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

NHTSA

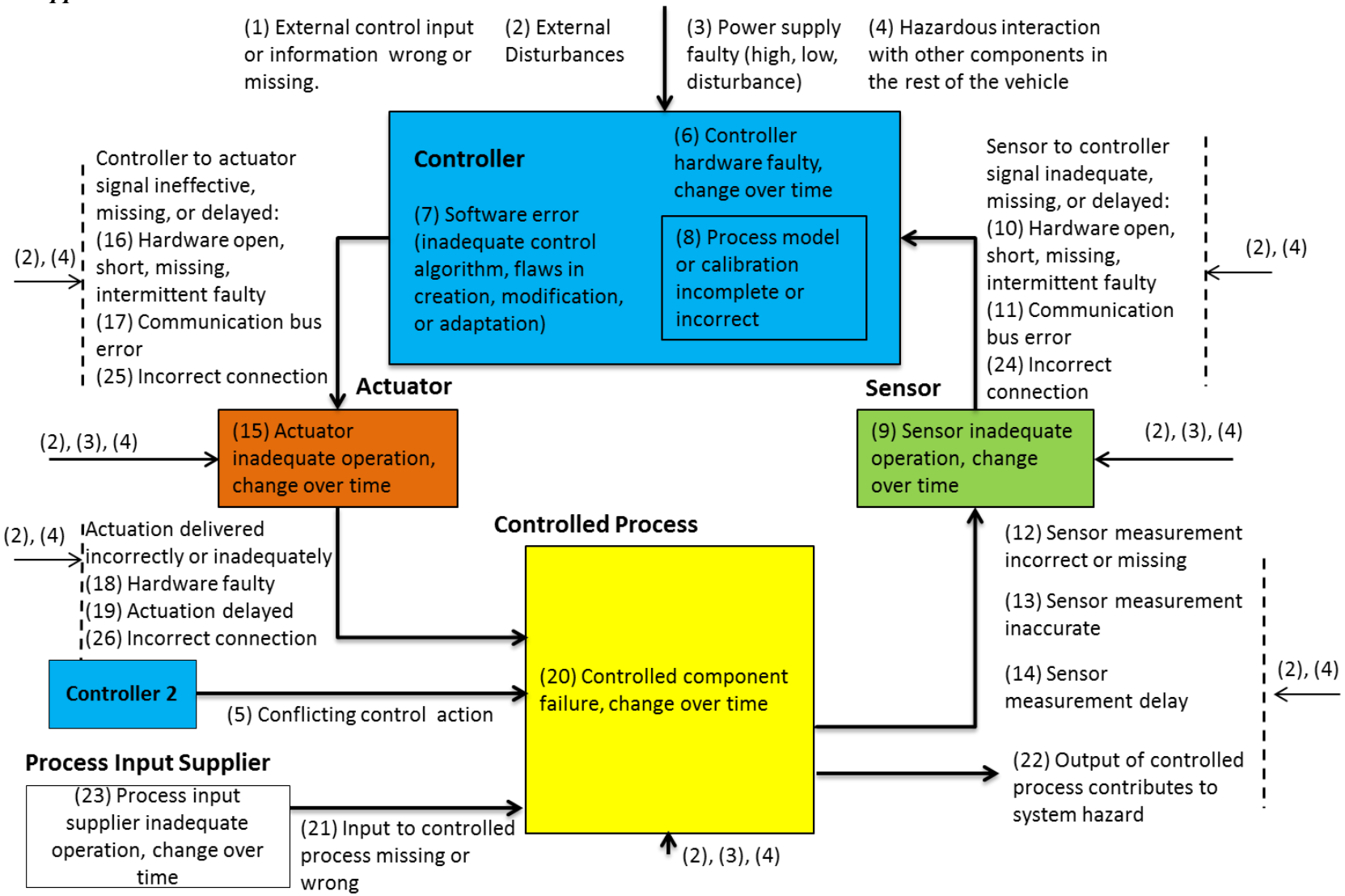
DOT HS 812 556

November 2018

Safety Management of Automotive Rechargeable Energy Storage Systems: The Application of Functional Safety Principles To Generic Rechargeable Energy Storage Systems

Appendices

Appendix A: STPA Causal Factor Guidewords



Appendix B: Functions and Malfunctions Defined in Hazard and Operability Analysis

B.1: First Implementation

The RESS provides the following functions.

1. Accepts and stores HV electrical energy from both on-board and off-board chargers
1. Accepts and stores electrical energy from the vehicle systems during regenerative braking
2. Delivers HV electrical energy to the vehicle's high-voltage DC bus
3. Provides a HV connect/disconnect system between the battery pack and the rest of the vehicle
4. Provides a high-voltage interlock safety system
5. Provides thermal management of the battery cells
6. Provides pressure equalization within the battery pack
7. Provides a battery pack protection against the environment and damage due to mechanical impact or thermal events
8. Provides management (estimation and control) of the battery pack state of charge (SOC)
9. Balances battery cell voltage
10. Monitors moisture condensation within the battery pack
11. Estimates battery state of health
12. Stores appropriate data
13. Measures the electrical current into and out of the battery pack
14. Monitors DC ground fault (HV Isolation) through high-voltage interlock
15. Monitors battery pack voltage
16. Monitors battery pack current
17. Monitors battery pack temperature
18. Monitors battery pack condensation
19. Detects ground faults
20. Provides a control system for the management of the RESS and its interfaces
21. Controls HV contactors
22. Controls battery pack charging, on and off board
23. Controls battery pack discharge (vehicle load management)
24. Controls battery pack regenerative charging
25. Manages faults (diagnostics)
26. Communicates with other vehicle systems and allows communications between the components of the RESS for status signals, control signals, and diagnostics

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
	F1	Does not accept energy	None	
	F1-1	Excessive acceptance of energy	Cell Overheating (Thermal Event)/Cell Venting	
	F1-2	Reduced acceptance of energy	None	
	F1-3	Accepts energy when not supposed to	Cell Overheating (Thermal Event)/Cell Venting	
	F1-4	Continues to accept energy after reaching full State of Charge	Cell Overheating (Thermal Event)/Cell Venting	Same as F1-1
	F2	Does not accept regenerative energy	None	
	F2-1	Excessive acceptance of regenerative energy	Cell Overheating (Thermal Event)/Cell Venting	
	F2-2	Reduced acceptance of regenerative energy	None	
	F2-3	Accepts regenerative energy when not supposed to	Cell Overheating (Thermal Event)/Cell Venting	
	F2-4	Continues to accept regenerative energy after reaching full state of charge	Cell Overheating (Thermal Event)/Cell Venting	Same as F2-1
	F3	Does not deliver energy (loss of high-voltage power)	Unintended deceleration/Loss of some primary vehicle functions	
	F3-1	Delivers excessive energy	None	No load management
	F3-2	Delivers reduced energy	None	
	F3-3	Continues to deliver energy when no demand exists	Exposure to high-voltage	Scenario not possible
F3-4		Delivers the same amount of energy (stuck)	None	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F4	Provides a HV connect/disconnect system between the battery pack and the rest of the vehicle	unintended disconnect from the high-voltage bus	Unintended Vehicle Deceleration/Loss of some primary vehicle functions	
F4-1		unintended connection to the high-voltage bus	Exposure to high-voltage	
F4-2		Intermittent connection when connection intended	unintended vehicle deceleration/Loss of some primary vehicle functions	
F4-3		Intermittent connection when disconnection intended	Exposure to high-voltage	
F4-4		Does not connect when requested	None	
F4-5		Does not disconnect when requested	Exposure to high-voltage	
F5	Provides a High-Voltage Interlock (HVIL) safety system	Does not monitor HVIL	Exposure to high-voltage	
F5-1		Reads open HVIL when closed	None	
F5-2		Reads closed HVIL when open	Exposure to high-voltage	
F5-3		Intermittently reads HVIL	Exposure to high-voltage	
F5-4		Stuck on the same HVIL status	Exposure to high-voltage	
F6	Provides thermal management of the battery cells	Does not command thermal management control	Cell Overheating (Thermal Event)	
F6-1		Commands over-cooling	None	
F6-2		Commands overheating	Cell Overheating (Thermal Event)	
F6-3		Commands under-cooling	Cell Overheating (Thermal Event)	
F6-4		Commands under-heating	None	
F6-5		Commands intermittent cooling	Cell Overheating (Thermal Event)	
F6-6		commands intermittent heating	None	
F6-7		Stuck on same cooling level	Cell Overheating (Thermal Event)	
F6-8		stuck on same heating level	None	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F7	Provides pressure equalization within the battery pack			Not covered by ISO 26262
F8	Provides battery pack protection against the environment and damage due to mechanical impact or thermal events			Not covered by ISO 26262
F9	Provides management (estimation and control) of the battery pack State of Charge (SOC)	Does not estimate the SOC	Cell Overheating (Thermal Event)/Cell Venting	
F9-1		Over estimates the SOC	None	
F9-2		Under estimates the SOC	Cell Overheating (Thermal Event)/Cell Venting	
F9-3		Estimates the SOC intermittently	Cell Overheating (Thermal Event)/Cell Venting	
F9-4		Stuck on one value estimate of the SOC	Cell Overheating (Thermal Event)/Cell Venting	
F10	Balances battery cell voltage	Does not balance the cell voltages	Cell Overheating (Thermal Event)/Cell Venting	in Case of Excessive overcharge
F10-1		Increases cell voltage (over-balance) when not required	Cell Overheating (Thermal Event)/Cell Venting	in Case of Excessive overcharge
F10-2		Decreases cell voltage (under-balance) when not required	None	
F10-3		Balances the cell voltage intermittently	None	
F10-4		Stuck on balance at the same voltage	None	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
		value		
F11	Monitors moisture condensation within the battery pack	Does not measure condensation	None	
F11-1		Measures condensation higher than actual	None	
F11-2		Measures condensation lower than actual	None	
F11-3		Measures condensation intermittently	None	
F11-4		Stuck on the same condensation measurement	None	
F12	Estimates battery State of Health (SOH)	Does not estimate battery SOH	None	None based on this parameter alone.
F12-1		Over estimates (to the better) the battery SOH	None	
F12-2		Under estimates (to the worst) the battery SOH	None	
F12-3		Intermittently estimates the battery SOH	None	
F12-4		Stuck on the same estimate for battery SOH	None	
F13	Stores appropriate data	BMS does not store data	None	
F13-1		BMS under-stores data	None	
F13-2		BMS over-stores data	None	
F13-3		BMS stores data intermittently	None	
F13-4		BMS stores the same data (stuck)	None	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F14	Measures the electrical current into and out of the battery pack	Does not measure current	Cell Overheating (Thermal Event)/Cell venting	SOC estimate on low side
F14-1		Over measurement of current	None	
F14-2		Under measurement of current	Cell Overheating (Thermal Event)/Cell venting	In case of current into the pack
F14-3		Intermittent current measurement	Cell Overheating (Thermal Event)	In case of current into the pack
F14-4		Measurement value stuck on same value	Cell Overheating (Thermal Event)/Cell venting	In case of current into the pack
F15	Monitors DC ground fault (HV Isolation) through High-Voltage Interlock (HVIL)	Does not monitor ground fault	Exposure to high-voltage	Requires multiple point fault
F15-1		Measures isolation higher than true value	Exposure to high-voltage	
F15-2		Measures isolation less than true values	None	
F15-3		Measures isolation intermittently	Exposure to high-voltage	
F15-4		Stuck on the same measured value	Exposure to high-voltage	
F16	Monitors battery pack voltage	Does not monitor the battery pack voltage	Exposure to high-voltage	Function in terms of RESS operation and not the sensors themselves
F16-1		Reads the battery pack voltage lower	None	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
		than it is		
F16-2		Reads the battery pack voltage higher than it is	Exposure to high-voltage	
F16-3		Monitors the battery pack voltage intermittently	Exposure to high-voltage	
F16-4		Stuck at the same reading of the battery pack voltage	Exposure to high-voltage	
F17	Monitors battery pack current	Does not monitor the battery pack current	Cell Overheating (Thermal Event)/Cell Venting	unable to estimate SOC
F17-1		Reads the battery pack discharge current lower than it is	None	
F17-2		Reads the battery pack charge current lower than it is	Cell Overheating (Thermal Event)/Cell Venting	
F17-3		Reads the battery pack discharge current higher than it is	None	
F17-4		Reads the battery pack charge current higher than it is	None	
F17-5		Monitors the battery pack current intermittently	Cell Overheating (Thermal Event)/Cell Venting	
F17-6		Reads positive (out) battery pack current when it is negative	Cell Overheating (Thermal Event)/Cell Venting	
F17-7		Reads negative (in) battery pack current when it is positive	None	
F17-8		Stuck at the same reading of the battery pack current	Cell Overheating (Thermal Event)/Cell Venting	
F18	Monitors battery pack temperature	Does not measure pack temperature	Cell Overheating (Thermal Event)	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F18-1		Measures pack temperature higher than actual	None	
F18-2		Measures pack temperature lower than actual	Cell Overheating (Thermal Event)	
F18-3		Measures pack temperature intermittently	Cell Overheating (Thermal Event)	
F18-4		Stuck on the same pack temperature measurement	Cell Overheating (Thermal Event)	
F19	BMS monitors the condensation within the battery pack	BMS does not monitor condensation sensor	None	BMS fault in itself does not cause a hazard; only a Multiple Point Fault
F19-1		BMS reads condensation sensor output higher	None	
F19-2		BMS reads condensation sensor output lower	None	
F19-3		BMS stuck on condensation sensor reading	None	
F19-4		BMS reads condensation sensor output intermittently	None	
F20	Detects ground fault	Does not detect ground fault	Exposure to high-voltage/Cell Overheating	
F20-1		Measures impedance higher than actual value	Exposure to high-voltage/Cell Overheating	
F20-2		Measures impedance lower than actual value	None	
F20-3		Measures impedance intermittently	Exposure to high-voltage	
F20-4		Stuck on the same impedance value	Exposure to high-voltage	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F21.1	Provides a control system for the management of the RESS and its interfaces: Communication between BMS and sensors	Sensor does not communicate	Cell Overheating (Thermal Event); Exposure to high-voltage/Cell Venting	No feedback from Contactors
F21.1-1		BMS Interprets the messages incorrectly	Cell Overheating (Thermal Event); Exposure to high-voltage/Cell Venting	
F21.1-2		Sensor communicates the wrong message	Cell Overheating (Thermal Event); Exposure to high-voltage/Cell Venting	
F21.1-3		Sensor communicates correct message intermittently	Cell Overheating (Thermal Event); Exposure to high-voltage/Cell Venting	Probably E0
F21.1-4		Sensor communicates message late	Cell Overheating (Thermal Event); Exposure to high-voltage/Cell Venting	Probably E0
F21.1-5		Communicates too frequently	None	
F21.1-6		Communicates less frequently than expected	Cell Overheating (Thermal Event); Exposure to high-voltage/Cell Venting	Probably E0
F21.2	Provides a control system for the management of the RESS and its interfaces: Communication between BMS and other vehicle modules	BMS does not communicate	Cell Overheating (Thermal Event)	
F21.2-1		BMS does not accept communications	Cell Overheating (Thermal Event); Exposure to high-voltage	Too much Regeneration
F21.2-2		BMS communicates incorrect message	Cell Overheating (Thermal Event)	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F21.2-3		BMS receives incorrect message	Exposure to high-voltage	
F21.2-4		BMS interprets the received message incorrectly	Cell Overheating; Exposure to high-voltage (including charger pilot); unintended deceleration;	-Cooling System not working -HVIL -Open contactors -Crash detection -Other
F21.2-5		BMS communicates intermittently	Cell Overheating (Thermal Event)	Probably E0
F21.2-6		BMS receives messages intermittently	Cell Overheating (Thermal Event); Exposure to high-voltage	Probably E0
F21.2-7		BMS communicates less frequently than required	Cell Overheating (Thermal Event)	Probably E0
F21.2-8		BMS receives messages less frequently than required	Cell Overheating (Thermal Event); Exposure to high-voltage	Probably E0
F21.2-9		BMS communicates more frequently	None	
F21.2-10		BMS receives messages more frequently	None	
F22	Controls high-voltage contactors	Does not control the main contactors	Exposure to high-voltage/unintended acceleration	
F22-1		Opens main contactors when not requested	Unintended deceleration	
F22-2		Closes main contactors when not	Exposure to high-voltage	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
		requested		
F22-3		Controls main contactors intermittently	Exposure to high-voltage/unintended acceleration	
F22-4		Stuck open - main contactors	None	
F22-5		Stuck closed - main contactors	Exposure to high-voltage/unintended acceleration	
F22-6		Does not control the charger contactors	None	
F22-7		Opens charger contactors when not requested	None	
F22-8		Closes charger contactors when not requested	None	
F22-9		Controls charger contactors intermittently	None	
F22-10		Stuck open - charger contactors	None	
F22-11		Stuck closed - charger contactors	None	
F22-12		Does not control the pre-charge contactors	None	
F22-13		Opens pre-charge contactors when not requested	None	
F22-14		Closes pre-charge contactors when not requested	None	
F22-15		Controls pre-charge contactors intermittently	None	
F22-16		Stuck open - pre-charge contactors	None	
F22-17		Stuck closed - pre-charge contactors	None	
F23	Controls battery pack charging, on and off board	Does not charge battery pack	None	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F23-1		Overcharges battery pack	Cell Overheating (Thermal Event)/Cell Venting	
F23-2		Under-charges battery pack	None	
F23-3		Intermittently charges the battery pack	None	
F23-4		Continues to charge the battery pack after full SOC	Cell Overheating (Thermal Event)/Cell Venting	
F23-5		Allows charging (charger pilot) when it should not	None	
F24	Controls battery pack discharge (vehicle load management)	Does not provide discharge control	None	
F24-1		allows over-discharge	None	
F24-2		permits only under-discharge	None	
F24-3		Provides discharge control intermittently	None	
F24-4		Stuck on same level of allowable discharge	None	
F25	Controls battery pack regenerative charging	Does not provide regenerative control	Cell Overheating (Thermal Event)/Cell Venting	
F25-1		Accepts more regenerative than the battery pack can handle	Cell Overheating (Thermal Event)/Cell Venting	
F25-2		Accepts less regenerative than the battery pack can handle	None	
F25-3		Accept regenerative intermittently	None	
F25-4		Stuck at accepting the same amount of regeneration	Cell Overheating (Thermal Event)/Cell Venting	

I.D.	Function	Malfunction	Potential Vehicle Level Hazard	Comment
F26	Manages faults (diagnostics)	BMS does not perform diagnostics	Exposure to high-voltage; Cell Overheating (Thermal Event)	
F26-1		BMS performs diagnostics incorrectly	Exposure to high-voltage; Cell Overheating (Thermal Event); Unintended acceleration	
F26-2		BMS performs diagnostics intermittently	Exposure to high-voltage; Cell Overheating (Thermal Event)	
F27	Communicates with other vehicle systems and allows communications between the components of the RESS for status signals, control signals, and diagnostics			Covered in details within other functions

B.2: Second Implementation

The RESS provides the following functions.

1. Provide means of charging Battery - Brake regeneration (ALL), external charging (EV, PHEV) and IC charging (HEV)
2. Provide stored electrical energy to the vehicle
3. Provide Isolation of electrical energy from vehicle chassis & external environment
4. Accept 12V Battery voltage from Vehicle
5. Accept Thermal management (external cooling function) from Vehicle
6. Data Communication with Vehicle
7. Receive Crash/Impact Signal

Functional Hazard and Operational Analysis							
RESS Function Description	**Malfunction (Effect)**						
	Loss of Function	**Incorrect Function (More Than Requested)**	**Incorrect Function (Less Than Requested)**	**Incorrect Function (Wrong Direction)**	**Unintended Activation of Function**	**Locked/Stuck Function**	**Other Malfunc-tions**
Provide means of charging Battery - Brake regeneration (ALL), external charging (EV, PHEV) and IC charging(HEV)	No Charging of Battery	Overcharged Battery	Undercharged or over-discharged Battery	N/A	Overcharged Battery	Overcharged Battery	
Description of Vehicle Hazard ==>	Excessive discharge condition and subsequent re-charge can lead to potential thermal event H2	*Excessive Overcharge condition can lead to potential thermal event* *H1*	*Excessive discharge condition and subsequent re-charge can lead to potential thermal event* *H2*	N/A	*Excessive Overcharge condition can lead to potential thermal event* *H1*	*Excessive Overcharge condition can lead to risk potential thermal event* *H1*	

Functional Hazard and Operational Analysis							
RESS Function Description	**Malfunction (Effect)**						
	Loss of Function	**Incorrect Function (More Than Requested)**	**Incorrect Function (Less Than Requested)**	**Incorrect Function (Wrong Direction)**	**Unintended Activation of Function**	**Locked/Stuck Function**	**Other Malfunc-tions**
Provide stored electrical energy to the vehicle	No availability of electrical energy to vehicle	Excess electrical energy provided to vehicle	Lessened or no availability of electrical energy to vehicle	N/A	Electrical energy provided to vehicle when not requested	Stuck "On" - Electrical energy provided to vehicle when not requested Stuck "off" - No Electrical energy provided to vehicle	RESS internal mechanical failures/ rupture, due to impact shock or mechanical fatigue, resulting in leakage of electrical energy storage medium (s) Single Cell internal failure resulting in excessive energy release to surrounding environment

Functional Hazard and Operational Analysis							
RESS Function Description	**Malfunction (Effect)**						
	Loss of Function	**Incorrect Function (More Than Requested)**	**Incorrect Function (Less Than Requested)**	**Incorrect Function (Wrong Direction)**	**Unintended Activation of Function**	**Locked/Stuck Function**	**Other Malfunc-tions**
Description of Vehicle Hazard ==>	Unintended deceleration (loss of torque) - EV H3 no hazard in HEV, PHEV - IC engine still available for propulsion	Electrical energy propulsion gated to vehicle by Vehicle ECU/Inverter/Motors H8	*Unintended deceleration (insufficient torque) - EV H3* no hazard in HEV, PHEV - IC engine still available for propulsion	N/A	Electrical energy propulsion gated to vehicle by Vehicle ECU/Inverter/Motors H8	Stuck "On" - Electrical energy propulsion gated to vehicle by Inverter/Motors H8 Stuck "Off" - No hazard in HEV, PHEV - IC engine still available for propulsion. In EV, vehicle immobilized/ stranded.	*Exposure to hazardous chemicals and/or gases H4* *Cell energy release can lead to potential thermal event H9*
Provide Isolation of electrical energy from vehicle chassis & external environment	No electrical isolation (Short to Chassis or external environment)	Excessive electrical isolation	Reduced electrical isolation	Reduced electrical isolation	N/A	N/A	
Description of Vehicle Hazard ==>	Electrical shock H5	None	*Electrical shock H5*	*Electrical shock H5*	N/A	N/A	

Functional Hazard and Operational Analysis							
RESS Function Description	**Malfunction (Effect)**						
	Loss of Function	**Incorrect Function (More Than Requested)**	**Incorrect Function (Less Than Requested)**	**Incorrect Function (Wrong Direction)**	**Unintended Activation of Function**	**Locked/Stuck Function**	**Other Malfunc-tions**
Accept 12V Battery voltage from Vehicle	Loss of 12V battery voltage	Overvoltage on 12V battery	Undervoltage on 12V battery	N/A	N/A	N/A	Transients on 12V battery (Load dump, Conducted EMC, etc.)
Description of Vehicle Hazard ==>	Potential for unintended deceleration (loss of torque) - EV only H3 no hazard in HEV, PHEV - IC engine still available for propulsion	*Potential for numerous hazardous RESS ECU malfunctions:* *1) Overcharge H2* *2) Unintended deceleration H3* *3) Excessive discharge H1* *All to be addressed in Safety Concept*	*Potential for numerous hazardous RESS ECU malfunctions:* *1) Overcharge H2* *2) Unintended deceleration H3* *3) Excessive discharge H1* *All to be addressed in Safety Concept*	N/A	N/A	N/A	*Potential for numerous hazardous RESS ECU malfunctions:* *1) Overcharge H2* *2) Unintended deceleration H3* *3) Excessive discharge H1* *All to be addressed in Safety Concept*
Accept Thermal management (external cooling function) from Vehicle	Loss of external cooling	Excessive external cooling	Reduced external cooling	N/A	External cooling activated when not required	N/A	Coolant leak (liquid) or water internal to RESS enclosure

Functional Hazard and Operational Analysis							
RESS Function Description	**Malfunction (Effect)**						
	Loss of Function	**Incorrect Function (More Than Requested)**	**Incorrect Function (Less Than Requested)**	**Incorrect Function (Wrong Direction)**	**Unintended Activation of Function**	**Locked/Stuck Function**	**Other Malfunc-tions**
Description of Vehicle Hazard ==>	Potential thermal event (limited conditions) H6	None	*Potential thermal event (Worst case is full loss at left) H6*	N/A	None	N/A	*Conductive coolant - risk of electrical shock (Isolation to enclosure). H5* *Conductive coolant - Potential thermal event due to resistive heating internal to RESS H6* *Electrolysis of coolant or water in contact with HV surfaces - Potential explosive event H7*
Data Communication with Vehicle	No data/commands	Unintended data/commands	Missing data/commands	Corrupted data/commands	N/A	Stuck data/commands	

Functional Hazard and Operational Analysis							
RESS Function Description	**Malfunction (Effect)**						
	Loss of Function	**Incorrect Function (More Than Requested)**	**Incorrect Function (Less Than Requested)**	**Incorrect Function (Wrong Direction)**	**Unintended Activation of Function**	**Locked/Stuck Function**	**Other Malfunc-tions**
Description of Vehicle Hazard ==>	RESS data interface to the Vehicle involves many functions: Propulsion, Charging/Re-Generation, RESS Electrical Isolation, Cooling and TBD. For each function, the hazards are detailed in the respective rows above. The Safety Concept will address specific failure modes and mitigation techniques for data communication						
Receive Crash/Impact Signal	No crash/impact signal when expected (latent failure)	Crash/impact signal active when not expected	Intermittent crash/impact signal when expected (latent failure)	Covered in scenarios at left	Crash/impact signal active when not expected	N/A	N/A
Description of Vehicle Hazard ==>	Battery not isolated/disconnected from vehicle under impact Potential thermal event H6 Electrical shock H5	Unintended battery disconnection from vehicle *Unintended deceleration (insufficient torque) - EV only* *H3* no hazard in HEV, PHEV - IC engine still available for propulsion	Battery may not be isolated/disconnected from vehicle under impact *Potential thermal event* *H6* *Electrical shock* *H5*	Covered in scenarios at left	Unintended battery disconnection from vehicle *Unintended deceleration (insufficient torque) - EV only* *H3* no hazard in HEV, PHEV - IC engine still available for propulsion	N/A	N/A

Appendix C: Functions, Hazardous Malfunctions, and ASIL Risk Assessment

C.1 First Implementation

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Accepts and stores electrical energy from charger	Cell Over-heating (Thermal Event)	1. Effect will be higher cell and pack temperatures that would result in a thermal event 2. With External Measures	1. Vehicle is home in the garage 2. Vehicle is on charge and un-attended 3. People are in the house 4. Probability of this scenario > 10% of operating time	E4	1. Thermal event may extend beyond the car into the living area of the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
	Cell Over-heating (Thermal Event)	1. Effect will be higher cell and pack temperatures that would result in a thermal event 2. Without External Measures	1. Vehicle is home in the garage 2. Vehicle is on charge and un-attended 3. People are in the house 4. Probability of this scenario > 10% of operating time	E4	1. Thermal event may extend beyond the car into the living area of the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C
	Cell Over-heating (Thermal Event)	Effect will be higher cell and pack temperatures that would result in a thermal event	1. Vehicle is on the road and on-charge in an open garage or on the street. 2. Pedestrians are present 3. Probability of this scenario is more than 1% but less than 10% of operating time	E3	1. Thermal event may endanger the pedestrians 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation is very controllable. More than 99% of the people can avoid the harm	C1	QM

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Accepts and stores electrical energy from charger	Cell Overheating (Thermal Event)	Effect will be higher cell and pack temperatures that would result in a thermal event	1. Vehicle is home in the garage 2. Vehicle on charge with occupants inside 3. Probability of this scenario is less than 1% of the operating time	E2	Severe and life-threatening injuries (survival probable) are possible	S2	This situation is very controllable. More than 99% of operators can avoid the harm	C1	QM
	Cell Venting	Cell Over-charging	1. Vehicle is On charge or unattended in the garage 2. This scenario occurs more than 10% of the vehicle's operating time.	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
Accepts and stores regenerative electrical energy	Cell Overheating (Thermal Event)	Effect will be higher cell and pack temperatures that would result in a thermal event	1. Vehicle is braking while driving at a high speed 2. SOC is maximum 3. Overcharging of the cells occurs 4. This is a duration based situation; Regeneration occurs less than 1% of the vehicle's operating time	E2	1. If a thermal event occurs while the car is moving, severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Accepts and stores regenerative electrical energy	Cell Venting	Cell overcharging	1. Vehicle is braking while driving at a high speed 2. SOC is maximum 3. Over-charging of the cells occur 4. This is a duration based situation; Regeneration occurs for less than 1%	E2	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
Delivers HV energy to the vehicle bus	Unintended Vehicle Deceleration	sudden loss of electrical energy causes the propulsion system to stop delivering torque	1. Vehicle is driving in heavy traffic at high speed 2. Another vehicle is close behind 3. Loss of electrical energy causes loss of torque 4. The vehicle starts to coast 5. This operating scenario occurs more than 10% of operating time.	E4	1. The speed of the vehicles and the size of the vehicle coming from behind could result in a collision with high change of speed before and after the collision 2. Taking external measures (seat belts and airbags) into consideration, severe and life-threatening injuries (survival probable) are possible	S2	This situation may be hard to control; less than 90% of all drivers can control it	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Delivers HV energy to the vehicle bus	Loss of Primary Vehicle functions (power steering, power braking, thermal management)	Sudden loss of electrical energy causes the loss of the low-voltage power that supports the controls of the vehicle's primary functions	1. Vehicle is driving in heavy traffic at high speed 2. Another vehicle is close behind 3. Loss of HV electrical energy causes loss of low-voltage power and consequently primary vehicle controls and functions 4. The vehicle starts to coast 5. This operating scenario occurs more than 10% of operating time	E4	1. The speed of the vehicles and the size of the vehicle coming from behind could result in a collision with Δ speed before and after the collision between 30 and 50 kph 2. Severe and life-threatening injuries (survival probable) are possible	S2	Loss of power steering, and power brakes; this situation may be hard to control; less than 90% of all drivers can control it	C3	C
	Loss of primary vehicle function – lighting	Sudden loss of electrical energy causes the loss of the low-voltage power that supports the lighting function	1. Vehicle is driving at nighttime and/or in low-visibility conditions (weather) 2. Vehicle is running in heavy traffic at high speed 3. Loss of HV electrical energy causes the loss of the generated low-voltage electrical energy and consequently the lighting function 4. The driver's vision is	E4	1. This hazard may result in a crash 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation may be hard to control; less than 90% of all drivers can control it	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
			severely impaired 5. This operating scenario occurs more than 10% of the operating time						
Connects/Disconnects Battery pack to the HV bus	Unintended Vehicle Deceleration	Sudden loss of electrical energy causes the propulsion system to stop delivering torque	1. Vehicle is running in heavy traffic at high speed 2. Another vehicle is close behind 3. Loss of electrical energy causes the torque production by the propulsion system to drop to zero 4. The vehicle starts to coast 5. This operating scenario occurs more than 10% of operating time.	E4	1. The speed of the vehicles and the size of the vehicle coming from behind could result in a collision with high change in speed before and after the collision 2. Taking external measures (seat belts and airbags) into consideration, Severe and life-threatening injuries (survival probable) are possible	S2	This situation may be hard to control; less than 90% of all drivers can control it	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
	Loss of Primary Vehicle functions (power steering, power braking, thermal management)	Disconnection of high-voltage power causes loss of the low-voltage power that supports the controls of the vehicle's primary functions	1. Vehicle is driving in heavy traffic at high speed 2. Another vehicle is close behind 3. Loss of HV electrical energy causes loss of low-voltage power and consequently primary vehicle controls and functions 4. The vehicle starts to coast 5. This operating scenario occurs more than 10% of operating time	E4	1. The speed of the vehicles and the size of the vehicle coming from behind could result in a collision with Δ speed before and after the collision between 30 and 50 kph 2. Severe and life-threatening injuries (survival probable) are possible	S2	Loss of power steering, and power brakes; this situation may be hard to control; less than 90% of all drivers can control it	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Connects/Disconnects Battery pack to the HV bus	Loss of primary vehicle function - lighting	Disconnection of high-voltage power causes loss of the low-voltage and consequently the vehicle's lighting function	1. Vehicle is driving at night time and/or in low visibility conditions (weather) 2. Vehicle is running in heavy traffic at high speed 3. Loss of HV electrical energy causes the loss of the generated low-voltage electrical energy and consequently the lighting function 4. The driver's vision is severely impaired 5. This operating scenario occurs more than 10% of the operating time	E4	1. This hazard may result in a crash 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation may be hard to control; less than 90% of all drivers can control it	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
	Exposure to high-voltage	Unintended connection to the HV bus. Potentially exposes a person (service personnel, owner, …) to the live high-voltage bus	1. Vehicle is off 2. Persons potentially in contact with HV bus (vehicle under hood is exposed or crash event) 3. Duration and frequency less than 1% of vehicle operating time 4. Frequency: may happen more than once per year but few than 10 times per year (per draft SAE J2980 - Propulsion, this is E2)	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous nature of the event	C3	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS provides HVIL safety system monitoring	Exposure to High Voltage	In the case where the HVIL is violated and the BMS does not react.	1. Service personnel or operator breaks the HVIL circuit 2. Frequency: may happen more than once per year but fewer than ten times per year.	E2	Exposure to the high-voltage bus: Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
(Sensor) Measures the current in/out of the battery pack	Cell Overheating (Thermal Event)	1. In case of low current reading into the pack, continuous charging of the battery occurs 2. With external measures	1. Vehicle is in the garage 2. Vehicle is on charge and unattended 3. People are in the house 4. Probability of this scenario more than 10% of operating time	E4	1. Thermal event may spread into the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
		1. In case of low current reading into the pack, continuous charging of the battery occurs 2. Without external measures	1. Vehicle is in the garage 2. Vehicle is on charge and unattended 3. People are in the house 4. Probability of this scenario more than 10% of operating time	E4	1. Thermal event may spread into the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
(Sensor) Measures the current in/out battery pack	Cell Overheating (Thermal Event)	In case of low current reading into the pack, continuous charging of the battery occurs during regeneration	1. Vehicle is braking while driving at a high speed 2. SOC is maximum 3. Overcharging of the cells occur 4. This is a duration based situation; Regeneration occurs for less than 1% of operating time	E2	1. If thermal event occurs while the car is in motion, severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	A
	Cell Venting	In case of low current reading into the pack, continuous charging of the battery occurs	1. Vehicle is On charge, or braking while driving at a high speed 2. SOC is maximum 3. Overcharging of the cells occur 4. Probability of this scenario is more than 10% of operating time	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
	Cell Overheating (Thermal Event)	In case of low current reading out of the pack with an outside short	1. Vehicle is On or driving 2. Overcurrent draw of the cells occurs 3. Probability of this scenario is more than 10% of operating time	E4	1. Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Communicates Within RESS/Between BMS and Sensors	Exposure to High Voltage	In case of erroneous data from ground fault sensor. Effect is exposure to HV to everyone who may come in contact with the vehicle	1. Vehicle is On or On-Charge but not moving 2. Engine compartment closed and HV not exposed or attempted to be exposed 2. This scenario occurs more than 10% of the vehicle operating time	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
			1. Vehicle is On or On-Charge but not moving 2. Engine compartment is open and HV is potentially exposed or attempted to be exposed 3. This scenario occurs less than 1% of the vehicle operating time 4. Frequency: this may happens more than once per year but fewer than 10 times per year	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B
			1. Vehicle is moving 2. Engine compartment is open and HV is potentially exposed or attempted to be exposed 3. This scenario is almost impossible	E0	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	N/A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Communicates Within RESS/Between BMS and Sensors	Exposure to HV	In case of erroneous data from ground fault sensor. Effect is exposure to HV to everyone who may come in contact with the vehicle	1. Vehicle high-voltage wiring is exposed due to accident 2. This scenario has very low probability	E1	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	A
	Cell Overheating (Thermal Event)	In case of erroneous data from temperature sensor. The cell may have enough time to reach the self-heating point and beyond	1. Vehicle is moving 2. Ambient cell temperature is high enough for heat generation to exceed heat dissipation without cooling 3. This scenario occurs more than 10% of the vehicles operating time	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	C
			1. Vehicle is On but not moving 2. Ambient cell temperature is high enough for heat generation to exceed heat dissipation without cooling 3. This scenario occurs more than 10% of the vehicles operating time	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable as the driver is alert to the state of the car	C2	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Communicates Within RESS/Between BMS and Sensors	Cell Overheating (Thermal Event)	In case of erroneous data from temperature sensor. The cell may have enough time to reach the self-heating point and beyond (with external measures)	1. Vehicle is On charge or Off 2. Ambient cell temperature is high enough for heat generation to exceed heat dissipation without cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	1. Thermal event may extend into the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
		In case of erroneous data from temperature sensor. The cell may have enough time to reach the self-heating point and beyond (without external measures)	1. Vehicle is On charge or Off 2. Ambient cell temperature is high enough for heat generation to exceed heat dissipation without cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	1. Thermal event may extend into the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C
		In case of erroneous data from cell balancer sensor; overcharging condition may occur. (with external measures)	1. Vehicle is On charge 3. This scenario occurs more than 10% of the vehicle operating time	E4	1. Thermal event may extend into the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Communicates Within RESS/Between BMS and Sensors	Cell Over-heating (Thermal Event)	In case of erroneous data from cell balancer sensor; overcharging may occur (without external measures)	1. Vehicle is On charge 2. This scenario occurs more than 10% of the vehicle operating time	E4	1. Thermal event may extend into the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C
		In case of erroneous data from cell balancer sensor; overcharging may occur (with external measures)	1. Vehicle is On charge 2. This scenario occurs more than 10% of the vehicle operating time	E4	1. Thermal event may extend into the house 2. Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
	Cell Venting	In case of erroneous data from cell balancer sensor; overcharging condition may occur.	1. Vehicle is On charge 2. This scenario occurs more than 10% of the vehicle operating time	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
(BMS) Communicates With other vehicle modules	Cell Overheating (Thermal Event)	In case of failure to communicate with the thermal management system, the cell may reach the self-heating point and beyond	1. Vehicle is On or running 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	C
		1. In case of failure to communicate with the thermal management system, the cell may reach the self-heating point and beyond 2. With external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
		1. In case of failure to communicate with the thermal management system, the cell may reach the self-heating point and beyond 2. Without external measures	1. Vehicle is On charge or OFF un-attended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	Thermal event may occur and severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
(BMS) Communicates with other vehicle modules	Unintended Vehicle Deceleration	In case of misinterpretation of the messages from the vehicle systems controller, unintended opening of the contactors may occur	1. Vehicle is moving at high speed in heavy traffic 2. Another vehicle is close behind 3. Loss of electrical energy causes the torque to drop to zero 4. The vehicle starts to coast 5. This operating scenario occurs more than 10% of operating time.	E4	1. The speed of the vehicles and the size of the vehicle coming from behind could result in a collision with high change in speed before and after the collision 2. Taking external measures (seat belts and airbags) into consideration, Severe and life-threatening injuries (survival probable) are possible	S2	This situation may be hard to control; fewer than 90% of all drivers can control it	C3	C
	Exposure to High Voltage	In case of misinterpretation of messages from other vehicle modules except the charger and HVIL, the contactors may stay closed when not intended to.	1. The vehicle is in a crash or 2. The vehicle is attempting to reach safe state 3. Frequency: this may happens more than once year but fewer than 10 times per year	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B

BMS provides thermal management control of the battery cells	Cell Overheating (Thermal Event)	In case of failure to control the thermal management system, the cell may reach the self-heating point and beyond	1. Vehicle is On or moving 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicles operating time	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	C

Function	**Hazardous Malfunction**	**Variables/Parameters**	**Situation/Exposure**	**E**	**Effect/Severity**	**S**	**Controllability**	**C**	**ASIL**
BMS provides thermal management control of the battery cells	Cell Overheating (Thermal Event)	1. In case of failure to control the thermal management system, the cell may reach the self-heating point and beyond 2. With external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
		1. In case of failure to control the thermal management system, the cell may reach the self-heating point and beyond 2. Without external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS provides battery pack state of charge estimate	Cell Overheating (Thermal Event)	1. Underestimation of SOC may cause continuation of cell charging 2. With external measures	1. Vehicle is On charge unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS provides battery pack state of charge estimate	Cell Overheating (Thermal Event)	1. Underestimation of SOC may cause continuation of cell charging 2. Without external measures	1. Vehicle is On charge or unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C
		1. Underestimation of SOC may cause continuation of cell charging 2. Without external measures	1. Vehicle is braking while driving at a high speed (regeneration mode) 2. This is a duration based situation; Regeneration occurs for less than 1% of the	E2	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative	C3	A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
			vehicle operating time				assessment is recommended by ISO 26262		
BMS provides Battery Cell Voltage Balancing	Cell Over-heating (Thermal Event)	1. In case of no balancing, cell overcharging may occur 2. With external measures	1. Vehicle is On charge unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS provides Battery Cell Voltage Balancing	Cell Overheating (Thermal Event)	1. In case of no-balancing, cell overcharging may occur 2. Without external measures	1. Vehicle is On charge or unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C
	Cell Venting	In case of no balancing, cell overcharging may occur	1. Vehicle is On charge or unattended in the garage 2. This scenario occurs more than 10% of the vehicle operating time.	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
BMS provides battery pack charging control (in some system architectures)	Cell Overheating (Thermal Event)	1. In case of cell overcharging 2. With external measures	1. Vehicle is On charge unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
	Cell Overheating (Thermal Event)	1. In case of cell overcharging 2. Without external measures	1. Vehicle is On charge or unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS provides battery pack charging control (in some system architectures)	Cell Venting	In case of cell overcharging	1. Vehicle is On charge or un-attended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case	S0		N/A	N/A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
(Sensor) Provides battery pack temperature measurement	Cell Overheating (Thermal Event)	In the case of incorrect temperature measurements.	1. Vehicle is On or moving 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	C
		1. In the case of incorrect temperature measurements. 2. With external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event	C2	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
(Sensor) Provides battery pack temperature measurement	Cell Overheating (Thermal Event)	1. In the case of incorrect temperature measurements. 2. Without external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C
BMS provides battery pack regeneration charging control	Cell Overheating (Thermal Event)	In case of cell overcharging	1. Vehicle is braking while moving at a high speed 2. SOC is maximum 3. Overcharging of the cells occur 4. This is a duration based situation; regeneration occurs for less than 1% of the vehicle operating time	E2	If thermal event occurs while the car is driving, Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	A
	Cell Venting	In case of cell overcharging	1. Vehicle is braking while moving at a high speed 2. SOC is maximum 3. Overcharging of the cells occur 4. This is a duration based situation; regeneration occurs for less than 1% of the vehicle operating time	E2	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS provides DC ground fault high-voltage isolation monitoring	Exposure to High Voltage	BMS malfunction may result in not detecting a ground fault condition	1. Vehicle is On or On-Charge 2. Engine compartment closed and HV not exposed or attempted to be exposed 2. This scenario occurs more than 10% of the vehicle operating time	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
			1. Vehicle is On or On-Charge 2. Engine compartment is open and HV is potentially exposed or attempted to be exposed 3. This scenario occurs less than 1% of the vehicle operating time 4. Frequency: this may happen more than once per year but fewer than 10 times per year	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B
			1. Vehicle high-voltage wiring is exposed due to a crash 2. This scenario has very low probability	E1	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS provides DC ground fault (HV) isolation monitoring	Cell Overheating (Thermal Event)	1. Internal shorts 2. With external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
		1. Internal shorts 2. Without external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS Provides High-Voltage Contactor Control	Unintended Vehicle Deceleration	Unintended opening of the contactors. Sudden loss of electrical energy causes the propulsion system to stop delivering torque	1. Vehicle is moving in heavy traffic at high speed 2. Another vehicle is close behind 3. Loss of electrical energy causes the torque to drop to zero 4. The vehicle starts to coast 5. This operating scenario occurs more than 10% of operating time.	E4	1. The speed of the vehicles and the size of the vehicle coming from behind could result in a collision with high change in speed before and after the collision 2. Taking external measures (seat belts and airbags) into consideration, Severe and life-threatening injuries (survival probable) are possible	S2	This situation may be hard to control; fewer than 90% of all drivers can control it	C3	C

	Exposure to HV	Unintended closing of the contactors	1. Vehicle is off (hence the "unintended" connection) 2. Persons in touch with the vehicle 3. Vehicle under hood exposed 4. This scenario can be a combination of time duration and frequency; this < 1% of vehicle operating time 5. Frequency: this may happen more than once per year but fewer than 10 times per year	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS Provides High-Voltage Contactor Control	Exposure to High Voltage	Unintended closing of the contactors	1. Vehicle is off (hence the "unintended" connection) 2. Crash situation 3. Vehicle under hood exposed 4. Persons in touch with the vehicle 5. This scenario has very low probability	E1	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	A
BMS Monitors the Voltage of the Battery Pack	Exposure to High Voltage	Misinterpretation of the pack voltage leading to incorrect detection of isolation	1. Vehicle is On or On-Charge or moving 2. Engine compartment closed and HV not exposed or attempted to be exposed 2. This scenario occurs more than 10% of the vehicle operating time	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
			1. Vehicle is On or On-Charge 2. Engine compartment is open and HV is potentially exposed or attempted to be exposed 3. This scenario occurs less than 1% of the vehicle operating time 4. Frequency: this may happens more than once per year but fewer than 10 times per year	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
BMS Monitors the Voltage of the Battery Pack	Exposure to High Voltage	Misinterpretation of the pack voltage leading to incorrect detection of isolation	1. Vehicle high-voltage wiring is exposed due to accident 2. This scenario has very low probability	E1	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	A
MBMS Monitors the Battery Pack Current	Cell Overheating (Thermal Event)	1. Misinterpretation of the pack current measurement leads to under-estimation of SOC; this may cause continuation of cell charging 2. With external measures	1. Vehicle is On charge unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
		1. Misinterpretation of the pack current measurement leads to under-estimation of SOC; this may cause continuation of cell charging 2. Without external measures	1. Vehicle is On charge or unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
MBMS Monitors the Battery Pack Current	Cell Venting	Misinterpretation of the pack current measurement leads to underestimation of SOC; this may cause cell overcharging	1. Vehicle is On charge, or braking while driving at a high speed (regeneration mode) 2. This scenario occurs more than 10% of the vehicle operating time.	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
BMS pBMS Provides Fault Management (Performs Diagnostics)	Unintended Vehicle Deceleration	Not detecting erroneous critical data associated with contactors opening/closing	1. Vehicle is moving in heavy traffic at high speed 2. Another vehicle is close behind 3. Loss of electrical energy causes the torque to drop to zero 4. The vehicle starts to coast 5. This operating scenario occurs more than 10% of operating time.	E4	1. The speed of the vehicles and the size of the vehicle coming from behind could result in a collision with high change in speed before and after the collision 2. Taking external measures (seat belts and airbags) into consideration, Severe and life-threatening injuries (survival probable) are possible	S2	This situation may be hard to control; fewer than 90% of all drivers can control it	C3	C

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
	Cell Overheating (Thermal Event)	Not detecting erroneous critical data associated with cell temperature and thermal management or cell overcharging	1. Vehicle is On, moving, Off, On- or Off-charge 2. Ambient cell temperature is high enough for heat generation to exceed heat dissipation without cooling 3. This scenario occurs more than 10% of the vehicle operating time	E4	Thermal event may occur and result in Severe injuries (survival probable) are possible	S2	1. This situation cannot be controlled by the majority of the people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	C
BMS pBMS Provides Fault Management (Performs Diagnostics)	Exposure to High Voltage	Not detecting erroneous critical data associated with high-voltage exposure	1. Vehicle is On but not driving, or on charge 2. Vehicle is moving, in the garage, or in storage 3. A person is handling the HV wires 4. The scenario is less than 1% of the vehicle's total operating time 5. Frequency: this may happen more than once per year but fewer than 10 times per year	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
Sensor Detects Ground Fault	Exposure to High Voltage	Failure to measure the isolation between the high-voltage bus and the vehicle ground	1. Vehicle is On or On-Charge 2. Engine compartment closed and HV not exposed or attempted to be exposed 2. This scenario occurs more than 10% of the vehicle operating time	E4	1. No person is potentially at risk in this scenario 2. There is no possibility for injury in this case.	S0		N/A	N/A
			1. Vehicle is On or On-Charge 2. Engine compartment is open and HV is potentially exposed or attempted to be exposed 2. This scenario occurs less than 1% of the vehicle operating time 3. Frequency: this may happen more than once per year but fewer than 10 times per year	E2	In case of exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability in this situation is extremely difficult, due to the almost instantaneous event	C3	B
Sensor Detects Ground Fault	Exposure to High Voltage	Failure to measure the isolation between the HV bus and the vehicle ground	1. Vehicle high-voltage wiring is exposed due to accident 2. This scenario has very low probability	E1	Exposure to the HV bus, Life Threatening Injuries (Survival Uncertain), or Fatal Injuries are possible	S3	Controllability is extremely difficult, due to the almost instantaneous event	C3	A

Function	Hazardous Malfunction	Variables/Parameters	Situation/Exposure	E	Effect/Severity	S	Controllability	C	ASIL
	Cell Overheating (Thermal Event)	Internal shorts	1. Vehicle is On or driving 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	1. This situation cannot be controlled by most people involved 2. Due to lack of data, a conservative assessment is recommended by ISO 26262	C3	C
	Cell Overheating (Thermal Event)	1. Internal shorts 2. With external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	C2	B
	Cell Overheating (Thermal Event)	1. Internal shorts 2. Without external measures	1. Vehicle is On charge or OFF unattended in the garage 2. The cell temperature reaches a temperature that requires active cooling 3. This scenario occurs more than 10% of the vehicle operating time.	E4	Thermal event may occur and Severe and life-threatening injuries (survival probable) are possible	S2	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event	C3	C

C.2 Second Implementation

Malfunction Effect	Vehicle-Level Hazard	Assumptions	Exposure	Severity	Controllability	ASIL
Overcharged Battery	Thermal Event	All RESS/vehicle types and technologies	E3: While driving, re-charge only occurs under extended re-generative braking	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Worst case Significant smoke or flames inside passenger compartment	C
Overcharged Battery	Thermal Event	All RESS/vehicle types and technologies	E3: While driving, re-charge only occurs under extended re-generative braking	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C2: No smoke or flames inside passenger compartment. Most drivers and passengers able to pull over and exit vehicle	B
Overcharged Battery	Thermal Event	All RESS/vehicle types and technologies. Include Service Technicians	E3: Charging in Service Bay (EV/PHEV) or test driving (HEV)	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C2: Service Techs are trained in fire containment	B
Overcharged Battery	Thermal Event	Unattended plug in charging, include home occupants	E4: EV/PHEV Charging in Garage	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Thermal event may easily spread to garage/home with little ability to avoid or control	D
Under-Charged or Over-Discharged Battery	Thermal Event	All RESS/ Vehicle types and technologies. Testing needed to validate severity.	E3: While driving, re-charge only occurs under extended re-generative braking	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Worst case - Significant smoke or flames inside passenger compartment	C

Malfunction Effect	Vehicle-Level Hazard	Assumptions	Exposure	Severity	Controllability	ASIL
Under-Charged or Over-Discharged Battery	Thermal Event	All RESS/vehicle types & technologies Testing needed to validate severity.	E3: While driving, re-charge only occurs under extended re-generative braking	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C2: No smoke or flames inside passenger compartment. Most drivers and passengers able to pull over and exit vehicle	B
Under-Charged or Over-Discharged Battery	Thermal Event	All RESS/ Vehicle types and technologies, include service technicians	E3: Charging in Service Bay (EV/PHEV)	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C2: Service Technicians are trained in fire containment	B
Under-Charged or Over-Discharged Battery	Thermal Event	Unattended plug in charging, include home occupants	E4: EV/PHEV Charging in Garage	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Thermal event may easily spread to garage/home with little ability to avoid or control	D
No or Lessened Availability of Electrical Energy to Vehicle	Unintended Deceleration (Loss of or Insufficient Torque)	EV only (no IC engine for backup propulsion), consider occupants of trailing vehicles	E4: Normal driving or parking situations	S1: Collision from rear with delta V < 20kph	C1: >90% of drivers are able to avoid harm by pulling off the active roadway	QM
RESS internal mechanical failure/ rupture/ fatigue - leakage of energy storage media	Exposure to hazardous chemicals and/or gases	Worst case- Testing needed to validate severity and controllability.	E4: Normal driving situations	S2: Release of toxic vented gases and/or electrolyte (non-lethal)	C2: >90% of drivers are able to avoid harm by pulling off the active roadway and exiting the vehicle	B

Malfunction Effect	Vehicle-Level Hazard	Assumptions	Exposure	Severity	Controllability	ASIL
RESS internal mechanical failure/ rupture/ fatigue - leakage of energy storage media	Exposure to hazardous chemicals and/or gases	RESS outside the passenger compartment	E4: Normal driving situations	S2: Release of toxic vented gases and/or electrolyte	C2: >90% of drivers are able to avoid harm by pulling off the active roadway and exiting the vehicle	B
RESS internal mechanical failure/ rupture/ fatigue - leakage of energy storage media	Exposure to hazardous chemicals and/or gases	Unattended plug in charging, include home occupants, Gases are non-lethal and not debilitating under short term exposure	E4: Normal in home charging of EV/PHEV	S2: Release of toxic vented gases and/or electrolyte(non-lethal)	C2: >90% of people are able to avoid harm by exiting home/garage	B
RESS internal mechanical failure/ rupture due to crash - leakage of energy storage media	Exposure to hazardous chemicals and/or gases	Include responders All RESS/vehicle types and technologies	E4: Responders at crash scenarios	S2: Release of toxic vented gases and/or electrolyte (non-lethal)	C2: Trained responders	B
RESS internal mechanical failure/ rupture due to crash - leakage of energy storage media	Exposure to hazardous chemicals and/or gases	Worst case Recommend validation of S2 rating testing of effects of toxic gases	E2: Severe crash scenario (rupture RESS)	S2: Release of toxic vented gases and/or electrolyte	C3: No controllability after crash	A
Reduced electrical isolation (Short circuit to Enclosure/ Chassis)	Electrical shock	Worst case both high-voltage potentials accessed - high exposure for service technicians and responders	E4: May occur in common scenarios for operators, ER and technicians (impact)	S3: RESS voltages well in excess of 60VDC are potentially fatal	C3: None	D

Malfunction Effect	Vehicle-Level Hazard	Assumptions	Exposure	Severity	Controllability	ASIL
RESS Over-temperature - Loss of or reduced external cooling	Thermal Event	RESS units with required external cooling (air or liquid) Recommend testing to validate Exposure rating at elevated ambient temperatures	E2: Risk of thermal events only occurs while driving under elevated ambient conditions (i.e., above 40C)	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Worst case - Significant smoke or flames inside passenger compartment	B
RESS Over-temperature - Localized heating due to conductive liquid coolant leak internal to RESS	Thermal Event	RESS units with required liquid external cooling Localized heating generated from resistive conduction through coolant	E4: Can occur at any time	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Worst case - Significant smoke or flames inside passenger compartment	D
RESS Over-temperature - Internal short circuit due to external liquid ingress to RESS (e.g., immersion)	Thermal Event	Cell direct heating generated from internal RESS short circuits between cells	E1: Flooding or immersion	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Worst case RESS system in garage attached to home	A
RESS Over-temperature - Localized heating due to resistive high current connection internal to RESS	Thermal Event	Localized heating generated from high resistance/high current connection (coolant conductivity, faulty high current connection, etc.) internal to RESS	E4: Can occur at any time	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Worst case - Significant smoke or flames inside passenger compartment	D

Malfunction Effect	Vehicle-Level Hazard	Assumptions	Exposure	Severity	Controllability	ASIL
Hydrogen gas formation - Liquid coolant leak or water intrusion internal to RESS (electrolysis)	Explosive event (RESS inside passenger compartment)	RESS units with required liquid external cooling; High-voltage electrolysis may produce hydrogen gas in explosive concentration Requires "spark" to ignite. Danger to all nearby.	E3: Can occur at any time, but needs a "spark event" to ignite which is an unlikely occurrence (separate failure mode)	S2: Flying debris external to vehicle - hazard to persons in close proximity to vehicle	C3: Flying debris external to vehicle, likely directed to ground	B
Hydrogen gas formation - Liquid coolant leak or water intrusion internal to RESS (electrolysis)	Explosive event (RESS outside passenger compartment)	RESS units with liquid external cooling; high-voltage electrolysis may produce hydrogen gas in explosive concentration Requires "spark" to ignite. Danger to all nearby.	E3: Can occur at any time, but needs a "spark event" to ignite which is an unlikely occurrence (separate failure mode)	S3: Uncontained explosion (flying debris inside passenger compartment)	C3: Worst case - flying debris inside passenger compartment	B
Single Cell internal failure resulting in excessive energy release to surrounding environment	Thermal Event	All RESS/ Vehicle types & technologies Assume single cell event may propagate to full RESS thermal event	E4: May occur at any time an any scenario	S3: Uncontained thermal event with exposed flames or explosion (flying debris)	C3: Worst case - Significant smoke or flames inside passenger compartment	D

Appendix D: Control Actions and Unsafe Control Actions

The STPA analysis identified 10 BMS control actions.

1. Thermal management of the RESS
2. Engage pre-charge contactor
3. Open main contactor for emergency shut off of the RESS current
4. Send RESS charge request to the hybrid vehicle controller
5. Send battery discharge request to the hybrid vehicle controller
6. Issue cell balancing commands
7. Send the battery state message to vehicle systems controller
8. Send power arbitration request to vehicle systems controller
9. Turn off the onboard charge controller for plug-in charging
10. Turn on onboard charge controller for plug-in charging

The STPA analysis identified 66 unsafe control actions from the BMS:

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Provided, but executed incorrectly	If BMS controller's battery discharge request is not delivered to the vehicle controller, the vehicle may be under powered.	Battery system does not provide propulsion power.
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller barely turns down the onboard charging current when it needs to be heavily turned down at the end of charging (i.e. the charger has been effectively left on "full blast"), this could lead to overcharging.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided when control action is not needed and unsafe	If the BMS controller commands cooling or heating when it's not needed, then the battery may enter a hazardous state.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting
Provided, but duration is too long or too short	If the BMS controller commands heating for too long, the battery may enter a hazardous state.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Separator melting

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller commands too little heating or cooling, the battery may enter a hazardous state.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller commands too much heating or cooling, the battery may enter a hazardous state.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting
Provided, but duration is too long or too short	If the BMS controller commands too short a time for heating or cooling, the battery may enter a hazardous state.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting
Provided when control action is not needed and unsafe	If the BMS controller disengages the contactor in order to initiate an emergency shutdown when this isn't needed, the car could stall at speed.	Battery system does not provide propulsion power.
Not provided when needed to maintain safety	If the BMS controller does not command the heating or cooling, the battery may enter a hazardous state.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Not provided when needed to maintain safety	If the BMS controller does not disengage the contactor in order to initiate an emergency shut down, it may lead to the battery being over charged, over discharged, or an electrocution during service.	1. Anode copper current collector is dissolved into the electrolyte 2. High Voltage Line Exposed to Human Contact 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Not provided when needed to maintain safety Provided, but executed incorrectly	If the BMS controller does not engage the precharge contactor before engaging the main contactors, it will lead to excessive in-rush current which could cause over discharge or electrical system components (e.g. contactor, controller, fuses) being damaged which in turn could lead to the vehicle stalling.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power. 3. High Voltage Line Exposed to Human Contact 4. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but duration is too long or too short	If the BMS controller does not provide balancing charging because overall charging duration requested from the hybrid vehicle controller is too short, the voltage will be out of balance which could lead to eventual over charge or over discharge of certain individual cells.	1. Anode copper current collector is dissolved into the electrolyte 2. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Not provided when needed to maintain safety	If the BMS controller does not request plug in charging when it's needed, this could lead to the vehicle over discharging or stalling.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power.
Not provided when needed to maintain safety	If the BMS controller does not send power arbitration request to the Vehicle System Controller, the battery may become over discharged.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power.
Not provided when needed to maintain safety	If the BMS controller does not send the battery SOC information to the vehicle controller, the vehicle system controller may not be able to optimize the battery charging. This could lead to battery under charge, over charge, and vehicle stalling.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power. 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Not provided when needed to maintain safety	If the BMS controller doesn't provide balancing charging, the cells can become badly out of balance which can in turn lead to more rapid over charge or over discharge.	1. Anode copper current collector is dissolved into the electrolyte 2. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Not provided when needed to maintain safety	If the BMS controller doesn't request charging from the hybrid vehicle controller when the voltage is below the lower limit, it could lead to over discharging.	Anode copper current collector is dissolved into the electrolyte
Not provided when needed to maintain safety	If the BMS controller doesn't request the battery to discharge when the driver needs to drive, this could lead to the vehicle stalling.	Battery system does not provide propulsion power.
Provided, but the starting time is too soon or too late	If the BMS controller doesn't requests plug in charging when it's needed until it's too late, this could lead to over discharging.	Anode copper current collector is dissolved into the electrolyte
Provided, but the starting time is too soon or too late	If the BMS controller engages the precharge contactor too late before engaging the main contactor, it could lead to the battery being over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided, but duration is too long or too short	If the BMS controller engages the precharge contactor for too short a time before engaging the main contactor, it could lead to the battery being over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided when control action is not needed and unsafe	If the BMS controller engages the precharge contactor too soon when the vehicle is being serviced (even though the 12 volt power should have already been disconnected and the contractors rendered unswitchable), it could lead to electrocution.	High Voltage Line Exposed to Human Contact
Provided when control action is not needed and unsafe	If the BMS controller engages the precharge contactor when the vehicle is being serviced, it may lead to electrocution.	High Voltage Line Exposed to Human Contact
Provided, but executed incorrectly	If the BMS controller incorrectly executes the balancing command by providing balance charging to the wrong cells, then the battery may become more out of balance.	1. Anode copper current collector is dissolved into the electrolyte 2. Lithium ions accumulate at the anode surface forming metallic lithium dendrite

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Provided when control action is not needed and unsafe	If the BMS controller provides cell balancing when it is unsafe to do so, it may lead to over charge, over discharge, and/or stalling.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power. 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but duration is too long or too short	If the BMS controller requests charging from the hybrid vehicle controller for too long a time, it could lead to over charge.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but duration is too long or too short	If the BMS controller requests discharging for too long, it could lead to unintended acceleration (not the focus of this study) or over discharging.	1. Anode copper current collector is dissolved into the electrolyte 2. High voltage battery releases too much current to the motor, or when it is not commanded by the driver
Provided, but duration is too long or too short	If the BMS controller requests plug-in charging for too long, it could lead to overcharging.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but duration is too long or too short	If the BMS controller requests plug-in charging for too short a time, it could lead to over discharging.	Anode copper current collector is dissolved into the electrolyte
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller requests plug-in charging that is too strong, it could lead to over charge.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller requests plug-in charging that is too weak, it could lead to over discharge.	Anode copper current collector is dissolved into the electrolyte
Provided, but the starting time is too soon or too late	If the BMS controller requests power arbitration too late, the battery may become over discharged.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power.
Provided, but the starting time is too soon or too late	If the BMS controller requests power arbitration too soon, the battery may not provide sufficient power.	Battery system does not provide propulsion power.
Provided when control action is not needed and unsafe	If the BMS controller requests the vehicle system controller to reduce the energy draw unnecessarily, it may cause the vehicle to decelerate or stall.	Battery system does not provide propulsion power.

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller requests the wrong amount of balancing (and the cells are badly out of balance), then the cells may be over charged or over discharged.	1. Anode copper current collector is dissolved into the electrolyte 2. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but the starting time is too soon or too late	If the BMS controller requests to turn off the onboard charge controller too soon, then the battery could be over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller requests too little charge current from the Vehicle System Controller, the battery could over discharge.	Anode copper current collector is dissolved into the electrolyte
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller requests too little discharge current, this could lead to the vehicle stalling.	Battery system does not provide propulsion power.
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller requests too much charge current from the hybrid vehicle controller, the battery could over charge.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided when control action is not needed and unsafe	If the BMS controller requests too much discharging, it could lead to unintended acceleration or over discharging.	1. Anode copper current collector is dissolved into the electrolyte 2. High voltage battery releases too much current to the motor, or when it is not commanded by the driver
Provided, but the intensity is incorrect (too much or too little)		
Provided, but the starting time is too soon or too late	If the BMS controller send the charging request to the hybrid vehicle controller too late, it may lead to the battery being over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided, but executed incorrectly	If the BMS controller sends a battery charge request to hybrid vehicle controller, and the request was delivered incorrectly, this could lead to undercharge, overcharge.	1. Anode copper current collector is dissolved into the electrolyte 2. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided when control action is not needed and unsafe	If the BMS controller sends a charging request to the hybrid vehicle controller when the external or battery temperature is too cold for charging, it could lead to plating of lithium ions on the anode.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Provided when control action is not needed and unsafe	If the BMS controller sends a charging request to the onboard charge controller (for plug in charging) when it's not needed, this could lead to overcharging.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller sends battery SOC information that is larger than the actual value, then the battery may get over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided, but the intensity is incorrect (too much or too little)	If the BMS controller sends battery SOC information that is lower than the actual value, then the battery may get over charged.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided when control action is not needed and unsafe	If the BMS controller sends charge request to the hybrid vehicle controller when the voltage is above the upper limit, it could lead to excessive current.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but the starting time is too soon or too late	If the BMS controller sends the balancing command too late, the cells with the lowest charge may be over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided, but the starting time is too soon or too late	If the BMS controller sends the battery discharge request to vehicle controller too soon, and the battery has not been sufficiently recharged from the last time it was used, then it may be over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided, but the starting time is too soon or too late	If the BMS controller sends the battery SOC information too late, the battery may be over charged or under charged.	1. Anode copper current collector is dissolved into the electrolyte 2. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but the starting time is too soon or too late	If the BMS controller sends the charging request to the hybrid vehicle controller too soon, it may lead to the battery being over charged.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but duration is too long or too short	If the BMS controller sends the signal for emergency shut down too late, it could lead to the battery being over charged, under charged, or someone being electrocuted.	1. Anode copper current collector is dissolved into the electrolyte 2. High Voltage Line Exposed to Human Contact 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but the starting time is too soon or too late		

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Provided, but the starting time is too soon or too late	If the BMS controller starts the cooling or heating too late, the battery could enter a hazardous state.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting
Provided when control action is not needed and unsafe	If the BMS controller stops onboard charging too soon, it could lead to over discharge.	Anode copper current collector is dissolved into the electrolyte
Provided, but executed incorrectly	If the BMS controller tries to disengage the emergency shut off contactor but executes the command incorrectly, then the contactor won't open leading to a possible over charge, over discharge, or electrocution.	1. Anode copper current collector is dissolved into the electrolyte 2. High Voltage Line Exposed to Human Contact 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided when control action is not needed and unsafe	If the BMS controller turns on plug in charging when not needed, it could lead to electrocution.	High Voltage Line Exposed to Human Contact
Provided, but duration is too long or too short	If the BMS controller's balancing command is too long, the low voltage cell may be over discharged.	Anode copper current collector is dissolved into the electrolyte
Provided, but duration is too long or too short	If the BMS controller's balancing command is too short, the high cell may be over charged.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but the starting time is too soon or too late	If the BMS controller's request to turn off the onboard charge controller too late, then the battery could be overcharged.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but duration is too long or too short	If the BMS controller's request to turn off the onboard charging is too short, then when the voltage is above the upper limit, it could lead to excessive current.	Lithium ions accumulate at the anode surface forming metallic lithium dendrite
Provided, but duration is too long or too short	The BMS controller continues to send the power arbitration request after the battery has recovered its state of charge.	Battery system does not provide propulsion power.

Unsafe Control Action Guideword	Unsafe Control Action	Potential Hazards
Not provided when needed to maintain safety	The BMS controller does not command the onboard charge controller to turn off charging when it is unsafe to charge the battery.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting
Provided, but executed incorrectly	The BMS controller may command the correct heating or cooling but the command is sent to the incorrect heater or cooler.	1. Anode passivation film (Solid Electrolyte Interface) breaks down 2. Cathode breaks down and releases Oxygen 3. Lithium ions accumulate at the anode surface forming metallic lithium dendrite 4. Separator melting
Provided, but the intensity is incorrect (too much or too little)	The BMS controller sends incorrect power arbitration requests to the Vehicle System Controller that does not correctly reflect the amount of battery energy available.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power.
Provided, but duration is too long or too short	The BMS controller stops sending the power arbitration request before the battery has recovered its state of charge.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power.
Provided, but executed incorrectly	The BMS controller's power arbitration request to the Vehicle System Controller is incorrectly delivered.	1. Anode copper current collector is dissolved into the electrolyte 2. Battery system does not provide propulsion power.

Appendix E: Key Definitions from HazOp and STPA

Hazard and Operability Analysis

Fault: abnormal condition that can cause an element or an item to fail

Failure: termination of the ability of an element to perform a function as required

Hazard: potential source of harm caused by malfunctioning behavior of the item

Functional Safety Requirement: specification of implementation-independent safety behavior, or implementation-independent safety measure, including its safety-related attributes

System Theoretic Process Analysis

Causal Factor: a problem with the electronic control system components (controller, sensor, actuator, communication links, and power supply), interactions among these components, and their interactions with the rest of the vehicle and the external environment that may cause the controller to issue a potentially unsafe control action and lead to vehicle hazard.

Unsafe Control Actions: actions commanded by controllers can potentially cause the vehicle system to transition from a safe to a hazardous state.

Hazard: a system state or set of conditions that, together with a particular set of unfavorable environmental conditions, can lead to a system level loss.

Loss: an undesired and unplanned event that results in death, injury, or other societal loss (e.g., property damage, environmental pollution).

Appendix F: Causal Factors (as reduced to exclude factors indirectly related to BMS)

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
394	Controller hardware faulty, change over time	The BMS controller has faulty hardware (e.g. a MOSFET stays open/closed).	BMS Controller
445	External control input or information wrong or missing	The BMS may receive wrong information from the Vehicle Systems Controller about whether the key is in the on or off position or what operational mode the vehicle is in.	BMS Controller
365	External control input or information wrong or missing	The vehicle system controller may issue a conflicting command from BMS controller to maintain the contactor closed. The BMS software algorithm may not know how to safely handle the conflict.	BMS Controller
367	External control input or information wrong or missing	The vehicle system controller's hardware may be faulty, software logic may have an error, and/or the calibration may be incorrect. These faults could lead to the vehicle system controller not issuing the open contactor command to BMS.	BMS Controller
469	External control input or information wrong or missing	The VSC's command to disengage the contactor may not arrive at the BMS controller due to faulty wiring/connector or bus communication. This communication could also be disturbed by EMI/ESD or interference with other vehicle components.	BMS Controller
501	External disturbances	EMI and/or ESD, moisture, and other elements from the surrounding environment may affect the BMS controller.	BMS Controller
429	External disturbances	The BMS controller acts as a sensor for the VSC. It reports the batteries charge level to the VSC. All BMS controller failure modes contained in this analysis could affect the accurate reporting of the battery charge level to VSC.	BMS Controller
234	Hazardous interaction with other components in the rest of the vehicle	EMI/ESD, moisture from a coolant line, A/C, other vehicle fluids, or physical interference with other vehicle systems could damage the BMS controller.	BMS Controller
429	Hazardous interaction with other components in the rest of the vehicle	The BMS controller acts as a sensor for the VSC. It reports the batteries charge level to the VSC. All BMS controller failure modes contained in this analysis could affect the accurate reporting of the battery charge level to VSC.	BMS Controller
393	Power supply faulty (high, low, disturbance)	The BMS controller loses 12 volt power.	BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
429	Power supply faulty (high, low, disturbance)	The BMS controller acts as a sensor for the VSC. It reports the batteries charge level to the VSC. All BMS controller failure modes contained in this analysis could affect the accurate reporting of the battery charge level to VSC.	BMS Controller
117	Process model or calibration incomplete or incorrect	If the calibration has an incorrect value for the cell voltage upper limit, then the BMS may not turn off onboard charging when the cell voltages reach their upper limit.	BMS Controller
307	Process model or calibration incomplete or incorrect	If the heater or cooler calibration is incorrect, then the BMS may not heat or cool the cells properly.	BMS Controller
330	Process model or calibration incomplete or incorrect	If the calibration for how the battery power accumulates with charge is incorrect, then the BMS may overcharge the battery or not charge it enough.	BMS Controller
333	Process model or calibration incomplete or incorrect	If the condensation sensor calibration is incorrect, the BMS may be aware of a buildup of condensation during charging.	BMS Controller
335	Process model or calibration incomplete or incorrect	If the cell voltage sensor calibration is incorrect, then the BMS may not be aware of the correct voltage of each cell.	BMS Controller
371	Process model or calibration incomplete or incorrect	If the pack temperature sensor calibration is incorrect, then the BMS may not know if the cells are too hot or too cold.	BMS Controller
372	Process model or calibration incomplete or incorrect	If the ground fault detection sensor calibration is incorrect, then the BMS may not be aware of a ground fault.	BMS Controller
413	Process model or calibration incomplete or incorrect	If the onboard charging current and voltage measurement calibration is incorrect, then the BMS may not be aware of the correct current and voltage delivered.	BMS Controller
239	Process model or calibration incomplete or incorrect	If the calibration has incorrect value for the safe operation voltage range, then the BMS may not balance the cells properly.	BMS Controller
336	Process model or calibration incomplete or incorrect	If the cell voltage balancer calibration is incorrect, then the BMS may not be aware of how it is actually balancing each cell voltage.	BMS Controller
410	Process model or calibration incomplete or incorrect	The process model in the BMS controller for the battery's change in voltage versus state of charge is incorrect.	BMS Controller
341	Process model or calibration incomplete or incorrect	If the pack current sensor calibration is incorrect, then the BMS may not be aware of how much current is leaving the battery.	BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
397	Process model or calibration incomplete or incorrect	If the traction motor, generator, and other high voltage components' calibration is incorrect, then the BMS may not have the correct understanding of the energy consumption request.	BMS Controller
340	Process model or calibration incomplete or incorrect	If the calibration has an incorrect value for the battery current rating, then the BMS may turn off the precharge contactor too quickly.	BMS Controller
373	Process model or calibration incomplete or incorrect	If the crash sensor calibration is incorrect, then the BMS may not be aware of an imminent crash.	BMS Controller
471	Process model or calibration incomplete or incorrect	If the off board charger plug status sensor calibration is incorrect, then the BMS may not be aware of a faulty plug status.	BMS Controller
506	Process model or calibration incomplete or incorrect	The Battery Management System Controller may have the incorrect understanding of the control modes of the generator/motor controller.	BMS Controller
518	Process model or calibration incomplete or incorrect	If the high voltage interlock sensor calibration is incorrect, then the BMS may not be aware of a high voltage component that has been opened up.	BMS Controller
429	Sensor inadequate operation, change over time	The BMS controller acts as a sensor for the VSC. It reports the batteries charge level to the VSC. All BMS controller failure modes contained in this analysis could affect the accurate reporting of the battery charge level to VSC.	BMS Controller
116	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	If the BMS controller logic does not consider all of the conditions to prevent continued charging when the battery has reached its voltage limit, then it may request charging when it isn't need.	BMS Controller
304	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	The BMS controller logic does not consider all of the conditions to correctly heat or cool the cells.	BMS Controller
238	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	The BMS controller logic does not consider all of the conditions to correctly rebalance the cells.	BMS Controller
395	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	The BMS controller logic error.	BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
339	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	The BMS controller logic does not consider all of the conditions to correctly implement the precharge routine.	BMS Controller
370	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	The BMS controller logic does not consider all of the conditions to correctly disengage the contactors.	BMS Controller
497	Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)	The BMS controller logic error causing the controller to request turning off the onboard charge controller too soon.	BMS Controller
241	Actuator inadequate operation, change over time	Resistor degradation due to heat, thermal fatigue, manufacturing defects, could cause the balancer to function improperly.	Cell Voltage Balancer
242	External disturbances	The resistor being shorted due to moisture would make the balancing ineffective.	Cell Voltage Balancer
243	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems may damage the resistor causing an open circuit. Moisture from other vehicle fluid systems could short the resistor. Physical contact with other components may also short the resistor.	Cell Voltage Balancer
118	External disturbances	EMI and/or ESD, moisture, and other elements from the surrounding environment may affect the cell voltage sensor.	Cell Voltage Sensor
119	Hazardous interaction with other components in the rest of the vehicle	Moisture from coolant or A/C lines could drip onto cell voltage sensors causing them to short out.	Cell Voltage Sensor
120	Hazardous interaction with other components in the rest of the vehicle	The location of the cell voltage sensor relative to other components should not create interference.	Cell Voltage Sensor
25	Power supply faulty (high, low, disturbance)	If the 12 volt battery doesn't supply power to the cell voltage sensor (but somehow still powers the BMS), the BMS won't know what the cell voltages are.	Cell Voltage Sensor
122	Sensor inadequate operation, change over time	If the cell voltage sensor degrades over time, the cell voltage reading will be incorrect.	Cell Voltage Sensor

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
398	Sensor inadequate operation, change over time	The cell voltage sensor fails permanently or intermittently.	Cell Voltage Sensor
169	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the condensation sensor's readings.	Condensation Sensor
170	Hazardous interaction with other components in the rest of the vehicle	EMI and/or ESD, moisture from the A/C or other fluid lines, or physical interference with other vehicle systems may affect the condensation sensor readings.	Condensation Sensor
168	Power supply faulty (high, low, disturbance)	If the condensation sensor loses 12 volt power, it won't be able to report the condensation level to the BMS controller.	Condensation Sensor
167	Sensor inadequate operation, change over time	The condensation sensor fails permanently or intermittently.	Condensation Sensor
262	Controller to actuator signal ineffective, missing, or delayed: Communication bus error	If the signal commanding the cell voltage balancer is delivered over bus connection, bus overload, error, or incorrect message priority setting may prevent the BMS controller command from reaching the cell voltage balancer.	Connection from BMS Controller to Cell Voltage Balancer
259	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the cell voltage balancer is open due to improperly seated connectors, open wire, or degrades over time, then cell voltage balancer won't receive any signals from the BMS.	Connection from BMS Controller to Cell Voltage Balancer
260	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the cell voltage balancer is shorted due to improper assembly, or degradation over time, then the signal commanding the cell voltage balancer won't arrive.	Connection from BMS Controller to Cell Voltage Balancer
265	Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	If the wiring between the BMS controller and the cell voltage balancer is incorrectly connected, then the signal commanding the cell voltage balancer won't arrive or will arrive at the wrong cell.	Connection from BMS Controller to Cell Voltage Balancer
266	External disturbances	EMI/ESD may affect the delivery of the commands from the BMS controller to the cell voltage balancers.	Connection from BMS Controller to Cell Voltage Balancer

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
267	External disturbances	Water, salt, and other environmental elements could degrade the connection between the BMS controller and the cell voltage balancers causing the command to not reach the cell voltage balancers.	Connection from BMS Controller to Cell Voltage Balancer
268	Hazardous interaction with other components in the rest of the vehicle	A/C condensation, coolant, and/or other vehicle fluids could drip onto the connection between the BMS controller and the cell voltage balancer, causing shorts and affecting the delivery of the command.	Connection from BMS Controller to Cell Voltage Balancer
269	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems may cause chafing of the wire between BMS controller and cell voltage balancer, leading to the command not being delivered.	Connection from BMS Controller to Cell Voltage Balancer
352	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the precharge contactor is open due to improperly seated connectors, open wire, or degrades over time, then the precharge contactor won't receive signals from the BMS consistently.	Connection from BMS Controller to Contactor
353	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the precharge contactor is shorted due to improper assembly, or degradation over time, then the signal commanding the precharge contactor won't arrive consistently.	Connection from BMS Controller to Contactor
385	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the main contactor is open due to improperly seated connectors, open wire, or degrades over time, then the main contactor won't receive signals from the BMS consistently.	Connection from BMS Controller to Contactor
386	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the main contactor is shorted due to improper assembly, or degradation over time, then the signal commanding the main contactor won't arrive consistently.	Connection from BMS Controller to Contactor
354	Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	If the wiring between the BMS controller and the pre-charge contactor is incorrectly connected, then the signal commanding the precharge contactor won't arrive or will arrive at the wrong contactor.	Connection from BMS Controller to Contactor

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
387	Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	If the wiring between the BMS controller and the main contactor is incorrectly connected, then the signal commanding the main contactor won't arrive or will arrive at the wrong contactor.	Connection from BMS Controller to Contactor
355	External disturbances	Water, salt, and other environmental elements could degrade the connection between the BMS controller and the contactors.	Connection from BMS Controller to Contactor
356	Hazardous interaction with other components in the rest of the vehicle	A/C condensation, coolant, and/or other vehicle fluids could drip onto the connection between the BMS controller and the precharge contactor, causing shorts and affecting the delivery of the command.	Connection from BMS Controller to Contactor
357	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems may cause chafing of the wire between BMS controller and the precharge contactor, leading to the command not being delivered.	Connection from BMS Controller to Contactor
388	Hazardous interaction with other components in the rest of the vehicle	A/C condensation, coolant, and/or other vehicle fluids could drip onto the connection between the BMS controller and the main contactor, causing shorts and affecting the delivery of the command.	Connection from BMS Controller to Contactor
389	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems may cause chafing of the wire between BMS controller and the main contactor, leading to the command not being delivered.	Connection from BMS Controller to Contactor
135	Controller to actuator signal ineffective, missing, or delayed: Communication bus error	If the signal commanding the onboard charge controller is delivered over bus connection, bus overload, error, or incorrect message priority setting may prevent the BMS controller command from reaching the onboard charge controller.	Connection from BMS Controller to Onboard Charging Controller
261	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the onboard charging controller is shorted due to improper assembly, or degradation over time, then the signal commanding the onboard charge controller won't arrive.	Connection from BMS Controller to Onboard Charging Controller
263	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the BMS controller and the onboard charging controller is open due to improperly seated connectors, open wire, or it degrades over time, then the signal commanding the onboard charge controller won't arrive.	Connection from BMS Controller to Onboard Charging Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
264	Controller to actuator signal ineffective, missing, or delayed: Incorrect connection	If the wiring between the BMS controller and the onboard charging controller is incorrectly connected, then the signal commanding the onboard charge controller won't arrive.	Connection from BMS Controller to Onboard Charging Controller
136	External disturbances	EMI/ESD may affect the delivery of the commands from the BMS controller to the onboard charge controller.	Connection from BMS Controller to Onboard Charging Controller
137	External disturbances	Water, salt, and other environmental elements could degrade the connection between the BMS controller and the onboard charge controller causing the command to not reach the onboard charge controller.	Connection from BMS Controller to Onboard Charging Controller
138	Hazardous interaction with other components in the rest of the vehicle	A/C condensation, coolant, and/or other vehicle fluids could drip onto the connection between the BMS controller and the onboard charge controller, causing shorts and affecting the delivery of the command.	Connection from BMS Controller to Onboard Charging Controller
139	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems may cause chafing of the wire between BMS controller and onboard charge controller, leading to the command not being delivered.	Connection from BMS Controller to Onboard Charging Controller
416	External disturbances	EMI/ESD, moisture, and other environmental elements may cause open or short between BMS controller and VSC controller.	Connection from BMS Controller to Vehicle Systems Controller
419	Hazardous interaction with other components in the rest of the vehicle	EMI/ESD, moisture from fluid lines, and physical interference with other vehicle systems causing chafing of the line between battery management system controller and vehicle system controller.	Connection from BMS Controller to Vehicle Systems Controller
418	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	The bus communication between the BMS controller and VSC controller may have problems such as bus overload, improper message priority, etc.	Connection from BMS Controller to Vehicle Systems Controller
417	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The wiring and the connectors between BMS controller and VSC controller may have manufacturing or assembly quality problems. They may also degrade over time, and this could cause open, short, or intermittent faults.	Connection from BMS Controller to Vehicle Systems Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
526	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	The connections between the BMS controller and VSC controller may be incorrect, caused by incorrect pin assignment, etc.	Connection from BMS Controller to Vehicle Systems Controller
270	Actuation delivered incorrectly or inadequately: Hardware faulty	If the connection between the cell voltage balancer and the high voltage battery cells is open due to improperly seated connectors, open wire, or degrades over time, then cell balancing will not occur.	Connection from Cell Voltage Balancer to High Voltage Battery Cells
271	Actuation delivered incorrectly or inadequately: Incorrect connection	If the wiring between the cell voltage balancer and the high voltage battery cell is incorrectly connected, then the incorrect cell will not be properly balanced.	Connection from Cell Voltage Balancer to High Voltage Battery Cells
272	External disturbances	Water, salt, and other environmental elements could degrade the connection between the high voltage cells and the cell voltage balancers.	Connection from Cell Voltage Balancer to High Voltage Battery Cells
273	Hazardous interaction with other components in the rest of the vehicle	A/C condensation, coolant, and/or other vehicle fluids could drip onto the connection between the cell voltage balancer and the high voltage battery cell, causing short circuits.	Connection from Cell Voltage Balancer to High Voltage Battery Cells
274	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems may cause chafing of the wire between cell voltage balancer and high voltage battery cells, leading to a lack of balancing.	Connection from Cell Voltage Balancer to High Voltage Battery Cells
166	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the cell voltage sensor to the BMS controller.	Connection from Cell Voltage Sensor to BMS Controller
164	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the cell voltage sensor and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults.	Connection from Cell Voltage Sensor to BMS Controller
126	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	In the case that cell voltages are reported in groups and the reporting makes a mistake on the cell and its corresponding voltage, then the BMS may not stop or control onboard charging.	Connection from Cell Voltage Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
123	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the voltage sensor cannot report the cell voltage to the BMS due to improperly seated connectors, then the BMS will have no way of knowing the current cell voltages.	Connection from Cell Voltage Sensor to BMS Controller
124	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the voltage sensor cannot report the cell voltage to the BMS due to an open wire, then the BMS will have no way of knowing the current cell voltages.	Connection from Cell Voltage Sensor to BMS Controller
125	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the voltage sensor cannot report the cell voltage to the BMS due to a missing wire, then the BMS will have no way of knowing the current cell voltages.	Connection from Cell Voltage Sensor to BMS Controller
216	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the voltage sensor to BMS controller wiring is shorted, the cell voltage reading will be incorrect.	Connection from Cell Voltage Sensor to BMS Controller
217	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the voltage sensor to BMS controller wiring is intermittently faulty, the cell voltage reading will be incorrect.	Connection from Cell Voltage Sensor to BMS Controller
128	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	If the cell voltage sensor wiring is incorrectly connected to the BMS controller, it may lead to an incorrect voltage reading.	Connection from Cell Voltage Sensor to BMS Controller
176	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the pack condensation sensor to the BMS controller.	Connection from Condensation Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
177	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the condensation sensor and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD from other vehicle systems could also cause problems	Connection from Condensation Sensor to BMS Controller
520	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the condensation sensor and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD from other vehicle systems.	Connection from Condensation Sensor to BMS Controller
172	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the condensation sensor cannot report or reports inaccurately to the BMS due to improperly seated connectors, then the BMS will have no way of knowing the pack condensation level.	Connection from Condensation Sensor to BMS Controller
173	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the condensation sensor cannot report or reports incorrectly to the BMS due to an open wire, then the BMS will have no way of knowing the condensation level within the pack.	Connection from Condensation Sensor to BMS Controller
174	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the condensation sensor cannot report or reports incorrectly to the BMS due to a missing wire, then the BMS will have no way of knowing the condensation level.	Connection from Condensation Sensor to BMS Controller
223	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the condensation sensor to BMS controller wiring is shorted, the condensation readings will be incorrect.	Connection from Condensation Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
224	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the condensation sensor to BMS controller wiring is intermittently faulty, the condensation readings will be incorrect.	Connection from Condensation Sensor to BMS Controller
175	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	If the condensation sensor wiring is incorrectly connected to the BMS controller, it may lead to an incorrect moisture level reading.	Connection from Condensation Sensor to BMS Controller
360	Actuation delivered incorrectly or inadequately: Hardware faulty	The wiring/connectors between the high voltage battery and the precharge contactor may be open or intermittently faulty.	Connection from Contactor to High Voltage Battery Cells
390	Actuation delivered incorrectly or inadequately: Hardware faulty	The wiring/connectors between the high voltage battery and the main contactor may be open or intermittently faulty.	Connection from Contactor to High Voltage Battery Cells
364	Hazardous interaction with other components in the rest of the vehicle	The wiring/connectors between the high voltage battery and the precharge and main contactors may be corroded due to moisture or chaffed by physical interference with other vehicle components.	Connection from Contactor to High Voltage Battery Cells
198	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the crash sensor to the BMS controller.	Connection from Crash Sensor to BMS Controller
199	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the crash sensor and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD from other vehicle systems.	Connection from Crash Sensor to BMS Controller
200	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	If crash imminent signal is sent via the CAN bus, bus overloading or improper signal priority may cause the signal to be incorrect, missing, or delayed.	Connection from Crash Sensor to BMS Controller
194	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the crash sensor cannot report or reports inaccurately to the BMS due to improperly seated connectors, then the BMS will have no way of knowing if a crash is imminent.	Connection from Crash Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
195	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the crash sensor cannot report or reports incorrectly to the BMS due to an open wire, then the BMS will have no way of knowing if a crash is imminent.	Connection from Crash Sensor to BMS Controller
196	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the crash sensor cannot report or reports incorrectly to the BMS due to a missing wire, then the BMS will have no way of knowing if a crash is imminent.	Connection from Crash Sensor to BMS Controller
227	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the crash sensor to BMS controller wiring is shorted, the crash sensor's readings will be incorrect.	Connection from Crash Sensor to BMS Controller
228	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the crash sensor to BMS controller wiring is intermittently faulty, the crash sensor's readings will be incorrect.	Connection from Crash Sensor to BMS Controller
197	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	If the crash sensor wiring is incorrectly connected to the BMS controller, the BMS will have no way of knowing if a crash is imminent.	Connection from Crash Sensor to BMS Controller
211	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the external air temperature sensor to the BMS controller.	Connection from External Air Temperature Sensor to BMS Controller
212	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the external air temperature sensor and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD from other vehicle systems.	Connection from External Air Temperature Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
213	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	If external air temperature sensor's signal is sent via the CAN bus, bus overloading or improper signal priority may cause the signal to be incorrect, missing, or delayed.	Connection from External Air Temperature Sensor to BMS Controller
207	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the external air temperature sensor cannot report or reports inaccurately to the BMS due to improperly seated connectors, then the BMS will have no way of knowing the external air temperature.	Connection from External Air Temperature Sensor to BMS Controller
208	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the external air temperature sensor cannot report or reports incorrectly to the BMS due to an open wire, then the BMS will have no way of knowing external air temperature.	Connection from External Air Temperature Sensor to BMS Controller
209	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the external air temperature sensor cannot report or reports incorrectly to the BMS due to a missing wire, then the BMS will have no way of knowing the external air temperature.	Connection from External Air Temperature Sensor to BMS Controller
229	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the external air temperature sensor to BMS controller wiring is shorted, the external air temperature reading will be incorrect.	Connection from External Air Temperature Sensor to BMS Controller
230	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the external air temperature sensor to BMS controller wiring is intermittently faulty, the external air temperature reading will be incorrect.	Connection from External Air Temperature Sensor to BMS Controller
210	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	If the external air temperature sensor wiring is incorrectly connected to the BMS controller, the BMS will have no way of knowing the external air temperature.	Connection from External Air Temperature Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
257	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the external ambient air to the external air temperature sensor.	Connection from External Ambient Air to External Air Temperature Sensor
214	Sensor measurement incorrect or missing	If the external air temperature sensor is improperly installed, it might affect the accuracy of sensor reading.	Connection from External Ambient Air to External Air Temperature Sensor
459	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the Generator/Motor controller to the BMS controller.	Connection from Generator/Motor Controller to BMS Controller
499	Hazardous interaction with other components in the rest of the vehicle	EMI/ESD, moisture from a coolant line, A/C, other vehicle fluids, or physical interference with other vehicle systems could damage the connection between the Battery Management System Controller and the Generator/Motor Controller.	Connection from Generator/Motor Controller to BMS Controller
432	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	If the communication between the BMS and the Generator/Motor controller is on a bus, bus overload or other types of errors may cause faulty communication.	Connection from Generator/Motor Controller to BMS Controller
420	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The generator/motor controller cannot report the energy it needs to the BMS due to improperly seated connectors.	Connection from Generator/Motor Controller to BMS Controller
454	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The generator/motor controller cannot report the energy it needs to the BMS due to an open wire.	Connection from Generator/Motor Controller to BMS Controller
455	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The generator/motor controller cannot report the energy it needs to the BMS due to a missing wire.	Connection from Generator/Motor Controller to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
456	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The generator/motor controller cannot report the energy it needs to the BMS due to wiring that is shorted out.	Connection from Generator/Motor Controller to BMS Controller
457	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The generator/motor controller cannot report the energy it needs to the BMS due to wiring that is intermittently faulty.	Connection from Generator/Motor Controller to BMS Controller
458	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	The generator/motor controller cannot report the energy it needs to the BMS due to an incorrect wiring connection.	Connection from Generator/Motor Controller to BMS Controller
433	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	The connector pins are incorrectly hooked up between the BMS controller and the Generator/Motor controller.	Connection from Generator/Motor Controller to BMS Controller
440	Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the connection between the Generator/Motor Controller and the Generator/Motor is open due to improperly seated connectors, open wire, or it degrades over time, then the signal commanding the Generator/Motor to engage regenerative braking won't arrive.	Connection from Generator/Motor Controller to Generator/Motor
528	Hazardous interaction with other components in the rest of the vehicle	EMI/ESD from other vehicle systems, physical interferences with other vehicle systems such as chafing, and moisture dripping from liquid lines such as AC condensation could potentially negatively affect the signal transmission between generator/motor controller and generator/motor.	Connection from Generator/Motor Controller to Generator/Motor
182	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the ground fault detection sensor to the BMS controller.	Connection from Ground Fault Detection Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
183	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the ground fault detection sensor and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD may also affect the signal transmission.	Connection from Ground Fault Detection Sensor to BMS Controller
178	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the ground fault detection sensor cannot report or reports inaccurately to the BMS due to improperly seated connectors, then the BMS will have no way of knowing if there is a ground fault.	Connection from Ground Fault Detection Sensor to BMS Controller
179	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the ground fault detection sensor cannot report or reports incorrectly to the BMS due to an open wire, then the BMS will have no way of knowing if a ground fault has occurred.	Connection from Ground Fault Detection Sensor to BMS Controller
180	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the ground fault sensor cannot report to the BMS due to a missing wire, then the BMS will have no way of knowing if a ground fault has occurred.	Connection from Ground Fault Detection Sensor to BMS Controller
225	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the ground fault detection sensor to BMS controller wiring is shorted, the ground fault detection readings will be incorrect.	Connection from Ground Fault Detection Sensor to BMS Controller
226	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the ground fault detection sensor to BMS controller wiring is intermittently faulty, the ground fault detection readings will be incorrect.	Connection from Ground Fault Detection Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
181	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	If the ground fault detection sensor wiring is incorrectly connected to the BMS controller, it may lead to an incorrect reading of the signal from the ground fault detector.	Connection from Ground Fault Detection Sensor to BMS Controller
244	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the high voltage battery cells to the cell voltage sensor.	Connection from High Voltage Battery Cells to Cell Voltage Sensor
248	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the high voltage battery cells and the cell voltage sensor. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD may also affect the reading.	Connection from High Voltage Battery Cells to Cell Voltage Sensor
515	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the high voltage battery cells and the cell voltage sensor. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD may also affect the reading.	Connection from High Voltage Battery Cells to Cell Voltage Sensor
132	Sensor measurement incorrect or missing	If the leads from the cell voltage sensor come loose or fall off the battery terminals over time, or are installed incorrectly, then they won't give the proper cell voltage reading.	Connection from High Voltage Battery Cells to Cell Voltage Sensor
252	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the high voltage battery pack to the pack condensation sensor.	Connection from High Voltage Battery Pack to Condensation Sensor
251	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the high voltage battery pack and the pack condensation sensor. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD may also affect the sensor reading.	Connection from High Voltage Battery Pack to Condensation Sensor
188	Sensor measurement incorrect or missing	If the condensation sensor is improperly installed or becomes loose over time, the sensor reading may be inaccurate or missing.	Connection from High Voltage Battery Pack to Condensation Sensor
249	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the high voltage battery pack to the pack current sensor.	Connection from High Voltage Battery Pack to Pack Current Sensor

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
250	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the high voltage battery pack and the pack current sensors. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD may also affect the reading.	Connection from High Voltage Battery Pack to Pack Current Sensor
232	Sensor measurement incorrect or missing	If the leads from a pack current sensor come loose or fall off over time, or is installed incorrectly, then it won't give the proper pack current reading. For a Hall effect current sensor, if the sensor alignment is faulty, the reading may be incorrect.	Connection from High Voltage Battery Pack to Pack Current Sensor
246	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the high voltage battery pack to the pack temperature sensor.	Connection from High Voltage Battery Pack to Pack Temperature Sensor
247	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the high voltage battery pack and the pack temperature sensors. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD may also affect the reading.	Connection from High Voltage Battery Pack to Pack Temperature Sensor
154	Sensor measurement incorrect or missing	If the temperature sensor is improperly installed or becomes loose over time, the sensor reading may be inaccurate or missing.	Connection from High Voltage Battery Pack to Pack Temperature Sensor
475	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the off-board charger plug status sensor's signal that's transmitted to the BMS controller.	Connection from Off-board Charging System to BMS Controller
476	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness that sends the off-board charger plug status sensor's signal to the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD could also affect the signal.	Connection from Off-board Charging System to BMS Controller
473	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the off-board charging port sensor's connection (connectors and wiring) to BMS controller is open, short, or intermittently faulty, then the BMS may not know when the off-board charger is plugged-in and when it's not.	Connection from Off-board Charging System to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
474	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	The off-board charger plug status sensor is incorrectly connected to BMS controller.	Connection from Off-board Charging System to BMS Controller
378	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the onboard charge controller current/voltage measurement signal that's transmitted to the BMS controller.	Connection from Onboard Charging Controller to BMS Controller
379	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness that sends the onboard charge controller current/voltage measurement to the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD could also affect the signal.	Connection from Onboard Charging Controller to BMS Controller
359	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The onboard charge controller current/voltage measurement connection (connectors and wiring) to BMS controller is open, short, or intermittently faulty.	Connection from Onboard Charging Controller to BMS Controller
451	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	The onboard charge controller current/voltage measurement connection is incorrectly connected to BMS controller.	Connection from Onboard Charging Controller to BMS Controller
163	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the pack current sensor to the BMS controller.	Connection from Pack Current Sensor to BMS Controller
165	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the pack current sensor and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults. EMI/ESD could also affect the signal transmitted.	Connection from Pack Current Sensor to BMS Controller
159	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the pack current sensor cannot report the current to the BMS due to improperly seated connectors, then the BMS will have no way of knowing the pack current.	Connection from Pack Current Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
160	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the current sensor cannot report the current to the BMS due to an open wire, then the BMS will have no way of knowing the current.	Connection from Pack Current Sensor to BMS Controller
161	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the current sensor cannot report the current to the BMS due to a missing wire, then the BMS will have no way of knowing the pack current.	Connection from Pack Current Sensor to BMS Controller
219	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the pack current sensor to BMS controller wiring is shorted, the pack current reading will be incorrect.	Connection from Pack Current Sensor to BMS Controller
220	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	If the pack current sensor to BMS controller wiring is intermittently faulty, the pack current reading will be incorrect.	Connection from Pack Current Sensor to BMS Controller
162	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	If the current sensor wiring is incorrectly connected to the BMS controller, it may lead to an incorrect pack current reading.	Connection from Pack Current Sensor to BMS Controller
152	External disturbances	EMI/ESD, moisture, or other environmental elements may affect the integrity of the connector and the wiring between cell temperature sensors and the BMS controller, causing the temperature reading to be faulty.	Connection from Pack Temperature Sensor to BMS Controller
153	Hazardous interaction with other components in the rest of the vehicle	EMI/ESD, moisture from A/C and other fluid lines, chafing caused by physical interference with other vehicle systems may affect the integrity of the connector and the wiring between cell temperature sensors and the BMS controller, causing the temperature reading to be faulty.	Connection from Pack Temperature Sensor to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
151	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Pack temperature sensor to BMS controller communication bus may be overload or the message priority may be incorrect, causing the temperature reading to not reach the controller.	Connection from Pack Temperature Sensor to BMS Controller
149	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Pack temperature sensor to BMS controller connectors may be improperly assembled or become loose over time, causing the temperature reading to not reach the controller.	Connection from Pack Temperature Sensor to BMS Controller
150	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Pack temperature sensor to BMS controller wiring may be improperly assembled or degrade over time, causing open, short, or intermittently faulty circuits.	Connection from Pack Temperature Sensor to BMS Controller
329	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	If a pack temperature sensor wiring is incorrectly connected to the BMS controller, it may lead to an incorrect temperature reading.	Connection from Pack Temperature Sensor to BMS Controller
467	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the Traction Motor controller to the BMS controller.	Connection from Traction Motor Controller to BMS Controller
468	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the Traction Motor controller and the BMS controller. Moisture from A/C and other fluid lines may cause short or other intermittent faults.	Connection from Traction Motor Controller to BMS Controller
461	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The Traction Motor controller cannot report the energy it needs to the BMS due to improperly seated connectors.	Connection from Traction Motor Controller to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
462	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The Traction Motor controller cannot report the energy it needs to the BMS due to an open wire.	Connection from Traction Motor Controller to BMS Controller
463	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The Traction Motor controller cannot report the energy it needs to the BMS due to a missing wire.	Connection from Traction Motor Controller to BMS Controller
464	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The Traction Motor controller cannot report the energy it needs to the BMS due to wiring that is shorted out.	Connection from Traction Motor Controller to BMS Controller
465	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	The Traction Motor controller cannot report the energy it needs to the BMS due to wiring that is intermittently faulty.	Connection from Traction Motor Controller to BMS Controller
466	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	The Traction Motor controller cannot report the energy it needs to the BMS due to an incorrect wiring connection.	Connection from Traction Motor Controller to BMS Controller
430	External disturbances	Failure modes related to how BMS estimates battery SOC have been analyzed in the BMS controller UCA's. If the HV consumers aren't able to report their power requirements to the BMS, then BMS controller cannot perform power arbitration for the VSC.	Connection from Vehicle to BMS Controller
430	Hazardous interaction with other components in the rest of the vehicle	Failure modes related to how BMS estimates battery SOC have been analyzed in the BMS controller UCA's. If the HV consumers aren't able to report their power requirements to the BMS, then BMS controller cannot perform power arbitration for the VSC.	Connection from Vehicle to BMS Controller

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
430	Sensor to controller signal inadequate, missing, or delayed: Communication bus error	Failure modes related to how BMS estimates battery SOC have been analyzed in the BMS controller UCA's. If the HV consumers aren't able to report their power requirements to the BMS, then BMS controller cannot perform power arbitration for the VSC.	Connection from Vehicle to BMS Controller
430	Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty	Failure modes related to how BMS estimates battery SOC have been analyzed in the BMS controller UCA's. If the HV consumers aren't able to report their power requirements to the BMS, then BMS controller cannot perform power arbitration for the VSC.	Connection from Vehicle to BMS Controller
430	Sensor to controller signal inadequate, missing, or delayed: Incorrect connection	Failure modes related to how BMS estimates battery SOC have been analyzed in the BMS controller UCA's. If the HV consumers aren't able to report their power requirements to the BMS, then BMS controller cannot perform power arbitration for the VSC.	Connection from Vehicle to BMS Controller
253	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the signal transmitted from the vehicle to the ground fault detection sensor.	Connection from Vehicle to Ground Fault Detection Sensor
255	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems might cause chafing of the wiring harness between the vehicle and the ground fault detection sensor. Moisture from A/C and other fluid lines may cause short or other intermittent faults.	Connection from Vehicle to Ground Fault Detection Sensor
189	Sensor measurement incorrect or missing	If the ground fault detection sensor is improperly installed or becomes loose over time, the sensor reading may be inaccurate or missing.	Connection from Vehicle to Ground Fault Detection Sensor
343	Actuator inadequate operation, change over time	The contactor or relay may be faulty or degrade over time.	Contactor
361	Actuator inadequate operation, change over time	The assembly of the precharge contactor circuit may be connected incorrectly.	Contactor
363	Actuator inadequate operation, change over time	The incorrect precharge resistor (power rating too low or resistance too low) may be installed.	Contactor
344	External disturbances	The contactor or relay may be corroded by moisture, rendering it ineffective.	Contactor
346	Hazardous interaction with other components in the rest of the vehicle	Physical interference with other vehicle systems may damage the contactors. Moisture from other vehicle fluid systems could corrode the contactors.	Contactor

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
345	Power supply faulty (high, low, disturbance)	The precharge contactor won't work if it loses 12 volt power (and if the main contactor still has power and closes, then there will be major in-rush current).	Contactor
384	Power supply faulty (high, low, disturbance)	The main contactor loses 12 volt power (this isn't a problem if normally open contactors are used).	Contactor
190	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the crash sensor's readings.	Crash Sensor
191	Hazardous interaction with other components in the rest of the vehicle	EMI and/or ESD, moisture from the A/C or other fluid lines, or physical interference with other vehicle systems may affect the crash sensor readings.	Crash Sensor
193	Power supply faulty (high, low, disturbance)	If the crash sensor loses 12 volt power, it won't be able to report the crash to the BMS controller.	Crash Sensor
192	Sensor inadequate operation, change over time	The crash sensor fails permanently or intermittently.	Crash Sensor
206	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the external air temperature sensor readings or cause degradation.	External Air Temperature Sensor
203	Hazardous interaction with other components in the rest of the vehicle	EMI and/or ESD, moisture from the A/C or other fluid lines, or physical interference with other vehicle systems may affect the external air temperature sensor readings.	External Air Temperature Sensor
205	Power supply faulty (high, low, disturbance)	If the external air temperature sensor loses 12 volt power, it won't be able to report the external air temperature to the BMS controller.	External Air Temperature Sensor
204	Sensor inadequate operation, change over time	The external air temperature sensor fails permanently or intermittently.	External Air Temperature Sensor
184	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the ground fault detection sensor's readings.	Ground Fault Detection Sensor
185	Hazardous interaction with other components in the rest of the vehicle	EMI and/or ESD, moisture from the A/C or other fluid lines, or physical interference with other vehicle systems may affect the ground fault detection sensor readings.	Ground Fault Detection Sensor
187	Power supply faulty (high, low, disturbance)	If the ground fault sensor loses 12 volt power, it won't be able to report the ground fault status to the BMS controller.	Ground Fault Detection Sensor
186	Sensor inadequate operation, change over time	The ground fault detection sensor fails permanently or intermittently.	Ground Fault Detection Sensor

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
414	Controlled component failure, change over time	The high voltage cells may have manufacturing quality problems, such as impurity or a broken internal separator.	High Voltage Battery Cells
411	Controlled component failure, change over time	Battery cell chemistry changes over time.	High Voltage Battery Cells
279	External disturbances	External objects might penetrate the high voltage battery cells. Also the cells may become shorted to the battery container or the external vehicle frame.	High Voltage Battery Cells
278	Hazardous interaction with other components in the rest of the vehicle	Other vehicle components might penetrate the high voltage battery cells.	High Voltage Battery Cells
276	Conflicting control action	If BMS requests balancing and the onboard charge controller is commanding charging at the same time, this could potentially lead to unsuccessful balancing.	High Voltage Battery Pack
391	Sensor inadequate operation, change over time	The High Voltage Interlock Loop sensor wears out or becomes stuck closed.	High Voltage Interlock Loop Sensor
470	Sensor inadequate operation, change over time	If the charge plug status sensor does not report hazardous state of the charger plug (for plug-in vehicles), the BMS won't request stopping charge, and it may result in overheating or damage of the charging system. This however, does not cause direct damage to the battery. Fire of the charging system will eventually damage the vehicle and the battery.	Off-board Charging System
447	Actuator inadequate operation, change over time	The onboard charge controller has hardware that is faulty or degrades over time.	Onboard Charging Controller
142	External disturbances	EMI and/or ESD from the environment may affect the onboard charge controller.	Onboard Charging Controller
381	Hazardous interaction with other components in the rest of the vehicle	EMI/ESD, moisture from a coolant line, A/C, other vehicle fluids, or physical interference with other vehicle systems could damage the onboard charging controller.	Onboard Charging Controller
448	Power supply faulty (high, low, disturbance)	Onboard charging controller loses 12 volt power.	Onboard Charging Controller
380	Sensor inadequate operation, change over time	The onboard charge controller current/voltage measurement fails permanently or intermittently.	Onboard Charging Controller
157	External disturbances	EMI/ESD, moisture, and other environmental factors could affect the pack current sensor's readings.	Pack Current Sensor

Causal Factor ID	Causal Factor Guideword	Causal Factor	Component or Connection
158	Hazardous interaction with other components in the rest of the vehicle	EMI/ESD, moisture from A/C and other fluid lines, and physical interference with other vehicle systems could affect the pack current sensor's readings.	Pack Current Sensor
348	Power supply faulty (high, low, disturbance)	If the pack current sensor loses 12 volt power, it won't be able to report the battery current.	Pack Current Sensor
347	Sensor inadequate operation, change over time	The pack current sensor may fail permanently or intermittently.	Pack Current Sensor
148	External disturbances	EMI and/or ESD from the external environment may affect pack temperature sensor readings.	Pack Temperature Sensor
310	External disturbances	If moisture or other environmental elements get into the temperature sensor, it might be shorted out and unable to report accurate temperature readings.	Pack Temperature Sensor
171	Hazardous interaction with other components in the rest of the vehicle	EMI and/or ESD, moisture from A/C or other fluid lines, or physical interference with other vehicles systems may affect the temperature sensor readings.	Pack Temperature Sensor
311	Power supply faulty (high, low, disturbance)	If the temperature sensor loses 12 volt power, it won't be able to communicate cell temperatures to the BMS.	Pack Temperature Sensor
309	Sensor inadequate operation, change over time	If the pack temperature sensor fails permanently or intermittently, the BMS won't know the correct battery temperature.	Pack Temperature Sensor
407	External disturbances	The energy consumption reporting portion of the high voltage components may be affected by EMI/ESD, moisture, and/or other environment elements.	Vehicle
409	Hazardous interaction with other components in the rest of the vehicle	The energy consumption reporting portion of the high voltage components may be affected by EMI/ESD, moisture from fluid lines, and physical interference with other vehicle systems.	Vehicle
408	Power supply faulty (high, low, disturbance)	The energy consumption reporting portion of the high voltage components may lose 12 volt power.	Vehicle
406	Sensor inadequate operation, change over time	The energy consumption reporting portion of the high voltage components may be faulty or degrade over time.	Vehicle

Appendix G: System Failures and Faults (First HazOp Implementation)

Failure	***Fault***
BMS does not open main contactors	Micro-controller fault
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
	Incorrect/corrupted software algorithm
	EMC/EMI
	External contaminationv
	Incorrect circuit design (component selection, thermal design, robustness to noise factors).
BSM does not set cell over-voltage flag	Micro-controller fault
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
	Incorrect/corrupted software algorithm
	EMC/EMI
	External contaminationv
	Incorrect circuit design (component selection, thermal design, robustness to noise factors).
Cell short circuit	Manufacturing defect
	physical damage
	Aging
	Incorrect charging
	Internal components failure (separator, electrode)
Communication messages corrupted during transfer from and to the RESS and interfacing vehicle modules	Outside the scope of this analysis
Corrupted critical communications	Micro-controller fault
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
Corrupted incoming message	Outside the scope of this analysis
Does not detect open cell sense line	Integrated Circuit fault
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
	EMC/EMI
	External contaminationv

	ESD
Does not detect reference voltage out of tolerance	Integrated circuit fault
	break in cell sense line
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
	EMC/EMI
	External contaminationv
	ESD
	Break in communication line
	Short circuit in communication line
Does not measure cell voltage	Integrated circuit fault
	Break in cell sense line
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
	EMC/EMI
	External contaminationv
	ESD
Does not report cell voltage when requested	Integrated circuit fault
	Break in cell sense line
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
	EMC/EMI
	External contaminationv
	ESD
	Break in communication line
	Short circuit in communication line
Ground fault circuit fails to detect short circuit	Dependent on GFD design
HVIL circuit operates intermittently	Vibration
	Contamination/corrosion
	Wear/aging
	Corrupted communication
HVIL circuit stuck closed	Contamination/corrosion
	Wear/aging
	Corrupted communication
HVIL circuit stuck Open	Contamination/corrosion
	Wear/aging
	Corrupted communication
Incorrect design of the thermal management system of the battery cells	Incorrect characterization of the cell thermal environment
	Incorrect characterization of the cell thermal profile
	Incorrect cell temperature sensor placement
	Insufficient number of temperature sensors
	Low capacity of the coolant pump subsystem

Internal diagnostics failure results in not detecting over-voltage fault	Integrated circuit fault
	Break in cell sense line
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
	EMC/EMI
	External contaminationv
	ESD
	Break in communication line
	Short circuit in communication line
Internal short circuit	Mechanical shock/vibration
	Corrosion
	Manufacturing defect
Leak/blocked	Mechanical shock/vibration
	Manufacturing defect
	Corrosion
Low voltage power loss	Outside the scope of this analysis
Main contactor shudder	External contamination
	Wear out
	EMI/EMC
Main contactor stuck open	External contamination
	Wear out
Main contactor unintended opening	External contamination
	Wear out
	EMI/EMC
Main contactors stuck closed	Over-current (welding)
	External contamination
	Wear out
Misinterpretation of the cell SOH parameters	Incorrect/corrupted SW algorithm
	Critical parameters corrupted
	Cell characteristics misinterpreted
	Misinterpretation of input parameters
	Memory hardware fault
	EMC/EMI
Misinterpretation of the on-board charger controller communication	Micro-controller fault
	Break in communication line
	Short circuit in communication line
	Incorrect/corrupted software algorithm
	EMC/EMI
	External contaminationv
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
No interface with the cell voltage sensing and balancing subsystem	Micro-controller fault
	Break in I/Os connections

	Short circuit in I/Os connections
	Incorrect/corrupted software algorithm
	EMC/EMI
	External contaminationv
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
	Misinterpretation of input values
On-board charging contactors do not open	Micro-controller fault
	Break in communication line
	Short circuit in communication line
	Incorrect/corrupted software algorithm
	EMC/EMI
	External contaminationv
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
Open connection	Mechanical shock/vibration
	Corrosion
	Manufacturing defect
Reports cell voltage incorrectly	Integrated circuit fault
	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
	EMC/EMI
	External contaminationv
	ESD
Sensor misreads the cell temperature	Integrated circuit fault
	Sensor components failure
	Break in I/Os connections
	Short circuit in I/Os connections
	EMC/EMI
Shorted connection	Mechanical shock/vibration
	Corrosion
	Manufacturing defect
State of charge estimation is too low	Incorrect/Corrupted software algorithm
	Critical parameters corrupted
	Cell characteristics misinterpreted (e.g., Does an acceptable cell voltage level at start of life turn into an over-voltage level at EOL?)
	Misinterpretation of input parameters
	Memory hardware fault
	EMC/EMI
System short circuit	Outside the scope of this analysis
The BMS does not act on the high temperature values received from the temperature sensor	Micro-controller fault
	Software algorithm failure

The BMS does not act on the HVIL message received	Micro-controller fault
	Software algorithm failure
The BMS does not act on the impedance values communicated by the ground fault monitoring circuit	Micro-controller fault
	Software algorithm failure
	Micro-controller fault
	Software algorithm failure
The BMS misinterprets the crash signal detection opens the main contactors	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
The BMS misinterprets the current values communicated by the current sensor	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
	Corrupted signal from the current sensor
The BMS misinterprets the HVIL message communicated by the HVIL circuit (directly or indirectly)	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
The BMS misinterprets the HVIL message communicated by the HVIL circuit (directly or indirectly) and opens the main contactors	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
The BMS misinterprets the impedance values communicated by the ground fault monitoring circuit	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections

	Corrupted signal from the GF monitoring circuit
The BMS misinterprets the impedance values communicated by the ground fault monitoring circuit and opens the main contactors	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
	Corrupted signal from the GF monitoring circuit
The BMS misinterprets the temperature values communicated by the cell temperature sensors and opens the main contactors	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
The BMS misinterprets the temperature values communicated by the temperature sensor	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	Break in communication line
	Short circuit in communication line
	Break in I/Os connections
	Short circuit in I/Os connections
	Corrupted signal from the temperature sensor
The BSM does not turn on the coolant pump controller	Incorrect circuit design (component selection, thermal design, robustness to noise factors)
The BSM does not turn on the coolant pump controller	Micro-controller fault
	Software algorithm failure
	EMC/EMI
	External contaminationv
	Break in I/Os connections
	Short circuit in I/Os connections
	Break in communication line
	Short circuit in communication line
	Corrupted communication messages with coolant pump subsystem
Thermal management failure	Outside the scope of this analysis
Under-reporting of charging current value	Integrated circuit fault
	Sensor components failure
	Break in I/Os connections
	Short circuit in I/Os connections

Appendix H: Electromagnetic Interference and Electromagnetic Compatibility

Rechargeable energy storage systems that supply high-voltage power to automotive electric drive systems present unique challenges. These systems have sophisticated battery management systems as well as other more conventional electronic vehicle control systems, all of which require protection from electromagnetic interference to maintain vehicle function and safety.

The RESS has interfaces with several vehicle systems including electric drive motors, power converters, and actuators that employ rapid switching strategies for high-voltage current. This switching of high current is a major source of EMI in vehicles equipped with high-voltage RESSs. There is also susceptibility to electrostatic discharge from the flow of dry air over conductors and electronic components.

EMI and ESD can have negative effects on several safety-critical elements of the RESS. In particular, they can corrupt safety-critical sensor readings, such as cell voltage, cell temperature, as well as critical communications. Faulty sensor readings can result in vehicle safety hazards if the electronic control systems are not sufficiently robust.

EMI and ESD can also damage memory chips and power components, resulting in potential safety issues. Similarly, input/output (I/O) pins of electronic components are particularly susceptible to ESD. Damage to I/O pins can result in erroneous data transfer and subsequently to faults in control system behavior. Software faults may also occur if the values of critical system parameters (calibrateable and non-calibrateable) are corrupted by EMI.

Limiting the generation and magnitude of EMI in RESSs is important to overall vehicle safety. Several techniques are used to keep these phenomena in the safe range:

- Providing a minimum separation between high-voltage and low-voltage conductors. When the high-voltage and low-voltage cables are in close proximity (especially in parallel), they can form an inductive coupling path. Nonetheless, design considerations make some overlap difficult to avoid. Larger separations reduce EMI.
- Routing high-voltage conductors at an angle to low-voltage conductors in order to minimize coupling. The angle that minimizes coupling is 90 degrees. Studies suggest that ~~at~~ an angle less than 45 degrees has negligible effectiveness.
- Shielding of high-voltage conductors and/or communication wires. Fortunately, high-voltage cables are usually shielded. However, since some electromagnetic compatibility requirements may not appropriately consider shielding, a methodology for determining sufficient emission limits must be developed. These limits must consider specific attributes of the high-voltage components and must be stringent enough to provide the EMC across the entire vehicle. Unfortunately, while shielding can facilitate EMC, it often results in vehicle assembly complications, higher costs and reduced design flexibility.
- Filtering of communication signals may be required if serial peripheral interface or serial communication interface communication protocols are used. EMI and ESD can disrupt electronic communication protocols such as SPI or SCI. When critical signals such as many of those on the CAN bus are corrupted, control of electronic devices is endangered. The malfunction of such devices could lead directly or indirectly to a vehicle safety hazard
- Twisting all communication lines.

- Electrical grounding to chassis. When the chassis is non-conductive, a conductive grounding path to the vehicle ground is required.
- Minimizing the length of the connection between the power converter and motor.

Assessing EMI and EMC

Guttowski, Weber, Hoene, John, & Reichl (2003) asserted that conventional electromagnetic compatibility design and testing protocols may not completely account for important aspects of such a system. Creating a high-voltage system using the nominal automotive design procedures could lead to substantial incompatibility problems requiring unreasonable filtering effort. Coupling paths were modeled to estimate EMI in order to establish emission limits that meet EMC requirements.

They analyzed the components of an electric drive system that could generate noise and potential coupling paths between the high-voltage and low-voltage electrical systems. The results of the coupling models enabled them to modify EMC requirements of the conventional electrical system to the new electrical drive components and specify maximum interference levels on the high-voltage bus. The power converter is known to be a major source of EMI within electric drive systems. Simplified methods to estimate the generated EMI of power electronic devices with changing pulse patterns were used.

Guttowski and colleagues also noted that the battery providing power to the converter is a main part of the path for EMI. Therefore, the battery behavior at high frequency range must be determined. The values of key electrical parameters (capacitance, inductance, resistance) can be dependent on the geometry of the battery electrodes, rolled (cylindrical batteries) or laminated (prismatic batteries). They were able to match experimental data using simplified models.

They asserted the approach could be used to compare design configurations with and without shielding to ascertain whether or not shielded cables between the power converter and the power supply could provide enough protection to eliminate the need for the EMI filter. Assuming that shielding can provide a 30 dB reduction in EMI noise, they determined that some configurations would still require filtering. Nonetheless, modeling could provide important input in design optimization.

Appendix I: Sample Safe State Definitions for Implementation 1

Table I-1: Safe States for Thermal Event Scenarios

Malfunction	Application	Fault Mitigation	Estimated Fault Tolerant Time	Low Operation Strategy	DTC	Data Logging*
Cell Overcharging: cell temperature less than T_{onset}	EV, HEV, PHEV	N/A	N/A	N/A	Internal to system	Cells overcharged, Voltages
Cell Overcharging: cell temperature between T_{onset} and T_a (Probable Thermal Event)	EV, HEV, PHEV	Reduced Charging	500 ms	Limp Home Mode in case of Regenerative charging	Battery Overvoltage, Battery Overheating	Cells overcharged, Voltages, Temperatures, FTT*
Cell Overcharging: cell temperature above T_a (Probable Thermal Event)	EV, HEV, PHEV	Open Contactors	500 ms	Disable Vehicle	Battery Overvoltage, Battery Overheating	Cells overcharged, Voltages, Temperatures, FTT*
Deficient RESS Thermal Design: cell temperature reaches T_{onset}	EV, HEV, PHEV	N/A	N/A	N/A	Battery Overheating	Temperatures
Deficient RESS Thermal Design: cell temperature between T_{onset} and T_a (Probable Thermal Event)	EV, HEV, PHEV	Turn on cooling system including in vehicle OFF mode	500 ms	Limp Home Mode	Battery Overheating	Temperatures, FTT*
Deficient RESS Thermal Design: cell temperature above T_a (Probable Thermal Event)	EV, HEV, PHEV	Open Contactors	500 ms	Disable Vehicle	Battery Overheating	Temperatures, FTT*
Cooling System Failure: detected while cell temperature below T_{onset}	EV, HEV, PHEV	N/A	N/A	N/A	Cooling System Fault, Battery Overheating	Cooling System Fault Details, Temperatures
Cooling System Failure: cell temperature between T_{onset} and T_a (Probable Thermal Event)	EV, HEV, PHEV	Limit RESS Power Output	500 ms	Limp Home Mode	Cooling System Fault, Battery Overheating	Cooling System Fault Details, Temperatures, FTT*

Malfunction	Application	Fault Mitigation	Estimated Fault Tolerant Time	Low Operation Strategy	DTC	Data Logging*
Cooling System Failure: cell temperature above T_a (Probable Thermal Event)	EV, HEV, PHEV	Open Contactors	500 ms	Disable Vehicle	Cooling System Fault, Battery Overheating	Cooling System Fault Details, Temperatures, FTT*
Cell Internal Short Circuit: cell temperature reaches T_{onset}	EV, HEV, PHEV	N/A	N/A	N/A	Cell short	Temperatures, FTT*
Cell Internal Short Circuit: cell temperature between T_{onset} and T_a (Probable Thermal Event)	EV, HEV, PHEV	Limit RESS Power Output	500 ms	Limp Home Mode	Cell Short Circuit, Battery Overheating	Temperatures, FTT*
Cell Internal Short Circuit: cell temperature above T_a (Probable Thermal Event)	EV, HEV, PHEV	Open Contactors	500 ms	Disable Vehicle	Cell Short Circuit, Battery Overheating	Temperatures, FTT*
Cell Internal Short Circuit: Cascading Failure	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	Cell Short Circuit, Battery Overheating	Temperatures, FTT*
Battery Pack Short Circuit: detected while average cell temperature below T_{onset}	EV, HEV, PHEV	N/A	N/A	N/A	Pack short circuit	Temperatures, FTT*, Battery Current Sensor Values
Battery Pack Short Circuit: average cell temperature between T_{onset} and T_a (Probable Thermal Event)	EV, HEV, PHEV	Limit RESS Power Output	200 ms	Limp Home Mode	Pack Short Circuit Battery Overheating	Temperatures, FTT*, Battery Current Sensor Values
Battery Pack Short Circuit: average cell temperature above T_a (Probable Thermal Event)	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	Pack Short Circuit, Battery Overheating	Temperatures, FTT*, Battery Current Sensor Values
External Short Circuit: detected	EV, HEV,	Limit RESS	200 ms	N/A	Excessive	FTT*,

Malfunction	Application	Fault Mitigation	Estimated Fault Tolerant Time	Low Operation Strategy	DTC	Data Logging*
while cell temperature below T_{onset}	PHEV	Power Output			Current Draw	Battery Current Sensor Values
External Short Circuit: cell temperature between T_{onset} and T_a (Probable Thermal Event)	EV, HEV, PHEV	Limit RESS Power Output	200 ms	Limp Home Mode (if vehicle system remains operable)	Excessive Current Draw, Battery Overheating	Temperatures, FTT*, Battery Current Sensor Values
External Short Circuit: cell temperature above T_a (Probable Thermal Event)	EV, HEV, PHEV	Current Limiting	200 ms	Disable Vehicle	Excessive Current Draw, Battery Overheating	Temperatures, FTT*, Battery Current Sensor Values
BMS Failure: detected while cell temperature below T_{onset}	EV, HEV, PHEV	N/A	N/A	N/A	Internal to System	BMS Fault Details
BMS Failure: cell temperature between T_{onset} and T_a (Probable Thermal Event)	EV, HEV, PHEV	Limit RESS Power Output	200 ms	Limp Home Mode	Applicable BMS Fault, Battery Overheating	BMS Fault Details, Temperatures, FTT*
BMS Failure: cell temperature above T_a (Probable Thermal Event)	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	Applicable BMS Fault, Battery Overheating	BMS Fault Details, Temperatures, FTT*

*Logged FTT is the actual measured fault tolerant time required to reach the appropriate safe state.

Table I-2: Description of Safe States Related to Electric Shock

Malfunction	Application	Fault Mitigation	Estimated Fault Tolerant Time	Low Operation Strategy	DTC	Data Logging*
Crash Detection Failure: vehicle speed above 5 kph	EV, HEV, PHEV	N/A	N/A	N/A	Crash Detection Fault	Communication Signal Details
Crash Detection Failure: vehicle speed below 5 kph	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	Crash Detection Fault	Communication Signal Details, FTT*
HVIL Circuit Failure: vehicle speed above 5 kph	EV, HEV, PHEV	N/A	N/A	N/A	HVIL Fault	HVIL Fault Details
HVIL Circuit Failure: vehicle speed below 5 kph	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	HVIL Fault	HVIL Fault Details, FTT*
HVIL Circuit Intrusion	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	HVIL Intrusion Fault	HVIL Intrusion Fault Details, FTT*
PDU Fault	EV, HEV, PHEV	Request to Vehicle System Controller to Manage Propulsion Torque	200 ms	To Be Decided by Vehicle System Controller	Main Contactor Welding or Sticking	PDU Fault Details, FTT*
Ground Fault: Isolation resistance reaches minimum allowable limit	EV, HEV, PHEV	N/A	N/A	N/A	Internal to System	Ground Fault Resistance Details
Ground Fault: vehicle speed above 5 kph and isolation resistance below minimum allowable limit	EV, HEV, PHEV	N/A	N/A	N/A	Low Isolation Resistance	Ground Fault Details
Ground Fault: vehicle speed below 5 kph and isolation resistance below minimum	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	Low Isolation Resistance	Ground Fault Details, FTT*

Malfunction	Application	Fault Mitigation	Estimated Fault Tolerant Time	Low Operation Strategy	DTC	Data Logging*
allowable limit						
BMS Failure: vehicle speed above 5 kph	EV, HEV, PHEV	N/A	N/A	N/A	Applicable BMS Fault	BMS Fault Details, HV Exposure Fault Details (e.g., Crash Detection Signal, Ground Fault, HVIL)
BMS Failure: vehicle speed below 5 kph	EV, HEV, PHEV	Open Contactors	200 ms	Disable Vehicle	Applicable BMS Fault	BMS Fault Details, HV Exposure Fault Details (e.g., Crash Detection Signal, Ground Fault, HVIL), FTT*

*Logged FTT is the actual measured fault tolerant time required to reach the appropriate safe state.

Table I-3: Description of Safe States Related to Unintended Deceleration and Power Loss

Malfunction	Application	Fault Mitigation	Estimated Fault Tolerant Time	Low Operation Strategy	DTC	Data Logging*
PDU Failure: Internal Combustion Engine Available	HEV, PHEV	Transition all torque production to the Internal Combustion powertrain	200 ms	Only Internal Combustion Power provided to Powertrain [No HV RESS power]	Loss of High Voltage Power, High Voltage Power Supply Malfunction, Main Contactor Fault	PDU Fault Details, FTT*
PDU Failure: No Internal Combustion Engine Available	EV	N/A	200 ms	Disable Vehicle	Loss of High Voltage Power, High Voltage Power Supply Malfunction, Main Contactor Fault	PDU Fault Details, FTT*
Battery Pack Failure: Internal Combustion Engine Available	HEV, PHEV	Transition all torque production to the Internal Combustion powertrain	200 ms	Only Internal Combustion Power provided to Powertrain [No HV RESS power]	Loss of High Voltage Power, High Voltage Power Supply Malfunction	Battery Pack Fault Details, FTT*
Battery Pack Failure: No Internal Combustion Engine Available	EV	N/A	200 ms	Disable Vehicle	Loss of High Voltage Power, High Voltage Power Supply Malfunction	Battery Pack Fault Details, FTT*
BMS Failure: Internal Combustion Engine Available	HEV, PHEV	Transition all torque production to	200 ms	Only Internal Combustion Power	Loss of High Voltage Power, High Voltage	BMS Fault Details, FTT*

Malfunction	Application	Fault Mitigation	Estimated Fault Tolerant Time	Low Operation Strategy	DTC	Data Logging*
		the Internal Combustion powertrain		provided to Powertrain [No HV RESS power]	Power Supply Malfunction	
BMS Failure: No Internal Combustion Engine Available	EV	N/A	TBD	Disable Vehicle	Loss of High Voltage Power, High Voltage Power Supply Malfunction	BMS Fault Details, FTT*

*Logged FTT is the actual measured fault tolerant time required to reach the appropriate safe state.

Appendix J: Three-Level Monitoring

The three-level monitoring strategy is a redundant design strategy that is employed to meet requirements for components that address high ASIL (C or D) hazards. When this design approach is applied to a RESS, the BMS will include two micro controllers: a main controller and an auxiliary controller.

The main controller is the one that runs the system. It receives the inputs, runs the algorithms, makes the decisions, and sends out the output. It is also the one that communicates with the rest of the vehicle systems, and takes the vehicle to a safe state in the case of a sufficiently severe hazard.

The sole purpose of the auxiliary controller is to ensure the health and "sanity" of the main controller. It cannot run any system controls. However, it is capable of shutting down the main controller and taking the vehicle into a safe state.

The three levels of the strategy can be described as follows:

Level 1: The main controller runs its calculations or algorithms. It re-runs them again using different calculation methods or algorithms. If the two results don't match, a fault is set, and a fault mitigation strategy is enacted.

Level 2: The auxiliary controller collects the inputs independently, and runs the calculations or algorithms that the main controller ran, although it uses different methods and algorithms. The auxiliary controller then compares its results to those of the main controller. If the results don't match, a fault is set, and a fault mitigation strategy is enacted.

Level 3: This level has different names in industry: "Seed & Key," "Quizzer," "Questions & Answers," etc. It employs a set of scenarios or questions with pre-determined answers. The auxiliary controller poses these questions or scenarios to the main controller randomly. If the main controller does not respond correctly, then a fault is set, and a fault mitigation strategy is enacted.

Appendix K: Prognostic Research

The condition of a RESS can be assessed in several ways. The state of charge is a short-term measure of the available energy and can be used to estimate range under nominal conditions. Short term prognostics are measures and methods that can be used to predict short term issues and hazards, such as impending thermal runaway. Longer term measures are intended to quantify the state of health of the RESS through parameters such as the remaining useful life.

Short Term Prognostics

Industry and the U.S. Department of Energy are conducting research into assessing when a RESS is approaching operating conditions in which a vehicle-level hazard may be imminent. In general, this is accomplished via calculations in the BMS. When sensors detect conditions (e.g., cell charge, temperature, or their rates of change) that are outside of the normal range or the BMS is made aware of equipment issues (e.g., cooling system failure), the BMS will seek to mitigate the situation and/or warn the driver. By monitoring relevant quantities across the RESS, problematic cells or modules might be identified, isolated, and tagged for service before they instigate a vehicle-level hazard.

Short-term prognostics are directed at assessing anomalous short term potential hazards. That is, while nominal use will normally result in nominal behavior, anomalous behavior must be evaluated to determine whether it is indicative of an imminent hazardous situation.

Many safety mechanisms for short-term hazards are not electronically controlled or actuated. For example, shutdown separators will prevent ionic conduction within a battery cell if the internal temperature exceeds a particular limit. Thus, there are often backups and design alternatives to relying on sensors, prognostics, and control systems to recognize and mitigate imminent hazards.

Industry is pursuing research into using prognostics and health management (Holland, Barajas, Salman, & Zhang, 2010) or integrated vehicle health management (Holland, 2012) as a methodology for learning systems to monitor the RESS and understand problematic status readings in situ. IVHM might head off maintenance and safety issues through real time optimization of operating parameters. The systems are intended to meet OBD II requirements, provide customer peace of mind, reduce unnecessary maintenance (including battery replacements) and enhance SOC estimation. For example, Steve Holland of General Motors reports on a system that monitors estimated battery capacity for which no battery replacement is recommended until there is a 25 percent loss of range.

Long Term Prognostics

Long term prognostics often seek to quantify remaining useful life. More generally, they attempt to assess the RESS's ability to store and deliver charge. RUL can then be estimated as the point when those capabilities no longer meet the operating specifications for the vehicle system. The operating specifications must of course consider the full range of performance requirements and environmental conditions that a vehicle will see in service.

RUL is generally affected by normal service over the long term. It can also be affected drastically by abnormal events, such as overcharging, under charging, or charging or discharging outside of normal temperature ranges. The effects of these events are dependent on the details of the event and the chemistry of the RESS cells. At the fundamental level, the RUL is affected by

physical changes to the RESS, particularly the condition of the electrodes and the formation of structural anomalies such as metallic dendrites that might puncture the separator. Long term prognostics must directly or indirectly account for the physical changes within the cells.

Harmonic Compensated Synchronous Detection

Work at Idaho National Laboratory is seeking to quantify RUL of a RESS. Dr. Jon Christophersen at INL has been leading research into the implementation of harmonic compensated synchronous detection (Christophersen, Morrison, Morrison, & Motloch, 2012). HCSD is an approach which periodically excites a battery with a sum-of-sines current signal. The duration is at least one period of the lowest frequency signal. The variations in the voltage response can then be interpreted as a measure of the real and imaginary components of the impedance as a function of frequency. (Note: "imaginary frequencies" are a measure of natural decay characteristics.) This technique is called electrochemical impedance spectroscopy. The plot of the real and imaginary components of the impedance (the "Nyquist curve") has a distinct shape. The details of the shape are dependent on the cell chemistry. The sloping segment to the right of the local minimum is called the "Warburg tail."

The value of Nyquist curves for RESS prognostics is that they shift as the RESS ages or is otherwise degraded. An example of a Nyquist curve from the reference article shows this shift in Figure J.1. OEMs have the opportunity to determine a set of reference Nyquist curves for new, old, and degraded RESSs. Thus, a BMS that can acquire a Nyquist curve for a RESS will have a useful measure of its current condition.

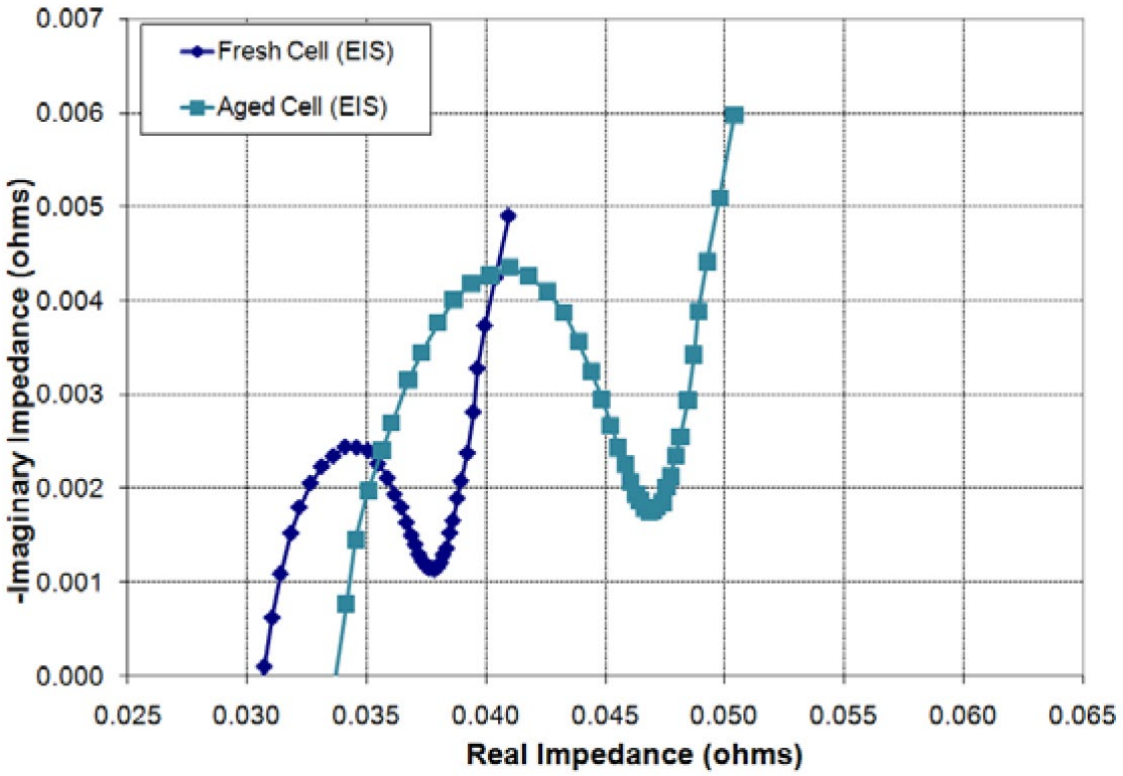


Figure K-1: EIS Nyquist curves for an aging cell (Christophersen, Morrison, Morrison, & Motloch, 2012)

It should be noted that EIS can be more difficult to perform as the system ages. Degradation mechanisms will result in lower frequency (longer period) components being needed to sufficiently define the local minimum and Warburg tail. The requirement that the excitation last at least one full period of the lowest frequency component will expand the minimum acceptable EIS excitation.

References

78 FR 24817 (Apr. 26, 2013).

California Center for Sustainable Energy [now called the Center for Sustainable Energy]. (2012). *California Plug-in Electric Vehicle Owner Survey*. San Diego: Author. Available at https://energycenter.org/sites/default/files/docs/nav/policy/research-and-reports/California%20Plug-in%20Electric%20Vehicle%20Owner%20Survey%20Report-July%202012.pdf

Christophersen, J., Morrison, J., Morrison, W., & Motloch, C. (2012). Rapid Impedance Spectrum Measurements for State-of-Health Assessment of Energy Storage Devices. Warrendale, PA: *SAE International Journal of Passenger Cars – Electronic and Electrical Systems, 5*(1). DOI:10.4271/2012-01-0657.

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

Deathrage, Bruce H. (1972). Auditory and Other Sensory Forms of Information Presentation. In H. Van Cott & R. Kinkaide (eds), *Human engineering guide to equipment design*. Washington, DC: American Institutes for Research. Retrieved from www.dtic.mil/dtic/tr/fulltext/u2/758339.pdf

Guttowski, S., Weber, S. Hoene, E., John, W., & Reichl, H. (2003, May). *EMI in Electric Vehicles*. Nuremberg, Germany: Fraunhofer Institute for Reliability and Microintegration. Available at www.stefan-peter-weber.de/publikationen/pcim03.pdf

Holland, S. W. (2012, January). *The Prognosis for Automotive IVHM*. First Indo-US Workshop on IVHM and Aviation Safety, Bangalore, India, January 9 & 10, 2012.

Holland, S. W., Barajas, L. G., Salman, M., & Zhang, Y. (2010, October). *PHM for Automotive Manufacturing and Vehicle Applications*. 2010 Annual Conference of the Prognostics and Health Management Conference, Portland Oregon, October 10-14, 2010.

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

International Electrotechnical Commission. (2006-2012). IEC 61025, second edition. Fault Tree Analysis (FTA). Geneva: Author.

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

J. D. Power (2012, November 8). *J. D. Power and Associates 2012 Electric Vehicle Ownership Experience Study*. Westlake Village, CA: Author.

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

National Highway Traffic Safety Administration, Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices, Docket NHTSA-2010-0053, February 15, 2012. Available at www.nhtsa.gov/staticfiles/rulemaking/pdf/Distraction_NPFG-02162012.pdf

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

Soden, M. (2011). *ISO 26262 for Safety-Related Automotive E/E Development – Introduction and Concept Phase*. Rome: Intecs SpA.

Sorenson, J. (2000). Hazard Warning Systems: Review of 20 Years of Progress. *Natural Hazards Review*, 119-125.

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

DOT HS 812 556
November 2018

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

13183-070518-v2c