess each of the six guidewords against each of the context variable combinations to determine if it could lead to one or more of the vehicle-level hazards. If new hazards are identified, add these hazards to the vehicle-level hazard list initiated in the previous step.

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

[9] The context variables describe the context in which the control commands act in. For example, the control command "enter brake-throttle override mode" may operate in the context of the "driver presses both the 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 interaction in the control structure representation of the system is analyzed to determine if the component or the interaction may contribute to one of the UCAs identified in STPA Step 1. STPA literature provides 17 guidewords to assist the analyst in identifying CFs [5]. This project used an expanded list of 26 guidewords for identifying CFs. Appendix A provides the list of CF guidewords and detailed causes under each guideword that are used in this project.

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

3 SYSTEM DEFINITION

3.1 System Analysis Scope

In ACS:

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

Furthermore, the components and connections in the ACS mean:

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

In addition, this analysis also considers incoming torque requests from other vehicle systems, such as cruise control (CC) or the traction control system (TCS). However, this analysis assumes that these other vehicle systems correctly issue torque requests to the ACS/ETC; failures in other vehicle systems that could result in incorrect torque requests are out of scope for this study.

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

1. All components leading from the driver-operated control to the HEV powertrain control module (PCM), including the following:
   - Accelerator pedal (AP)
   - Accelerator pedal position sensor (APPS)
   - HEV PCM
2. For all three HEV architectures, all components leading from the HEV PCM to the high voltage (HV) power supply connection to the electric motor, including the following:
   - Traction inverter control module (TICM)
   - Gate drive board
   - Inverter/converter (also known as the power stage)
   - Phase/current sensor
   - Motor position and speed sensor
   - Inverter temperature sensor
3. For the series-parallel HEV architecture, all additional sensors associated with operation of the second electric motor[10], including the following:
   - Phase/current sensor
   - Motor position and speed sensor

[10] This analysis assumes that the hardware required to drive the second electric motor is shared with the first electric motor, including the TICM, gate drive board, and inverter/converter.

4. For the parallel and series-parallel HEVs, all components leading from the HEV PCM to the air throttling device on the engine, including the following:
    - Engine control module (ECM)/throttle actuator controller
    - Throttle motor
    - Throttle valve
    - Throttle position sensor (TPS)
5. For the parallel and series-parallel HEVs, all components that combine the engine and electric motor power output, including the following:
    - Mechanical coupling (for the parallel HEV)
    - Power split device (PSD) (for the series-parallel HEV)
6. All connections between the components listed above, including:
    - Wired connections
    - Communication over the vehicle bus (e.g., Controller Area Network (CAN))
7. Brake Throttle Override (BTO) function
8. Incoming torque requests from other vehicle systems
9. Interfaces with the Rechargeable Energy Storage System (RESS), including:
    - HV power supply to the inverter/converter
    - High voltage interlock loop (HVIL) information
    - Requests to discharge the HV bus
10. Interfaces with the vehicle cooling system
11. Interfaces with the occupant restraint system to identify crash events
12. Interfacing sensors, including:
    - Vehicle speed data
    - Brake pedal position sensor (BPPS)
    - Vehicle direction data (forward or reverse gear)
    - Engine sensors

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

- Torque generation by the electric motor(s) and engine, and downstream torque transmission (e.g., reduction gears)
- Hazards not directly caused by malfunctioning behavior of the electronic control system, such as fire hazards
- Brake system malfunctions that may lead to acceleration- or deceleration-related hazards, including regenerative braking malfunctions
- Malfunctions in other vehicle systems leading to incorrect torque requests
- Malfunctions in the HV system, including the RESS
- Malfunctions in fuel delivery or engine combustion
- Notifications from the ACS/ETC to the driver, such as malfunction indicator lights
- Driver errors, such as incorrect pedal application or gear selection

- Failures due to improper maintenance over the lifetime of the vehicle (e.g., incorrect parts, incorrect assembly, and failure to conduct scheduled inspections)
- Multiple point failures in the ACS/ETC system or interfacing systems

3.2 Analysis Assumptions

In addition to the system scope described in Section 3.1, this analysis includes several assumptions regarding the operation of the HEV 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.

3.2.1 Assumptions Applicable to All Three HEV Architectures

- The vehicle speed is primarily provided to the HEV PCM by a dedicated sensor in the drivetrain, with secondary sources of speed provided by the brake/stability[11] control module. Some system architectures may obtain the vehicle speed from other components.
  - *Requirements related to vehicle speed would apply to whichever component is responsible for providing this information to the HEV PCM.*
- In order to exit BTO mode and resume acceleration, the driver needs to not only remove the pedal conflict, but also explicitly increase the AP angle. This assumption is based on a brake override process flow diagram published by Toyota [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 unintentionally press the pedals. It also does not examine other sources of unintentional pedal interference or entrapment by objects inside the vehicle.
  - *Requirements related to other types of driver-operated controls for acceleration and braking may require additional analysis. Additional analysis is also needed to understand why the driver may incorrectly or non-intuitively apply the AP or the BP.*
- Cooling for the inverter/converter is provided by a separate vehicle cooling system that is not part of the HEV ACS/ETC. This analysis assumes that the HEV ACS/ETC requests cooling from the cooling system based on the inverter/converter temperature. Some system designs may have other cooling strategies, such as permanent cooling (e.g., immersion).
  - *The requirements related to the cooling system identified in this study would apply to architectures where the inverter/converter has a dedicated cooling system. However, additional analysis may be required to identify requirements related to other types of cooling strategies.*

- The RESS is responsible for monitoring the HV system and disconnecting the HV system in the event of a failure. The HEV ACS/ETC is responsible for discharging the HV bus when requested by the RESS.
    - *Requirements related to the incoming request to discharge the bus apply to whichever system issues this request to the HEV ACS/ETC. If discharging the HV bus is not performed through the HEV ACS/ETC, then these requirements would not apply.*
- The HEV PCM is responsible for opening the contactor when the vehicle is in a crash or when the HVIL is violated. In other designs, the contactor may be controlled through the RESS or another vehicle system.
    - *If the system design does not use the HEV PCM to open the HV contactor in the event of a crash or HVIL violation, requirements related to opening the contactor would not apply.*
- The position and speed for the electric motor(s) are provided to the TICM, which communicates the health of the electric motor(s) to the HEV PCM. Some system architectures may have relevant motor data provided directly to the HEV PCM.
    - *Requirements related to the position, speed, and other critical parameters for assessing the health of the motor(s) would apply regardless of whether this information is provided to the TICM or HEV PCM. Similarly, requirements related to the communication of this data can be readily adapted to other system architectures.*
- Safety strategies, such as redundant sensors, are not considered in the hazard analysis or safety analysis stages.
    - *Once specific design strategies have been adopted, additional hazard and safety analyses should be performed.*

3.2.2 Series HEV Specific Assumptions

- The series HEV powertrain operates a single electric motor which is used to provide torque to the drivetrain.
    - *Additional analysis may be required for architectures with multiple electric motors (e.g., wheel hub motors) to ensure coordination and proper supply of HV power to each motor.*
- Operation of the gasoline ICE is controlled by the RESS in order to maintain the battery state-of-charge.
    - *Additional analysis is required to assess how failures in the gasoline ICE system may affect the availability of HV power. This analysis only considers that HV power may not be supplied to the ACS/ETC, regardless of whether the loss of HV power results from a failure of the gasoline ICE system or the RESS.*

3.2.3 Parallel HEV Specific Assumptions

- The HEV PCM operates clutches in the mechanical coupling to connect the gasoline ICE and/or electric motor to the drivetrain.

- *This is a conservative assumption that allows consideration of incorrect HEV PCM control of the coupling. In system designs where the mechanical coupling only has one configuration, the requirements related to controlling the mechanical coupling would not apply.*

3.2.4 Series-Parallel HEV Specific Assumptions

- The second electric motor (called a generator in some configurations) may also supply propulsion power under certain circumstances.
  - *This is a conservative assumption that allows consideration of the HEV PCM controlling both electric motors as propulsion sources. In designs where one electric motor is a dedicated generator and does not supply propulsion, requirements related to the generator supplying propulsion would not apply.*
- The PSD may allow for multiple configurations, which are controlled by the HEV PCM.
  - *Some PSDs may only have one configuration, while "compound-split" PSDs may have multiple configurations. In designs where the PSD only has one configuration, the HEV PCM does not control the PSD and requirements relating to adjusting the PSD configuration would not apply.*

3.3 System Block Diagram

The HEVs include two types of powertrain subsystems, an electric powertrain subsystem (EPS) and a gasoline ICE powertrain subsystem. As with the EV, the EPS converts electrical energy supplied by the HV system to mechanical energy, which provides propulsion for the vehicle. The gasoline ICE converts chemical energy to mechanical energy, which is then converted to electrical energy to power the electric motor or recharge the HV battery. In the parallel and series-parallel architectures, the mechanical energy produced by the gasoline ICE may also be used directly to provide propulsion for the vehicle. Therefore in these architectures, the gasoline ICE subsystem is considered as part of the ACS/ETC.

Figure 5 shows a block diagram representation of the series HEV ACS/ETC system considered in this study. The ACS/ETC components and interfaces for the series HEV are essentially identical to the EV. The gasoline ICE is considered an interfacing system controlled by the RESS, and is only used to generate electrical energy.

Figure 6 shows a block diagram representation of the parallel HEV ACS/ETC system considered in this study. The ACS/ETC includes both the EPS components as well as components that regulate air flow to the gasoline ICE. The gasoline ICE subsystem is controlled by the HEV PCM to meet the power requested by the driver.

Figure 7 shows a block diagram representation of the series-parallel HEV ACS/ETC system considered in this study. As with the parallel HEV, the ACS/ETC includes both the EPS and gasoline ICE subsystem components. However, the EPS also provides current to a second electric motor, which may either operate as a generator or supply propulsion to the drivetrain.

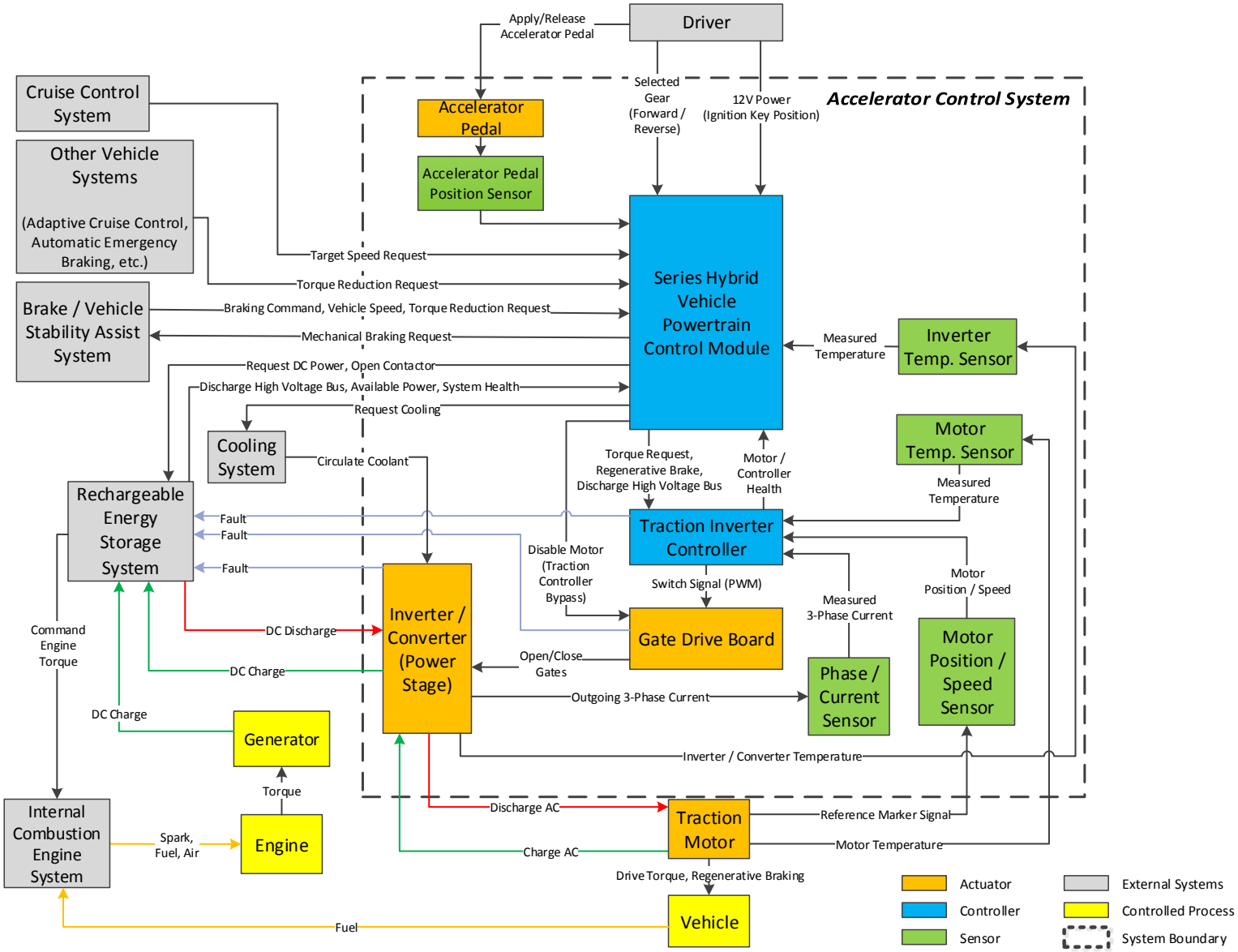


Figure 5. Block Diagram of a Generic ACS/ETC for a Series Hybrid Electric Vehicle

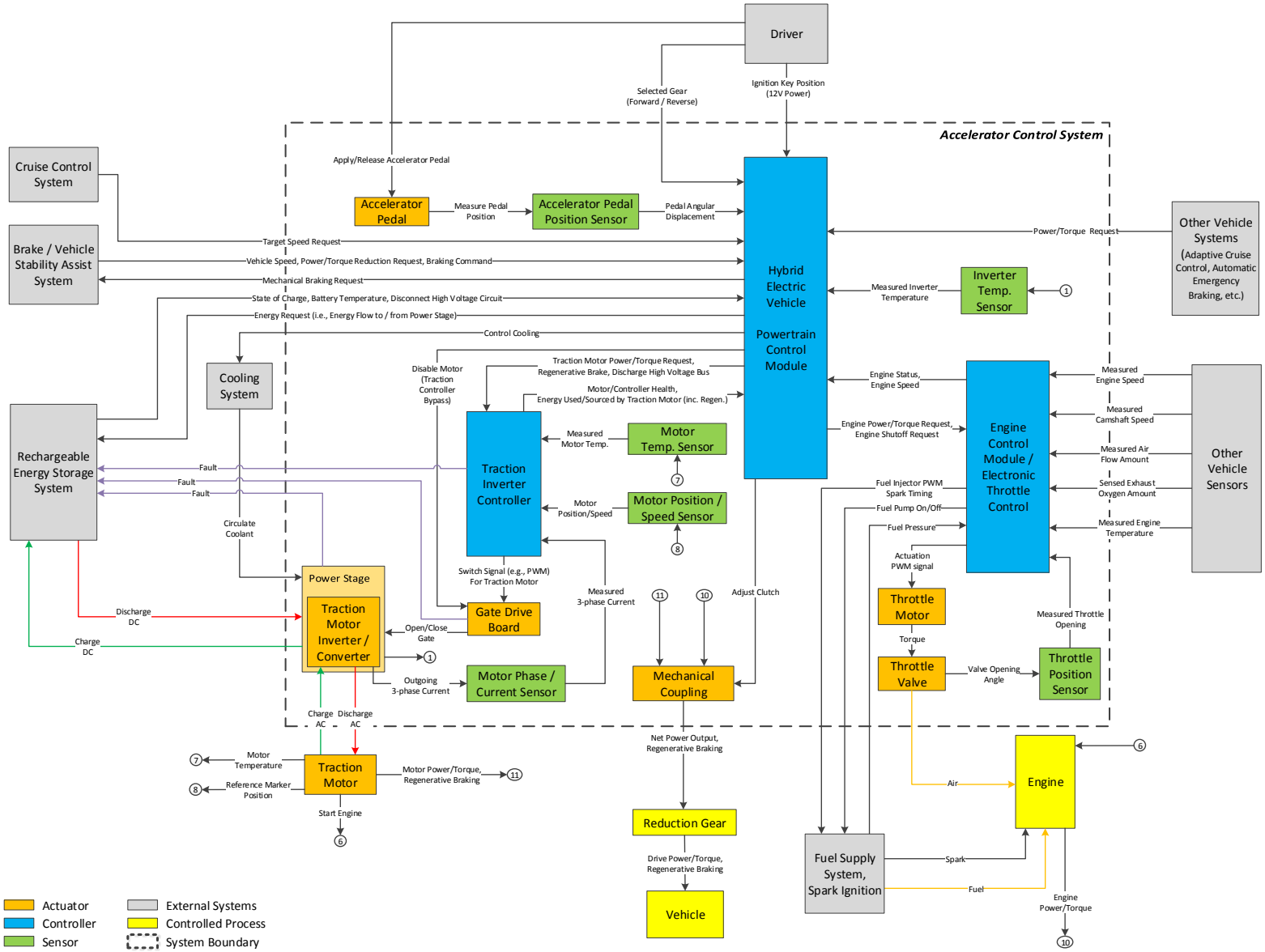


Figure 6. Block Diagram of a Generic ACS/ETC for a Parallel Hybrid Electric Vehicle

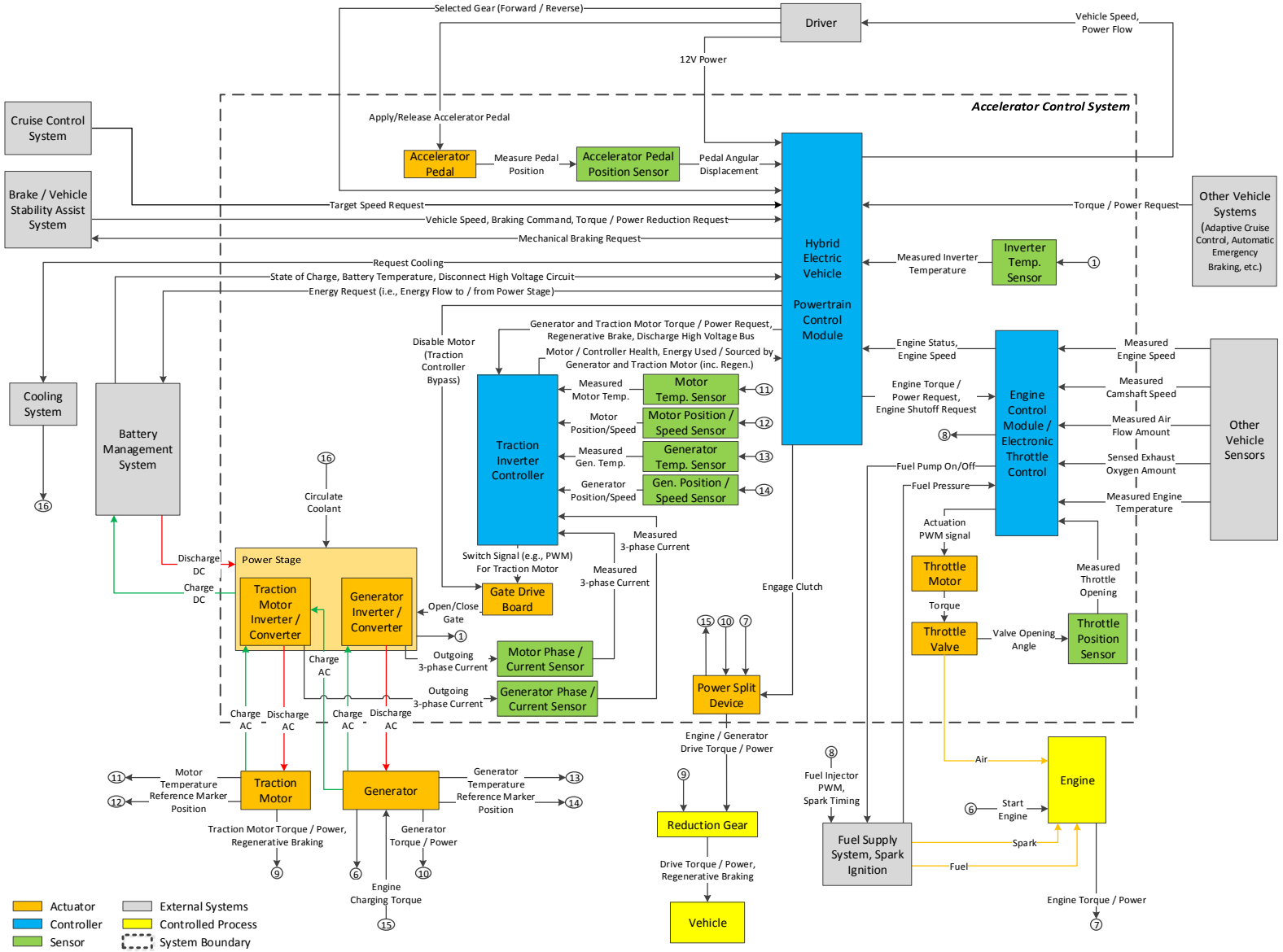


Figure 7. Block Diagram of a Generic ACS/ETC for a Series-Parallel Hybrid Electric Vehicle

3.4 System Description

The following description outlines the functions of each of the three HEV ACS/ETC systems [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20].

3.4.1 Series HEV System Description

3.4.1.1 Driver-Operated Control

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

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

- Torque requests from the brake/stability system
- Torque requests from the CC system

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

3.4.1.2 Electric Motor Current Control

After the HEV PCM computes the direction and amount torque necessary to meet the driver's request and other vehicle demands, the HEV PCM sends a torque command to the TICM. The TICM computes the amount of electrical current required by the electric motor to meet the torque requested by the HEV PCM. The electrical current supplied to the electric motor determines both the direction and amount of torque produced.

The TICM causes current to flow to the electric motor by sending switching signals to the gate drive board. The gate drive board serves as a power amplifier that drives transistors in the inverter/converter according to the TICM's command. The gate drive board may also electrically isolate the TICM from the high-voltage inverter/converter to prevent damage to the microcontroller.

Depending on the system design, the electric motor may operate using either HV direct current (DC) or alternating current (AC). The inverter/converter is designed to provide the appropriate HV power supply to the electric motor. For systems with DC motors, the inverter/converter

converts the HV DC from the RESS to the appropriate voltage level for the electric motor. For systems with AC motors, the inverter/converter converts the HV DC from the RESS to the AC required by the electric motor. The inverter/converter also contains a converter which converts high-voltage DC to the low-voltage DC needed for the vehicle's auxiliary systems.

A phase/current sensor measures the current supply from the inverter/converter to the electric motor. The phase/current sensor measurement provides feedback to the TICM allowing closed-loop control of the switching signal provided to the gate drive board.

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

3.4.1.3 Idle Speed Control

When the driver releases the AP, mechanical components (e.g., springs) in the AP assembly return the pedal to the idle (i.e., undepressed) position. In a series HEV, the electric motor torque output can be reduced to zero when the AP is released. In order to simulate the "creep" speed found in ICEs, some HEV PCMs are designed to provide a small amount of current to the electric motor when the AP is released based on a pre-programmed idle torque level.

If the AP is released when the vehicle speed is above the idle creep speed, the HEV PCM may either allow the vehicle to coast down to the idle creep speed or may activate regenerative braking to slow the vehicle at a faster rate. This latter approach is typically used to simulate the effect of engine braking found on vehicles with ICEs. Regenerative braking also serves to re-charge the RESS, as noted later in this report.

3.4.1.4 Brake Throttle Override Function

As an example OEM strategy, when the driver presses the BP, the BPPS sends a signal to the HEV PCM. If both the AP and BP are pressed, the HEV PCM must determine if the driver's intent is to stop the vehicle. To accomplish this, the HEV PCM may consider other factors in addition to the accelerator pedal position (APP) and brake pedal position (BPP), 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 HEV PCM engages the BTO feature.

In BTO mode, the HEV PCM will override the torque request from the driver via the AP and either reduce the current supply to the pre-set current level for BTO mode or reduce the current supply to zero. Since regenerative braking relies on the electric motor, it is possible the HEV PCM may engage regenerative braking while in BTO mode, effectively overriding the AP torque request. The HEV PCM will maintain the current supply to the electric motor at the BTO level

until BTO mode is disengaged. The HEV PCM should not exit BTO mode while a conflict between the AP and BP still exists.

3.4.1.5 Fault Detection

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

Some examples of system faults include:

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

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

3.4.1.6 Related System: Braking System

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

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

The HEV PCM sends a request for regenerative braking to the TICM. The TICM controls the electric motor to achieve the required level of regenerative braking. The electrical energy generated by the electric motor is converted to HV DC suitable for the RESS through the inverter/converter.

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

3.4.1.7 Related System: Rechargeable Energy Storage System

The RESS is not considered part of the series HEV ACS/ETC, but it is a closely related system and is essential for achieving the desired torque output from the electric motor. The RESS is responsible for controlling charging and discharging the high-voltage battery, including charging the battery through regenerative braking. The RESS supplies the inverter/converter with high-voltage DC and receives high-voltage DC from the inverter/converter during regenerative braking.

In the series HEV, the RESS is also responsible for commanding torque from the gasoline ICE subsystem to generate electrical energy. The electrical energy may be used either to charge the HV battery or to supply HV directly to the inverter/converter.

When a voltage or current abnormality is detected or when the RESS receives a signal from the occupant restraint system crash sensors, the RESS may send a signal to the HEV PCM to discharge the HV bus. The HEV PCM transmits the request to discharge the HV bus to the TICM. The TICM commands the inverter/converter, through the gate drive board, to discharge the HV bus across resistors integrated into the inverter/converter.

3.4.1.8 Related System: Vehicle Cooling System

The HEV PCM is responsible for regulating the temperature of the inverter/converter. As the inverter/converter heats up during operation, the inverter temperature sensor reports the inverter/converter temperature to the HEV PCM. When the inverter/converter temperature reaches a threshold value, the HEV PCM requests cooling from the vehicle cooling system. The vehicle cooling system circulates cooling fluid to reduce the inverter/converter temperature. The vehicle cooling system may also be responsible for maintaining the temperature of other vehicle components, such as the electric motor. Note that in configurations where the inverter/converter is continually cooled, the HEV PCM may not need to request cooling in response to temperature changes in the inverter/converter.

3.4.2 Parallel HEV System Description

3.4.2.1 Driver-Operated Control

The accelerator pedal assembly allows the driver to command a desired net power output from the ACS/ETC. Similar to the series HEV, when the driver presses the accelerator pedal the APPS measures the angular displacement of the accelerator pedal. The APPS converts the angular displacement of the accelerator pedal to a voltage signal, which is transmitted to the HEV PCM.

Based on the driver's input via the APPS and torque requests from other vehicle systems, the HEV PCM determines the desired net power output from the ACS/ETC.

3.4.2.2 Powertrain Subsystem Power Assignment

Since there are two powertrain subsystems in the parallel HEV architecture, the HEV PCM is responsible for determining the power output from each powertrain subsystem to achieve the desired net power output. The HEV PCM uses an optimization algorithm to determine how much power should be supplied from the gasoline ICE and the EPS. The specifics of the optimization algorithm depend on the system design, but may consider factors such as:

- Requests from the driver and other vehicle systems,
- Battery state of charge (SOC),
- Vehicle speed,
- Emissions, and
- Engine speed and operating point.

Table 1, below, shows some typical driving scenarios and how the HEV PCM may elect to assign power to the powertrain subsystems. Note that depending on the parallel HEV design, some of the driving scenarios shown below may not be possible.

Table 1. Example Power Assignments for Typical Driving Scenarios in a Parallel HEV

	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Scenario Description	• Low Speed • High SOC	• Cruising • High SOC	• Cruising • Low SOC	• Acceleration	• Regenerative Braking
Gasoline ICE	Off	Propulsion	Propulsion	Propulsion	Off
Electric Motor	Propulsion	Off	As Generator	Propulsion	As Generator

Once the HEV PCM determines the power required from each powertrain subsystem, the HEV PCM issues requests to the TICM and the ECM/Throttle Actuator Controller. These secondary controllers are responsible for implementing the HEV PCM's command within the EPS and gasoline ICE powertrain subsystem, respectively.

In some parallel HEV architectures, the HEV PCM may also be responsible for operating the mechanical coupling to combine the power output from the gasoline ICE and electric motor. For example, the HEV PCM may disengage a clutch to decouple the gasoline ICE from the drivetrain, allowing "motor-only" operation. Engaging the clutch couples the gasoline ICE to the drivetrain, allowing both powertrains to provide torque to the drivetrain or allowing the electric motor to recharge the battery from the gasoline ICE. Unlike the more complex series-parallel HEVs, however, the EPS in a parallel HEV cannot simultaneously provide torque to the drivetrain and recharge the HV battery.

3.4.2.3 Electric Motor Current Control

The HEV PCM issues a power request to the TICM, based on the assignment computed from the optimization algorithm. The TICM converts the power request from the HEV PCM to the electric current required by the electric motor to produce the required power output. Similar to

the series HEV, the TICM causes current to flow to the electric motor by sending switching signals to the gate drive board. The gate drive board operates the high-power transistors in the inverter and also electrically isolates the TICM from the inverter/converter.

Depending on the system design, the electric motor may operate using either HV DC or AC, similar to the series HEV ACS/ETC. Additionally, feedback from the electric motor to the TICM operates similar to the series HEV ACS/ETC.

In some instances the HEV PCM may command more power from the gasoline ICE than is required to meet the desired power output from the ACS/ETC. The excess power from the ICE is diverted to the electric motor, which acts as a generator to convert this mechanical energy into electric energy to charge the high voltage battery. A rectifier converts the AC produced from the electric motor into DC. However, the electric motor can only provide propulsion or operate as a generator; the parallel HEV cannot simultaneously recharge the battery and provide power to the drivetrain from the EPS.

3.4.2.4 Gasoline ICE Control

The ECM/Throttle Actuator Controller receives a power request from the HEV PCM. Unlike the series HEV, the power output from the ICE in a parallel HEV is delivered directly to the drivetrain of the vehicle. The ECM/Throttle Actuator Controller computes the quantity of air required by the ICE to produce the desired power output. To adjust the volume of air reaching the ICE, the ECM/Throttle Actuator Controller controls the throttle motor. The throttle motor adjusts the throttle valve position to regulate air flow to the intake manifold.

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

In order to maximize fuel efficiency, parallel HEV designs may try to avoid engine idling or operating the engine at low vehicle speeds. To accomplish this, the HEV PCM can command the ECM/Throttle Actuator Controller to shut off the engine when it is not needed for propulsion (e.g., when the vehicle is stopped). When the engine is needed for propulsion, the HEV PCM commands the ECM/Throttle Actuator Controller to start the ICE. Unlike the series-parallel HEV, which uses one of the electric motors as a starter, the parallel HEV ACS/ETC may have a dedicated starter motor for the ICE.

3.4.2.5 Idle Speed Control

Similar to the series HEV PCM, the parallel HEV PCM may incorporate idle-type features into the operation of the electric motor to more closely simulate behavior of non-hybrid ICE vehicles. These features may include:

- Simulating the idle creep speed by allowing a small current to flow to the electric motor when the accelerator pedal is released, and
- Simulating engine braking by having regenerative braking start when the AP is released.

As described previously, the HEV PCM may try to maximize fuel efficiency by shutting down the gasoline ICE at low vehicle speeds or when the vehicle is stopped. If the gasoline ICE is shut down, then it would not need to maintain an idle speed. However, if the HEV PCM needs to operate using only the gasoline ICE at low vehicle speeds or while the vehicle is stopped (e.g., if there is a failure of the EPS), the HEV PCM or ECM/Throttle Actuator Controller would need to operate the gasoline ICE in an idle state.

To operate the gasoline ICE in an idle state, ECM/Throttle Actuator Controller must determine the mass air flow required by the engine to run at the idle speed. This value may be stored in the ECM/Throttle Actuator Controller calibration data. As the vehicle ages, the ECM/Throttle Actuator Controller can rewrite the throttle valve idle angular position calibration data to ensure that the engine receives the required air flow.

The engine shaft speed is measured in revolutions per minute (RPM) by the engine speed sensor. The ECM/Throttle Actuator Controller may use the engine shaft speed as a feedback mechanism to control the engine idle speed. If the measured engine idle speed does not match the expected engine idle speed programmed into the ECM/Throttle Actuator Controller software, the ECM/Throttle Actuator Controller may adjust 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 air conditioning,
- Ambient air temperature and pressure, and
- Exhaust quality, measured by the heated exhaust gas oxygen (HEGO) sensor.

3.4.2.6 Brake Throttle Override Function

The BTO function in the parallel HEV ACS/ETC operates similar to the series HEV. In BTO mode, the HEV PCM will override the power request from the driver via the APPS. The HEV PCM will command a net power output suitable for BTO mode. This may be the idle speed power output or a pre-programmed power output for BTO. Depending on the parallel HEV design and operating conditions, the BTO power output may be achieved in different ways, such as:

- Operating using a simulated “idle creep speed” in the electric motor,
- Operating using the idle engine speed of the gasoline ICE, or

- Operating using a combination of power outputs from the gasoline ICE and electric motor (e.g., operating the electric motor as a generator).

3.4.2.7 Fault Detection

The HEV PCM is also responsible for monitoring the ACS/ETC system components to determine if faults are present. If the HEV PCM detects a fault in the system, the HEV PCM will log a DTC and may transition the ACS/ETC into a safe state, such as "limp-home mode". The HEV PCM may also cause an indicator light to display on the vehicle's instrument display panel.

Some examples of system faults include:

- APPS voltage signals exceeding the calibration range,
- Faults in the EPS,
- Faults in the gasoline ICE subsystem,
- Voltage or current abnormalities (reported to the RESS), or
- Internal software or hardware faults in the HEV PCM.

In addition to the HEV PCM, the TICM and ECM/Throttle Actuator Controller may be responsible for monitoring for faults in the EPS and gasoline ICE powertrain subsystem, respectively. The TICM and ECM/Throttle Actuator Controller may report the health of their respective subsystems to the HEV PCM. If the HEV PCM receives a reported fault in the EPS or gasoline ICE powertrain subsystem, the HEV PCM may elect not to use that subsystem for vehicle propulsion or may transition the ACS/ETC into a "limp-home mode".

3.4.2.8 Related System: Braking System

In addition to providing vehicle propulsion, the electric motor is responsible for supporting the parallel HEV brake system through regenerative braking. Regenerative braking in the parallel HEV operates similarly to the series HEV, as described in Section 3.4.1.6.

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

3.4.2.9 Related System: Rechargeable Energy Storage System

The RESS is not considered part of the parallel HEV ACS/ETC, but it is a closely related system and is essential for achieving the desired power output from the electric motor. The RESS is responsible for controlling charging and discharging the high-voltage battery, including charging the battery through regenerative braking. The RESS supplies the inverter/converter with high-voltage DC and receives high-voltage DC from the inverter/converter during regenerative braking or when the electric motor is in generating mode. Unlike the series HEV, the RESS in a parallel HEV is not responsible for operating the gasoline ICE.

When a voltage or current abnormality is detected or when the RESS receives a signal from the occupant restraint system crash sensors, the RESS may send a signal to the HEV PCM to discharge the HV bus. The HEV PCM transmits the request to discharge the HV bus to the TICM. The TICM commands the inverter/converter, through the gate drive board, to discharge the HV bus across resistors integrated into the inverter/converter.

3.4.2.10 Related System: Vehicle Cooling System

Similar to the series HEV, the parallel HEV ACS/ETC is responsible for maintaining the temperature of the inverter. The HEV PCM issues commands to the vehicle cooling system in a similar manner as described in Section 3.4.1.8.

3.4.2.11 Related System: Fuel Delivery System

Since the parallel HEV ACS/ETC controls the air flow to the gasoline ICE, the fuel delivery system is considered a closely related system that is essential for achieving the desired engine torque output.

The ECM/Throttle Actuator Controller uses the measured air flow to the engine 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. The ECM/Throttle Actuator Controller also controls the spark timing. The ECM adjusts the fuel quantity and spark timing to achieve maximum engine power output while meeting emission requirements.

3.4.3 Series-Parallel HEV System Description

3.4.3.1 Driver-Operated Control

In the series-parallel HEV, the driver input via the APPS translates to a desired net power output from the ACS/ETC. The driver-operated control for the series-parallel HEV is identical to the driver-operated control for the parallel HEV, as described in Section 3.4.2.1.

3.4.3.2 Powertrain Subsystem Power Assignment

The series-parallel HEV has two powertrain subsystems, similar to the parallel HEV ACS/ETC architecture. The HEV PCM is responsible for determining the power output from each powertrain subsystem to achieve the desired net power output. However, unlike the parallel HEV, the series-parallel HEV EPS includes two electric motors. While one electric motor is typically operated as a generator, in some series-parallel HEV designs both motors can be used to supply propulsion.

The HEV PCM uses an optimization algorithm to determine how much power should be supplied from the gasoline ICE and the EPS. The optimization algorithm differs between manufacturers, but may consider factors such as:

- Requests from the driver and other vehicle systems,

- Battery state of charge (SOC),
- Vehicle speed,
- Emissions, and
- Engine speed and operating point.

Table 1, below, shows some typical driving scenarios and how the HEV PCM may elect to assign power to the powertrain subsystems. Note that depending on the series-parallel HEV design, some of the driving scenarios shown below may not be possible.

Table 2. Example Power Assignments for Typical Driving Scenarios in a Series-Parallel HEV

	Scenario 1	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**
Scenario Description	• Low Speed • High SOC	• Cruising • High SOC	• Cruising • Low SOC	• Maximum Acceleration	• Regenerative Braking
Gasoline ICE	Off	Propulsion	Propulsion	Propulsion	Off
Electric Motor 1 (M/G 1)	Propulsion	Off	Off	Propulsion	As Generator
Electric Motor 2 (M/G 2)	Off	Off	As Generator	Propulsion	Off

M/G – Motor/Generator

Once the HEV PCM determines the power required from each powertrain subsystem, the HEV PCM issues requests to the TICM and the ECM/Throttle Actuator Controller. As with the parallel HEV, these secondary controllers are responsible for implementing the HEV PCM's command within the EPS and gasoline ICE powertrain subsystem, respectively.

3.4.3.3 Electric Motor Current Control

The series-parallel HEV EPS has two electric motors. This study considers a series-parallel HEV design that allows both electric motors to provide propulsion.

Based on the assignment computed from the optimization algorithm, the HEV PCM issues power requests to the TICM for both the electric motors. The TICM converts the power request for each electric motor to the electric current required to produce the requested power output. Similar to the series and parallel HEVs, the TICM causes current to flow to the electric motor by sending switching signals to the gate drive board. The gate drive board operates the high-power transistors in the inverter/converter and also electrically isolates the TICM from the high voltage inverter/converter. As with both the series and parallel HEVs, the system design may specify either HV DC or AC electric motors.

The series-parallel HEV EPS has separate phase/current sensors to measure the current supplied to each of the electric motors. Resolvers integrated into the motor assemblies measures the position and speed of each electric motor. Both the phase/current sensor measurement and motor position/speed measurement provide feedback to the TICM allowing closed-loop control of the switching signal provided to the gate drive board.

When one of the electric motors is used as a generator, the power split device diverts excess power from the gasoline ICE to this motor. A rectifier converts the AC produced from the electric motor into DC to charge the HV battery. Unlike the parallel HEV, since the series-parallel HEV has two electric motors, one motor can be operated as a generator while the other motor is supplying propulsion to the drivetrain.

3.4.3.4 Gasoline ICE Torque Control

Control of the gasoline ICE in the series-parallel HEV is similar to the control of the gasoline ICE in the parallel HEV, as described in Section 3.4.2.4.

3.4.3.5 Power-Split Device Control

In the series-parallel HEV, the PSD is responsible for directing power flow between the gasoline ICE, the electric motors, and the vehicle's drivetrain. The PSD is typically more complex than the mechanical coupling in the parallel HEV. In some series-parallel HEV designs, the PSD consists of a single planetary gear set. These PSDs are not actively controlled.

In other series-parallel HEV designs, the PSD consists of several gear sets (e.g., two sets of planetary gears). These PSDs may contain one or more clutches that are controlled by the HEV PCM. Engaging different clutches affects the power flow from the gasoline ICE to the electric motors and drivetrain.

3.4.3.6 Idle Speed Control

Idle speed control in the series-parallel HEV is similar to the idle speed control in the parallel HEV, as described in Section 3.4.2.5.

3.4.3.7 Brake Throttle Override Function

BTO control in the series-parallel HEV is similar to BTO control in the parallel HEV, as described in Section 3.4.2.6.

3.4.3.8 Fault Detection

The HEV PCM is also responsible for monitoring the ACS/ETC system components to determine if faults are present. Fault detection in the series-parallel HEV is similar to fault detection the parallel HEV.

Some examples of system faults include:

- APPS voltage signals exceeding the calibration range,
- Faults in the EPS,
- Faults in the gasoline ICE subsystem,
- Faults in the PSD
- Voltage or current abnormalities (reported to the RESS), or
- Internal software or hardware faults in the HEV PCM.

In addition to the HEV PCM, the TICM and ECM/Throttle Actuator Controller may be responsible for monitoring for faults in the electric powertrain and gasoline ICE powertrain subsystems, respectively. In particular, the TICM is responsible for monitoring the health for both electric motors.

3.4.3.9 Related System: Braking System

In addition to providing vehicle propulsion, the electric motor is responsible for supporting the series-parallel HEV brake system through regenerative braking. Regenerative braking in the series-parallel HEV operates similarly to the series HEV, as described in Section 3.4.1.6.

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

3.4.3.10 Related System: Rechargeable Energy Storage System

The RESS is responsible for providing HV power to the HEV ACS/ETC as well as receiving electric power from regenerative braking or when the electric motors are operating generating mode. The series-parallel HEV ACS/ETC interface with the RESS is similar to the description for the parallel HEV in Section 3.4.2.9.

3.4.3.11 Related System: Vehicle Cooling System

Similar to the series HEV, the series-parallel HEV ACS/ETC is responsible for maintaining the temperature of the inverter. The HEV PCM issues commands to the vehicle cooling system in a similar manner as described for the series HEV in Section 3.4.1.8.

3.4.3.12 Related System: Fuel Delivery System

Similar to the parallel HEV, the ECM/Throttle Actuator Controller is responsible for coordinating fuel injection and spark timing with the fuel delivery system, as described in Section 3.4.2.11.

3.4.4 Comparison of Key ACS/ETC Features Across All Three HEV Architectures

Table 3 compares key features of the ACS/ETC for the three HEV with gasoline ICE architectures.

Table 3. Key Differences between the Three HEV ACS/ETC Architectures

	Series HEV	**Parallel HEV**	**Series-Parallel HEV**
Propulsion Source(s)	Electric motor	• Electric motor • Gasoline ICE	• Electric motor • Gasoline ICE
Accelerator Pedal Regulates	Current to electric motor	Net power output to drivetrain	Net power output to drivetrain
Number of Electric Motors	2	1	2
Simultaneous Electric Motor Propulsion and Charging	Yes	No	Yes
Examples	BMW i3	Honda Civic Hybrid	Toyota Prius

The series and parallel HEV represent two distinct architectures, with little commonality in their operation. However, as the name suggests, the series-parallel HEV shares elements of both the series and parallel HEV architectures.

The series and series-parallel HEV architectures both include two electric motors, although one of the electric motors in the series HEV architecture is not considered as part of the ACS/ETC because it does not directly supply propulsion to the drivetrain. Both the series and series-parallel HEV architectures are capable of simultaneously charging the HV battery and producing propulsion via the EPS.

The parallel and series-parallel HEV architectures consist of two propulsion subsystems connected directly to the drivetrain. The driver controls the net power output from these two systems. The HEV PCM determines the appropriate power split between the two subsystems based on the vehicle's operating conditions.

4 VEHICLE-LEVEL HAZARD ANALYSIS

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

4.1 Vehicle-Level Hazards

In this study, HAZOP and STPA identify similar vehicle-level hazards. These hazards were synthesized to produce a consistent list. Table 4 shows the vehicle-level hazards for all three HEV architectures and their definitions. Table 5 shows which vehicle-level hazards apply to each HEV architecture.

Table 4. Vehicle-Level Hazards and Definitions

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

	Driver Action	Vehicle Response	Hazards
			an HV circuit and individuals (such as someone performing vehicle repairs or first responder emergency personnel) who might come in contact with an exposed HV circuit.
			H8: Potential RESS Thermal Event – refers to situations where the ACS/ETC overcharges the RESS, potentially resulting in a thermal event.
[i] This hazard may not apply in ACS/ETC systems designed to give the driver's command priority over all active safety systems.			

This study considers "Potential Electric Shock" and "Potential RESS Thermal Event" as HEV ACS/ETC vehicle-level hazards even though they are not related to vehicle motion. These potential hazards are directly related to functions of the HEV ACS/ETC system and therefore fall within the scope of the HEV ACS/ETC according to ISO 26262 (Part 3 Clause 1) [2].

Table 5. Allocation of Vehicle-Level Hazards to the Three HEV ACS/ETC Architectures

Vehicle-Level Hazard	HEV Architecture		
	Series HEV	Parallel HEV	Series-Parallel HEV
H1: Potential Uncontrolled Vehicle Propulsion	●	●	●
H1a: Potential Uncontrolled Vehicle Propulsion from Zero Start Speed	●	●	●
H2: Potential Insufficient Vehicle Propulsion	●	●	●
H3: Potential Vehicle Movement in an Unintended Direction	●	●	●
H4: Potential Propulsion Power Reduction/Loss or Vehicle Stalling	●	●	●
H5: Potential Insufficient Vehicle Deceleration	●	●	●
H6: Potentially Allowing Driver's Command to Override Active Safety Systems	●	●	●
H7: Potential Electric Shock	●	●	●
H8: Potential RESS Thermal Event		●	●

Both the parallel HEV and series-parallel HEV ACS/ETC architectures include operation of a coupling or PSD to divert power from the gasoline ICE powertrain subsystem to the RESS via the traction motor. Therefore, the hazard "Potential RESS Thermal Event" would apply to these two architectures; malfunctions in the ACS/ETC in these architectures could potentially result in overcharging of the RESS. On the other hand, the gasoline ICE and generator are considered outside the ACS/ETC system boundary for the series HEV. Therefore, the "Potential RESS Thermal Event" hazard does not apply to this ACS/ETC architecture.[11]

[11] This hazard may still apply to other systems in series HEV vehicles, such as the RESS itself.

4.2 Hazard and Operability Study

4.2.1 Series HEV HAZOP Study

4.2.1.1 Series HEV HAZOP System Description

The HAZOP study uses a block diagram as a visual representation of the series HEV ACS/ETC system. The HAZOP study block diagram identifies the key system elements, internal interfaces, and high-level external interfaces. Figure 8 illustrates the block diagram used in the HAZOP study for the series HEV.

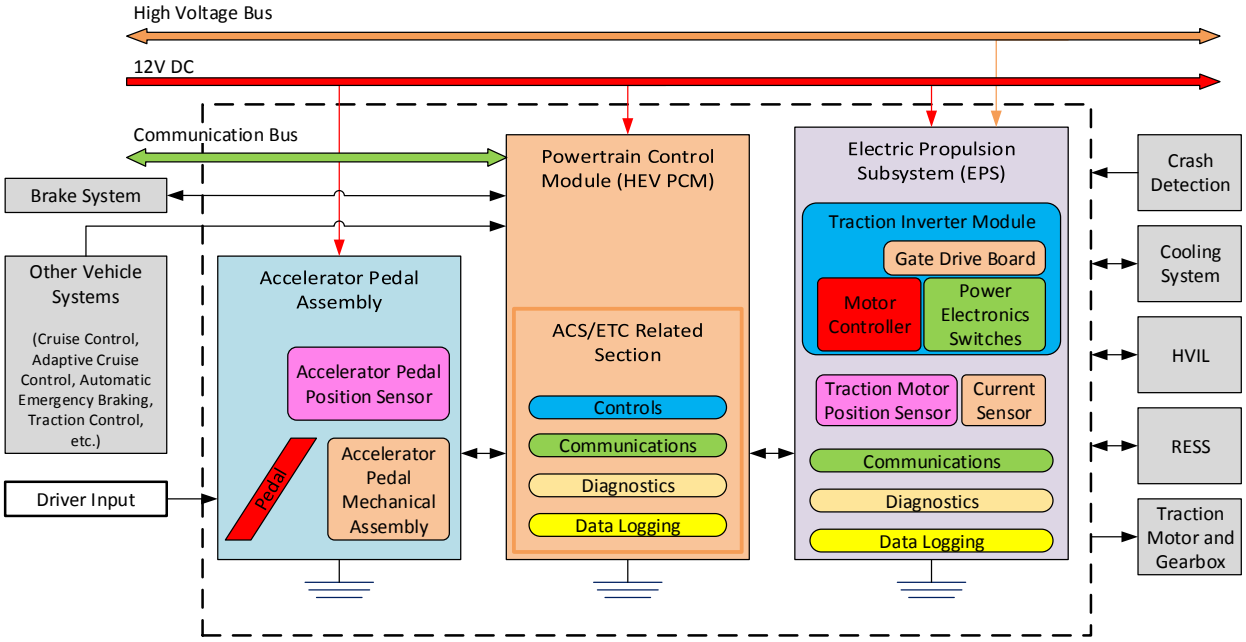


Figure 8. HAZOP Block Diagram for the Series HEV ACS/ETC System

The dashed line in Figure 8 defines the boundary of the series HEV ACS/ETC system considered in the HAZOP study. The series HEV ACS/ETC contains three main subsystems:

- AP Assembly
- HEV PCM
- EPS

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

- Adaptive cruise control (ACC)
- Automatic emergency braking (AEB)
- TCS

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

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

- Brake system – regenerative braking, vehicle speed data, etc.
- Cooling system – inverter/converter cooling
- HVIL – high voltage circuit faults
- RESS – HV system status, discharge bus requests, etc.
- Occupant restraint system – crash detection

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

4.2.1.2 Series HEV System Functions

The HAZOP study identifies 20 system functions for the series HEV ACS/ETC:

1. Command torque from the EPS.[12]
2. Receive energy from the HV DC bus.[12]
3. Deliver current to the electric motor.[12]
4. Control the HV RESS contactors.[12]
5. Provide the APP to the HEV PCM. [12]
6. Return the AP to the at-rest (i.e., undepressed) position within the specified time.[12]
7. Provide AP request rate limiting.[12]
8. Communicate the delivered torque magnitude and direction to the HEV PCM.[12]
9. Return the torque output to the creep value within the specified time.[12, 13]
10. Establish the creep torque value.[12, 14]
11. Provide creep state control.[12, 14]
12. Provide BTO control.[12]
13. Store the APP and motor speed torque maps.
14. Provide bus capacitance discharge request to the EPS.[12]

[12] This function is common to all three HEV ACS/ETC architectures.
[13] If the series HEV ACS/ETC is not designed to simulate an idle creep speed, the analogous function would be to return the torque output to zero within the specified time.
[14] This function may not apply if the series HEV ACS/ETC is not designed to simulate an idle creep speed.

15. Discharge the bus capacitance.[12]
16. Communicate with internal subsystems and external vehicle systems.
17. Provide diagnostics.[12]
18. Provide fault detection and failure mitigation.[12]
19. Store relevant data.[12]
20. Provide motor current values.[12]

Functions 18, 19, and 20 are shown here for completeness. Function 18 is part of the design to mitigate hazards resulting from other malfunctions in the system. The HAZOP study concludes that malfunctions derived from Function 19 would not result in vehicle-level hazards. Function 20 is part of the design implementation and may be considered by some analysts to be integral to the TICM.

4.2.1.3 Series HEV System Malfunctions

The application of the seven HAZOP study guidewords presented in Section 2.2.1 to each of the 20 series HEV ACS/ETC functions listed above results in a list of 139 malfunctions. Each of these malfunctions is assessed to determine if the malfunction could lead to one or more of the potential vehicle-level hazards.

Table 6 provides an example of how malfunctions were derived from one of the series HEV ACS/ETC functions. Table 7 shows the number of malfunctions identified for each of the 20 series HEV ACS/ETC functions. Appendix B provides the complete results of the HAZOP study.

Table 6. Derivation of Malfunctions and Hazards Using the HAZOP Study (Example)

Function: Provide the APP to the HEV PCM.

HAZOP Guidewords	***Malfunction***	***Operating Mode***	***Potential Vehicle Level Hazard***
Loss of function	Does not provide the APP to the FCEV PCM	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2, 3, 4) Potential insufficient vehicle propulsion 1, 2) Potential insufficient vehicle deceleration 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2) Potential vehicle movement in the wrong direction
More than intended	Provides larger AP travel position than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential uncontrolled vehicle propulsion 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling
Less than intended	Provides smaller AP travel position than intended	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential insufficient vehicle propulsion 1, 2) Potential insufficient vehicle deceleration
Intermittent	Provides APP intermittently	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential uncontrolled vehicle propulsion 1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2, 3, 4) Potential insufficient vehicle propulsion 1, 2) Potential insufficient vehicle deceleration 3, 4) Potential uncontrolled vehicle propulsion when the vehicle speed is zero 1, 2) Potential vehicle movement in the wrong direction
Incorrect direction	Provides AP travel position in the wrong direction	1) ON; D; Moving 2) ON; R; Moving 3) ON; D; Stopped 4) ON; R; Stopped	1, 2, 3, 4) Potential propulsion power reduction/loss or vehicle stalling 1, 2) 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 7. Number of Identified Malfunctions for Each HAZOP Function in the Series HEV

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

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

4.2.2 Parallel HEV HAZOP Study

4.2.2.1 Parallel HEV HAZOP System Description

The HAZOP study block diagram in Figure 10 identifies the key system elements, internal interfaces, and high-level external interfaces considered in the HAZOP study for the parallel HEV.

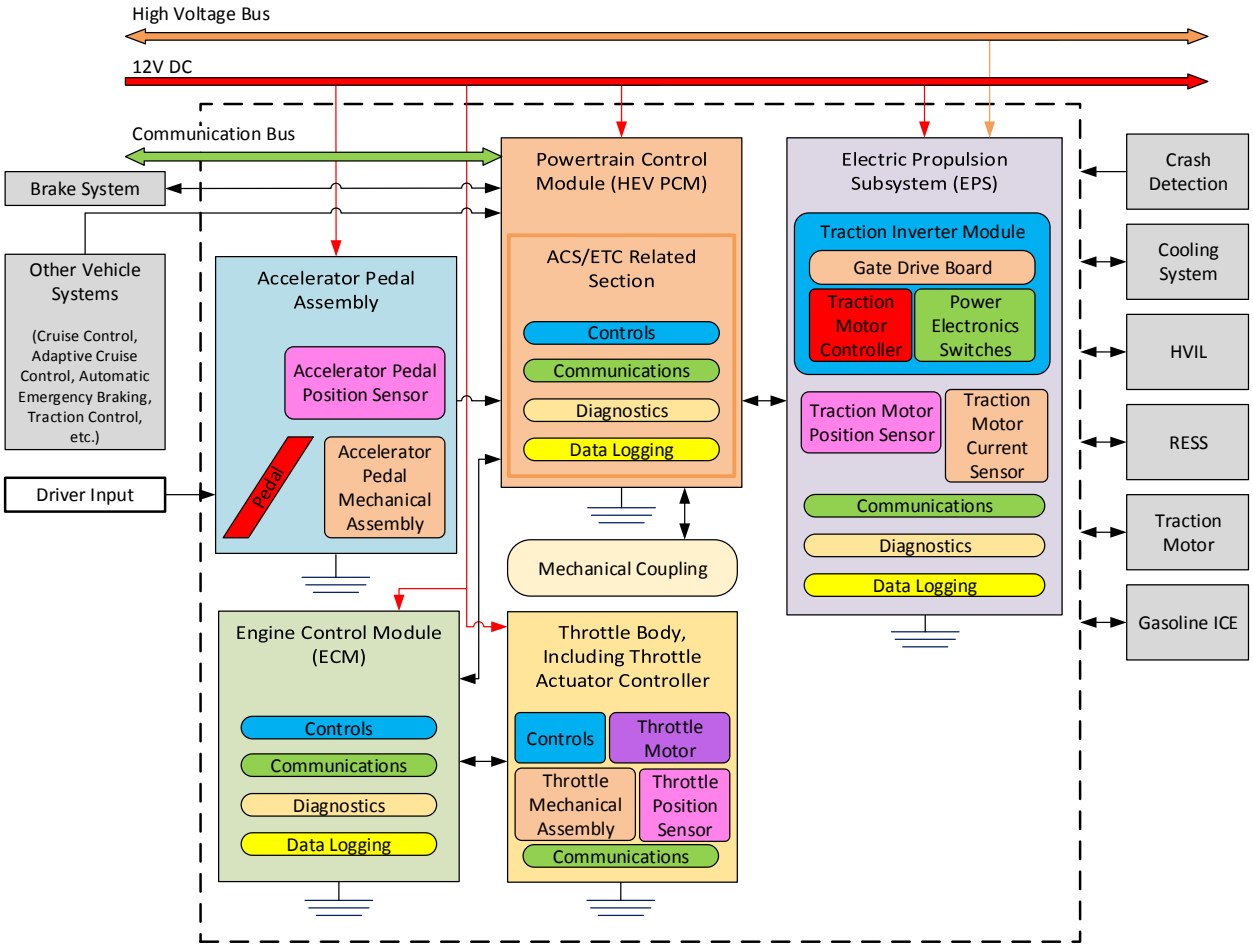


Figure 9. HAZOP Block Diagram of the Parallel HEV ACS/ETC System

The dashed line in Figure 10 defines the boundary of the parallel HEV ACS/ETC system considered in the HAZOP study. The parallel HEV ACS/ETC contains five main subsystems:

- AP Assembly
- HEV PCM
- EPS
- ECM/Throttle Actuator Controller
- Mechanical coupling

The HEV PCM determines the net power output from the ACS/ETC, considering relevant parameters of the vehicle operating conditions, such as vehicle speed, vehicle direction, and torque requests from other vehicle systems. The HEV PCM also responds to requests for HV power generation from the RESS.

The HEV PCM transmits the desired power output from the electric motor to the EPS. The EPS supplies current to the electric motor, which provides torque to the drivetrain. The HEV PCM also transmits the desired power output from the gasoline ICE to the ECM/Throttle Actuator Controller. The ECM/Throttle Actuator Controller adjusts the throttle valve to regulate the gasoline ICE power output.

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

- Brake system – regenerative braking, vehicle speed data, etc.
- Cooling system – inverter/converter cooling
- HVIL – high voltage circuit faults
- RESS – HV system status, discharge bus requests, etc.
- Occupant restraint system – crash detection

The parallel HEV ACS/ETC is also connected to the 12-volt direct current power supply, the HV power supply, and communication bus (e.g., CAN bus).

4.2.2.2 Parallel HEV System Functions

The HAZOP study identifies 31 system functions for the parallel HEV ACS/ETC:

1. Command torque from the EPS.[15]
2. Command torque from the gasoline ICE.
3. Combine torque output from the electric motor and gasoline ICE.
4. Receive energy from the HV DC bus.[15]
5. Deliver current to the electric motor.[15]
6. Control the HV RESS contactors.
7. Deliver HV energy to the RESS.
8. Provide APP to the HEV PCM.
9. Return the AP to the at-rest (i.e., undepressed) position within the specified time.[15]
10. Provide AP request rate limiting.[15]
11. Communicate the delivered torque magnitude and direction to the HEV PCM.[15]
12. Return the torque output to the creep value within the specified time.[15, 16]

[15] This function is common to all three HEV variants.
[16] If the EPS portion of the parallel HEV ACS/ETC is not designed to simulate an idle creep speed, the analogous function would be to return the torque output to zero within the specified time.

13. Establish the creep torque value. [18, 17]
14. Provide creep state control. [18, 14]
15. Provide BTO control. [18]
16. Command throttle position.
17. Control throttle position.
18. Communicate the throttle position to the ECM/Throttle Actuator Controller.
19. Return the throttle to the idle position within the specified time.
20. Establish the throttle idle position.
21. Provide idle state control.
22. Store the APP, electric motor speed, and engine speed torque maps.
23. Provide bus capacitance discharge request to the EPS. [18]
24. Discharge the bus capacitance. [18]
25. Command the gasoline ICE to start/stop.
26. Communicate with external vehicle systems.
27. Communicate with internal ACS/ETC subsystems (i.e., EPS and gasoline ICE).
28. Provide diagnostics. [18]
29. Provide fault detection and failure mitigation. [18]
30. Store relevant data. [18]
31. Provide electric motor current values. [18]

Functions 29, 30, and 31 are shown here for completeness. Function 29 is part of the design to mitigate hazards resulting from other malfunctions in the system. The HAZOP study concludes that malfunctions derived from Function 30 would not result in vehicle-level hazards. Function 31 is part of the design implementation and may be considered by some analysts to be integral to the TICM.

4.2.2.3 Parallel HEV System Malfunctions

The application of the seven HAZOP study guidewords presented in Section 2.2.1 to each of the 31 parallel HEV ACS/ETC functions listed above results in a list of 224 malfunctions. Each of these malfunctions is assessed to determine if the malfunction could lead to one or more of the potential vehicle-level hazards.

Table 6 provides an example of how malfunctions were derived from one of the series HEV ACS/ETC functions. This process is the same for the parallel HEV. Table 8 shows the number of malfunctions identified for each of the 31 parallel HEV ACS/ETC functions. Appendix B provides the complete results of the HAZOP study.

[17] This function may not apply if the EPS portion of the parallel HEV ACS/ETC is not designed to simulate an idle creep speed.

Table 8. Number of Identified Malfunctions for Each HAZOP Function in the Parallel HEV

Parallel HEV HAZOP Function	Identified Malfunctions
Command torque from the EPS	7
Command torque from the gasoline ICE	7
Combine torque output from the electric motor and gasoline ICE	7
Receive energy from the HV DC bus	7
Deliver current to the electric motor	7
Control the HV RESS contactors	7
Deliver HV energy to the RESS	7
Provide APP to the HEV PCM	7
Return the AP to the at-rest (i.e., undepressed) position within the specified time	9
Provide AP request rate limiting	7
Communicate the delivered torque magnitude and direction to the HEV PCM	7
Return the torque output to the creep value within the specified time [i]	9
Establish the creep torque value [ii]	7
Provide creep state control [ii]	7
Provide BTO control	7
Command throttle position	7
Control throttle position	7
Communicate the throttle position to the ECM/Throttle Actuator Controller	7
Return the throttle to the idle position within the specified time	9
Establish the throttle idle position	7
Provide idle state control	7
Store the APP, electric motor speed, and engine speed torque maps	7
Provide bus capacitance discharge request to the EPS	7
Discharge the bus capacitance	7
Command the gasoline ICE to start/stop	14
Communicate with external vehicle systems	6
Communicate with internal ACS/ETC subsystems	6
Provide diagnostics	6
Provide fault detection and failure mitigation [iii]	6
Store relevant data [iii]	6
Provide electric motor current values [iii]	6

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

4.2.3 Series-Parallel HEV HAZOP Study

4.2.3.1 Series-Parallel HEV HAZOP System Description

The HAZOP study block diagram in Figure 10 identifies the key system elements, internal interfaces, and high-level external interfaces considered in the HAZOP study for the series-parallel HEV.

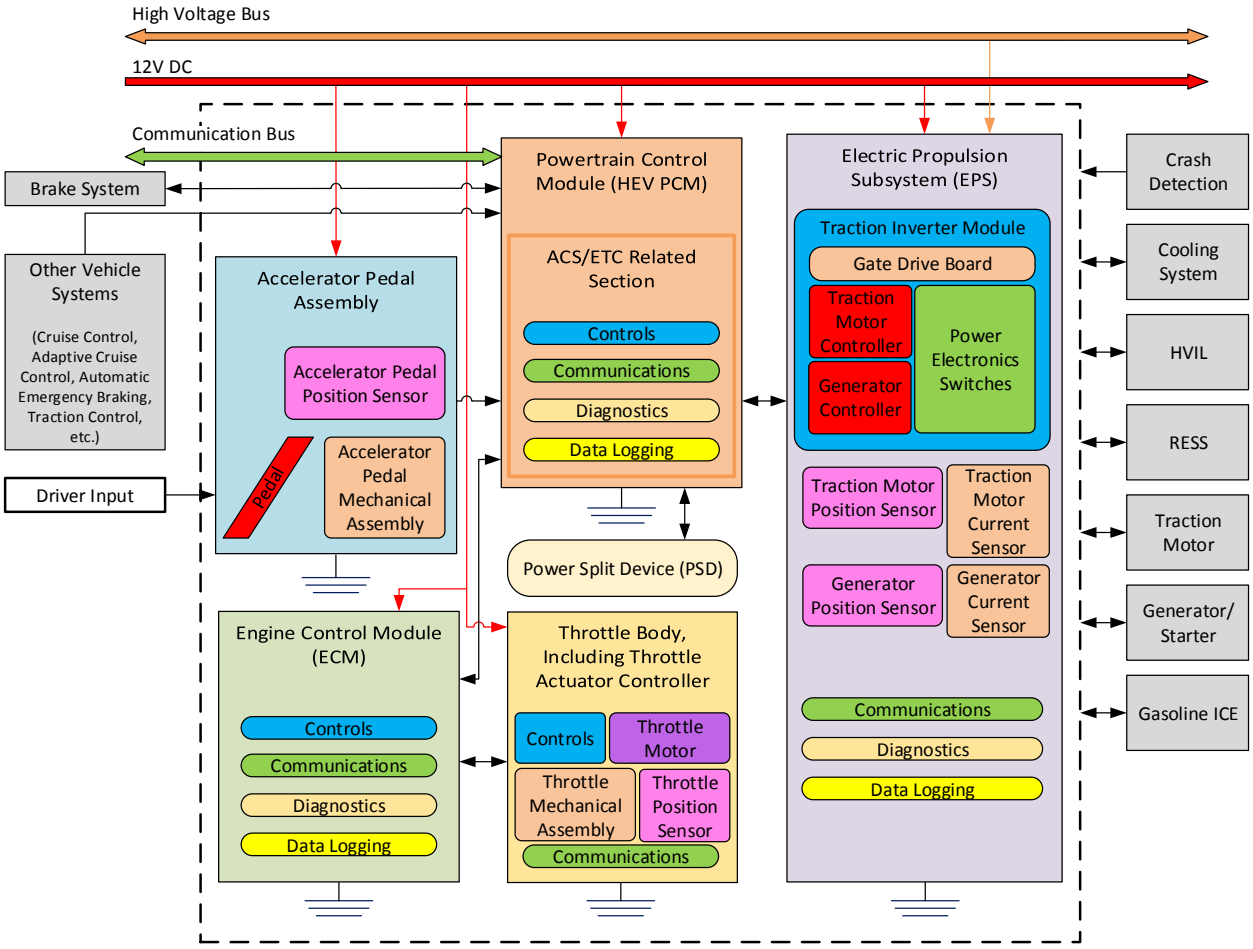


Figure 10. HAZOP Block Diagram of the Series-Parallel HEV ACS/ETC System

The dashed line in Figure 10 defines the boundary of the series-parallel HEV ACS/ETC system considered in the HAZOP study. The series-parallel HEV ACS/ETC contains five main subsystems:

- AP Assembly
- HEV PCM
- EPS
- ECM/Throttle Actuator Controller
- PSD

The HEV PCM determines the net power output required from the ACS/ETC, considering relevant parameters of the vehicle operating conditions, such as vehicle speed, vehicle direction, and torque requests from other vehicle systems. The HEV PCM also responds to requests for HV power generation from the RESS.

The HEV PCM transmits the desired power output from the electric motors to the EPS. The EPS supplies current to the electric motors, which provide propulsion to the drivetrain. In most situations, one of the electric motors operates in generating mode and is not supplying propulsion r to the drivetrain.

The HEV PCM transmits the desired power output from the gasoline ICE to the ECM/Throttle Actuator Controller. The ECM/Throttle Actuator Controller adjusts the throttle valve to regulate the gasoline ICE power output.

In addition to torque requests, the series-parallel HEV ACS/ETC has other interfaces with the following vehicle systems:

- Brake system – regenerative braking, vehicle speed data, etc.
- Cooling system – inverter/converter cooling
- HVIL – high voltage circuit faults
- RESS – HV system status, discharge bus requests, etc.
- Occupant restraint system – crash detection

The series-parallel HEV ACS/ETC is connected to the 12-volt direct current power supply, the HV power supply, and communication bus (e.g., CAN bus).

4.2.3.2 Series-Parallel HEV System Functions

The HAZOP study identifies 35 system functions for the series-parallel HEV ACS/ETC:

1. Command the gasoline ICE to start/stop.
2. Command torque from the EPS for the first electric motor.[18]
3. Receive energy from the HV DC bus.[18]
4. Deliver current to the first electric motor.[18]
5. Command torque from the EPS for the second electric motor.
6. Deliver current to the second electric motor.
7. Control the HV RESS contactors.
8. Command torque partitioning between the gasoline ICE and two electric motors.
9. Deliver HV energy to the RESS.
10. Provide APP to the HEV PCM.
11. Return the AP to the at-rest (i.e., undepressed) position within the specified time. [18]
12. Provide AP request rate limiting. [18]
13. Communicate the delivered torque magnitude and direction to the HEV PCM. [18]
14. Return the torque output to the creep value within the specified time. [18, 19]

[18] This function is common to all three HEV variants.
[19] If the EPS portion of the series-parallel HEV ACS/ETC is not designed to simulate an idle creep speed, the analogous function would be to return the torque output to zero within the specified time.

15. Establish the creep torque value. [18, 20]
16. Provide creep state control. [18, 14]
17. Provide BTO control. [18]
18. Command throttle position.
19. Control throttle position.
20. Communicate the throttle position to the ECM/Throttle Actuator Controller.
21. Return the throttle to the idle position within the specified time.
22. Establish the throttle idle position.
23. Provide idle state control.
24. Split ICE torque between the electric motor in generating mode and vehicle reduction gears.
25. Store the APP, electric motor speed, and engine speed torque maps.
26. Provide bus capacitance discharge request to the EPS. [18]
27. Discharge the bus capacitance. [18]
28. Communicate with external vehicle systems.
29. Communicate with internal ACS/ETC subsystems (i.e., EPS and gasoline ICE).
30. Provide diagnostics. [18]
31. Provide fault detection and failure mitigation. [18]
32. Store relevant data. [18]
33. Command torque from the gasoline ICE.
34. Provide current values for the first electric motor. [18]
35. Provide current values for the second electric motor.

Functions 31, 32, 34, and 35 are shown here for completeness. Function 31 is part of the design to mitigate hazards resulting from other malfunctions in the system. The HAZOP study concludes that malfunctions derived from Function 32 would not result in vehicle-level hazards. Functions 34 and 35 are part of the design implementation and may be considered by some analysts to be integral to the TICM.

4.2.3.3 Series-Parallel HEV System Malfunctions

The application of the seven HAZOP study guidewords presented in Section 2.2.1 to each of the 35 series-parallel HEV ACS/ETC functions listed above results in a list of 252 malfunctions. Each of these malfunctions is assessed to determine if the malfunction could lead to one or more of the potential vehicle-level hazards.

Table 6 provides an example of how malfunctions were derived from one of the series HEV ACS/ETC functions. The process is the same for the series-parallel HEV. Table 9 shows the

[20] This function may not apply if the EPS portion of the series-parallel HEV ACS/ETC is not designed to simulate an idle creep speed.

number of malfunctions identified for each of the 35 series-parallel HEV ACS/ETC functions. Appendix B provides the complete results of the HAZOP study.

Table 9. Number of Identified Malfunctions for Each HAZOP Function in the Series-Parallel HEV

Series-Parallel HEV HAZOP Function	Identified Malfunctions
Command the gasoline ICE to start/stop	14
Command torque from the EPS for the first electric motor	7
Receive energy from the HV DC bus	7
Deliver current to the first electric motor	7
Command torque from the EPS for the second electric motor	7
Deliver current to the second electric motor	7
Control the HV RESS contactors	7
Command torque partitioning between the gasoline ICE and the two electric motors	7
Deliver HV energy to the RESS	7
Provide APP to the HEV PCM	7
Return the AP to the at-rest (i.e., undepressed) position within the specified time	9
Provide AP request rate limiting	7
Communicate the delivered torque magnitude and direction to the HEV PCM	7
Return the torque output to the creep value within the specified time [i]	9
Establish the creep torque value [ii]	7
Provide creep state control [ii]	7
Provide BTO control	7
Command throttle position	7
Control throttle position	7
Communicate the throttle position to the ECM/Throttle Actuator Controller	7
Return the throttle to the idle position within the specified time	9
Establish the throttle idle position	7
Provide idle state control	7
Split ICE torque between the electric motor in generating mode and vehicle reduction gears	8
Store the APP, electric motor speed, and engine speed torque maps	7
Provide bus capacitance discharge request to the EPS	7
Discharge the bus capacitance	7
Communicate with external vehicle systems	6
Communicate with internal ACS/ETC subsystems	6
Provide diagnostics	6
Provide fault detection and failure mitigation [iii]	6
Store relevant data [iii]	6
Command torque from the gasoline ICE	7
Provide current values for the first electric motor [iii]	6
Provide current values for the second electric motor [iii]	6

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

4.3 Systems-Theoretic Process Analysis: Step 1

4.3.1 Series HEV STPA Step 1 Results

4.3.1.1 Series HEV Detailed Control Structure Diagram

Figure 11 illustrates the detailed control structure diagram used in the STPA method to represent a generic series HEV ACS/ETC system and its interfacing systems and components. The series HEV ACS/ETC components are delineated by the dashed line. The 12-volt power supply is only shown on this diagram as an effect of the driver's action on the ignition key. However, the impact of the 12-volt power supply on the system is considered in detail as part of STPA Step 2.

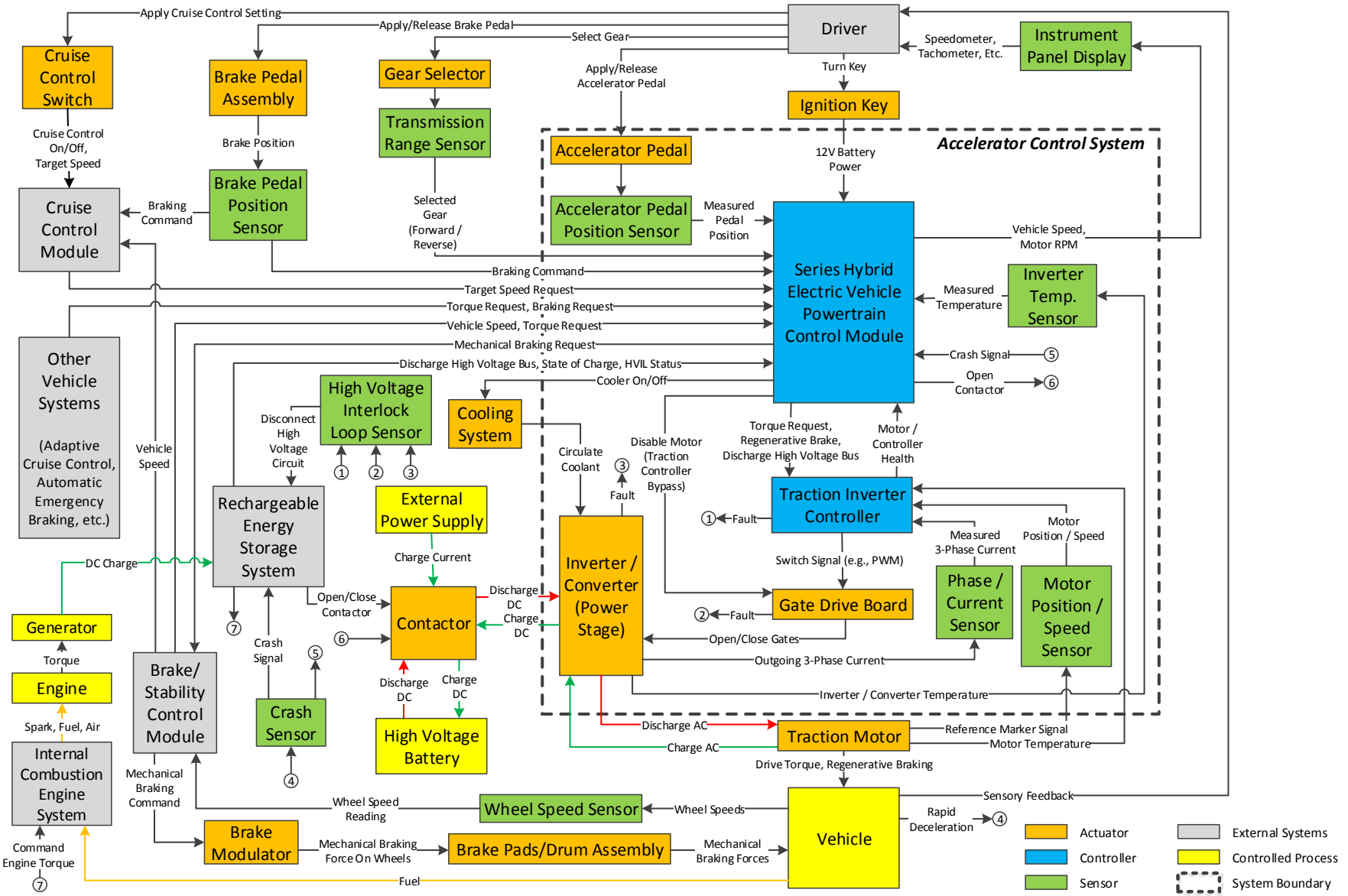


Figure 11. Detailed Control Structure Diagram for the Series HEV ACS/ETC System

4.3.1.2 Series HEV Vehicle-Level Losses and Initial Hazards

STPA begins by identifying specific losses that the study is trying to prevent. In the STPA method, these losses result from a combination of a hazardous state along with a worst-case set of environmental conditions [5]. The vehicle-level losses relevant to the series HEV ACS/ETC are:

- A vehicle crash, and
- Electrocution.

An initial list of vehicle-level hazards is generated based on a literature search and engineering experiences. As the analyst identifies UCAs as part of STPA Step 1, the initial hazard list may be refined. Section 4.3.1.3 and Section 4.3.1.4 provide the details of this process. Then, the hazards generated from both the HAZOP study and STPA are synthesized to produce the hazard list shown in Table 4.

4.3.1.3 Series HEV Control Actions and Context Variables

STPA Step 1 studies ways in which control actions in the system may become unsafe, leading to vehicle-level hazards. This study identifies 11 control actions issued by the series HEV PCM and two control actions issued by the TICM related to the series HEV ACS/ETC function. The 11 HEV PCM control actions include the following:

1. Two control actions are related to mode switching.[21] These control actions are internal to the HEV PCM and result in a change in the HEV PCM operating state.
    i. **Enter BTO mode** – the HEV PCM issues this control action to enter an operating state that causes the driver's request for braking to override the AP command.
    ii. **Enter normal mode** – the HEV PCM issues this control action to resume normal series HEV ACS/ETC operation (i.e., exit BTO mode).

    The context variable states used to analyze the mode switching control actions are listed in Table 10. The vehicle speed states in Table 10 are based on the maximum speed above which BTO must engage. Manufacturers may elect to have lower vehicle speed threshold values.

Table 10. Series HEV STPA Context Variables for Mode Switching

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

[21] These control actions are common to all three HEV ACS/ETC architectures.

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

    These control actions assume that the electric motor torque output is in the correct direction. The context variable states used to analyze the control actions related to the electric motor torque output are listed in Table 11.

Table 11. Series HEV STPA Context Variables for Commanding Torque (Magnitude)

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

3. Two control actions are used to controlling the direction of the torque supplied by the electric motor.[22] As described in Section 3.4.1, the series HEV electric motor is capable of directly supplying torque in both the forward and reverse directions. These control actions are issued to the TICM, which controls the current flow to the electric motor to provide the correct direction of rotation.
    i. **Provide torque in the forward direction** – the HEV PCM issues this control action to provide torque from the electric motor that propels the vehicle in the forward direction.
    ii. **Provide torque in the reverse direction** – the HEV PCM issues this control action to provide torque from the electric motor that propels the vehicle in the reverse direction.

[22] These control actions are common to all three HEV ACS/ETC architectures.

These control actions assume that the magnitude of the electric motor torque output is correct based on the inputs from the driver and other vehicle systems. The context variable states used to analyze the control actions related to the direction of the torque output from the electric motor are listed in Table 12.

Table 12. Series HEV STPA Context Variables for the Commanding Torque (Direction)

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

4. Two control actions are related to requesting cooling for the inverter/converter from the vehicle's cooling system, based on the inverter temperature.[23] The HEV PCM issues these control actions to maintain the inverter/converter within an allowable temperature range.
    i. **Turn cooling on** – the HEV PCM issues this control action to request cooling for the inverter/converter from the vehicle's cooling system. For example, this request may cause the vehicle cooling system to activate a cooling pump.
    ii. **Turn cooling off** – the HEV PCM issues this control action to stop the cooling supply to the inverter/converter.

    The specific threshold temperature value for requesting cooling depends on the design of the cooling system as well as the inverter/converter. Therefore, this analysis simply refers to a threshold value and it is up to manufacturers to specify this value for their specific design. Table 13 lists the context variable states used to analyze the request for inverter/converter cooling control action.

    Table 13. Series HEV STPA Context Variables for Inverter/Converter Cooling

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

5. One control action is related to discharging the HV bus in response to a request from the RESS.[23] The logic for determining when to discharge the HV bus resides in the RESS control module; the HEV PCM simply executes this request. The command is issued by the HEV PCM to the TICM, which controls the current flow in the inverter/converter to discharge the HV bus.

[23] These control actions are common to all three HEV ACS/ETC architectures.

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

Table 14. Series HEV STPA Context Variables for Discharging the HV Bus

Context Variable	Context Variable States
RESS Request to Discharge HV Bus	Yes
	No

6. One control action is related to opening the contactor for the HV power supply.[24] Depending on the vehicle design, this control action may be issued by the HEV PCM or may be part of the RESS.
   i. **Open the contactor** – the HEV PCM issues this control action to disconnect the RESS from the series HEV ACS/ETC in the event of a vehicle crash or when the HVIL is violated.

Table 15. Series HEV STPA Context Variables for Opening the Contactor

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

7. One control action is related to requesting DC power from the RESS.[24] This enables the RESS to arbitrate the HV power demands from the series HEV ACS/ETC with high voltage power requests from other vehicle systems.
   i. **Request DC Power** – the HEV PCM issues this control action to inform the RESS of the power required to meet the driver's torque request.

Table 16. Series HEV STPA Context Variables for Requesting DC Power

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

There are two control actions issued by the TICM:

1. Two control actions are related to controlling the current supply to the electric motor.[24] The TICM issues these control actions to the gate drive board, which operates the transistors in the inverter/converter to regulate the HV power supply to flow to the electric motor.

[24] These control actions are common to all three HEV ACS/ETC architectures.

i. **Increase current supply to the electric motor** – the TICM issues this control action to increase the current supply to the electric motor, resulting in an increase in torque output.

ii. **Decrease current supply to the electric motor** – the TICM issues this control action to decrease the current supply to the electric motor, resulting in a decrease in torque output.

Table 17. Series HEV STPA Context Variables for Regulating Current Supply

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

4.3.1.4 Series HEV Unsafe Control Actions

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

The analysts then assess whether the control action would result in a vehicle-level hazard, given the particular combination of context variable states. Table 18 shows how this is done for one of the control actions – "Enter BTO Mode." Appendix C contains all of the UCA assessment tables for the 13 control actions studied.

Table 18. 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		H4	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Not Pressed	Not Pressed	≥10 MPH		H4	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		H4	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Not Pressed	≥10 MPH		H4	N/A	N/A	N/A	N/A	Hazardous if Provided	Hazardous if Provided	Hazardous if Provided
Pressed	Pressed	<10 MPH		H4	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	H4	H1

Vehicle-Level Hazards:

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

Each cell in Table 18 represents a UCA. For example, the last row and fourth column of the table may generate the following UCA:

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

  This may result in Uncontrolled Vehicle Propulsion.

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

Overall, STPA Step 1 identifies a total of 95 UCAs for the generic series HEV ACS/ETC system studied. The breakdown of these UCAs by control action is provided in Table 19.

Table 19. Number of Identified UCAs for Each Series HEV STPA Control Action

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

Appendix D presents a complete list of the UCAs identified in STPA Step 1. Table 20 and Table 21 show examples of UCAs for the HEV PCM and their associated vehicle-level hazards. Table 22 shows an example of a UCA for the TICM and its associated vehicle-level hazard.

Table 20. Example STPA UCA Statement for Electric Motor Torque Control (Magnitude)

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

Table 21. Example STPA UCA Statement for the Direction of Torque Output Control

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

Table 22. Example STPA UCA Statement for Electric Motor Current Control

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

4.3.2 Parallel HEV STPA Step 1 Results

4.3.2.1 Parallel HEV Detailed Control Structure Diagram

Figure 11 illustrates the detailed control structure diagram used in the STPA method to represent a generic parallel HEV ACS/ETC system and its interfacing systems and components. The parallel HEV ACS/ETC components are delineated by the dashed line.

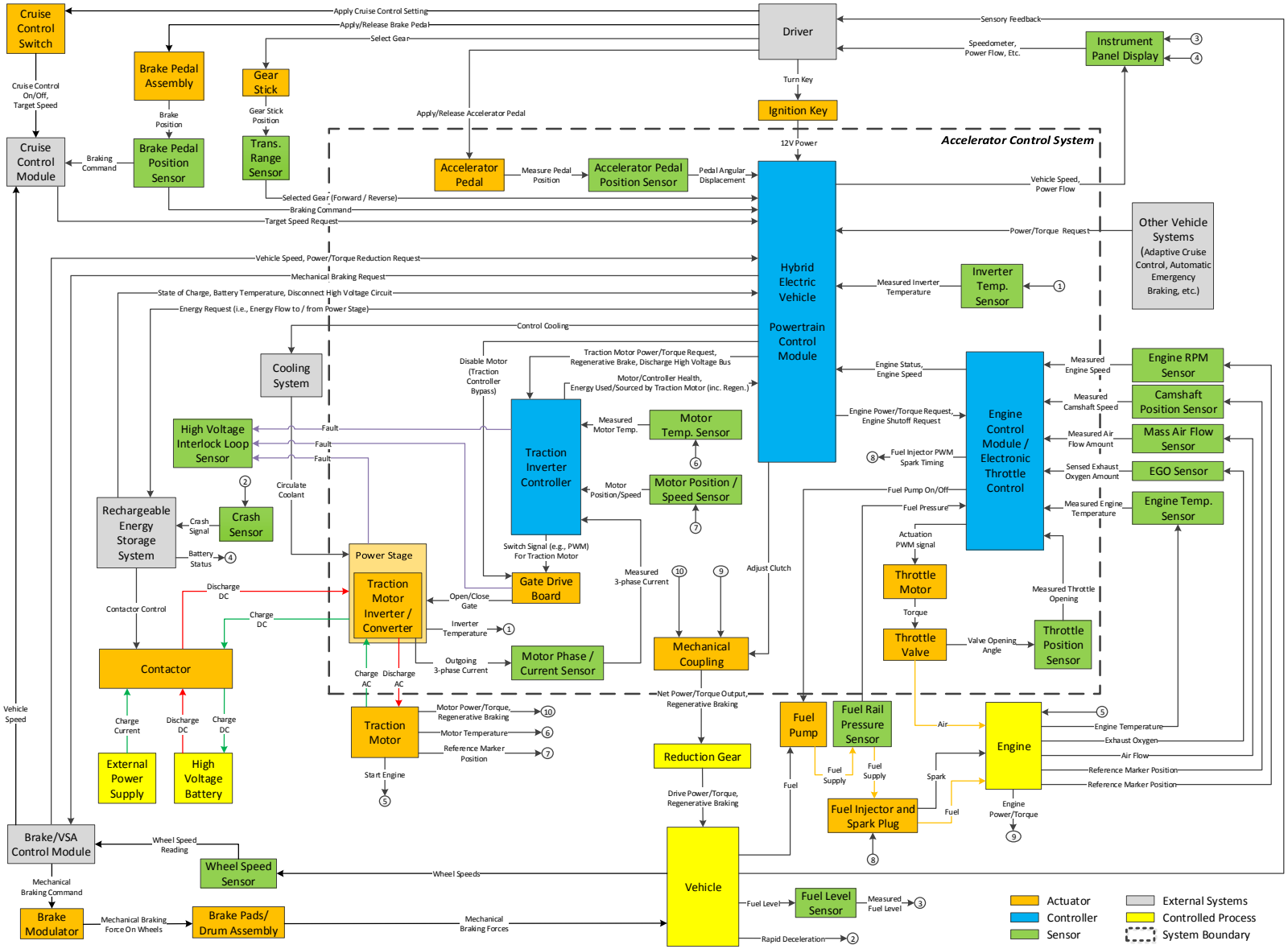


Figure 12. Detailed Control Structure Diagram for the Parallel HEV ACS/ETC System

4.3.2.2 Parallel HEV Vehicle-Level Losses and Initial Hazards

Identification of the parallel HEV vehicle-level losses and initial hazards follows the same procedure outlined in Section 4.3.1.2. The vehicle-level losses relevant to the parallel HEV ACS/ETC are:

- A vehicle crash,
- Electrocution, and
- A battery fire/explosion.

4.3.2.3 Parallel HEV Control Actions and Context Variables

This study identifies a total of 17 control actions related to the parallel HEV ACS/ETC function. Thirteen of the control actions are issued by the parallel HEV PCM, two control actions are issued by the ECM/Throttle Actuator Controller, and two control actions are issued by the TICM.

The 13 HEV PCM control actions include nine control actions which are identical to control actions issued by the HEV PCM in the series HEV and were assessed using the same context variables presented in Section 4.3.1.3. These control actions include

- Enter BTO mode (see Table 10)
- Enter Normal mode (see Table 10)
- Provide torque in the forward direction (see Table 12)
- Provide torque in the reverse direction (see Table 12)
- Turn cooling on (see Table 13)
- Turn cooling off (see Table 13)
- Discharge the HV bus (see Table 14)
- Open the contactor (see Table 15)
- Request HV DC power (see Table 16)

The following control actions are control actions related to the parallel HEV ACS/ETC that are not in the series HEV ACS/ETC:

1. Two control actions are related to controlling the magnitude of the net power output from the ACS/ETC.[25] These control actions are internal to the HEV PCM and are used to determine the amount of power required from each of the propulsion subsystems.
    iii. **Increase the net power output** – the HEV PCM issues this control action to initiate a propulsion strategy that results in more power output from the ACS/ETC relative to the current operating point.

[25] These control actions are common to the parallel HEV and series-parallel HEV architectures.

iv. **Decrease the electric motor torque** – the HEV PCM issues this control action to initiate a propulsion strategy that results in less power output from the ACS/ETC relative to the current operating point.

The context variable states used to analyze the mode switching control actions are listed in Table 23.

Table 23. Parallel HEV STPA Context Variables for Commanding the Net Power Output

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
HEV PCM Operating Mode	BTO mode
	Normal mode
	BTO transitioning to normal mode
	Normal mode transitioning to BTO mode
Torque Requests from Other Vehicle Systems	None
	Reduce torque
	Increase torque
	Both reduce and increase torque

2. One control action is related to allocating power between the two propulsion subsystems. The HEV PCM issues commands to each of the propulsion subsystems based on the power assignments.
    i. **Assign power to electric motor and engine** – the HEV PCM issues power requests to the TICM and ECM/Throttle Actuator Controller through this control action to produce the desired net power output.

    The context variables for allocating power between the propulsion subsystems are design specific. Therefore, this control action is assessed only using the six guide words presented in Section 2.2.3.

3. One control action is related to adjusting the mechanical coupling in designs where the mechanical coupling may have multiple states. The HEV PCM adjusts the mechanical coupling to connect the gasoline ICE and electric motor to the drivetrain.
    i. **Adjust mechanical coupling** – the HEV PCM issues this control action to clutches or other mechanisms used to connect the propulsion subsystems to the drivetrain.

    No relevant context variables were identified for this control action. Therefore, this control action is assessed only using the six guide words presented in Section 2.2.3.

There are two control actions issued by the ECM/Throttle Actuator Controller:

1. Two control actions are related to controlling the throttle valve position.[26] The ECM/Throttle Actuator Controller issues these control actions to the throttle motor, which adjusts the throttle valve position.
    i. **Increase throttle opening** – the ECM/Throttle Actuator Controller increases the throttle valve opening to increase the power output from the gasoline ICE.
    ii. **Decrease throttle opening** – the ECM/Throttle Actuator Controller decreases the throttle valve opening to decrease the power output from the gasoline ICE.

Table 24. Parallel HEV STPA Context Variables for Adjusting the Throttle Position

Context Variable	Context Variable States
HEV PCM Power Request	Increase power
	Decrease power

There are two control actions issued by the TICM that are identical to the control actions for the series HEV. These control actions were assessed using the same context variables presented in Section 4.3.1.3. These control actions include:

- Increase current supply to the electric motor (see Table 17)
- Decrease current supply to the electric motor (see Table 17)

4.3.2.4 Parallel HEV Unsafe Control Actions

The method for deriving UCAs from the control actions is identical to the process outlined in Section 4.3.1.4. Overall, STPA Step 1 identifies a total of 123 UCAs for the generic parallel HEV ACS/ETC system studied. The breakdown of these UCAs by control action is provided in Table 25. Appendix D presents a complete list of the UCAs identified in STPA Step 1.

Table 25. Number of Identified UCAs for Each Parallel HEV STPA Control Action

STPA Control Action	Identified UCAs
Enter BTO Mode	6
Enter Normal Mode	4
Increase the Net Power Delivered to Wheels	12
Decrease the Net Power Delivered to Wheels	26
Provide Torque in the Forward Direction	4
Provide Torque in the Reverse Direction	4
Turn Cooling On	5
Turn Cooling Off	2
Discharge the HV Bus	5
Open Contactor	8
Request DC Power	5
Assign Torque to Electric Motor and Engine	6

[26] These control actions are common to the parallel HEV and series-parallel HEV architectures.

STPA Control Action	Identified UCAs
Adjust Mechanical Coupling	4
Increase Throttle Opening	8
Decrease Throttle Opening	8
Increase Current Supply to the Electric Motor	8
Decrease Current Supply to the Electric Motor	8

4.3.3 Series-Parallel HEV STPA Step 1 Results

4.3.3.1 Series-Parallel HEV Detailed Control Structure Diagram

Figure 13 illustrates the detailed control structure diagram used in the STPA method to represent a generic series-parallel HEV ACS/ETC system and its interfacing systems and components. The series-parallel HEV ACS/ETC components are delineated by the dashed line.

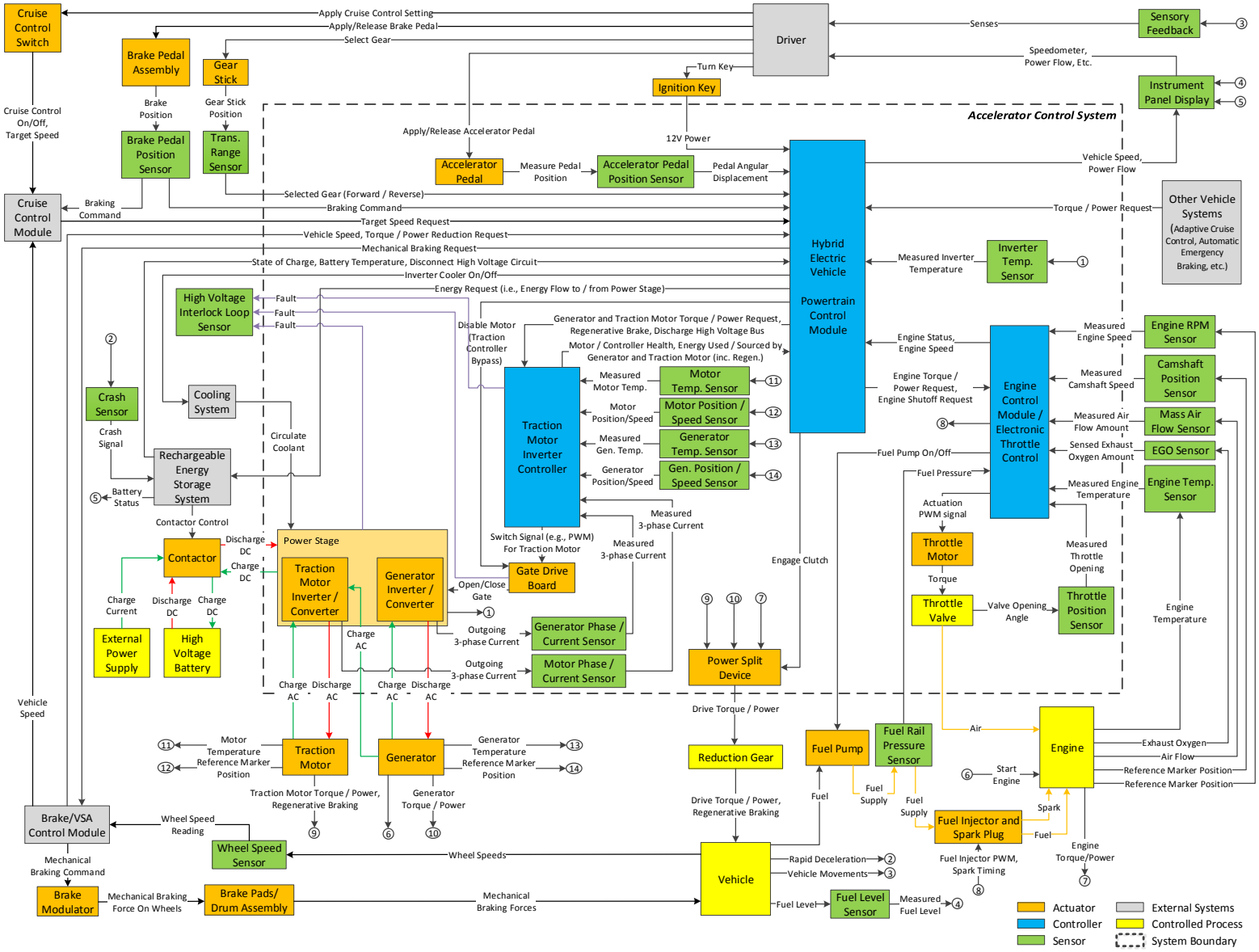


Figure 13. Detailed Control Structure Diagram for the Series-Parallel HEV ACS/ETC System

4.3.3.2 Series-Parallel HEV Vehicle-Level Losses and Initial Hazards

The vehicle-level losses relevant to the series-parallel HEV are the same as the parallel HEV, and include:

- A vehicle crash,
- Electrocution, and
- A battery fire/explosion.

4.3.3.3 Series-Parallel HEV Control Actions and Context Variables

This study identifies a total of 19 control actions related to the series-parallel HEV ACS/ETC function. Thirteen of the control actions are issued by the series-parallel HEV PCM, two control actions are issued by the ECM/Throttle Actuator Controller, and four control actions are issued by the TICM.

Nine of the control actions issued by the HEV PCM are identical to control actions issued by both the series HEV PCM and parallel HEV PCM. These control actions were assessed using the same context variables presented in Section 4.3.1.3. These control actions include:

- Enter BTO mode (see Table 10)
- Enter Normal mode (see Table 10)
- Provide torque in the forward direction (see Table 12)
- Provide torque in the reverse direction (see Table 12)
- Turn cooling on (see Table 13)
- Turn cooling off (see Table 13)
- Discharge the HV bus (see Table 14)
- Open the contactor (see Table 15)
- Request HV DC power (see Table 16)

In addition, two control actions issued by the HEV PCM are identical to control actions issued by the parallel HEV PCM. These control actions were assessed using the same context variables presented in Section 4.3.2.3. These control actions include:

- Increase net power delivered to the wheels (see Table 23)
- Decrease net power delivered to the wheels (see Table 23)

The following control actions are control actions unique to the series-parallel HEV ACS/ETC:

1. One control action is related to allocating power between the two propulsion subsystems. The HEV PCM issues commands to each of the propulsion subsystems based on the power assignments.

i. **Assign power to both electric motors and the engine** – the HEV PCM issues power requests to the TICM and ECM/Throttle Actuator Controller through this control action to produce the desired net power output.

The context variables for allocating power between the propulsion subsystems are design specific. Therefore, this control action is assessed only using the six guide words presented in Section 2.2.3.

2. One control action is related to adjusting the configuration of the PSD in designs where the mechanical coupling may have multiple states. The HEV PCM adjusts the PSD to control how the power produced by the gasoline ICE is allocated between the electric motor in generating mode and the drivetrain.
    i. **Adjust PSD** – the HEV PCM issues this control action to clutches or other mechanisms used to control the PSD configuration.

    No relevant context variables were identified for this control action. Therefore, this control action is assessed only using the six guide words presented in Section 2.2.3.

There are two control actions issued by the ECM/Throttle Actuator Controller that are identical to the control actions issued by the ECM/Throttle Actuator Controller for the parallel HEV ACS/ETC. These control actions were assessed using the same context variables presented in Section 4.3.2.3. These control actions include:

- Increase throttle opening (see Table 24)
- Decrease throttle opening (see Table 24)

There are four control actions issued by the TICM in the series-parallel HEV ACS/ETC. Two of these control actions are identical to the control actions issued by the TICM for both the series HEV and parallel HEV. These control actions were assessed using the same context variables presented in Section 4.3.1.3. These control actions include:

- Increase current supply to the first electric motor (see Table 17)
- Decrease current supply to the first electric motor (see Table 17)

The following control actions are control actions unique to the series-parallel HEV ACS/ETC:

1. Two control actions are related to controlling the current supply to the second electric motor. The TICM issues these control actions to the gate drive board, which operates the transistors in the inverter/converter to regulate the HV power supply to flow to the second electric motor.
    i. **Increase current supply to the second electric motor (when supplying propulsion or starting the engine)**[27] – the TICM issues this control action to

[27] This control action is only relevant when the generator is used to supply propulsion or start the gasoline ICE. Operation of the second electric motor in generating mode falls outside the scope of the ACS/ETC.

increase the current supply to the second electric motor, resulting in an increase in power output.

ii. **Decrease current supply to the second electric motor (when supplying propulsion or starting the engine)**[28] – the TICM issues this control action to decrease the current supply to the second electric motor, resulting in a decrease in power output.

Table 26. Series-Parallel HEV STPA Context Variables for Regulating Current Supply to the Second Electric Motor

Context Variable	Context Variable States
HEV PCM Power Request	Increase power
	Decrease power

4.3.3.4 Series-Parallel HEV Unsafe Control Actions

The method for deriving UCAs from the control actions is identical to the process outlined in Section 4.3.1.4. Overall, STPA Step 1 identifies a total of 140 UCAs for the generic series-parallel HEV ACS/ETC system studied. The breakdown of these UCAs by control action is provided in Table 25. Appendix D presents a complete list of the UCAs identified in STPA Step 1.

Table 27. Number of Identified UCAs for Each Series-Parallel HEV STPA Control Action

STPA Control Action	Identified UCAs
Enter BTO Mode	6
Enter Normal Mode	4
Increase the Net Power Delivered to Wheels	12
Decrease the Net Power Delivered to Wheels	26
Provide Torque in the Forward Direction	4
Provide Torque in the Reverse Direction	4
Turn Cooling On	5
Turn Cooling Off	2
Discharge the HV Bus	5
Open Contactor	8
Request DC Power	5
Assign Torque to Both Electric Motors and the Engine	6
Adjust PSD	4
Increase Throttle Opening	8
Decrease Throttle Opening	8
Increase Current Supply to the First Electric Motor	8
Decrease Current Supply to the First Electric Motor	8
Increase Current Supply to the Second Electric Motor	8
Decrease Current Supply to the Second Electric Motor	8

[28] This control action is only relevant when the second electric motor is used to supply propulsion or start the gasoline ICE.

5 RISK ASSESSMENT

This study follows the risk assessment approach in ISO 26262. The assessment derives the ASIL for each of the eight 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 of the situation and the vehicle in the potential crash scenario.
    e. Look up the ASIL per ISO 26262 based on the exposure, severity, and controllability.
3. Assign the worst-case ASIL to the hazard.

5.1.1 Vehicle Operational Situations

Operational Situations are scenarios that can occur during a vehicle's life (Part 1 Clause 1.83 in ISO 26262 [2]). This study generates 77 vehicle operational situations that are provided in Appendix E. Sixty-nine of these 77 vehicle operational situations are common to all three HEV architectures. The other eight vehicle operational situations apply to only the parallel and series-parallel HEV architectures.

Below are two examples of vehicle operational situations that are common to all three HEV architectures:

- Driving at high speeds (100 Kilometers per Hour (KPH) < V < 130 KPH), heavy traffic, good visibility, and good road conditions.

- Driving in the city with heavy traffic and pedestrians present, stop-and-go driving above 16 KPH, low visibility, and slippery road conditions.

Seventy-four of the 77 operational situations are described by ten variables and their states as shown in Table 28. These variables and their states are identified following current industry practices.

Table 28. Variables and States for Description of Vehicle Operational Situations

Vehicle Speed	Very high speed (V>130 KPH)	**Rail Road Track**	Near a rail road track
	High speed (100 KPH<V≤130 KPH)		Over a rail road track
	Medium speed (40 KPH<V≤100 KPH)		Not near or over a rail road track
	Inside city (16 KPH<V≤40 KPH)	**Road Condition**	Slippery
	Inside city very low speed (V≤16 KPH)		Good
	Parking lot or drive way (V=0)	**Driving Maneuver**	Stop and go (applicable only at low speed)
	In a traffic stop (V=0)		Overtaking another vehicle
Traffic	Heavy		Evasive maneuver deviating from desired path
	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

The hazard “Potential Electric Shock” does not result from the same operating scenarios as the vehicle motion related hazards. Therefore, the variables in Table 28 were not used to determine the ASIL for “Potential Electric Shock”. Instead, three additional operating scenarios were developed to describe this hazard:

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

5.1.2 Automotive Safety Integrity Level Assessment

ISO 26262 assesses the ASIL of identified hazards according to the severity, exposure, and controllability (Part 3 in ISO 26262 [2]).

Exposure is defined as the state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis (Part 1 Clause 1.37 in ISO 26262 [2]). Table 29 is directly copied from ISO 26262 Part 3 Table 2.

Table 29. Exposure Assessment

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

E = Exposure

Severity is defined as the estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation (Part 1 Clause 1.120 in ISO 26262 [2]). Table 30 is directly quoted from ISO 26262 Part 3 Table 1.

Table 30. Severity Assessment

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

S = Severity

Table 31 is an acceptable approach to assess severity shown in ISO 26262 [2] (Part 3 Clause 7.4.3.2 and Annex B Table B.1).

Table 31. 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

S = Severity
AIS = Abbreviated Injury Scale

ISO 26262 defines controllability as the "ability to avoid a specified harm or damage through the timely reactions of the persons[29] involved, possibly with support from external measures" (Part 1

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

Clause 1.19 in ISO 26262 [2]). Table 32 is ISO 26262's approach to assessing controllability (Table 3 in Part 3 in ISO 26262 [2]). Table 33 shows how ASIL is assessed based on exposures, severity, and controllability (Table 4 in Part 3 of ISO 26262 [2]).

Table 32. Controllability Assessment

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

C = Controllability

Table 33. 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
S = Severity
E = Exposure
C = Controllability

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

Example 1:

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

Example 2:

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

Appendix F contains the full ASIL assessment table.

5.2 Automotive Safety Integrity Level Assignment for Each Hazard

The ASIL assessment for each operational situation forms the basis for the ASIL assignment to each of the seven vehicle-level hazards. ISO 26262 requires the most severe ASIL be chosen for each hazard. Table 34 shows the resulting ASIL values for each hazard.

Table 34. Vehicle-Level Hazards and Corresponding ASIL

	Hazard	ASIL	S HEV	P HEV	S-P HEV
H1	Potential uncontrolled vehicle propulsion	D	●	●	●
H1.a	Potential uncontrolled vehicle propulsion when the vehicle speed is zero	B[i]	●	●	●
H2	Potential insufficient vehicle propulsion	C[ii]	●	●	●
H3	Potential vehicle movement in an unintended direction	C	●	●	●
H4	Potential propulsion power reduction/loss or vehicle stalling	D	●	●	●
H5	Potential insufficient vehicle deceleration	C[ii]	●	●	●
H6	Potentially allowing driver's command to override active safety systems[iv]	D[iii]	●	●	●
H7	Potential electric shock	B	●	●	●
H8	Potential RESS thermal event	C		●	●

S HEV = Series HEV
P HEV = Parallel HEV
S-P HEV = Series-Parallel HEV

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 BP is released.*
ii. *The ASIL assessment for this hazard varied among safety analysts in the absence of objective data. This study finds that objective data are not readily available for the assessment of the three dimensions used to determine the ASIL--severity, exposure, and controllability.*
iii. *The effects of H6 are contained in H1, H2, H4, and H5. Therefore, H6 takes on the most severe ASIL value among those four hazards.*
iv. *This hazard may not apply in ACS/ETC systems designed to give driver's command priority over all active safety systems.*

6 VEHICLE-LEVEL SAFETY GOALS

Based on the hazard analysis and risk assessment, the safety goals (i.e., vehicle-level safety requirements) are established as listed in Table 35. Each safety goal (SG) corresponds to the potential hazards in Table 34.

Table 35. Safety Goals with ASIL

ID	Safety Goals	ASIL	S HEV	P HEV	S-P HEV
SG 1	Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than To-Be-Determined (TBD) m/s^2 for a period greater than TBD seconds is to be mitigated in accordance with the identified ASIL.	D	●	●	●
SG 1a	Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 with zero speed at start is to be mitigated in accordance with the identified ASIL.	B	●	●	●
SG 2	Potential insufficient vehicle propulsion[i] is to be mitigated in accordance with the identified ASIL.	C[ii]	●	●	●
SG 3	Potential vehicle movement in the wrong direction is to be mitigated in accordance with the identified ASIL.	C	●	●	●
SG 4	Potential propulsion power loss/reduction resulting in vehicle deceleration greater than TBD m/s^2 is to be mitigated in accordance with the identified ASIL.	D	●	●	●
SG 5	Potential insufficient vehicle deceleration[i] is to be mitigated in accordance with the identified ASIL.	C[ii]	●	●	●
SG 6	The ACS/ETC control algorithm is to choose the torque/power command that has the highest priority for safety in accordance with the identified ASIL.	D	●	●	●
SG 7	Potential electric shock is to be mitigated in accordance with the identified ASIL.	B	●	●	●
SG 8	Potential RESS thermal events are to be prevented.	C		●	●

S HEV = Series HEV
P HEV = Parallel HEV
S-P HEV = Series-Parallel HEV

i. *Insufficient vehicle propulsion/deceleration is defined as the vehicle deviating from the correctly functioning speed increase/decrease profile under any operating conditions by more than TBD sigma. These hazards specifically relate to speed increases or decreases that result from the driver increasing or decreasing the angular position of the AP.*
ii. *The ASIL assessment for the hazard associated with this safety goal varied among safety analysts in the absence of objective data. This study finds that objective data are not readily available for the assessment of the three dimensions used to determine the ASIL--severity, exposure, and controllability.*

7 SAFETY ANALYSIS

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

7.1 Functional Failure Modes and Effects Analysis

7.1.1 Series HEV Functional FMEA

This study identifies seven vehicle-level hazards for the series HEV ACS/ETC. The Functional FMEA was carried out for hazards H1, H1a, H2, H3, H4, H5, and H7 (Table 4). Because the consequences of H6 are captured in hazards H1, H2, H4, and H5, a separate Functional FMEA was not performed for H6.

Overall, the Functional FMEA covers four series HEV ACS/ETC subsystems and six interfacing systems. The Functional FMEA identifies 30 failure modes and 90 potential causes of failures. Table 36 shows the number of identified causes for each of the failure modes.

Table 36. Number of Identified Faults by Failure Mode for the Series HEV

System / Subsystem	Failure Mode	Identified Faults
AP assembly	APP value interpreted higher than actual	19
	APP value interpreted lower than actual	19
	AP is not returned to idle position correctly	1[i]
	APP communicates with HEV PCM incorrectly	19
HEV PCM	Commands a larger amount of torque than requested by the driver	20
	Commands a smaller amount of torque than requested by the driver	20
	Commands torque in the wrong direction	20
	Misinterprets the APPS input	20
	APP-Torque map corrupted	18
	APP rate limiting fault (over-limiting/under-limiting)	20
	Incorrectly establishes idle torque [ii]	20
	BTO control fault	5
	Miscommunicates with internal subsystems	4
	Miscommunicates with external systems	3
	Fails to command a discharge of the HV bus capacitance	19
	Diagnostics fault	1[iii]
EPS	Delivers more torque than requested by the HEV PCM	28
	Delivers less torque than requested by the HEV PCM	30
	Delivers torque in the opposite direction of the HEV PCM command	28
	Fails to maintain idle torque [ii]	30
	Does not discharge the HV bus capacitance	21
Motor speed sensor	Provides incorrect motor speed to HEV PCM	1
Vehicle speed sensor	Provides incorrect vehicle speed to HEV PCM	1
Vehicle direction sensor	Provides incorrect vehicle direction to HEV PCM	1
BPPS	Provides incorrect input to HEV PCM	1
Other interfacing vehicle systems	Provides request for incorrect (more) propulsion torque	1
	Provides request for incorrect (less) propulsion torque	1
RESS controller	Communicates incorrect state of charge to HEV PCM	1
	Incorrectly communicates HV bus capacitance discharge request to HEV PCM	1

System / Subsystem	Failure Mode	Identified Faults
Vehicle communication system (e.g., CAN bus)	Communication messages corrupted during transfer within the series HEV ACS/ETC, or between the series HEV ACS/ETC and interfacing vehicle systems	1
Note: Some faults may potentially result in multiple failure modes. [i] These faults are mechanical in nature and are outside the scope of ISO 26262. [ii] This failure mode only applies to designs where the HEV PCM simulates an idle creep speed. [iii] This failure mode is only considered as part of a multiple point failure analysis.		

The Functional FMEA also identified the possibility of faults within interfacing vehicle systems. However, as described in Section 3.2, other vehicle systems are assumed to be operating correctly. Therefore, these faults are not included in Table 36.

Table 37 shows a few examples of the Functional FMEA. Appendix G provides the complete Functional FMEA results.

Table 37. Sample Functional FMEA for Potential Uncontrolled Vehicle Propulsion (H1) (Not Complete)

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

7.1.2 Parallel HEV Functional FMEA

This study identifies eight vehicle-level hazards for the parallel HEV ACS/ETC. The Functional FMEA was carried out for hazards H1, H1a, H2, H3, H4, H5, H7, and H8 (Table 4). Because the consequences of H6 are captured in hazards H1, H2, H4, and H5, a separate Functional FMEA was not performed for H6.

Overall, the Functional FMEA covers five parallel HEV ACS/ETC subsystems and seven interfacing systems. The Functional FMEA identifies 44 failure modes and 129 potential causes of failures. Table 38 shows the number of identified causes for each of the failure modes.

Table 38. Number of Identified Faults by Failure Mode for the Parallel HEV

System / Subsystem	Failure Mode	Identified Faults
AP Assembly	APP value interpreted higher than actual	19
	APP value interpreted lower than actual	19
	AP is not returned to idle position correctly	1[i]
	APP communicates with HEV PCM incorrectly	19
HEV PCM	Commands a larger amount of torque than requested by the driver	20
	Commands a smaller amount of torque than requested by the driver	20
	Commands torque in the wrong direction	20
	Misinterprets the APPS input	20
	APP-Torque map corrupted	18
	APP rate limiting fault (over-limiting/under-limiting)	20
	Incorrectly establishes idle torque [ii]	20
	BTO control fault	5
	Miscommunicates with internal subsystems	7
	Miscommunicates with external systems	4
	Fails to command a discharge of the HV bus capacitance	19
	Allows overcharging of the HV battery	20
	Diagnostics fault	1[iii]
EPS	Delivers more torque than requested by the HEV PCM	28
	Delivers less torque than requested by the HEV PCM	30
	Delivers torque in the opposite direction of the HEV PCM command	28
	Fails to maintain idle torque [ii]	30
	Does not stop the electric motor in generating mode as intended	27
	Does not discharge the HV bus capacitance	21
ECM/Throttle Actuator Controller	Commands larger throttle opening than requested by the HEV PCM	20
	Commands smaller throttle opening than requested by the HEV PCM	20
	Misinterprets the HEV PCM inputs	20
	Torque map corrupted	18
	Drives the throttle to a larger opening than commanded	22
	Drives the throttle to a smaller opening than commanded	22
	Fails to maintain throttle idle position	22
	Miscommunicates with internal subsystems	3
	Miscommunicates with external systems	3
	Mechanical failure prevents throttle movement to correct position	1[i]
	Diagnostics fault	1[iii]
Motor speed sensor	Provides incorrect motor speed to EPS	1
Engine speed sensor	Provides incorrect engine speed to ECM	1

System / Subsystem	Failure Mode	Identified Faults
Vehicle speed sensor	Provides incorrect vehicle speed to HEV PCM	1
Vehicle direction sensor	Provides incorrect vehicle direction to HEV PCM	1
BPPS	Provides incorrect input to HEV PCM	1
Other interfacing vehicle systems	Provides request for incorrect (more) propulsion torque	1
	Provides request for incorrect (less) propulsion torque	1
RESS controller	Communicates incorrect state of charge to HEV PCM	1
	Incorrectly communicates HV bus capacitance discharge request to HEV PCM	1
Vehicle communication system (e.g., CAN bus)	Communication messages corrupted during transfer within the parallel HEV ACS/ETC, or between the parallel HEV ACS/ETC and interfacing vehicle systems	1
Note: Some faults may potentially result in multiple failure modes. [i] These faults are mechanical in nature and are outside the scope of ISO 26262. [ii] This failure mode only applies to designs where the HEV PCM simulates an idle creep speed. [iii] This failure mode is only considered as part of a multiple point failure analysis.		

As with the series HEV Functional FMEA, faults in other vehicle systems are outside the scope of this project and are not included in Table 38. An example of the Functional FMEA is provided in Table 37. Appendix G provides the complete Functional FMEA results.

7.1.3 Series-Parallel HEV Functional FMEA

This study identifies eight vehicle-level hazards for the parallel HEV ACS/ETC. The Functional FMEA was carried out for hazards H1, H1a, H2, H3, H4, H5, H7, and H8 (Table 4). Because the consequences of H6 are captured in hazards H1, H2, H4, and H5, a separate Functional FMEA was not performed for H6.

Overall, the Functional FMEA covers six parallel HEV ACS/ETC subsystems and seven interfacing systems. The Functional FMEA identifies 47 failure modes and 133 potential causes of failures. Table 39 shows the number of identified causes for each of the failure modes.

Table 39. Number of Identified Faults by Failure Mode for the Series-Parallel HEV

System / Subsystem	Failure Mode	Identified Faults
AP Assembly	APP value interpreted higher than actual	19
	APP value interpreted lower than actual	19
	AP is not returned to idle position correctly	1[i]
	APP communicates with HEV PCM incorrectly	19
HEV PCM	Commands a larger amount of torque than requested by the driver	20
	Commands a smaller amount of torque than requested by the driver	20
	Commands torque in the wrong direction	20
	Incorrect command to split engine power between the electric motor in generating mode and reduction gears	20
	Misinterprets the APPS input	20
	APP-Torque map corrupted	18
	APP rate limiting fault (over-limiting/under-limiting)	20
	Incorrectly establishes idle torque [ii]	20
	BTO control fault	6

System / Subsystem	Failure Mode	Identified Faults
	Miscommunicates with internal subsystems	9
	Miscommunicates with external systems	4
	Fails to command a discharge of the HV bus capacitance	19
	Allows overcharging of the HV battery	20
	Diagnostics fault	1[iii]
EPS	Delivers more torque than requested by the HEV PCM	28
	Delivers less torque than requested by the HEV PCM	30
	Delivers torque in the opposite direction of the HEV PCM command	28
	Fails to maintain idle torque [ii]	30
	Does not stop the electric motor in generating mode as intended	27
	Electric motor does not start the engine	27
	Does not discharge the HV bus capacitance	21
ECM/Throttle Actuator Controller	Commands larger throttle opening than requested by the HEV PCM	20
	Commands smaller throttle opening than requested by the HEV PCM	20
	Misinterprets the HEV PCM inputs	20
	Torque map corrupted	18
	Drives the throttle to a larger opening than commanded	22
	Drives the throttle to a smaller opening than commanded	22
	Fails to maintain throttle idle position	22
	Miscommunicates with internal subsystems	3
	Miscommunicates with external systems	3
	Mechanical failure prevents throttle movement to correct position	1[i]
	Diagnostics fault	1[iii]
PSD	Does not split power between the electric motors and reduction gears as commanded by the HEV PCM	1
Motor speed sensor	Provides incorrect motor speed to EPS	1
Engine speed sensor	Provides incorrect engine speed to ECM	1
Vehicle speed sensor	Provides incorrect vehicle speed to HEV PCM	1
Vehicle direction sensor	Provides incorrect vehicle direction to HEV PCM	1
BPPS	Provides incorrect input to HEV PCM	1
Other interfacing vehicle systems	Provides request for incorrect (more) propulsion torque	1
	Provides request for incorrect (less) propulsion torque	1
RESS controller	Communicates incorrect state of charge to HEV PCM	1
	Incorrectly communicates HV bus capacitance discharge request to HEV PCM	1
Vehicle communication system (e.g., CAN bus)	Communication messages corrupted during transfer within the series-parallel HEV ACS/ETC, or between the series-parallel HEV ACS/ETC and interfacing vehicle systems	1

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

As with the series HEV Functional FMEA, faults in other vehicle systems are outside the scope of this project and are not included in Table 39. An example of the Functional FMEA is provided in Table 37. 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 eight 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 diagrams for each of the HEV ACS/ETC architectures (Figure 11, Figure 12, and Figure 13). Specifically, the STPA Step 2 analysis includes the following components and connections:

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

The choices of these components and connections enable the analysis to focus on the defined scope of this study while still considering critical interfaces between the HEV 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 HEV PCM. However, other failures in the brake system, such as faults in the wheel speed sensor, are not considered as part of this study.

Each identified CF relates to one or more of the UCAs identified in STPA Step 1, providing a traceable pathway from CFs up to vehicle-level hazards (Figure 14).

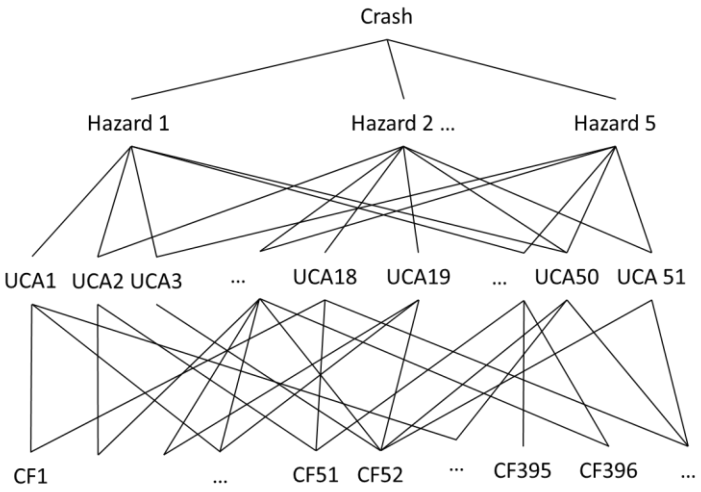


Figure 14. Traceability in STPA Results

7.2.1 Series HEV STPA Step 2 Results

The STPA Step 2 analysis identifies a total of 1,104 unique CFs for the series HEV ACS/ETC. Below is a breakdown of CFs by the type of UCAs they affect. As shown in Figure 14, each CFs can potentially lead to more than one type of UCA. Therefore the breakdown below exceeds the number of unique CFs.

- 253 CFs may lead to UCAs related to mode switching
- 210 CFs may lead to UCAs related to commanding the electric motor torque output
- 465 CFs may lead to UCAs related to supplying current to the electric motor
- 86 CFs may lead to UCAs related to providing torque in the requested direction
- 186 CFs may lead to UCAs related to controlling the inverter/converter temperature
- 192 CFs may lead to UCAs related to discharging the HV bus
- 105 CFs may lead to UCAs related to opening the HV contactor
- 106 CFs may lead to UCAs related to requesting DC power

Table 40 shows a breakdown of the identified CFs by the 26 CF guidewords applied in this study.

Table 40. Number of Identified Causal Factors by Causal Factor Category for the Series HEV

Causal Factor Category	Identified Causal Factors
Actuation delivered incorrectly or inadequately: Actuation delayed	2
Actuation delivered incorrectly or inadequately: Hardware faulty	4
Actuation delivered incorrectly or inadequately: Incorrect connection	3
Actuator inadequate operation, change over time	27
Conflicting control action	1
Controlled component failure, change over time	5
Controller hardware faulty, change over time	31
Controller to actuator signal ineffective, missing, or delayed: Communication bus error	20
Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	37
Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	12
External control input or information wrong or missing	13
External disturbances	338
Hazardous interaction with other components in the rest of the vehicle	321
Input to controlled process missing or wrong	3
Output of controlled process contributes to system hazard	2
Power supply faulty (high, low, disturbance)	35
Process model or calibration incomplete or incorrect	20
Sensor inadequate operation, change over time	31
Sensor measurement delay	5
Sensor measurement inaccurate	5
Sensor measurement incorrect or missing	6
Sensor to controller signal inadequate, missing, or delayed: Communication bus error	42
Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	65
Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	22
Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	54

Appendix H provides the complete list of CFs. Table 41 shows two examples of CFs for a UCA related to commanding a torque increase.

Table 41. Examples of Causal Factors for a Torque Increase UCA

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

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

Table 42 shows three examples of CFs for a UCA related to decreasing the current supply to the electric motor.

Table 42. Examples of Causal Factors for a UCA for Decreasing the Current Supply

Hazard	Potential propulsion power reduction / loss or vehicle stalling	
UCA (Example)	The TICM decreases the current to the electric motor when: • the HEV PCM requests a decrease in torque, but the current is decreased by too much.	
Potential Causal Factors (Examples)	**Component or Interaction**	**Potential Causal Factor**
	Motor Position / Speed Sensor to TICM	Moisture, corrosion, or contamination could affect the connection terminals of the motor position/speed sensor or the TICM, resulting in an incorrect motor position/speed reported to the TICM.
	TICM	The TICM may incorrectly think there is a problem with the electric motor (e.g., over-temperature).
	Motor Position / Speed Sensor	The reporting frequency of the motor position / speed sensor may be too low.

- The first CF describes moisture or other contamination affecting the connection between the motor position speed sensor and TICM. If the TICM has the incorrect motor position or speed information, this could affect how the TICM computes the current required by the electric motor.
- The second CF describes an error in the TICM process model where the TICM software logic incorrectly thinks that there is a fault in the electric motor. The TICM may attempt to shut down the motor or limit the motor torque output, resulting in decreasing the current supply by too much.
- The third CF describes a delay in the transmission of critical sensor data to the TICM. If the TICM does not receive the motor position or speed data in a timely manner and continues to operate using the old data, the TICM may continue to decrease the current supplied to the motor.

7.2.2 Parallel HEV STPA Step 2 Results

The STPA Step 2 analysis identifies a total of 1,635 unique CFs for the parallel HEV ACS/ETC. Below is a breakdown of CFs by the type of UCAs they affect. As shown in Figure 14, each CFs can potentially lead to more than one type of UCA. Therefore the breakdown below exceeds the number of unique CFs.

- 302 CFs may lead to UCAs related to mode switching
- 355 CFs may lead to UCAs related to commanding the net power output
- 378 CFs may lead to UCAs related to requesting power from the propulsion subsystems
- 358 CFs may lead to UCAs related to throttle position adjustment
- 475 CFs may lead to UCAs related to supplying current to the electric motor
- 84 CFs may lead to UCAs related to providing torque in the requested direction
- 82 CFs may lead to UCAs related to adjusting the mechanical coupling
- 191 CFs may lead to UCAs related to controlling the inverter/converter temperature
- 209 CFs may lead to UCAs related to discharging the HV bus
- 125 CFs may lead to UCAs related to opening the HV contactor
- 63 CFs may lead to UCAs related to requesting DC power

Table 40 shows a breakdown of the identified CFs by the 26 CF guidewords applied in this study.

Table 43. Number of Identified Causal Factors by Causal Factor Category for the Parallel HEV

Causal Factor Category	Identified Causal Factors
Actuation delivered incorrectly or inadequately: Actuation delayed	2
Actuation delivered incorrectly or inadequately: Hardware faulty	6
Actuation delivered incorrectly or inadequately: Incorrect connection	3
Actuator inadequate operation, change over time	40

Causal Factor Category	Identified Causal Factors
Conflicting control action	1
Controlled component failure, change over time	5
Controller hardware faulty, change over time	46
Controller to actuator signal ineffective, missing, or delayed: Communication bus error	40
Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	59
Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	18
External control input or information wrong or missing	21
External disturbances	477
Hazardous interaction with other components in the rest of the vehicle	454
Input to controlled process missing or wrong	2
Output of controlled process contributes to system hazard	2
Power supply faulty (high, low, disturbance)	53
Process model or calibration incomplete or incorrect	48
Sensor inadequate operation, change over time	49
Sensor measurement delay	6
Sensor measurement inaccurate	9
Sensor measurement incorrect or missing	9
Sensor to controller signal inadequate, missing, or delayed: Communication bus error	72
Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	95
Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	34
Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	84

Appendix H provides the complete list of CFs. Table 42 shows three examples of CFs for a UCA related to controlling the throttle opening. Examples of CFs for other types of UCAs are provided in Table 41 and Table 42.

Table 44. Examples of Causal Factors for a UCA for Decreasing the Throttle Opening

Hazard	Potential uncontrolled vehicle propulsion	
UCA (Example)	The ECM/Throttle Actuator Controller does not issue the command to decrease the throttle opening when: • the HEV PCM requests a decrease in engine torque.	
Potential Causal Factors (Examples)	**Component or Interaction**	**Potential Causal Factor**
	TPS	The TPS may have an internal hardware failure (e.g., short circuit). This could affect the measurement of the throttle position.
	ECM/Throttle Actuator Controller	If other vehicle systems, aside from the HEV PCM, have the authority to command torque from the ECM/Throttle Actuator Controller, the torque command from these other vehicle systems may differ from the HEV PCM command.
	Throttle Valve to TPS	If the TPS is incorrectly mounted on the throttle valve, the measurement of the throttle position may be incorrect.

- The first CF describes an internal hardware failure, such as a short or open circuit, in the TPS. This may cause the ECM/Throttle Actuator Controller to receive an incorrect TPS signal. For example, the signal from the TPS may indicate that the throttle valve is in the idle position.
- The second CF describes a situation where the ECM/Throttle Actuator Controller responds to a request from another vehicle system. If this request conflicts with the HEV PCM command - for example, a request for more engine power – the ECM/Throttle Actuator Controller may not decrease the throttle opening.
- The third CF describes a failure where the TPS becomes incorrectly positioned relative to the throttle valve. This could cause the TPS measurement to differ from the actual throttle valve position (e.g., an offset). With an incorrect TPS measurement, the ECM/Throttle Actuator Controller may think the throttle opening has already decreased.

7.2.3 Series-Parallel HEV STPA Step 2 Results

The STPA Step 2 analysis identifies a total of 1,792 unique CFs for the series-parallel HEV ACS/ETC. Below is a breakdown of CFs by the type of UCAs they affect. As shown in Figure 14, each CFs can potentially lead to more than one type of UCA. Therefore the breakdown below exceeds the number of unique CFs.

- 296 CFs may lead to UCAs related to mode switching
- 351 CFs may lead to UCAs related to commanding the net power output
- 373 CFs may lead to UCAs related to requesting power from the propulsion subsystems
- 345 CFs may lead to UCAs related to throttle position adjustment
- 475 CFs may lead to UCAs related to supplying current to the first electric motor
- 475 CFs may lead to UCAs related to supplying current for the second electric motor
- 84 CFs may lead to UCAs related to providing torque in the requested direction
- 81 CFs may lead to UCAs related to adjusting the PSD
- 191 CFs may lead to UCAs related to controlling the inverter/converter temperature
- 210 CFs may lead to UCAs related to discharging the HV bus
- 98 CFs may lead to UCAs related to opening the HV contactor
- 64 CFs may lead to UCAs related to requesting DC power

Table 40 shows a breakdown of the identified CFs by the 26 CF guidewords applied in this study.

Table 45. Number of Identified Causal Factors by Causal Factor Category for the Series-Parallel HEV

Causal Factor Category	Identified Causal Factors
Actuation delivered incorrectly or inadequately: Actuation delayed	3
Actuation delivered incorrectly or inadequately: Hardware faulty	8

Causal Factor Category	Identified Causal Factors
Actuation delivered incorrectly or inadequately: Incorrect connection	4
Actuator inadequate operation, change over time	38
Conflicting control action	1
Controlled component failure, change over time	5
Controller hardware faulty, change over time	44
Controller to actuator signal ineffective, missing, or delayed: Communication bus error	36
Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	52
Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	16
External control input or information wrong or missing	16
External disturbances	534
Hazardous interaction with other components in the rest of the vehicle	510
Input to controlled process missing or wrong	2
Output of controlled process contributes to system hazard	3
Power supply faulty (high, low, disturbance)	55
Process model or calibration incomplete or incorrect	48
Sensor inadequate operation, change over time	66
Sensor measurement delay	9
Sensor measurement inaccurate	12
Sensor measurement incorrect or missing	13
Sensor to controller signal inadequate, missing, or delayed: Communication bus error	78
Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	110
Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	40
Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	89

Appendix H provides the complete list of CFs. Examples of the CFs derived through STPA are provided in Table 41, Table 42, and Table 44.

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 [2]). Figure 15 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.

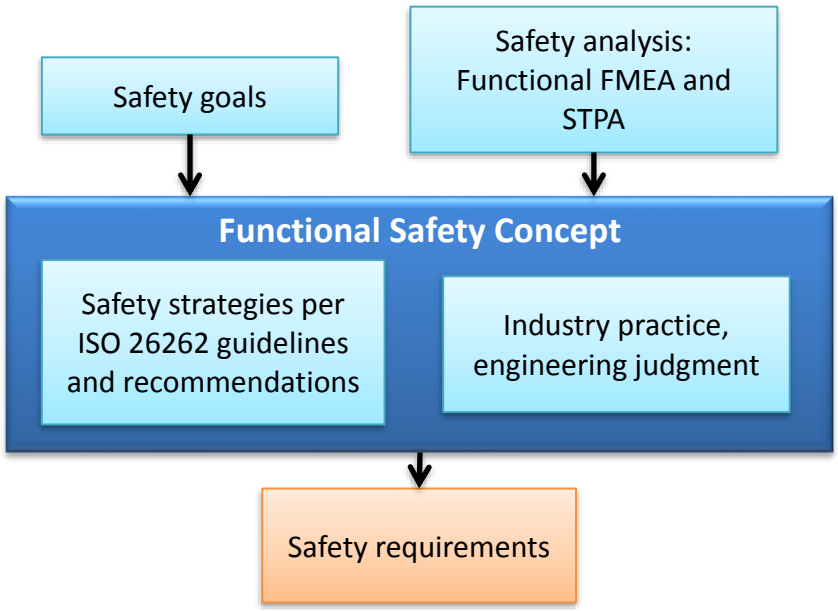


Figure 15. Functional Safety Concept Process

8.1 Safety Strategies

As stated in ISO 26262 Part 3 Clause 8.2 [2], "*the functional safety concept addresses:*

- *Fault detection and failure mitigation;*
- *Transitioning to a safe state;*
- *Fault tolerance mechanisms, where a fault does not lead directly to the violation of the safety goal(s) and which maintains the item in a safe state (with or without degradation)*
- *Fault detection and driver warning in order to reduce the risk exposure time to an acceptable interval (e.g., engine malfunction indicator lamp, anti-lock brake fault warning lamp);*
- *Arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by different functions*."

Typical safety strategy elements may include the following:

1. Ensure that the system elements are functioning correctly.
2. Ensure that the critical sensors' inputs to the main controller are valid and correct (redundant measurements paths).
3. Validate[30] the health of the main controller (using an auxiliary processor).
4. Ensure the validity and correctness[31] 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[32]).
6. Ensure the correct torque/power, in terms of magnitude and direction, is delivered to the drivetrain with the correct timing.
7. Ensure the health and sanity of the BTO control algorithm.
8. Ensure that low voltage power is available until the safe state is reached under all hazard conditions.
9. Mitigate the safety hazards when an unsafe condition is detected.
10. Ensure that the safe state is reached on time when a hazard is detected.
11. Ensure driver warnings are delivered when an unsafe condition is detected.
12. Ensure the correctness and timeliness of the arbitration strategy.

8.2 Example Safe States

A safe state may be the intended operating mode, a degraded operating mode, or a switched off mode (Part 1 Clause 1.102 of ISO 26262 [2]). The developer of the functional safety concept attempts to maximize the availability of the item while ensuring the safety of the vehicle operation. Therefore, careful consideration is given to selecting the safe states in relation to the potential failure modes.

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

For example, in cases where a good APPS signal is received by the HEV PCM, but the signal cannot be confirmed, the safe state may allow full torque/power but at a ramp rate slower than normal in order to give the driver more time to react in case of unintended vehicle behavior. On the other hand, if the APPS signal is unreliable but the vehicle can still be controlled by the

[30] "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.
[31] "Correctness" means that the value of a parameter is the correct one from the valid set.
[32] Quality factors refer to techniques for error detection in data transfer and communication including checksums, parity bits, cyclic redundancy checks, error correcting codes, etc.

brakes and at least one of the powertrain subsystems, the HEV PCM may allow a torque/power level higher than creep torque but may limit the maximum torque/power output of the ACS/ETC.

Safe states commonly used in the automotive industry may include, but are not limited to, the following:

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

The five safe states listed above are common to all three HEV architectures. In addition, for the parallel HEV and series-parallel HEV architectures, two additional safe states are identified:

- Safe State 8: Torque production limited to one propulsion system, with the other propulsion system disconnected (e.g., EPS fault, ECM/Throttle Actuator Controller fault).
- Safe State 9: Disconnection of the electric motor from the HV bus when the motor is operating as a generator.

The safe states listed above describe propulsion reduction (Safe States 2, 4-6) or deviations from the specified speed decrease or increase profiles (Safe State 3). While these vehicle responses may be similar to vehicle behaviors resulting from the identified hazards H2, H4, H5, and H6, there are key differences:

- The propulsion reduction or modified speed decrease/increase profiles are controlled when entering a safe state, while the hazards describe uncontrolled changes in propulsion (e.g., changes may not be smooth or consistent).
- When entering a safe state, the driver is informed that the vehicle is in a degraded operating state and can take appropriate action. The driver may not be notified of the degraded operating state when hazard H2, H4, H5, or H6 manifests.

8.3 Example Driver Warning Strategies

The following is an example of driver warning strategies commonly seen in the automotive industry:

- Amber Light: Potential violation of a safety goal is detected, but the probability of violating the safety goal is moderate (e.g., single APPS fault, BTO algorithm fault regardless of the need to execute the BTO algorithm)
- Red Light: Potential violation of a safety goal is detected and probability of violating the safety goal is high (e.g., AP torque map corruption, AP or BP communication/data transfer fault), or a violation of a safety goal is detected
- Chime: Audible notification of the driver is implemented whenever the conditions for the Red Light driver warning are identified. The chime may continue until the fault is removed.
- Messages: Messages are displayed to the driver when the Red Light driver warning is issued. Manufacturers may also elect to display messages in other situations, such as when the Amber Light driver warning is issued. The messages include instructions to the driver, such as exiting or staying away from the vehicle.
- Haptic warning: Haptic warnings may be an additional driver warning strategy. Dashboard lights and audible chimes are commonly used in conjunction with haptic warning. It may be beneficial to assess the drivers' reactions to haptic warning at the same time the system attempting to reach a safe state and degraded operation mode.

9 APPLICATION OF THE FUNCTIONAL SAFETY CONCEPT

This study uses the example safety goals identified for the generic HEV ACS/ETC system introduced in this research and exercises the functional safety concept process depicted in Figure 15. Through this process, this study identifies a total of 260 illustrative safety related engineering requirements for the concept ACS/ETC system and components.[33]

These include 171 HEV ACS/ETC system and component functional safety requirements identified by following the Concept Phase (Part 3) in the ISO 26262 standard. Section 9.2 presents these findings.

Furthermore, this study derives an additional 89 safety requirements related to the generic HEV ACS/ETC system and components based on the use of STPA and the additional safety strategies suggested in MIL-STD-882E [3]. These 89 requirements are out of the scope of the Functional Safety Concept in ISO 26262 (Part 3 of the standard). However, the subsequent parts in ISO 26262 — Systems Engineering (Part 4), Hardware Development (Part 5), and Software Development (Part 6) — cascade the Functional Safety Concept requirements into additional development-specific safety requirements, and may capture these additional safety requirements. Section 9.3 presents these additional 89 requirements.

The 260 safety requirements derived in this study include general requirements applicable to all three HEV architectures as well as safety requirements specific to only one or two HEV architectures. Figure 16 illustrates the commonality of the safety requirements between the three HEV ACS/ETC architecture types:

[33] 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.

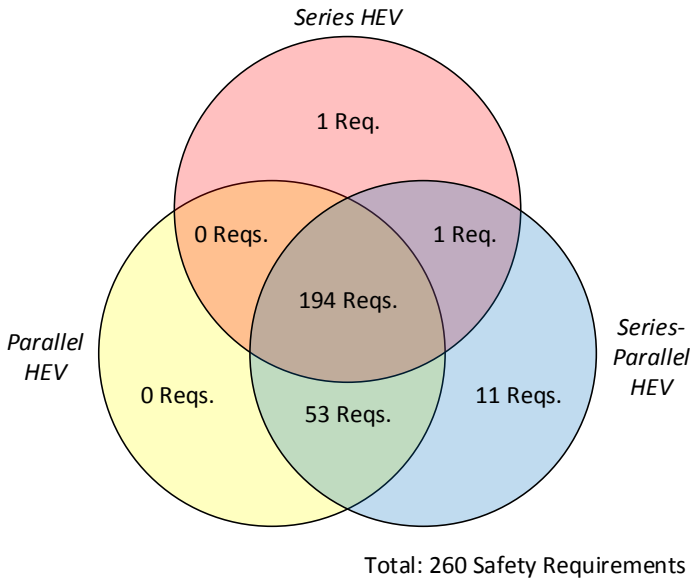


Figure 16. Commonality of Safety Requirements between HEV ACS/ETC Architecture Types

The majority of the safety requirements derived in this study are general safety requirements that apply to all three HEV ACS/ETC architectures. There is also a strong overlap in the safety requirements derived for the parallel HEV and series-parallel HEV ACS/ETC architectures, which largely stems from the inclusion of the gasoline ICE propulsion subsystem in both of these architectures.

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 35. The safety goals are summarized below, along with the recommended safety strategies.

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

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

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

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

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

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

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

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

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

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

SG 8: Potential RESS thermal events are to be prevented.

- This safety goal only applies to the parallel HEV and series-parallel HEV ACS/ETC architectures, where the ACS/ETC is responsible for generating electric power using a portion of the gasoline ICE power output.

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

- The HEV ACS/ETC is to prevent or detect faults and failures that could lead to vehicle-level hazards that the safety goals intend to mitigate.
- If a failure that could lead to the vehicle-level hazards occurs, the HEV ACS/ETC is to transition into a safe state within the fault tolerant time interval (FTTI).
    - 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 any actions required by the driver are to be communicated to him or her.

In addition, the following safety strategies are to be followed for a subset of the derived safety goals (specifically, SG 1, SG 1A, SG 2, SG4, SG 5, and SG 6):

- 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.

9.2 HEV ACS/ETC System and Components Functional Safety Requirements

Following the Concept Phase (Part 3) in the ISO 26262 standard, this study derives 171 example functional safety requirements for the three generic HEV ACS/ETC architectures and their respective components. The distribution of these requirements is as follows:

1. General HEV ACS/ETC System – 11 requirements
2. AP Assembly – 8 requirements
3. HEV PCM – 55 requirements
4. EPS – 39 requirements
5. Gasoline ICE Powertrain Subsystem – 33 requirements
6. PSD – 9 requirements
7. Communication Signals – 5 requirements
8. Power Supply (low and high voltage) – 6 requirements
9. Interfacing Systems – 5 requirements

Table 46 shows examples of safety requirements associated with the HEV PCM and how they are developed, and how the vehicle-level safety goal (SG 1) is allocated to one of the components in the system — the HEV PCM. The safety analysis identifies many HEV PCM failure modes and CFs that could potentially lead to the violation of SG 1. Here, two HEV PCM controller hardware failures are chosen as examples to illustrate the development process of safety requirements.

Table 46. Examples of HEV PCM Safety Requirements

Safety Goal	SG 1: Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 for a duration longer than TBD seconds is to be mitigated in accordance to the identified ASIL level.
ASIL	D
Component	HEV PCM
Safety Analysis (Examples)	• Hardware fault (sensors, integrated circuits (ICs), etc.) • Internal connection fault (short or open)
Safety Strategy	**Potential Safety Requirements (Examples)**
Detection	All single-point HEV PCM hardware faults that lead to potential violations of a safety goal are to be detected within the fault detection time and mitigated within the FTTI (ASIL B/C/D). In case of a failure, the system is to transition to the corresponding safe state. Hardware faults include those occurring in the ICs, circuit components, printed circuit boards, input/output (I/O) pins, signal connectors, and power connectors.
Fault Tolerance	
Safe State	
Warning	The HEV PCM is to log and save the following data every time a transition to safe state is executed due to a potential violation of a safety goal (ASIL QM): • The diagnostics information of the 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

In case of a controller hardware fault, the first mitigation strategy is for the system to be able to detect the abnormality and transition the system to a safe state. This requirement corresponds to the safety strategy that involves detection, fault tolerance, and transitioning to a safe state in Table 46. Additionally, if the vehicle is to transition to a safe state with reduced or very limited propulsion power (e.g., limp-home mode) the driver would need to be notified so that he or she can maneuver the vehicle to a safe location and get the needed repair service to the vehicle. Therefore, a potential additional requirement associated with a driver warning could be the one described in Table 46.

Although only one safety goal and one ASIL are shown in Table 46, a functional safety requirement may cover more than one safety goal. In addition, these safety goals may have different ASILs so more than one ASIL may be associated with a functional safety requirement. Requirements with more than one ASIL may be implemented using different ASIL classification

if independence among the implementation solutions can be demonstrated (Part 9 Clause 5.2 of ISO 26262 [2]).

The rest of this section lists the 171 HEV ACS/ETC functional safety requirements derived through this process. The columns to the right of each functional safety requirement indicate which of the three HEV ACS/ETC architectures are covered by the functional safety requirement.

9.2.1 General HEV ACS/ETC System-Level Functional Safety Requirements

There are 11 general system-level functional safety requirements derived for the generic HEV ACS/ETC system examined in this study. These requirements correspond to all established safety goals.

Table 47. General HEV ACS/ETC System Level Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The ACS/ETC is to perform Power On tests, periodic tests or continuous monitoring tests to ensure the correctness of safety critical parameters and the integrity of critical system elements. **(ASIL B/C/D)** • Critical parameters are those that are used to calculate the magnitude and direction of the propulsion torque, the vehicle speed, the motor speed, the vehicle direction, the state of the PSD, the safety of the HV power bus from unauthorized intrusion, the HV DC bus voltage, the low voltage, and the thermal state and the SOC of the RESS. • Other critical parameters may include calculation and comparison results that confirm the proper operation of the system • The APP-speed torque maps are to be checked. • The proper operation of the followings critical system elements is to be checked before any propulsion torque command is issued by the ACS/ETC: o The APPS o The motor position sensor o The TPS o The critical communications channels • A confirmation of the health and sanity of the HEV PCM, ECM/Throttle Actuator Controller, and TICM is to be confirmed via an acceptable strategy before any propulsion torque command is issued by the ACS/ETC • State-of-health checks may include: o Random Access Memory/Read-Only Memory/Electrically Erasable Programmable Read-Only Memory Tests o Analog/Digital (A/D) Converter Test o Shut Down Test • Sanity Checks may include Quizzer or Seed & Key strategies • The frequency of the periodic tests is to be selected based on the FTTI, the fault detection time interval, and the fault reaction time interval. • In case of a failure in the periodic self-tests, the ACS/ETC is to transition to the appropriate safe state within TBD ms.	●[34]	●	●
2	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 violation of a safety goal and appropriate DTCs are to be set. The diagnostics are to cover: **(ASIL QM/A/B)** • Hardware, including: the APPS, HEV PCM, ECM/Throttle Actuator Controller, TICM, motor sensor, TPS, and communication hardware • Software Functions including: APP calculations, torque command determination, torque control, and BTO.	●[34]	●	●
3	DTCs are to be set every time a safety goal is violated. **(ASIL QM)**	●	●	●
4	The hardware architectural Single Point Fault and Latent Fault metrics targets per ISO 26262 are to be demonstrated for each safety goal. **(No ASIL)**	●	●	●
5	If redundant elements are used, they are to be verified against common cause failures. **(ASIL C/D)** • Failure in the electric power supply of one element is not to affect the power supply of the other element. • Failure in the communication path of one element is not to affect the communication path of the other element.	●	●	●

[34] Portions of the requirement related to the gasoline ICE powertrain subsystem and PSD do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
6	If redundant elements are used and one element fails, the ACS/ETC is to transition into Safe State 3 within the FTTI of TBD seconds and an Amber Light driver warning is to be communicated to the driver. **(ASIL B/C/D)**	●	●	●
7	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 QM/A/B)**	●	●	●
8	Diagnostics covering the safety related functionality of the ACS/ETC system components and connections are to be instituted with a level of coverage corresponding to the ASIL of the safety goal that is affected. ISO 26262 diagnostics coverage guidelines for Low, Medium, and High are to be adhered to in order to comply with the hardware architectural metrics targets. **(ASIL QM/A/B)**	●	●	●
9	Diagnostics mechanisms are to adhere to ASIL B classification for ASIL D related elements and ASIL A classification for ASIL C related elements. **(ASIL QM/A/B)**	●	●	●

10	Diagnostics covering the following failure modes are to be implemented: **(ASIL QM/A/B)**
	• APPS:
	  o IC faults
	  o Open/short I/Os
	  o Stuck on the same reading
	  o Out of range
	  o Offset
	  o State of Health
	• Power Split Device
	  o Stuck on same state
	• Harnesses and Connectors
	  o Open/short circuits
		●[35]	●[35]	●

[35] Portions of the requirement related to the PSD do not apply to the series HEV or parallel HEV ACS/ETC architectures.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV

	The ACS/ETC is to log and retain data that can be used to reconstruct the vehicle operating scenario prior to any fault(s) that leads to a violation of a safety goal. The recording time period is TBD seconds before and TBD seconds after the safety goal violation event. The data may include sensor data, HMI data, communication signals, and values of some critical parameters used in the propulsion torque calculations. The flowing data may be considered: (**ASIL QM**)
	• Ignition switch status
	• Gear stick position
	• Vehicle speed
	• Vehicle direction
	• APPS value
	• ACC system settings
	• AEB system state
	  o Object distance from vehicle
	• Driver assist safety systems status
	• Brake/stability control system state
	  o ABS
	  o TCS
	  o ESC
	• Traction motor rotational speed
	• Traction motor current sensors readings
	• System low voltage value
	• Driver actions regarding vehicle systems capable of initiating and or commending changes to propulsion torque, including driver override decisions of vehicle systems capable of initiating and or commanding changes to propulsion torque.
	• Arbitration logic decisions by the HEV PCM
	• HEV PCM torque request
	• EPS torque received request
	• EPS motor current command
	• HEV PCM received torque request from ACC
	• HEV PCM torque request received from AEB
	• HV bus state of charge
	• Steering torque sensor value
	• Vehicle yaw rate
		●	●	●

S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.2.2 Accelerator Pedal Assembly Functional Safety Requirements

There are eight AP assembly functional safety requirements derived for the generic HEV ACS/ETC systems studied in this project. The AP assembly functional safety requirements correspond to Safety Goals SG 1, SG 2, SG 4, SG 5, SG 6, and SG 7, unless otherwise specified.

Table 48. Accelerator Pedal Assembly Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The APP corresponding to the propulsion torque requested by the driver is to be mapped correctly and consistently, and the results are to be qualified for validity and correctness under all vehicle operating conditions, over the usable life of the vehicle. **(ASIL B/C/D)**	●	●	●
2	The health and sanity of the APPS is to be monitored and confirmed under all operating vehicle conditions. **(ASIL C/D)**	●	●	●
3	The APP value is to be measured, and the measured value is to be valid and correct. **(ASIL B/C/D)**	●	●	●
4	The APP to electrical conversion method is to be validated. **(ASIL B/C/D)**	●	●	●
5	Critical communication and data transfer between the APPS and the HEV PCM, including the APP and diagnostics of the APPS, are to be qualified for validity and correctness (plausibility and rationality). In case of a fault, the correct failure mode effect mitigation strategy is to be applied. **(ASIL B/C/D)**	●	●	●
6	In case of a fault that violates a safety goal, the APPS is to communicate the fault to the HEV PCM. **(ASIL B/C/D)**	●	●	●
7	The APPS is to have diagnostics for safety relevant failures caused by EMI/electromagnetic compatibility (EMC), ESD, contamination, Single Event Effects, and other environmental conditions. **(ASIL A/B)**	●	●	●
8	All single point APPS hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. In case of a failure, the system is to transition to the corresponding safe state. **(ASIL B/C/D)** • Hardware faults include those occurring in the IC, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors.	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.2.3 HEV Powertrain Control Module Functional Safety Requirements

There are 55 HEV PCM functional safety requirements that are derived in this project. Many of these requirements correspond to all established safety goals. However, some of the functional safety requirements only correspond to a subset of the established safety goals. These requirements have the specific safety goals listed in the end of the requirement statement.

Table 49. HEV PCM Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The health and sanity of the HEV PCM controller is to be ensured. Power-on self-tests are to be implemented to check the health of the controller. These tests may include: **(ASIL C/D)** • CPU and Register Tests to check the internal working of the CPU. All CPU registers associated with the torque control functions are to be checked during 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 microcontroller used on the circuit board.	●	●	●
2	The HEV PCM's I/Os pins are to be monitored for shorts to high voltages or ground. **(ASIL B/C/D)**	●	●	●
3	The HEV PCM is to have diagnostics for safety relevant failures caused by EMI/EMC, ESD, contamination, Single Event Effects, and other environmental conditions. **(ASIL B/C/D)**	●	●	●
4	All single point HEV PCM hardware faults that lead to violations of a safety goal are to be detected within the fault detection time 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 boards, I/O pins, signal connectors, and power connectors.	●	●	●
5	The HEV PCM torque/power command and control communication channel(s) with the ECM/Throttle Actuator Controller and EPS are to be validated at start up. Torque/power commands are not to be issued until the validation of this communication channel(s) is successful. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6** • In case of failure of validation, the ACS/ETC is to transition into Safe State 6 within a FTTI of TBD seconds, and a Red Light driver warning is to be communicated to the driver.	● [36]	●	●
6	All electrical hardware and software elements associated with the delivery of the torque/power control function are to comply with ASIL D classification for SG 1 and SG 4, ASIL C classification for SG 3, SG 5 and SG 6, and ASIL B classification for SG 2 and SG 7 unless otherwise specified. If independence of the elements (per ISO 26262) cannot be demonstrated, then the higher ASIL classification is to be adopted. **(ASIL B/C/D)**	●	●	●
7	The data, in addition to the APP, used in determining the requested propulsion torque/power are to be qualified for correctness and validity; this includes vehicle speed (ASIL D), vehicle direction (ASIL C), motor speed (ASIL D), and engine speed (ASIL D). **(ASIL D/C) Safety Goals 1, 2, 3, 4, 5, and 6** • If torque/power maps or look up tables are used, their content is to be checked for validity and correctness	● [37]	●	●
8	The data used in determining how the ICE power is split between the vehicle drivetrain and the electric motor are to be qualified for correctness and validity at the correct frequency. This includes vehicle speed (ASIL D), motor speed (ASIL D), engine speed (ASIL D), and the RESS SOC (ASIL C). **(ASIL C/D)**		●	●

[36] Portions of this requirement relating to the ECM/Throttle Actuator Controller do not apply to the series HEV ACS/ETC architecture.
[37] Portions of this requirement relating to the engine speed do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
9	The HEV PCM is to qualify the APP input(s) for validity and correctness (plausibility and rationality). **(ASIL C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
10	Communication and data transfer between the HEV PCM and the APPS are to be qualified for validity and correctness (plausibility and rationality). In case of a fault, the correct failure mode effect mitigation strategy is to be applied. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6** • The critical communications include the APP and the diagnostics of the APPS.	●	●	●
11	The HEV PCM algorithm or method for calculating the torque/power command is to be validated. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
12	The HEV PCM algorithm or method for calculating how the ICE power is split between the vehicle drivetrain and electric motor in generation mode is to be validated. **(ASIL B/C/D) Safety Goals 1, 2, 4, 5, 6, and 8**		●	●
13	The torque/power command corresponding to the propulsion torque/power requested by the driver is to be calculated correctly and the results are to be qualified for validity and correctness under all vehicle operating conditions. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
14	The torque/power command is to be controlled and updated in the correct direction and within the correct time duration. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
15	The HEV PCM's torque control algorithm is to include a vehicle speed increase/decrease profile. The torque calculation algorithm is to specify the parameters that form the basis for the speed increase/decrease profile (e.g., vehicle speed). **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
16	The command to split the gasoline ICE power between the drivetrain and electric motor (in generation mode) is to be controlled and updated within the correct time duration. **(ASIL B/C/D) Safety Goals 1, 2, 4, 5, 6, and 8**		●	●
17	The time duration required to update the torque/power command is not to result in violation of a safety goal. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6** • The time duration is to be reflected in the relevant software function's execution time, and the transient response of the motor.	●	●	●
18	The APP to propulsion torque/power rate of change mapping is to be monitored for correctness. **(ASIL C) Safety Goals 2 and 5**	●	●	●
19	The HEV PCM torque/power control algorithm is to be checked periodically based on the correct FTTI in order to prevent violation of any safety goals. **(ASIL C/D) Safety Goals 1, 2, 3, 4, 5, and 6** • A fault tolerant strategy is to be applied for the torque/power control algorithm. Fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the torque/power control algorithm.	●	●	●
20	In case of a fault in the torque/power control that leads the HEV PCM to become unable to control the torque/power command, the ACS/ETC is to transition into Safe State 6 within the TBD ms time, and the Red Light driver warning is to be issued. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6** • Some industry practices establish this TBD time at 200 ms. • For failures that prevent the HEV PCM from controlling the idle torque command, the FTTI may be larger than the FTTI for operating speeds above idle speed. • DTCs are to be set.	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
21	In case of a fault in the torque/power control that leads the HEV PCM to be unable to control how the ICE power is split between the vehicle drivetrain and electric motor in generation mode, the ACS/ETC is to transition into Safe State 4 within the TBD ms time, and Red Light driver warning is to be issued. **(ASIL B/C/D) Safety Goals 1, 2, 4, 5, and 6** • DTCs are to be set.		●	●
22	The HEV PCM is to communicate the correct torque/power command, including the torque direction, to the TICM and ECM/Throttle Actuator Controller under all vehicle operating scenarios within TBD seconds. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	● [38]	●	●
23	The HEV PCM is to communicate the correct command to split the ICE power between the vehicle drivetrain and electric motor in generation mode under all vehicle operating scenarios within TBD seconds. **(ASIL B/C/D)**		●	●
24	The HEV PCM is to be able to shut down the EPS. **(ASIL C/D)**	●	●	●
25	The HEV PCM is to be able to shut down the ECM/Throttle Actuator Controller. **(ASIL C/D)**		●	●
26	Communication of the torque/power command between the HEV PCM and the TICM is 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) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
27	Communication of the torque/power command between the HEV PCM and the ECM/Throttle Actuator Controller is 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) Safety Goals 1, 2, 4, 5, 6, and 8**		●	●
28	Communication between the HEV PCM and PSD related to the torque/power allocation between the vehicle drivetrain and electric motor (in generation mode) is 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)**		●	●
29	Critical communications and data transfer between the HEV PCM and other vehicle systems/components are to be qualified for validity and correctness (plausibility and rationality) including the BPPS (ASIL D), vehicle speed sensor (ASIL D), motor speed sensor (ASIL D), engine speed sensor (ASIL D), RESS (ASIL D), vehicle direction sensor (ASIL C) and all other inputs that are used for torque/power control. **(ASIL C/D)** • If the vehicle speed and motor speed/engine speed are used redundantly, then the ASIL classification may be applied based on a selected ASIL decomposition strategy. • If torque/power maps or look up tables are used, their content is to be checked for validity and correctness at the correct frequency.	● [39]	●	●
30	The HEV PCM 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) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
31	The HEV PCM is to correctly adjust the propulsion torque in response to propulsion torque modification requests by other vehicle systems, including AEB and ACC. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●

[38] Portions of this requirement related to the ECM/Throttle Actuator Controller do not apply to the series HEV ACS/ETC architecture.

[39] Portions of this requirement related to the engine speed sensor do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
32	The HEV PCM is to correctly adjust the propulsion torque when it receives a communication of a braking action by the braking system. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
33	All other critical parameters used for torque/power control are to be checked periodically based on the FTTI requirements. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
34	The HEV PCM is to access the metrics that clearly define the limits of vehicle stability from the appropriate vehicle system (e.g., brake/stability control system).	●	●	●
35	The HEV PCM is to qualify the stability metrics input(s) for validity and correctness (plausibility and rationality).	●	●	●
36	The propulsion torque computed by the control algorithm is to be validated against the vehicle stability metrics before any propulsion torque command is issued. • In case the calculated torque exceeds the vehicle stability limits, the ACS/ETC is to transition into Safe State 2 within a FTTI of TBD seconds and an Amber Light driver warning is to be issued. • Appropriate warnings to the driver from affected interfacing systems are to be issued.	●	●	●
37	All electrical hardware and software elements associated with the delivery of the BTO function are to comply with ASIL C unless otherwise stated. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
38	The HEV PCM is to provide BTO control. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
39	The HEV PCM BTO control is to command a pre-determined torque output when both the AP and BP are pressed and when the vehicle speed is above the pre-determined threshold value, regardless of the amount of torque/power requested via the APPS. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
40	The HEV PCM BTO control strategy is to include provisions, if necessary, for a modified control strategy if it is determined that simultaneous AP and BP applications are intended and confirmed by the driver. The modified strategy is to include a maximum allowable torque/power and a torque/power ramp rate that will not lead to a violation of a safety goal. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
41	The BTO control algorithm, including the algorithm for exiting BTO mode, is to execute within TBD seconds. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
42	The HEV PCM BTO control algorithm is to be checked periodically based on the correct FTTI in order to prevent violation of the safety goals. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6** • A fault tolerant strategy is to be applied. Typical fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the BTO algorithm. • In case of a fault in the BTO control algorithm that leads to a failure and a violation of a safety goal, the system is to transition into Safe State 6 within TBD ms (200 ms is considered in the industry for similar safety goals), and the Red Light driver warning is to be issued. • DTCs are to be set.	●	●	●
43	Critical communication and data transfer between the BPPS and the HEV PCM are to be qualified for validity and correctness (plausibility and rationality). In case of a fault, the correct failure mode effect mitigation strategy is to be applied. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
44	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 C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
45	Critical communications and data transfer between the HEV PCM and other vehicle systems that can request or command changes to the propulsion torque are to be qualified for validity and correctness (plausibility and rationality). In case of a fault, the correct failure mode effect mitigation strategy is to be applied. **(ASIL B/C/D) Safety Goals 1, 2, 4, 5, and 6** • This includes requests for propulsion torque modifications, and diagnostics (failure) information of these systems.	●	●	●
46	All requests or commands for a change in the propulsion torque by other vehicle systems are to be ignored when BTO is activated. **(ASIL C) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
47	The HEV PCM arbitration logic strategy and algorithm are to be checked for health and sanity periodically based on the FTTI. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6** • In case of a failure in this arbitration strategy, the ACS/ETC is to transition into Safe State 1 within a FTTI of TBD seconds and an amber light driver warning is to be issued	●	●	●
48	The HEV PCM is to have arbitration logic that prioritizes between the driver's torque/power request via the AP and torque requests from other vehicle systems based on a pre-established safety strategy. The arbitration logic execution time is not to result in any violations of the safety goals. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
49	The output of the HEV PCM arbitration logic is to be qualified for validity and correctness. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
50	The arbitration strategy is to clearly define the action of the ACS/ETC when the driver’s intended request conflicts with the request(s) or input(s) of safety relevant system(s). **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, 5, and 6**	●	●	●
51	The HEV PCM is to have a mechanism to prevent unauthorized access to the propulsion torque control calculations and command path.	●	●	●
52	All single point faults that result in a failure to prevent unauthorized access to the HEV PCM are to be detected and mitigated. • In case of unauthorized access to the HEV PCM, the ACS/ETC is to transition to Safe State 6 within TBD ms and a red light driver warning is to be issued. • A DTC is to be set.	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
53	Diagnostics covering the failures for the following parts of the HEV PCM are to be implemented: **(ASIL QM/A/B)** • Execution logic (wrong coding, wrong or no execution, execution out of order, execution too fast or too slow, stack overflow or underflow) • On-chip communication and bus arbitration • The main controller's: o central processing unit (CPU) o processor memory o arithmetic logic unit o registers o A/D converter o signal conditioning and converting (e.g., signal filters) o software program execution o connections I/O faults (short/open/drift/oscillation) o power supply o temperature • If an auxiliary processor is used, then diagnostics are to cover its: o CPU o processor memory o arithmetic logic unit o registers o A/D converter o signal conditioning and converting (e.g., signal filters) o software program execution o I/O faults (short/open/drift/oscillation) o power supply o temperature • The wiring harnesses and connectors for open and short circuits • Critical messages including CAN messages	●	●	●
54	The HEV PCM is to log and save the following data every time a transition to safe state is executed due to a violation of a safety goal: **(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 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/power 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.	●	●	●
55	In the event of an HEV PCM malfunction resulting in the loss of the BTO control function, the ASC/ETC is to still be able to reduce the net power or torque output. Examples of implementation strategies include: • Entering a safe state • Implementing a BTO control function that is subordinate to the HEV PCM 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 HEV PCM BTO function.	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.2.4 Electric Powertrain Subsystem Functional Safety Requirements

The EPS contains the power electronics used to drive the electric motor or motors. This includes the TICM, gate drive board, inverter/converter, and relevant sensors. There are 39 EPS functional safety requirements derived in the three HEV ACS/ETC systems. The majority of these safety requirements correspond to safety goals SG 1 through SG 6, except where otherwise noted.

Table 50. EPS Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The motor output torque is to be controlled and updated in the correct direction within the correct time duration. The time duration required to update the motor torque must not result in an uncontrolled vehicle propulsion condition (e.g., failure mode in software execution, execution time, motor inertia). **(ASIL D) Safety Goal 1 and 2**	●	●	● [40]
2	The motor speed is to be validated against the vehicle speed. **(ASIL B/C/D) Safety Goal 1, 2, 4, 5, and 6**	●	●	● [40]
3	The motor speed and torque combination is to be validated for the driver's intended direction of travel. **(ASIL C) Safety Goal 3**	●	●	● [40]
4	The EPS is to have motor torque current calculations and control algorithms for all motor speeds. **(ASIL B/C/D)**	●	●	● [40]
5	The EPS is to deliver motor torque current to drive the motor in both the clockwise and counterclockwise directions. **(ASIL B/C/D)**	●	●	● [40]
6	The EPS is to receive HV electric energy from the HV bus. If there is a fault in the HV system that may lead to a violation of a safety goal, the ACS/ETC is to transition into a safe state and a driver warning is to be issued. **(ASIL C/D)**	●	●	●
7	The EPS is to deliver the motor torque current at the correct value, in the correct direction, with the correct torque increase/decrease rate, and the correct time to the electric motor. **(ASIL B/C/D)** • The motor torque current direction is defined in terms of the intended direction of the output motor torque. This means that for a 3-phase current, the motor rotor position may have to be considered when establishing the current direction. • The transient response of the EPS is to be established to prevent a violation of any safety goal.	●	●	● [40]
8	All electrical hardware and software elements associated with the delivery of the motor torque current to the electric motor, or to discharge the high voltage bus are to comply with ASIL D classification for SG 1 and SG 3, ASIL C classification for SG 4, SG 5, and SG 6, and ASIL B classification for SG 2 and SG 7 unless otherwise specified. **(ASIL B/C/D) Safety Goals 1through 7** • If independence of the elements (per ISO 26262) cannot be demonstrated, the higher ASIL classification is to be adopted.	●	●	● [40]
9	The EPS is to control the current supplied to the electric motor such that the motor torque output is controlled to within a pre-established tolerance band (in both magnitude and torque increase/decrease rate) based on the vehicle operating scenario. The tolerance is not to result in a violation of a safety goal. **(ASIL B/C/D)**	●	●	● [40]
10	The electric motor torque current value, increase/decrease rate, and direction are to be qualified for validity and correctness. **(ASIL B/C/D)**	●	●	● [40]

[40] This requirement also includes the second electric motor in the series-parallel HEV ACS/ETC architecture if both motors can be used to provide propulsion.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
11	If look up tables are used to determine the value of the current required to achieve the target electric motor torque, the content of the tables are to be checked for correctness every time the ACS/ETC is started. **(ASIL B/C/D)**	●	●	● [41]
12	The motor torque current calculations are to result in the correct torque increase/decrease rate. (**ASIL C**)	●	●	●
13	The transient response of the EPS is to be established to prevent a violation of any safety goal. (**ASIL C/D**)	●	●	●
14	The motor position sensor end of line calibration process capability is to be monitored. (**ASIL B/C/D**)	●	●	●
15	The motor position sensor input(s) is to be checked for validity and correctness. **(ASIL B/C/D)**	●	●	● [41]
16	The motor current sensor input(s) is to be checked for validity and correctness. **(ASIL B/C/D)**	●	●	● [41]
17	All faults that result in a failure to determine the motor torque current are to be detected and mitigated. **(ASIL B/C/D)** • In case of a failure in establishing the validity and correctness of the motor torque current, the ACS/ETC is to transition into Safe State 6 (zero torque output) and a Red Light driver warning is to be issued. • DTCs are to be set	●		
18	All faults that result in a failure to determine the motor torque current are to be detected and mitigated. **(ASIL B/C/D)** • In case of a failure in establishing the validity and correctness of the motor torque current, the ACS/ETC is to transition into Safe State 8 (allowing torque production from the ICE only) and a Red Light driver warning is to be issued. • DTCs are to be set		●	● [41]
19	The health and sanity of the TICM algorithms for computing the motor torque current are to be checked periodically based on the correct FTTI in order to prevent violations of the safety goals (via an auxiliary processor or equivalent means). **(ASIL C/D)** • A fault tolerant strategy is to be applied. Typical fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied.	●	●	● [41]
20	The EPS is to have a mechanism to prevent unauthorized access to the HV bus. **(ASIL B) Safety Goal 7**	●	●	●
21	All single point faults that result in a failure to disconnect the EPS from the HV bus when unauthorized access occurs are to be detected and mitigated. **(ASIL B) Safety Goal 7** • In case of a failure that prevents the EPS from disconnecting the HV bus when unauthorized access occurs, the ACS/ETC is to transition into Safe State 7 within TBD ms, and a Red Light driver warning is to be issued. • A DTC is to be set.	●	●	●
22	When requested by the HEV PCM, the EPS is to discharge the HV bus to a pre-determined level and within the required time. **(ASIL B) Safety Goal 7**	●	●	●
23	All single point faults that result in a failure to discharge the HV bus when requested by the PCM are to be detected and mitigated. **(ASIL B) Safety Goal 7** • In case of a failure that leads the EPS to be unable to discharge the HV bus, the ACS/ETC is to transition into Safe State 7 within TBD ms, and a Red Light driver warning is to be issued.	●	●	●

[41] This requirement also includes the second electric motor in the series-parallel HEV ACS/ETC architecture if both motors can be used to provide propulsion.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
24	Critical communications and data transfer between the TICM and other EPS components are to be qualified for validity and correctness (plausibility and rationality). This includes the electric motor position sensor and diagnostics associated with the motor position determination/sensing mechanism. **(ASIL B/C/D)**	●	●	● [41]
25	All other critical parameters used by the TICM in calculating the motor torque current are to be checked periodically based on the FTTI requirements. Critical parameters are parameters, which when incorrect, may lead to a violation of any safety goal. **(ASIL B/C/D)**	●	●	● [41]
26	In case of a fault, the EPS is to communicate the fault to the HEV PCM. **(ASIL B/C/D) Safety Goals 1 through 7**	●	●	●
27	All single point EPS hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. **(ASIL B/C/D) Safety Goals 1 through 7** • 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 board, I/O pins, signal connectors, and power connectors.	●	●	●
28	The electric motor is to start the engine when requested by the PCM. **(ASIL QM) Safety Goals 2 and 4**			●
29	The electric motor (in generating mode) is to deliver HV electric energy to the HV bus. **(ASIL QM) Safety Goals 2 and 4**		●	●
30	The EPS is to have an electric energy generation control algorithm for all motor speeds (when operating as a generator). **(ASIL C) Safety Goal 8**		●	●
31	The TICM is to suspend delivering electric energy to the HV bus when commanded by the HEV PCM. In case of a failure to stop the motor in generating mode, the ACS/ETC is to transition to Safe State 9 (disconnect the electric motor from the RESS). **(ASIL C) Safety Goal 8**		●	●
32	All electrical hardware and software elements associated with the delivery of the HV energy to the HV bus are to comply with ASIL C. **(ASIL C) Safety Goal 8**		●	●
33	The charging current value is to be validated for correctness. **(ASIL C) Safety Goal 8**		●	●
34	All faults that result in a failure to control the electric motor charging current (when in generating mode) are to be detected within the fault detection interval and mitigated within the FTTI. **(ASIL C) Safety Goal 8** • Hardware faults include those occurring in the ICs, circuit components, printed circuit board, I/O pins, signal connectors, and power connectors. • In case of a failure in establishing the correctness of the electric motor charging current, the ACS/ETC is to transition into Safe State 9 and an Amber Light driver warning is to be issued. DTCs are to be set.		●	●
35	All single point faults that result in a failure to disconnect the EPS from the HV bus when unauthorized access occurs are to be detected and mitigated. **(ASIL B) Safety Goal 7** • In case of a failure that leads the EPS to be unable to disconnect from the HV bus when unauthorized access occurs, the ACS/ETC is to transition into Safe State 7 within TBD ms, and a Red Light driver warning is to be issued. • DTCs are to be set	●	●	●
36	Critical communications and data transfer between the EPS and the HEV PCM are to be qualified for validity and correctness (plausibility and rationality). **(ASIL B/C/D) Safety Goals 1 through 7**	●	●	●
37	The EPS is to have a mechanism to prevent unauthorized access to the torque current control calculations and command path. **(ASIL B/C/D)**	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
38	All single point faults that result in a failure to prevent unauthorized access to the EPS torque current control calculations and command path are to be detected and mitigated. **(ASIL B/C/D)** • In case of unauthorized access to the EPS, the ACS/ETC is to transition to Safe State 6 within TBD ms and a red light driver warning is to be issued. • A DTC is to be set.	●	●	●
39	Diagnostics covering the failures for the following parts of the EPS are to be implemented: **(ASIL QM/A/B) Safety Goals 1 through 7** • Execution logic (wrong coding, wrong or no execution, execution out of order, execution too fast or too slow, stack overflow or underflow) • On-chip communication and bus arbitration • The main controller's: o CPU o processor memory o arithmetic logic unit o registers o A/D converter o signal conditioning and converting (e.g., signal filters) o software program execution o connections I/O faults (short/open/drift/oscillation) o power supply o temperature • If an auxiliary processor is used, then cover its: o CPU o processor memory (if auxiliary processor is used) o arithmetic logic unit o registers o A/D converter o signal conditioning and converting (e.g., signal filters) o software program execution o I/O faults (short/open/drift/oscillation) o power supply o temperature • The motor position sensor o IC faults o connection I/O faults (short/open) o stuck on the same reading o out of range o offset o State of Health • The motor current sensors (if only two sensors are used) o IC faults o connection I/O faults (short/open) o stuck on the same reading o out of range (not required if three sensors are used) o offset (not required if three sensors are used) o State of Health (not required if three sensors are used) • The wiring harnesses and connectors for open and short circuits • Critical messages, including CAN messages	●	●	●

S HEV = Series HEV
P HEV = Parallel HEV
S-P HEV = Series-Parallel HEV

9.2.5 Gasoline ICE Powertrain Subsystem Functional Safety Requirements

The gasoline ICE powertrain subsystem contains the components used in regulating air flow to the gasoline ICE. This includes the ECM/Throttle Actuator Controller, throttle motor, TPS, and throttle valve. There are 31 functional safety requirements derived for the gasoline ICE powertrain subsystem. These requirements only apply to the parallel HEV and series-parallel HEV ACS/ETC architectures. In the series HEV ACS/ETC architecture, the gasoline ICE powertrain subsystem is considered an interfacing system since it does not directly provide propulsion to the vehicle's drivetrain.

The safety requirements included in this section correspond to Safety Goals SG 1, SG 2, SG 4, SG 5, SG 6, and SG 8, except where otherwise noted.

Table 51. Gasoline ICE Powertrain Subsystem Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The ICE torque/power output is to be controlled and updated within the correct time duration. The time duration required to update the torque/power must not result in an unintended acceleration condition (failure mode in software execution and execution time). (**ASIL D)**		●	●
2	The ICE speed is to be validated against the vehicle speed. **(ASIL B/C/D) Safety Goal 1, 2, 4, 5, and 6**		●	●
3	The health and sanity of the ECM/Throttle Actuator Controller is to be ensured. Power-on self-tests are to be implemented to check the health of the controller. These test may include: **(ASIL C/D)** • CPU and Register Tests to check the internal working of the CPU. All CPU registers associated with the throttle position control functions are to be checked during this test. • Interrupt and Exception Tests to check the interrupt and exception processing of the controller. • EEPROM Checksum Tests to check the EEPROM health. • Device Tests to check the peripheral devices connected to the microcontroller used on a board.		●	●
4	The ECM/Throttle Actuator Controller I/O pins are to be monitored for shorts or ground. **(ASIL B/C/D)**		●	●
5	The ECM/Throttle Actuator Controller is to have diagnostics for safety relevant failures caused by EMI/EMC, ESD, contamination, Single Event Effects, and other environmental conditions. **(ASIL B/C/D)**		●	●
6	All single point ECM/Throttle Actuator Controller hardware faults that lead to violations of a safety goal are to be detected within the fault detection interval and mitigated within the FTTI. **(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.		●	●
7	All electrical hardware and software elements associated with the delivery of the throttle position control function are to comply with ASIL D classification for SG1 and SG4, ASIL C classification for SG5 and SG6, and ASIL B classification for SG2 unless otherwise specified. If independence of the elements (per ISO 26262) cannot be demonstrated, the higher ASIL classification is to be adopted. **(ASIL B/C/D)**		●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
8	The data used in determining the requested propulsion torque/power are to be qualified for correctness and validity, including vehicle speed (ASIL D), engine speed (ASIL D), RESS state of charge (ASIL C), and altitude measurement (QM). If torque/power maps or look up tables are used, their content is to be checked for validity and correctness at the correct frequency. **(ASIL QM/C/D)**		●	●
9	Communication and data transfer between the ECM/Throttle Actuator Controller and the HEV PCM is 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)**		●	●
10	The ECM/Throttle Actuator Controller algorithm or method for calculating the throttle position is to be validated. **(ASIL B/C/D)**		●	●
11	The throttle position corresponding to the propulsion torque/power requested by the HEV PCM is to be calculated correctly and the results are to be qualified for validity and correctness under all vehicle operating conditions. **(ASIL B/C/D)**		●	●
12	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)** • The time duration required to update the throttle position is not to result in a 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.		●	●
13	The ECM/Throttle Actuator Controller control algorithm for the throttle position is to be checked periodically based on the correct FTTI in order to prevent violation of any safety goal. **(ASIL C/D)** • A fault tolerant strategy is to be applied for the throttle position control algorithm. The fault tolerant techniques may include redundancy, voting logic, or other techniques. • A control flow monitoring strategy is to be applied for the throttle position control algorithm.		●	●
14	In case of a fault in the control algorithm that leads the ECM/Throttle Actuator Controller to be unable to control the throttle position, the ACS/ETC is to transition into Safe State 8 (allowing torque production from the EPS only) within TBD ms. The Red Light driver warning is to be issued. **(ASIL B/C/D)** • Some industry practices establish this TBD time at 200 ms. • For failures that prevent the ECM/Throttle Actuator Controller from controlling the throttle idle position, the FTTI may be larger than the FTTI for operating speeds above idle engine speed. • DTCs are to be set.		●	●
15	If the ECM and Throttle Actuator Controller are separate control modules, the ECM is to communicate the correct throttle position to the Throttle Actuator Controller under all vehicle operating situations within TBD time. **(ASIL B/C/D)**		●	●
16	If the ECM and Throttle Actuator Controller are separate control modules, communications 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)**		●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
17	Critical communications and data transfer between the ECM/Throttle Actuator Controller and other vehicle systems/components are to be qualified for validity and correctness (plausibility and rationality) including the vehicle speed sensor (ASIL D), engine speed sensor (ASIL D), and all other inputs that are used by the throttle position control algorithm. **(ASIL B/C/D)** • If the vehicle speed and engine speed are used redundantly, then the ASIL classification may be applied based on a selected ASIL decomposition strategy.		●	●
18	All other critical parameters used by the throttle position control algorithm are to be checked periodically based on the FTTI requirements. **(ASIL B/C/D)**		●	●
19	Diagnostics covering the failures for the following parts of the ECM/Throttle Actuator Controller are to be implemented: **(ASIL QM/A/B)** • Execution logic (wrong coding, wrong or no execution, execution out of order, execution too fast or too slow, stack overflow or underflow) • On-chip communication and bus arbitration • The main controller's: o CPU o processor memory o arithmetic logic unit o registers o A/D converter o software program execution o connections I/O faults (short/open/drift/oscillation) o power supply o temperature • If an auxiliary processor is used, then cover its: o CPU o processor memory (if auxiliary processor is used) o arithmetic logic unit o registers o A/D converter o software program execution o I/O faults (short/open/drift/oscillation) o power supply o temperature • The wiring harnesses and connectors for open and short circuits • Critical messages including CAN messages		●	●
20	The ECM/Throttle Actuator Controller is to have a control algorithm to drive the throttle position for all engine speeds. **(ASIL B/C/D)**		●	●
21	All electrical hardware and software elements associated with the delivery of the control algorithm that drives the throttle position are to comply with ASIL D classification for SG1 and SG4, ASIL C classification for SG5 and SG6, and ASIL B classification for SG2 unless otherwise specified. If independence of the elements (per ISO 26262) cannot be demonstrated, the higher ASIL classification is to be adopted. **(ASIL B/C/D)**		●	●
22	If the ECM and Throttle Actuator Controller are separate control modules, the Throttle Actuator Controller is to drive the throttle to the position commanded by the ECM within TBD time. **(ASIL B/C/D)**		●	●
23	The ECM/Throttle Actuator Controller is to control the throttle position to within a pre-established tolerance band based on the vehicle operating situation. The throttle position is to be controlled to within a tolerance that does not result in a violation of a safety goal. **(ASIL B/C/D)**		●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
24	The ECM/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)**		●	●
25	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 8 (allowing torque production from EPS only) and a Red Light driver warning is to be issued. **(ASIL B/C/D)**		●	●
26	The health and sanity of the control algorithm to drive the throttle position are to be checked periodically based on the correct FTTI in order to prevent 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 to the control algorithm to drive the throttle position. The fault tolerant techniques may include redundancy, voting logic, or other techniques. • Control flow monitoring strategy is to be applied for the control algorithm to drive the throttle position.		●	●
27	Critical communications and data transfer between the ECM/Throttle Actuator Controller and other gasoline ICE propulsion subsystem components are to be qualified for validity and correctness (plausibility and rationality); this includes: **(ASIL B/C/D)** • 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.		●	●
28	All other critical parameters used by the control algorithm to drive the throttle position are to be checked periodically based on the FTTI requirements. Critical parameters are parameters, which when incorrect, may lead to violation of a safety goal. **(ASIL B/C/D)**		●	●
29	The output of the control algorithm that drives the throttle position is to be verified for validity and correctness. **(ASIL B/C/D)**		●	●
30	The ECM is to have a mechanism to prevent unauthorized access to the throttle position control calculations and command path. **(ASIL B/C/D)**		●	●
31	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 case of unauthorized access to the ECM, the ACS/ETC is to transition to Safe State 6 within TBD ms and a red light driver warning is to be issued. • A DTC is to be set.		●	●
32	If the Throttle Actuator Controller and ECM are separate control modules, the Throttle Actuator Controller is to communicate any faults to the ECM. **(ASIL B/C/D)**		●	●
33	In case of a fault in the control algorithm that drives the throttle position that leads to violation of a safety goal, the system is to transition into Safe State 8 (allowing torque production from EPS only) within TBD ms time. **(ASIL B/C/D)** • 200 ms is considered in the industry for similar safety goals. • A Red Light driver warning is to be issued. • DTCs are to be set.		●	●

S HEV = Series HEV
P HEV = Parallel HEV
S-P HEV = Series-Parallel HEV

9.2.6 Power Split Device Functional Safety Requirements

There are nine functional safety requirements derived for the PSD subsystem. These requirements only apply to the series-parallel HEV ACS/ETC architecture. The series HEV ACS/ETC architecture only has one propulsion system and does not include a PSD. The parallel HEV ACS/ETC uses a mechanical coupling to connect the EPS and gasoline ICE powertrain subsystem. The mechanical coupling is typically not as complex as the PSD, which may include multiple gear sets to control power flow between the ICE, the two electric motors, and the drivetrain.

The safety requirements included in this section correspond to Safety Goals SG 1 through SG 6, and SG 8, except where otherwise noted.

Table 52. PSD Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The status of the PSD is to be validated. **(ASIL C/D)**			●
2	The HEV PCM is to command and control the split of the mechanical power of the ICE between the electric motor (in generating mode) and the vehicle drivetrain. **(ASIL B/C/D)**			●
3	The PSD is to split the mechanical power from the ICE between the electric motor (in generating mode) and the vehicle drivetrain in the correct proportion and at the correct time. **(ASIL B/C/D)**			●
4	All electrical hardware and software elements (if any) associated with the split of the ICE power between the electric motor (in generating mode) and the vehicle drivetrain are to comply with ASIL D classification for SG 1 and SG 3, ASIL C classification for SG 4 and SG 5, and ASIL B classification for SG 8 unless otherwise specified. **(ASIL B/C/D)** • If independence of the elements (per ISO 26262) cannot be demonstrated, the higher ASIL classification is to be adopted.			●
5	The PSD is to control the torque to the electric motor (in generating mode) and the vehicle drivetrain to within a pre-established tolerance band based on the vehicle operating scenario. The tolerance is not to result in a violation of a safety goal. **(ASIL B/C/D)**			●
6	The output torque value(s) of the PSD is to be qualified for validity and correctness. **(ASIL B/C/D)**			●
7	All electrical hardware or software single point faults that result in a failure to correctly split and control the split of the ICE power between the electric motor (in generating mode) and the vehicle drivetrain are to be detected and mitigated. **(ASIL B/C/D)** • In case of a failure that leads the PSD to be unable to correctly split or control the split of the ICE power between the electric motor and the vehicle drivetrain, the ACS/ETC is to transition into Safe State 4 within TBD ms, and an Amber Light driver warning is to be issued. • DTCs are to be set.			●
8	Critical communications and data transfer between the PSD and the HEV PCM are to be qualified for validity and correctness (plausibility and rationality). **(ASIL B/C/D)**			●
9	In case of a fault, the PSD is to communicate the fault to the HEV PCM. **(ASIL B/C/D)**			●

S HEV = Series HEV
P HEV = Parallel HEV
S-P HEV = Series-Parallel HEV

9.2.7 Communication Signals Functional Safety Requirements

Five functional safety requirements were derived for the communication signals in the ACS/ETC. Each functional safety requirement corresponds to all safety goals. The critical communication signals for the HEV ACS/ETC may include:

- APPS signal(s) from the APPS to the HEV PCM
- APPS fault diagnostics signal
- BPPS signal to the HEV PCM
- Communication channel "secure" signals between the HEV PCM and the EPS
    - Command for torque/power from HEV PCM to EPS
    - Request to discharge the HV bus from the HEV PCM to the EPS
    - Unauthorized access to HV signal from the EPS to the HEV PCM
    - EPS fault diagnostics signal(s)
    - Motor position signal from the motor position sensor to the TICM
    - Motor position sensor fault diagnostics signal(s)
- Communication channel "secure" signals between the HEV PCM and the ECM/Throttle Actuator Controller[42]
    - Command for torque/power from the HEV PCM to the ECM/Throttle Actuator Controller
    - ECM/Throttle Actuator Controller fault diagnostics signal(s)
- Communication channel "secure" signals between ECM and Throttle Actuator Controller, if these are separate control modules
    - Command for throttle position from the ECM to the Throttle Actuator Controller
    - Throttle Actuator Controller fault diagnostics signal(s)
    - Throttle position signal from the throttle position sensor to the Throttle Actuator Controller
    - Throttle position sensor fault diagnostics signal(s)
- Communication channel "secure" signals between the HEV PCM and the PSD[43]
    - Command to change the power split configuration from the HEV PCM to the PSD
    - Power generation command signal from the HEV PCM to the EPS
    - Start command signal from the HEV PCM to the EPS
    - PSD fault diagnostics signal(s)
- Communication channel "secure" signals between the HEV PCM and:
    - ACC/CC
    - AEB
    - RESS Controller
    - Other systems that can request modification to the propulsion torque

[42] This communication signal only applies to the parallel HEV and series-parallel HEV ACS/ETC architectures.
[43] This communication signal only applies to the series-parallel HEV ACS/ETC architecture.

- Commands/Requests for propulsion torque modifications from interfacing systems to the HEV PCM
- Requests to discharge the HV bus from other vehicle systems to the HEV PCM
- Unauthorized access to HV bus signal from the HEV PCM to the RESS controller
- Open contactors command from the HEV PCM to the RESS
- Vehicle speed signal
- Engine speed signal
- Vehicle direction signal
- Driver warning signal(s)
- Low voltage power loss signal from the low voltage power system to the HEV PCM
- Communication bus failure signal from the communication bus to the HEV PCM

Table 53. Communication Signal Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	All critical communication signals are to be qualified for validity and correctness (plausibility and rationality). The ASIL classifications for the signals are to correspond to the relevant safety goal. If a signal is associated with more than one safety goal, then it is to adhere to the higher ASIL classification. **(ASIL QM/A/B)**	●	●	●
2	The communication bus is to support the communication of the ACS/ETC with the rest of the vehicle systems in order to support the safe operation of the ACS/ETC. **(ASIL B/C/D)**	●	●	●
3	The communication bus is to support the qualification of all critical communication bus signals between the ACS/ETC and the interfacing vehicle systems. **(ASIL B/C/D)**	●	●	●
4	The communication bus is to prevent the corruption of critical communication signals during transmission between the ACS/ETC and the interfacing vehicle systems. **(ASIL B/C/D)**	●	●	●
5	In case of a malfunction of the communication bus or communication bus module, the communication bus system is to inform the HEV PCM. **(ASIL B/C/D)**	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.2.8 Power Supply Functional Safety Requirements

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

Table 54. Power Supply Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The low voltage power supply is to provide the ACS/ETC with the required low voltage (e.g., 12V) power supply for operation. **(ASIL B/C/D)**	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
2	The supply voltage and current are to meet the quality parameters (levels (min, max), ripple, transient, and overshoot) as set by the ACS/ETC system components. The ASIL classification of this requirement is to be based on the safety analysis and the safety goal impacted. **(No ASIL)**	●	●	●
3	The ACS/ETC is to be notified of any malfunction or disruption in the low voltage (e.g., 12V) power supply system operation. **(ASIL B/C/D)**	●	●	●
4	All communications and data transfer sent by the low voltage (e.g., 12V) 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 B/C/D)**	●	●	●
5	The ACS/ETC system is to have a redundant low voltage power supply. In case of a fault in the vehicle 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 system for a duration greater than the longest FTTI of the ACS/ETC. **(ASIL B/C/D)**	●	●	●
6	All single point failure modes that cause the loss of low voltage power (e.g., 12V) are to be prevented or mitigated. **(ASIL B/C/D)** • 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 a Red Light driver warning is to be issued.	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.2.9 Interfacing Systems Functional Safety Requirements

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

Table 55. Interfacing Systems Functional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	All requests or commands from interfacing vehicle systems for propulsion torque modifications or to discharge the HV bus are to be sent to the HEV PCM. This includes: **(ASIL B/C/D)** • Request for a torque increase or decrease from the CC/ACC system • Request for torque reduction from the brake system including the AEB module (directly or indirectly through the braking system module) • Request for torque modification from the TCS • Request for torque modification from the Stability Control System • Request for discharging the HV bus from the RESS • Request for charging from the RESS	● [44]	●	●
2	All communications and data transfer sent by interfacing vehicle systems to the HEV PCM regarding requests or commands for propulsion torque modifications, RESS charging, or discharging the HV bus are to be qualified for validity and correctness (plausibility and rationality) by the sending system. **(ASIL B/C/D)**	● [44]	●	●

[44] Portions of the requirement related to charging the RESS do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
3	All interfacing systems are to inform the HEV PCM in case of any failure that may cause the system to transition into a degraded mode of operation. **(ASIL B/C/D)**	●	●	●
4	In case of a fault in the transmitted information to the HEV PCM from the interfacing system, the correct failure mode effect mitigation strategy is to be applied. **(ASIL B/C/D)**	●	●	●
5	When opened following a vehicle crash or HVIL fault, the contactors are to remain open until the integrity of the HV system has been confirmed. Some examples for confirming the integrity of the HV system may include successful system self-checks and removal of faults. **(ASIL B)**	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

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 [3] in order to ensure the generation of a comprehensive list of safety requirements:

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

Subsequently, this study derives an additional 89 safety requirements related to the ACS/ETC system and components for the three HEV ACS/ETC architectures. 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 HEV ACS/ETC System – 18 requirements
2. AP Assembly – 2 requirements
3. HEV PCM – 24 requirements
4. EPS – 9 requirements
5. Gasoline ICE Powertrain Subsystem – 7 requirements
6. PSD – 1 requirement
7. Communication Signals – 4 requirements
8. Power Supply (low and high voltage) – 2 requirements
9. Interfacing Systems – 22 requirements

9.3.1 Additional General HEV ACS/ETC System-Level Safety Requirements

This study derives 18 general system-level safety requirements for the HEV ACS/ETC system outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements correspond to all safety goals, unless otherwise specified.

Table 56. Additional General HEV ACS/ETC Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The packaging for ACS/ETC components and connections is to meet the standards for 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 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)**	●	●	●
4	The calibration of the safety critical sensors, safety critical actuators, and other safety critical parameters is to be checked and verified to be correct. This includes, but is not limited to, the following: **(ASIL B/C/D)** Safety-critical sensors: • APPS • BPPS • Electric motor speed/position sensor(s) • Electric motor phase/current sensor(s) • Inverter temperature sensor • Transmission range sensor • TPS • Engine speed sensor • Mass air flow sensor • Vehicle speed sensor (may be provided by the Brake/Stability Control Module) • Battery SOC sensor (may be provided by the RESS) • Vehicle crash detection sensors (may be provided by the Occupant Restraint System) Safety critical actuators: • Inverter/converter (power stage) • PSD • Throttle motor Other critical components: • Electric motors • Throttle valve	● [45]	●	●
5	The ACS/ETC components are to meet the reliability and functional degradation requirements. **(ASIL B/C/D)**	●	●	●

[45] Portions of this requirement that reference components in the gasoline ICE powertrain subsystem (e.g., TPS, engine speed sensor, etc.) do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
6	Safety-critical ACS/ETC sensors and actuators are to have TBD failure rate for 100,000 miles and under all normal (TBD) vehicle operating conditions (temperature, vibration, moisture, etc.). **(ASIL C/D)** Failures may include, but not limited to: • Hardware failure • Degradation over time • Internal shorts and increased resistance Safety-critical sensors may include: • APPS • Electric motor speed/position sensor(s) • Electric motor phase/current sensor(s) • Inverter temperature sensor • TPS Safety-critical actuators may include: • Gate drive board • Inverter/converter (power stage) • PSD • Throttle motor	● [45]	●	●
7	The ACS/ETC components and connections are to meet the standards for EMI/EMC and other electrical interference from the environment and other components in the vehicle in order to prevent malfunctioning of the HEV PCM, TICM, ECM/Throttle Actuator Controller, or corruption of software algorithms and critical parameters including the torque maps. **(ASIL B/C/D)**	● [46]	●	●
8	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)**	●	●	●
9	The ACS/ETC components and connections are to meet the vibration and shock impact requirements. **(ASIL B/C/D)**	●	●	●
10	The ACS/ETC components and connections are to be designed to meet the ambient temperature requirements taking into account the packaging location in the vehicle. The temperatures of thermally-sensitive ACS/ETC components are to be monitored. **(ASIL B/C/D)**	●	●	●
11	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)**	●	●	●
12	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)**	●	●	●
13	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)**	●	●	●
14	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)**	●	●	●
15	The AP and BP are to return to the at-rest (i.e., undepressed) position when released by the driver. **(No ASIL)**	●	●	●

[46] Portions of this requirement that reference components in the gasoline ICE powertrain subsystem (e.g., ECM/Throttle Actuator Controller) do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
16	ACS/ETC sensors are to have TBD reporting frequency so that safety critical data is updated with sufficient frequency to prevent violation of a safety goal. Typical ACS/ETC sensors include: **(ASIL B/C/D)** • APPS • Electric motor speed/position sensor(s) • Electric motor phase/current sensor(s) • Inverter temperature sensor • TPS	●	●	●
17	The ACS/ETC software development process is to comply with the state-of-the-art standards for software development like ISO/IEC 15504 and Motor Industry Software Reliability Association (MISRA) C/C++. **(ASIL B/C/D)**	●	●	●
18	The ACS/ETC is to be designed to prevent damage to vehicle components and connections (including other ACS/ETC components) by the HV system (e.g., electrical arcing, corona effects, etc.). **(ASIL B/C/D)**	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.3.2 Accelerator Pedal Assembly Additional Safety Requirements

This study derives two safety requirements for the AP assembly outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements correspond to Safety Goals SG 1, SG 2, SG 4, SG 5, and SG 6.

Table 57. Accelerator Pedal Assembly Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	AP assembly mechanical faults that result in incorrect measurement of the APP are to be detected and mitigated. **(ASIL QM)** • Incorrect measurements include deviations from the correct AP position value or being stuck at the same value permanently or intermittently	●	●	●
2	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)**	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.3.3 HEV Powertrain Control Module Additional Safety Requirements

This study derives 24 HEV PCM safety requirements outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements correspond to all vehicle-level safety goals, unless otherwise specified.

Table 58. HEV PCM Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
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 the appropriate safe state. **(ASIL B/C/D)**	●	●	●
2	The HEV PCM software is to be secured against all unauthorized access. **(ASIL B/C/D)**	●	●	●
3	The HEV PCM is to correctly calculate the motor torque required to maintain the creep speed, and the results are to be qualified for validity and correctness under all vehicle operating conditions. **(ASIL B/C/D) Safety Goal 1 and 4**	●	●	●
4	The HEV PCM is to have specific conditions for entering a degraded operating state (e.g., "limp-home" mode), and is not to enter a degraded operating state unless these conditions are met. **(ASIL C/D) Safety Goals 2 and 4** • The driver is to be notified when the HEV PCM enters a degraded operating state.	●	●	●
5	The HEV PCM software code is to be verified for correctness, including any automatically generated code. **(ASIL B/C/D)**	●	●	●
6	The HEV PCM is to verify the correctness of all clock or internal timing signals. **(ASIL B/C/D)**	●	●	●
7	Any unused circuits or pins in the HEV PCM are to be properly managed so as to prevent unwanted signals or other interference with the ACS/ETC function. **(ASIL B/C/D)**	●	●	●
8	The HEV PCM is to enter or exit BTO mode at the correct time when the conditions for entering or exiting BTO mode are met (dead-time, activation delay, vehicle speed, APP and BPP, etc.). **(ASIL C/D) Safety Goals 1, 2, 4, and 5**	●	●	●
9	In case of a fault in entering or exiting BTO mode, the HEV PCM is to invoke the proper fault mitigation strategy, including transitioning into a safe state, if required, and alerting the driver. **(ASIL C/D) Safety Goals 1, 2, 4, and 5**	●	●	●
10	The HEV PCM BTO control algorithm is to enter BTO mode when the driver presses both the AP and BP simultaneously and the vehicle speed is above the pre-set vehicle speed threshold value for BTO. If the vehicle speed is below the pre-set vehicle speed threshold value for BTO, then the HEV PCM is not to enter the BTO mode. The HEV PCM is to monitor the vehicle speed. **(ASIL C/D) Safety Goals 1, 2, 4, and 5**	●	●	●
11	The HEV PCM is not to enter BTO mode when the BP is not pressed. **(ASIL C/D) Safety Goals 1, 2, 4, and 5**	●	●	●
12	The HEV PCM is not to exit BTO mode while both the AP and BP are still pressed. **(ASIL C/D) Safety Goals 1, 2, 4, and 5**	●	●	●
13	When exiting BTO mode, the HEV PCM is to resume responding to the driver's request via the AP. **(ASIL C) Safety Goal 2**	●	●	●
14	The HEV PCM is not to command an increase in the net power/torque delivered to the wheels while in BTO mode or while transitioning into BTO mode. **(ASIL C/D) Safety Goals 1 and 5**	●	●	●
15	The HEV PCM is not to command an increase in the net power/torque to the wheels 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 D) Safety Goal 1**	●	●	●
16	Incorporating additional requirements into the BTO algorithm beyond the APP, BPP, and vehicle speed is not to prevent the HEV PCM from entering BTO mode when the driver's intention is to stop the vehicle. **(ASIL C/D) Safety Goals 1 and 5**	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
17	Incorporating additional requirements into the BTO algorithm beyond the APP and BPP, and vehicle speed is not to prevent the HEV PCM from exiting BTO mode when the driver's intention is to resume acceleration. **(ASIL C) Safety Goal 2**	●	●	●
18	The ACS/ETC is to supply the correct reference voltage to the ACS/ETC sensors. **(ASIL B/C/D)**	●	●	●
19	The HEV PCM is to detect disruptions in the reference voltage supplied to the ACS/ETC sensors (e.g., too high, too low, missing, etc.) and transition into the appropriate safe state. **(ASIL A/B)**	●	●	●
20	The HEV PCM is to detect erroneous torque commands issued by malicious intruders or aftermarket components. **(ASIL C/D) Safety Goals 1 through 5**	●	●	●
21	The HEV PCM is to open the contactors following a vehicle crash or HVIL fault within TBD seconds. **(ASIL B) Safety Goal 7**	●	●	●
22	The HEV PCM is to qualify the vehicle crash sensor (or Occupant Restraint System) signal for validity and correctness. **(ASIL B) Safety Goal 7**	●	●	●
23	The HEV PCM is to qualify the HVIL sensor signal for validity and correctness. **(ASIL B) Safety Goal 7**	●	●	●
24	If the engine is operating as the sole propulsion source (e.g., the electric powertrain subsystem is offline), the HEV PCM is to have algorithms to maintain the engine torque output at the idle speed. **(ASIL B/C/D) Safety Goals 1 and 5**		●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.3.4 Electric Powertrain Subsystem Additional Safety Requirements

This study derives nine safety requirements for the EPS outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements correspond to all safety goals, unless otherwise specified.

Table 59. EPS Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The TICM software is to be secured against all unauthorized access. **(ASIL B/C/D)**	●	●	●
2	The TICM is to have specific conditions for entering a degraded operating state (e.g., "limp-home" mode), and is not to enter a degraded operating state unless these conditions are met. **(ASIL C/D) Safety Goals 2 and 4** • The HEV PCM and the driver are to be notified when the TICM enters a degraded operating state.	●	●	●
3	The TICM software code is to be verified for correctness, including any automatically generated code. **(ASIL B/C/D)**	●	●	●
4	The TICM is to verify the correctness of all clock or internal timing signals. **(ASIL B/C/D)**	●	●	●
5	Any unused circuits or pins in the TICM are to be properly managed so as to prevent unwanted signals or other interference with the ACS/ETC function. **(ASIL B/C/D)**	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
6	The HEV PCM is to detect failures in the cooling system, including the coolant delivery mechanism (e.g., hoses, piping, ducts, etc.). In the event of a failure in the cooling system, the ACS/ETC is to enter the appropriate safe state to prevent violation of any safety goals. **(ASIL C/D) Safety Goals 2 and 4**	●	●	●
7	The inverter temperature sensor is to be positioned to ensure accurate and representative measurements of the power stage temperature. **(ASIL A/B) Safety Goals 2 and 4**	●	●	●
8	The HV power supply to the electric motor is to meet the requirements for quality (e.g., transients, phase, spikes, noise, etc.). **(ASIL QM)**	●	●	● [47]
9	The ACS/ETC is to maintain the power stage temperature within the operating range. This includes ensuring proper calibration of safety critical parameters for the cooling system in the HEV PCM. **(ASIL B/C/D) Safety Goals 2 and 4** • If the power stage temperature cannot be maintained within the acceptable operating range, the ACS/ETC is to enter the appropriate safe state and warn the driver. • If the cooling system does not operate continually, this includes ensuring the cooling system is operated with the correct timing and duration.	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.3.5 Gasoline ICE Powertrain Subsystem Additional Safety Requirements

This study derives seven safety requirements for the gasoline ICE powertrain subsystem outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements only apply to the parallel HEV and series-parallel HEV ACS/ETC architectures, where the gasoline ICE is used to supply propulsion to the drivetrain. These requirements correspond to Safety Goals SG 1, SG 2, SG 4, SG 5, and SG 8, unless otherwise specified.

Table 60. Gasoline ICE Powertrain Subsystem Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The ECM/Throttle Actuator Controller software is to be secured against all unauthorized access. **(ASIL B/C/D)**		●	●
2	The gasoline ICE powertrain subsystem is to have specific conditions for entering a degraded operating state (e.g., "limp-home" mode), and is not to enter a degraded operating state unless these conditions are met. **(ASIL C/D) Safety Goals 2 and 4** • The HEV PCM and the driver are to be notified when either the gasoline ICE powertrain subsystem enters a degraded operating state.		●	●
3	The ECM/Throttle Actuator Controller software code is to be verified for correctness, including any automatically generated code. **(ASIL B/C/D)**		●	●
4	The ECM/Throttle Actuator Controller is to verify the correctness of all clock or internal timing signals. **(ASIL B/C/D)**		●	●

[47] This requirement includes both electric motors in the series-parallel HEV ASC/ETC architecture, if both motors are used to supply propulsion.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
5	Any unused circuits or pins in the ECM/Throttle Actuator Controller are to be properly managed so as to prevent unwanted signals or other interference with the ACS/ETC function. **(ASIL B/C/D)**		●	●
6	If maintaining the engine at idle speed, the ECM/Throttle Actuator Controller 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) Safety Goal 1 and 4**		●	●
7	The air intake stream is to be protected against any contamination or debris that could affect the movement of the throttle valve. **(ASIL B/C/D)**		●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.3.6 Power Split Device Additional Safety Requirements

This study derives one safety requirement for the PSD that is outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). This requirement only applies to the series-parallel HEV ACS/ETC architecture and applies to all safety goals.

Table 61. PSD Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The PSD is to prevent mechanical locked conditions. **(No ASIL)** • In case of a failure to prevent a mechanical locked condition, the HEV PCM is to transition into Safe State 6, and a Red Light driver warning is to be issued.			●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.3.7 Communication Signals Additional Safety Requirements

This study derives four safety requirements for critical communication signals that are outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements correspond to all safety goals. The critical communication signals are listed in Section 9.2.7.

Table 62. Communication Signal Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The communication bus is to be secured against unauthorized access. **(ASIL B/C/D)**	●	●	●
2	The communication bus signal prioritization strategy is to allow the TBD reporting frequency for data critical to the safe functioning of the ACS/ETC. The reporting frequency is to allow for the timely update of safety-critical data to prevent violation of any safety goals. **(ASIL B/C/D)**	●	●	●
3	The HEV PCM is to detect intermittent communication signals in the ACS/ETC system. **(ASIL QM/A/B)**	●	●	●

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
4	Interfacing vehicle systems are to detect and inform the HEV PCM of intermittent communication signals between safety critical sensors and the ACS/ETC system. **(ASIL QM/A/B)**	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

9.3.8 Power Supply Additional Safety Requirements

This study derives two safety requirements for the power supply that are outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements correspond to all safety goals, unless otherwise specified.

Table 63. Power Supply Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The necessary supply voltage is to be supplied to interfacing sensors critical to the safe operation of the ACS/ETC and is to meet the quality parameters (levels (min, max), ripple, transient, and overshoot) as set by these safety critical sensors. The ASIL classification of this requirement is to be based on the safety analysis and the safety goal impacted. Typical safety critical interfacing sensors include: **(No ASIL)** • BPPS • Transmission range sensor • Engine speed sensor • Mass air flow sensor • Vehicle speed sensor (may be provided by the Brake/Stability Control Module) • Battery SOC sensor (may be provided by the RESS) • Vehicle crash detection sensor (may be provided by the Occupant Restraint System)	● [48]	●	●
2	In the event of a vehicle crash, the low voltage power supply is to maintain the low voltage (12V) power supply to the ACS/ETC for a sufficient duration to allow discharging of the HV bus and opening of the contactors. **(ASIL B) Safety Goal 7**	●	●	●
S HEV = Series HEV P HEV = Parallel HEV S-P HEV = Series-Parallel HEV				

[48] Portions of this requirement related to the gasoline ICE powertrain subsystem (e.g., engine speed sensor) do not apply to the series HEV ACS/ETC architecture.

9.3.9 Interfacing Systems Additional Safety Requirements

This study derives 22 safety requirements for interfacing vehicle systems that are outside the ISO 26262 Functional Safety Concept scope (Part 3 of ISO 26262 [2]). These requirements correspond to all safety goals, unless otherwise specified.

Table 64. Interfacing Systems Additional Safety Requirements

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
1	The electric motor is to prevent locked motor rotor conditions. This requirement is not covered by ISO 26262, but it is to be assigned a safety relevant classification during the development effort. **(ASIL B/C/D) Safety Goals 1, 2, 3, 4, and 5** • In case of a failure to prevent a locked rotor condition, the vehicle system controller is to transition into Safe State 6, and a Red Light driver warning is to be issued.	●	●	●
2	Interfacing sensors critical to the safe functioning of the ACS/ETC are to have the correct reference voltage supply. Safety-critical interfacing sensors may include: **(ASIL B/C/D)** • BPPS • Transmission range sensor • Engine speed sensor • Mass air flow sensor • Vehicle speed sensor (may be provided by the Brake/Stability Control Module) • Battery SOC sensor (may be provided by the RESS) • Vehicle crash detection sensor (may be provided by the Occupant Restraint System)	● [49]	●	●
3	Interfacing systems are to inform the HEV PCM of any disruptions to the reference voltage supplied to sensors critical to the safe functioning of the ACS/ETC (e.g., too high, too low, missing, etc.). **(ASIL B/C/D)**	●	●	●
4	The BPP value is to be measured, and the value is to be valid and correct. **(ASIL B/C/D) Safety Goals 1, 2, 4, and 5**	●	●	●
5	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) Safety Goals 1, 2, 4, and 5**	●	●	●
6	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) Safety Goals 1, 2, 4, and 5**	●	●	●
7	BP mechanical assembly faults that result in incorrect measurement of the BPP are to be detected and mitigated. **(No ASIL) Safety Goals 1, 2, 4, and 5** • Incorrect measurements include deviations from the correct BPP value or being stuck at the same value permanently or intermittently.	●	●	●
8	Propulsion torque modification capable systems are to correctly identify themselves according to the HEV PCM prioritization strategy when issuing torque requests to the HEV PCM. **(ASIL B/C/D) Safety Goals 1, 2, 4, 5, and 6**	●	●	●
9	The interfacing system components critical to the safe functioning of the ACS/ETC are to meet the reliability and degradation requirements. **(ASIL B/C/D)**	●	●	●

[49] Portions of this requirement related to the gasoline ICE propulsion subsystem (e.g., engine speed sensor) do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
10	The packaging for interfacing system components and connections critical to the safe functioning of the ACS/ETC is to meet the standards for packaging clearances. **(ASIL B/C/D)**	●	●	●
11	The interfacing system components and connections critical to the safe functioning of the ACS/ETC are to be protected from physical interference from foreign objects (e.g., road debris). **(ASIL B/C/D)**	●	●	●
12	The interfacing system components and connections critical to the safe functioning of the ACS/ETC (e.g., vehicle speed, battery SOC, transmission range, etc.) are to be designed to meet the ambient temperature requirements, taking into account the packaging location in the vehicle. **(ASIL B/C/D)** • The temperatures of the interfacing system sensors critical to the safe functioning of the ACS/ETC (e.g., transmission range sensor, vehicle speed sensor, battery SOC sensor, etc.) are to be monitored.	●	●	●
13	The interfacing system assemblies critical to the safe functioning of the ACS/ETC are to be free from manufacturing defects. This includes component and connection manufacturing quality in the assembly process. **(ASIL B/C/D)**	●	●	●
14	The interfacing vehicle system components and connections critical to the safe functioning of the ACS/ETC are to meet the standards for EMI/EMC and other electrical interference from the environment and other components in the vehicle. **(ASIL B/C/D)**	●	●	●
15	The interfacing system components and connections critical to the safe functioning of the ACS/ETC are to meet the contamination ingress protection requirements and the corrosion protection requirements. This includes moisture, corrosion, or contamination from the environment or other vehicle components. **(ASIL B/C/D)**	●	●	●
16	The interfacing system components and connections critical to the safe functioning of the ACS/ETC are to meet the vibration and shock impact requirements. **(ASIL B/C/D)**	●	●	●
17	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)**	●	●	●
18	The interfacing system components critical to the safe functioning of the ACS/ETC are to mitigate the effects of magnetic interference from other vehicle components, as well as the external environment. **(ASIL B/C/D)**	●	●	●
19	Interfacing sensors critical to the safe functioning of the ACS/ETC are to have TBD reporting frequency so that the safety critical data is updated with sufficient frequency to prevent violation of a safety goal. Typical safety critical interfacing sensors include: **(ASIL B/C/D)** • BPPS • Transmission range sensor • Engine speed sensor • Mass air flow sensor • Vehicle speed sensor (may be provided by the Brake/Stability Control Module) • Battery SOC sensor (may be provided by the RESS) • Vehicle crash detection sensor (may be provided by the Occupant Restraint System)	● [50]	●	●

[50] Portions of this requirement related to the gasoline ICE propulsion subsystem (e.g., engine speed sensor) do not apply to the series HEV ACS/ETC architecture.

Req. No.	Functional Safety Requirement	S HEV	P HEV	S-P HEV
20	Interfacing sensors critical to the safe functioning of the ACS/ETC are to have TBD failure rate for 100,000 miles and under all normal (TBD) vehicle operating conditions (temperature, vibration, moisture, etc.). Sensor failures may include, but not limited to: **(ASIL QM)** • Hardware failure • Degradation over time • Internal short and increased resistance Typical safety critical interfacing sensors include: • BPPS • Transmission range sensor • Engine speed sensor • Mass air flow sensor • Vehicle speed sensor (may be provided by the Brake/Stability Control Module) • Battery SOC sensor (may be provided by the RESS) • Vehicle crash detection sensor (may be provided by the Occupant Restraint System)	● [50]	●	●
21	Software code for control modules in interfacing systems that are critical for the safe functioning of the ACS/ETC is to be verified for correctness, including any automatically generated code. This may include the following control modules: **(ASIL B/C/D)** • Brake/Stability Control Module (if used to process and communicate vehicle speed information) • RESS (if used to process and communicate information about the status of the high voltage system) • Occupant Restraint System (if used to detect and report a vehicle crash)	●	●	●
22	The inverter cooling system is to provide sufficient cooling for the power stage under all vehicle operating conditions. If the inverter cooling system also supplies cooling for other vehicle components (e.g., the electric motor), then cooling system is to be able to provide sufficient cooling for all connected components under all vehicle operating conditions. **(ASIL C/D) Safety Goal 2 and 4**	●	●	●

S HEV = Series HEV
P HEV = Parallel HEV
S-P HEV = Series-Parallel HEV

10 OBSERVATIONS

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

10.1 ASIL Dependence on a Feature's Operational Situations

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

However, for a feature that may not be used in all of the vehicle operational situations, the ASIL could be too stringent. This project identified at least one feature that only operates in a subset of the operational situations — the Hill Holder feature only operates when the vehicle speed is zero. The ASIL for operational situations when vehicle speed is zero is much less severe than the worst-case operational situation, mainly due to the lower severity at the lower speed (this assumes the vehicle does not reach high speeds, which may have higher severity). Therefore, H1.a has an ASIL B, while H1 has an ASIL D (Table 34).

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 28 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 28, 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 [21]. In addition, naturalistic driving data may also help contribute to the variable list. The benefits of using the variables in the existing NHTSA databases could include:

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

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

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

10.3 Variations in the Automotive Safety Integrity Level Assessment

In the course of this study, not all safety analysts on the project team agreed to the same assessment for exposure and controllability. This is due to the fact that objective data typically do not exist to support the assessment, and expert opinions are often used. This observation corroborates previous assessments of ISO 26262 [22] [23].

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 [24]. 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 [22] [23].

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 publically 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 154 potential safety requirements for the three HEV ACS/ETC system architectures following the Concept Phase process (Part 3) in ISO 26262 standard [2]. 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 HEV ACS/ETC system.
- This study applies three hazard and safety analysis methods — the HAZOP study, Functional FMEA, and STPA. While the automotive industry is familiar with the HAZOP study and Functional FMEA, STPA is a relatively new method. For those who are following the ISO 26262 process for functional safety, this study may serve as an example of the use and results of STPA.

12 CONCLUSIONS

This study followed the Concept Phase process (Part 3) in ISO 26262 standard [2] to derive a list of potential safety requirements for a generic ACS/ETC system. Specifically, this research:

1. Identified eight vehicle-level safety goals for the three HEV ACS/ETC architectures and assessed their ASILs:

ID	Safety Goals	ASIL	S HEV	P HEV	S-P HEV
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 with the identified ASIL.	D	●	●	●
SG 1a	Potential uncontrolled vehicle propulsion resulting in vehicle acceleration greater than TBD m/s^2 with zero speed at start is to be mitigated in accordance with the identified ASIL.	B	●	●	●
SG 2	Potential insufficient vehicle propulsion[i] is to be mitigated in accordance with the identified ASIL.	C[ii]	●	●	●
SG 3	Potential vehicle movement in the wrong direction is to be mitigated in accordance with the identified ASIL.	C	●	●	●
SG 4	Potential propulsion power loss/reduction resulting in vehicle deceleration greater than TBD m/s^2 is to be mitigated in accordance with the identified ASIL.	D	●	●	●
SG 5	Potential insufficient vehicle deceleration[i] is to be mitigated in accordance with the identified ASIL.	C[ii]	●	●	●
SG 6	ACS/ETC control algorithm is to choose the torque command that has the highest priority for safety in accordance with the identified ASIL.	D	●	●	●
SG 7	Potential electric shock is to be mitigated in accordance with the identified ASIL.	B	●	●	●
SG 8	Potential RESS thermal events are to be prevented in accordance with the identified ASIL.	C		●	●

S HEV = Series HEV
P HEV = Parallel HEV
S-P HEV = Series-Parallel HEV

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

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

As shown by SG 2 and SG 5 in the above table, ASIL assessments can vary between analysts without the support of objective data. Variations in the ASIL assessment may lead to different 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 publically available data are available to support assessment of controllability.

2. Developed the functional safety concept and identified 171 illustrative functional safety requirements by following the Concept Phase in the ISO 26262 standard, combining the results of the two safety analyses (Functional FMEA and STPA), and leveraging industry practice experiences. The breakdown of the number of requirements is as follows:

    - General HEV ACS/ETC System – 11 requirements
    - AP Assembly – 8 requirements
    - HEV PCM – 55 requirements
    - EPS – 39 requirements
    - Gasoline ICE Powertrain Subsystem – 33 requirements
    - PSD – 9 requirements
    - Communication Signals – 5 requirements
    - Power Supply (low and high voltage) – 6 requirements
    - Interfacing Systems – 5 requirements

3. Identified additional 89 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 [3]. The breakdown of the number of requirements is as follows:

    - General HEV ACS/ETC System – 18 requirements
    - AP Assembly – 2 requirements
    - HEV PCM – 24 requirements
    - EPS – 9 requirements
    - Gasoline ICE Powertrain Subsystem – 7 requirements
    - PSD – 1 requirement
    - Communication Signals – 4 requirements
    - Power Supply (low and high voltage) – 2 requirements
    - Interfacing Systems – 22 requirements

    These 89 requirements are out of the scope of the Functional Safety Concept phase in ISO 26262 (Part 3 of the ISO 26262 standard). 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 89 requirements.

REFERENCES

[1] Van Eikema Hommes, Q. D., Becker, C., & Najm, W. (2018, August). *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.

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

[3] US Department of Defense, "MIT-STD-882E: Department of Defense Standard Practice: System Safety.," 2012.

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

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

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

[7] J. Thomas, "Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis," MIT Ph.D. Dissertation, 2013.

[8] O. Coudert, "Two Level Logic Minimization: An Overview," *Integration, the VLSI Journal*, vol. 17, no. 2, pp. 97-140, 1994.

[9] Toyota Motor Sales, UCA, Inc., "Brake Override System," 10 March 2010. [Online]. Available: http://toyota2.tekgroupweb.com/article_download.cfm?article_id=2390. [Accessed 28 January 2015].

[10] Allison Electric Drives, "eLearning - Allison Electric Drive Theory of Operation," 20 November 2008. [Online]. Available: http://portal1.cdta.org/maintenance/eLearning/Allison%20Electric%20Drive%20Theory%20of%20Operation.pdf. [Accessed 8 December 2014].

[11] B. Berman, "Hybrid Car Affordability Leaps Forward with P2 Technology," HybridCars.com, 19 April 2011. [Online]. Available: http://www.hybridcars.com/hybrid-car-affordability-leaps-forward-p2-technology-29761/. [Accessed 8 December 2014].

[12] M. Ehsani, Y. Gao and A. Emadi, "Technical Overview of Toyota Prius," in *Modern Electric, Hybrid Electric, and Fuel Cell Vehicles*, Boca Raton, CRC Press, 2010, pp. 499-518.

[13] M. Ehsani, Y. Gao and J. Miller, "Hybrid Electric Vehicles: Architecture and Motor Drives," *Proceedings of the IEEE*, vol. 95, no. 4, pp. 719-728, 2007.

[14] W. Liu, Introduction to Hybrid Vehicle System Modeling and Control, Hoboken: John Wiley & Sons, Inc., 2013.

[15] C. Mi, M. A. Masrur and D. W. Gao, Hybrid Electric Vehicles: Principles and Applications with Practical Perspectives, West Sussex: John wiley & Sons, Ltd., 2011.

[16] J. M. Miller, "Hybrid Electric Vehicle Propulsion System Architectures of the e-CVT Type," *IEEE Transactions on Power Electronics*, vol. 21, no. 3, pp. 756-767, 2006.

[17] J. Miller, Propulsion Systems for Hybrid Vehicles, London: Institution of Electrical Engineers, 2004.

[18] Toyota Motor Corporation, *Toyota Hybrid System: THS II*, Toyota Motor Corporation, Public Affairs Division, 2003.

[19] N. Gordon-Bloomfield, "Should Electric Cars Mimic the Gasoline Driving Experience," Green Car Reports, 15 June 2011. [Online]. Available: http://www.greencarreports.com/news/1061657_should-electric-cars-mimic-the-gasoline-driving-experience. [Accessed 8 December 2014].

[20] Honda Motor Co., Inc., *The Honda IMA System*, American Honda Motor Co., Inc., 2012, pp. 10-11.

[21] National Highway Traffic Safety Administration, "National Automotive Sampling System (NASS) General Estimate System (GES) Analytical User's Manual, 1998-2012," US Department of Transportation, National Highway Traffic Safety Administration, Washington DC.

[22] Q. Van Eikema Hommes, "Review and Assessment of the ISO 26262 Draft Road Vehicle - Functional Safety (SAE 2012-01-0025)," in *Society of Automotive Engineers World Congress*, Detroit, MI, 2012.

[23] Q. Van Eikema Hommes, "Assessment of Relevant Safety Standards for Automotive Electronic Control Systems," US Department of Transportation, 2014 (under review by the National Highway Traffic Safety Administration).

[24] D. Kahneman, Thinking, Fast and Slow, Farrar, Strause, and Giroux, April 2013.

[25] Robert Bosch GmbH, "Gasoline Port Fuel Injection," 2013. [Online]. Available: http://www.bosch-mobility-solutions.com/media/en/ubk_europe/db_application/downloads/pdf/antrieb/de_5/pfi_full_de.pdf. [Accessed 6 February 2015].

[26] Clemson University, "Electronic Throttle Control," The Clemson University Vehicular Electronics Laboratory, [Online]. Available: http://www.cvel.clemson.edu/auto/systems/throttle_control.html. [Accessed 6 February 2015].

[27] NASA Engineering and Safety Center, "National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation," NESC Assessment #: TI-10-00618, 2011.

[28] Q. Van Eikema Hommes, "Applying STAMP Framework to Analyze Automotive Recalls," in *MIT STAMP/STPA Workshop 2014*, Cambridge, MA, 2014.

[29] Q. Van Eikema Hommes, C. Becker, W. Najm and C. Won, "A Scientific Foundation for Analyzing Safety Issues in Automotive Electronic Control Systems," 2014 (under review by the National Highway Traffic Safety Administration).

[30] W. Rippel, "Induction Versus DC Brushless Motors," Tesla Motors, 9 January 2007. [Online]. Available: http://www.teslamotors.com/blog/induction-versus-dc-brushless-motors. [Accessed 14 August 2015].

[31] G. Solberg, "The Magic of Tesla Roadster Regenerative Braking," TeslaMotors.com, 29 June 2007. [Online]. Available: http://www.teslamotors.com/blog/magic-tesla-roadster-regenerative-braking. [Accessed 8 December 2014].

[32] C. Lampton, "How Regenerative Braking Works," HowStuffWorks.com, 23 January 2009. [Online]. Available: http://auto.howstuffworks.com/auto-parts/brakes/brake-types/regenerative-braking.htm. [Accessed 8 December 2014].

[33] I. Alcala, A. Claudio and G. V. Guerrero, "Analysis of Propulsion Systems in Electric Vehicles," in *International Converence on Electrical and Electronics Engineering*, Mexico City, 2005.

[34] N. Krohn, "Freescale - Building a Basic Inverter," September 2013. [Online]. Available: http://www.freescale.com/files/training/doc/dwf/DWF13_AMF_AUT_T0144.pdf. [Accessed 14 August 2015].

[35] C. Whaling, "Electric Drive Power Electronics: An Overview," IEEE Transportation Electrification, 2 December 2013. [Online]. Available: http://electricvehicle.ieee.org/2013/12/02/electric-drive-power-electronics-an-overview/. [Accessed 19 August 2015].

Appendix A: STPA Causal Factor Guidewords and Guidewords Subcategories

Figure A-1. Causal Factor Categories for Automotive Electronic Control Systems A-2

Table A-1. Causal Factor Sub-Categories A-3

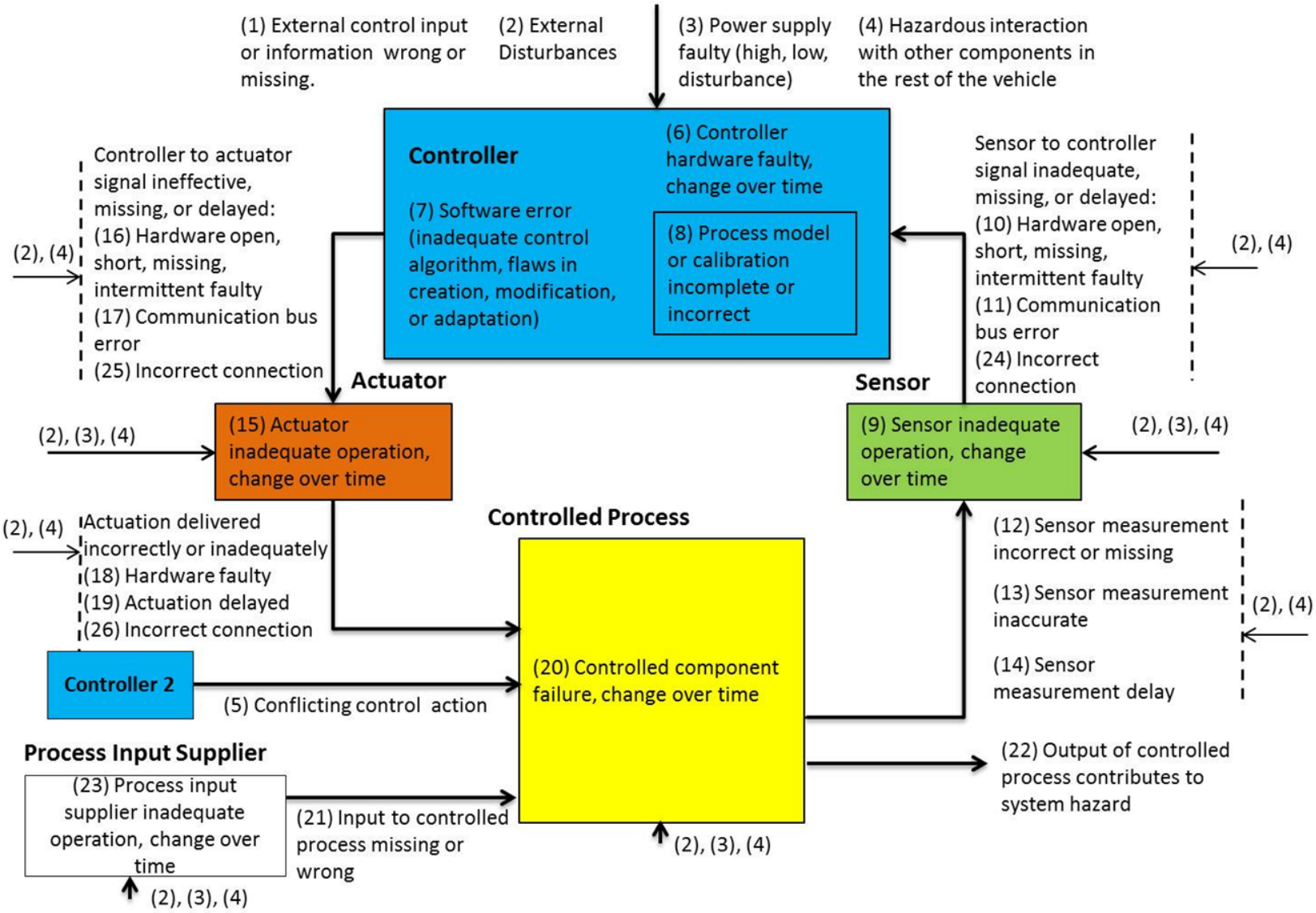


Figure A-1. Causal Factor Categories for Automotive Electronic Control Systems

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

Actuator	**(15) Actuator inadequate operation, change over time** • 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
	(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)
Controlled Process	**(20) Controlled component failure, change over time** • Internal hardware failure • Degradation over time
	(3) Power supply faulty (high, low, disturbance) • Loss of 12-volt power • Power supply faulty (high, low, disturbance)

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 B-2

Table B-2. Function 2: Provide Accelerator Pedal Position to the Engine Control Module B-3

Table B-3. Function 3: Return AP to the Off (Un-Depressed) Position Within a Specified Time B-4

Table B-4. Function 4: Provide AP Request Rate Limiting B-5

Table B-5. Function 5: Control the Throttle Position B-6

Table B-6: Function 6: Communicate the Throttle Position to the ECM B-8

Table B-7. Function 7: Return Throttle to Idle Position Within the Specified Time B-9

Table B-8. Function 8: Establish Throttle Idle Position B-10

Table B-9. Function 9: Provide Idle State Control B-11

Table B-10. Function 10. Provide Brake-Throttle Override Control - Engages at speed > 10 mph B-12

Table B-11. Function 11: Store the APP Torque Maps B-14

Table B-12. Function 12: Communicate With Internal Sub-Systems and External Vehicle Systems B-16

Table B-13. Function 13: Provide Diagnostics and Diagnostics Trouble Codes B-18

Table B-14. Function 14: Provide Fault Detection and Failure Mitigation B-19

Table B-15. Function 15: Store Relevant Data B-20

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 C-2

Table C-2: UCA Assessment for the “Enter Normal Mode” Control Action..... C-3

Table C-3: UCA Assessment for the “Increase Throttle Opening” Control Action..... C-4

Table C-4: UCA Assessment for the “Decrease Throttle Opening” Control Action C-12

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 D-2

Table D-2: Unsafe Control Actions for the "Enter Normal Mode" Control Action..... D-3

Table D-3: Unsafe Control Actions for the "Increase Throttle Opening" Control Action..... D-4

Table D-4: Unsafe Control Actions for the "Decrease Throttle Opening" Control Action..... D-6

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 F-2

Table F-2: Unintended Vehicle Propulsion with Destabilization F-9

Table F-3: Unintended Vehicle Propulsion With Zero Starting Speed F-12

Table F-4: Insufficient Vehicle Propulsion F-14

Table F-5: Propulsion Power Reduction/Loss or Vehicle Stalling without Destabilization F-22

Table F-6: Propulsion Power Reduction/Loss or Vehicle Stalling with Destabilization F-31

Table F-7: Insufficient Vehicle Deceleration F-35

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..... G-2

Table G-2. FMEA for H1a: Uncontrolled Vehicle Propulsion
WWith Zero Starting Speed..... G-10

Table G-3. FMEA for H2: Insufficient Vehicle Propulsion G-17

Table G-4. FMEA for H3: Propulsion Power Reduction/Loss or Vehicle Stalling..... G-24

Table G-5. FMEA for H4: Insufficient Vehicle Deceleration G-31

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		

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	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		
	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/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

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 H-2

Table H-2: Accelerator Pedal Position Sensor H-5

Table H-3: Engine Control Module H-13

Table H-4: Throttle Motor H-24

Table H-5: Throttle Position Sensor H-29

Table H-6: Throttle Valve H-33

Table H-7: Brake/Vehicle Stability Assist Control Module H-37

Table H-8: Brake Pedal Mechanical Assembly H-48

Table H-9: Brake Pedal Position Sensor H-51

Table H-10: Engine Speed (rpm) Sensor H-56

Table H-11: Engine Temperature Sensor H-65

Table H-12: Ignition Key H-71

Table H-13: Mass Air Flow/Manifold Absolute Pressure Sensor H-72

Table H-14: Accelerator Pedal Mechanical Assembly to Accelerator Pedal Position Sensor H-78

Table H-15: Accelerator Pedal Position Sensor to Engine Control Module H-81

Table H-16: Engine Control Module to Throttle Motor H-89

Table H-17: Throttle Motor to Throttle Valve H-97

Table H-18: Throttle Position Sensor to Engine Control Module H-100

Table H-19: Throttle Valve to Throttle Position Sensor H-106

Table H-20: Brake/Vehicle Stability Assist Control Module to Engine Control Module H-108

Table H-21: Brake Pedal Mechanical Assembly to Brake Pedal Position Sensor H-120

Table H-22: Brake Pedal Position Sensor to Engine Control Module H-123

Table H-23: Engine Speed (rpm) Sensor to Engine Control Module H-129

Table H-24: Engine Temperature Sensor to Engine Control Module H-140

Table H-25: Mass Air Flow/Manifold Absolute Pressure Sensor to Engine Control Module H-148

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 812 657
August 2019

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

13779-081519-v3