AN14911

X-in-1 Functional safety concept (OBC, DCDC, inverter)

Rev. 1.0 — 24 April 2026 Application note

Document information

Information	Content
Keywords	Safety, OBC, DCDC, inverter, X-in-1, FSC, safety concept
Abstract	This document is intended to provide an overview of the safety concept of the project X-in-1 system which embed OBC, propulsion inverter, low voltage (LV) generation functions.

1 Introduction

This document is intended to provide an overview of the safety concept of the project X-in-1 system which embed OBC, propulsion inverter, low voltage (LV) generation functions. It helps identify scope of this X-in-1 safety concept and its abstraction to ensure process compliance to ISO26262. The document covers the assumed item definition and describes the functional safety concept (FSC).

The technical safety concept is derived and described in a separate document X-in-1 technical safety concept specification.

The system safety concept for this X-in-1 captured the intended safety strategy proposed for achieving the safety goals for those three system functions (OBC, Inverter, HV-LV DCDC). The preliminary hazard and risk analysis activity produced high level system safety requirements and system design constraints (as applicable) for the system. Using those high-level system safety requirements as a starting point, the high-level system safety concept for the system was developed.

The concept then provided direction for safety requirements for the system. The safety concept included high level strategies to achieve the safety goals. Within the framework of this high-level safety strategy, plans for achieving integrity of sensors, controllers, actuators, and communication mechanisms were described. System safety degradation concept was also considered.

1.1 Scope of the document

The safety concept for X-in-1 project is created upon overall safety management from concept phase to the product development. The scope of the X-in-1 is to focus on control strategy of the motor torque on acceleration and deceleration, the charge strategy of the HV battery and the LV (12V) generation . For the rest of the vehicle which include as well the charge of the LV battery.

This document aims to describe the system modules and functions involved to make a hybrid architecture of such X-in-1. It lists down the safety related failure modes of the X-in-1 system, and define the functional safety requirements and architecture to achieve the safety goals that those systems must adhere to.

The outputs from this document will be used to generate the technical safety requirement for the X-in-1 project and consequently design of this system, 3-in1 (OBC + Inverter+ HV-LV DCDC) . It will support as well the state of the art of those systems.

2 Item and system use case definition

2.1 Item description

The X-in-1 item is one of the domains of the electric vehicle (EV) responsible for propulsion and the management of energy during charging and driving.

The main functions of X-in-1 are based on the control strategy of the motor torque decision as well as the control strategy of the battery charging and LV generation for the rest of the vehicle.

This document seeks to explain and to provide a support for the system safety concept for the project X-in-1.

2.2 Item diagram

Figure 1 represents an overview of X-in-1 assumption of use with interaction between Electric Vehicle systems.

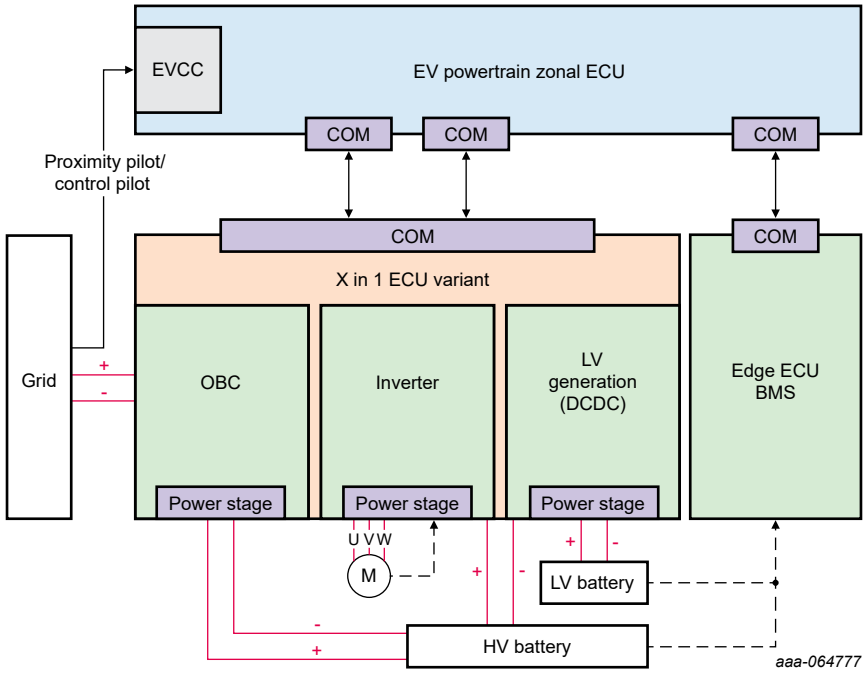

Figure 1. EV-powertrain assumption of use

2.3 Item assumptions

For this X-in-1 functional safety concept the following assumptions are consider :

- It is assumed that X-in-1 ECU communicates via CAN Bus with the rest of the vehicle through an EV powertrain zonal gateway.
- It is assumed that X-in-1 receives regenerative torque request information from Chassis domain responsible of Braking and reports braking torque feedback.
- It is assumed that X-in-1 receives propulsion torque request information and reports propulsion feedback.
- It is assumed that X-in-1 receives HV battery charging request information from battery management system and report about charging status.
- It is assumed that X-in-1 report status and failure to the rest of vehicle through the Zonal gateway.

- It is assumed that the X-in-1 Item is composed of E-Motor (3 phases), HV battery lithium nickel cobalt aluminum (NCA) oxide, LV battery (lead-acid), charging plug to connect it to an external charger and X-in-1 domain controller.
- It is assumed that the X-in-1 domain controller is a smart edge power box limited to control the regulation for the motor propulsion, HV battery charging, and LV generation.
- It is assume that the HV battery is composed by 96 cells modules of 36 V in series for 360 V nominal charge up to 400 V full charge.
- It is assume that the LV battery is a state of the art 14V lead-acid battery 14.3V nominal charge up to 15.4 V full charge.
- It is assumed that the HV contactors are managed by the BMS system not by X-in-1.
- It is assumed that the Grid connection is manage by the EVCC system not by X-in-1.
- It is assumed that the high compute torque strategy processing is done by the Zonal powertrain ECU.
- It is assumed that the charging strategy processing is done by the Zonal powertrain ECU.

2.4 Item operating states

The scope of our safety analysis is limited to operation mode, the non-operation like maintenance are not considered into the scope of this FSC analysis. We assume the following three main operating modes of the vehicle for our analysis:

- **Driving mode :** The vehicle is inside the car, and the X-in-1 domain manages the torque of the vehicle according to the driver and the chassis request.
- **Charging mode:** The user plugs the vehicle to a charging station, and the X-in-1 manages the charge of the vehicle.
- **Parked:** The vehicle is not charging nor driving (standby).
- **Non operational:** The HV battery and LV battery are disconnected, the vehicle is in maintenance or in long parking storage.

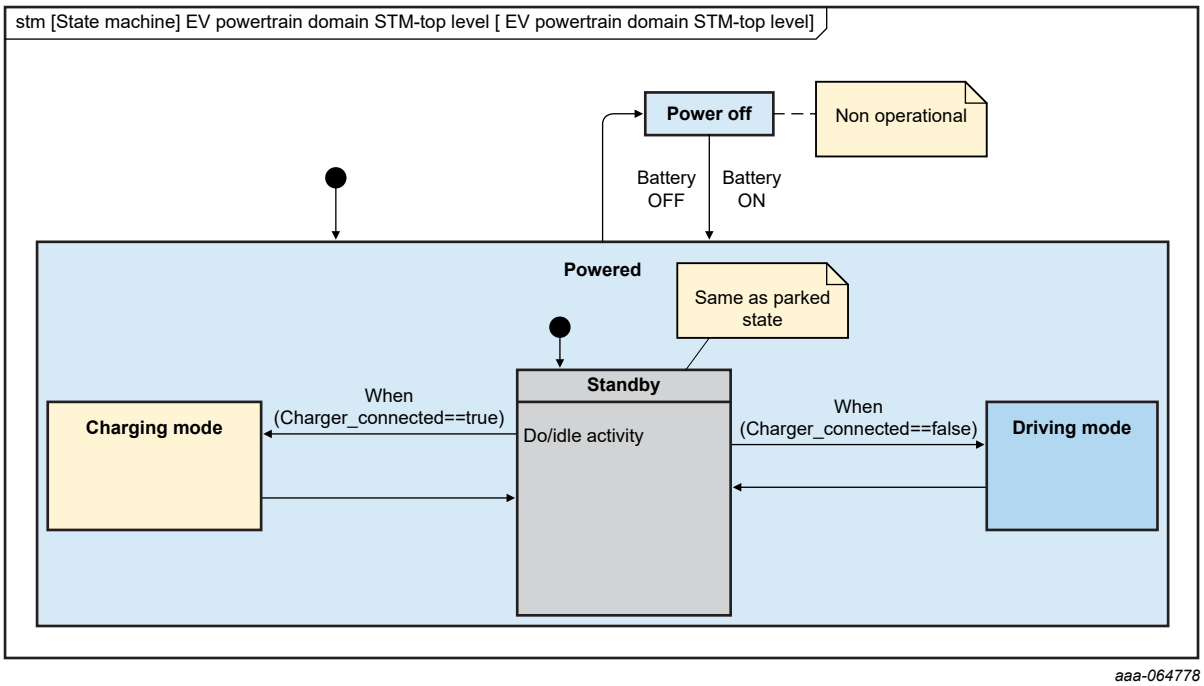

Figure 2. X-in-1 top level state machine

2.5 X-in-1 system use case diagram

Figure 3 gives an overview of X-in-1 ECU controller main functions and its interaction with the entire vehicle systems.

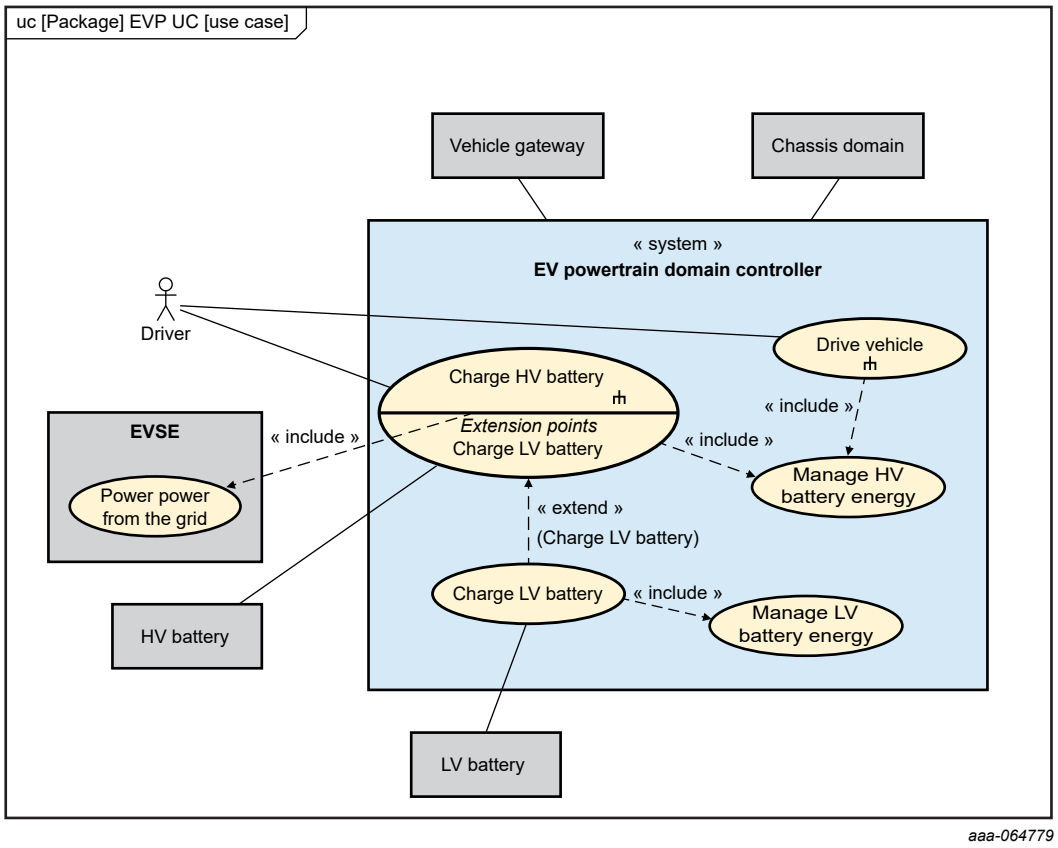

Figure 3. X- in -1 controller use case diagram

2.6 X-in-1 system functional architecture

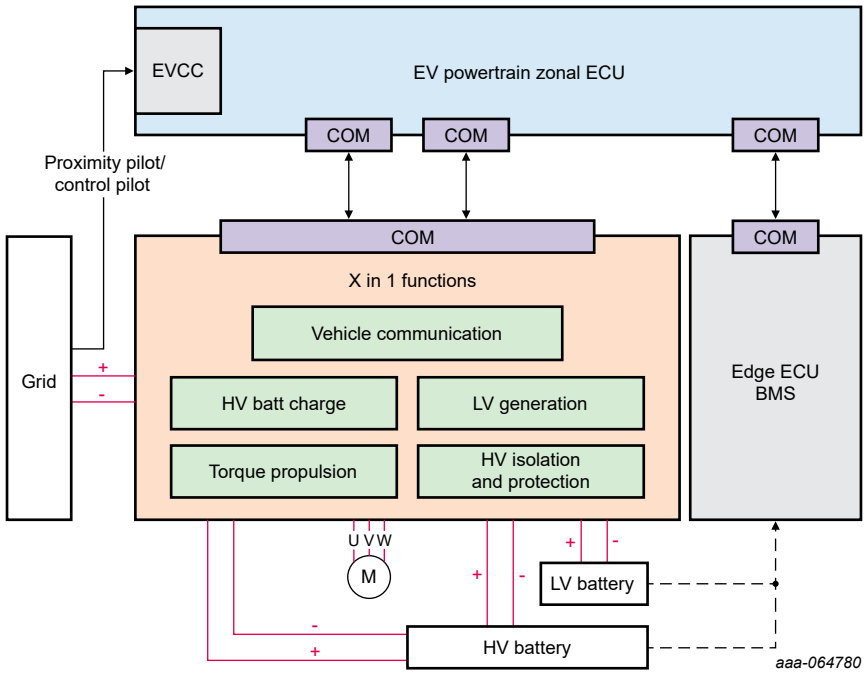

Figure 4. X-in-1 system functional architecture diagram

Table 1. X-in-1 controller main functions

ID	Functions
F1	HV battery charging from grid
F2	LV generation and LV battery charging
F3	Pre-charge HV DC link
F4	EV propulsion motor drive
F5	HV battery regenerative charge from e.motor
F6	Communicate with the rest of the vehicle
F7	Isolate and protect human from HV domain

3 X-in-1 functional safety concept

3.1 Hazard events

The purpose of the hazard analysis and risk assessment is to identify and categorize the hazards based on estimating three factors Severity (S), Exposure (E) and Controllability (C) also to formulate the safety goals to prevent or mitigate these hazards.

Table 2. ASIL determination

Severity S	Exposure E	Controllability C		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Table 3. Hazardous events assumptions

ID	Hazardous event	ASIL	Effect on vehicle	Operating state
HE01	Insufficient propulsion torque	A	The vehicle will be controlled by braking and taking appropriate action.	**Driving**
HE02	Excessive propulsion torque	B	May lead to serious collision from the opposite vehicle.	**Driving**
HE03	Unintended sudden loss of propulsion torque at high speed	B	May lead to high braking torque and create skidding or destabilizing the vehicle.	**Driving**
HE04	Unexpected propulsion torque when in stop	D	Sudden acceleration may result in a pedestrian crash at a stop.	**Driving**
HE05	Unexpected regenerative braking torque	D	The vehicle will be out of control and this will lead into a serious accident with obstacles/other vehicles.	**Driving**
HE06	Unintended e.motor lock	D	Almost impossible to get back the control the vehicle at very high speed if it went out of control.	**Driving**

Table 4. Drive hazardous events Summary

ID	Hazardous event	ASIL	Effect on vehicle	Operating state
HE07	OBC or HV battery damaged by overvoltage	B	No controllable in the worst case - significant smoke or flames.	**Charging**
HE08	OBC or HV battery damaged by overcurrent	B	No controllable in the worst case - significant smoke or flames.	**Charging**
HE09	OBC damaged by overtemperature (fire and smoke)	B	No controllable in the worst case - significant smoke or flames.	**Charging**
HE10	Battery pack not charged	QM	Controllability in this situation is extremely difficult, due to over discharge under safe range.	**Charging**

Table 5. LV generation (HV-LV DCDC) hazardous events summary

ID	Hazardous event	ASIL	Effect on vehicle	Operating state
HE11	Unintended sudden loss of LV DC energy (due to SC)	C	This situation cannot be controlled by the majority of the people involved, as they may not be alert to the event.	**Charging driving**
HE12	Unintended sudden loss of LV DC energy (DCDC output UV)	B	The people involved may be alert to the event but cannot well control the vehicle if some safety system start to fail at same time.	**Charging driving**
HE13	Overvoltage on the LV DC bus	C	Loss of vehicle safety functions due to ECU overvoltage damage. Difficult to control and achieve safe state.	**Charging driving**
HE14	Fire and smoke (OT, OC of the system)	B	Start fire cannot be stop by users.	**Charging driving**

Table 6. Isolation and communication hazardous events summary

ID	Hazardous event	ASIL	Effect on vehicle	Operating state
HE15	Human electrocution by OBC plug or chassis while in charge or in parking. (AC or HV DC leakage)	B	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	**Charging parking**
HE16	Human electrocution by HV DC leakage while in driving	B	This situation is normally controllable with external measures (fire alarms), as people will be alerted to the event.	**Driving**
HE17	Human electrocution while in maintenance or crash.	A	This situation is normally controllable with external measures	**Parking driving**
HE18	Communication bus is lock by the system damaged by overvoltage	B	Loss of vehicle safety functions due to ECU overvoltage damage which block the rest of vehicule CAN or ethernet BUS. Difficult to control and achieve safe state.	**Driving charging parking**

3.2 Safety goals assumptions

The following safety goals are assumed for the X-in-1 of (OBC, PIM, HV-LV DCDC) based on Section 3.1 and customer and original equipment manufacturer documentations:

Table 7. Safety goals of X-in-1

		Safety goals	ASIL	FTTI
Propulsion E. Motor	SG01	Prevent insufficient propulsion torque	A	200ms
	SG02	Prevent excessive propulsion torque	B	200ms
	SG03	Prevent unintended sudden loss of propulsion torque	B	200ms
	SG04	Prevent unexpected propulsion torque when in stop	D	200ms
	SG05	Prevent unexpected regenerative braking torque	D	200ms
	SG06	Prevent unintended E.Motor lock	D	200ms
Energy management	SG07	Prevent OBC damaged by overvoltage	B	200ms
	SG08	Prevent OBC damaged by overcurrent	B	200ms
	SG09	Prevent OBC damage by overtemperature	B	30s
	SG010	Prevent unintended loss of LV DC energy (due to SC)	C	200ms
	SG011	Prevent unintended OV (>17V) of LV DC output	C	200ms
	SG012	Prevent unintended UV (<9V) of LV DC energy	B	200ms
	SG013	Prevent DCDC damage by overtemperature (OT, OC)	B	30s
Insulation	SG014	Prevent human electrocution (HV DC) while in drive	B	5000ms
	SG015	Prevent human electrocution (by AC line or HV DC) while in charge or parked	B	5000ms
	SG016	Prevent human electrocution while in maintenance or crash	A	5000ms
COM	SG017	Insure safety communication (warning) to other ECU/system (availability SG)	B	1s
	SG018	Prevent inter-system safety data communication corruption	Up to D	200ms

3.3 Safety Concept functions for X-in-1

According to Section 3.1 and Section 3.2 assumed for the X-in-1 item use case, the following safety concept shall be developed, addressing the above safety goals and deriving functional safety requirements and architectures to mitigate the hazard risk.

Table 8. Functional safety concept of X-in-1

ID	Main functional safety concept	ASIL level
FSC1	Insure Integrity of e.motor drive	ASIL D
FSC2	Insure Integrity of HV battery charging	ASIL B
FSC3	Insure integrity and availability of LV generation (see note below)	ASIL C
FSC4	Insure HV protection against electrocution	ASIL B
FSC5	Insure integrity and availability of communication	ASIL B

Note: *In this X in 1 concept the availability goal is not to maintain LV generation by DCDC redundancy but to do a fault containement of a DCDC critical failure which can lead to a loss of LV energy in the vehicle. The availability concept is derived from the SG 10 in Table 7.*

3.4 Functional safe states definition

The safe states are defined as a state of the vehicle after acting to remove the hazard resulting in no significant harm. Mainly it is when the vehicle is stopped with each system failure mitigated by a succession of system safety reactions (SSR) which we could call system safe state (SS).

In order of priority, the system safe states can be classified in three categories:

- **Fail-operational**: (Still providing the functionality to nominal)
- **Degraded modes**: (Functionality with limitations)
  - Limp-home: (functionality with minimal performance and time until next ignition off)
  - Limp-aside: (functionality with limited time of some minutes, permitting to park on the side of the road)
  - Ramp down: (shut-down in some seconds)
- **Shut-down**: (zero torque, or zero charge current almost sudden, it shall be avoided or limited to very few cases of failures in motor control and charge control)

For the X-in-1, the goal is to achieve fail operational for failure in communication to external system. Availability of system communication is crucial for maintaining informed the central vehicle system and the driver in order to achieving safe state of the vehicle with minimum of risk.

Degraded mode is required as much as possible while driving in order to maintain propulsion for a certain time to be able to park the car in a safe location and not stopping in the middle of a road. After the degraded mode, when the car is parked, the system shall achieve the safe state.

The target of X-in-1 is to achieve as much as possible degraded modes for a reaction after a fault in the Inverter or LV generation architecture.

3.4.1 Functional Safe State of X-in-1

Following the main FSC defined for X-in-1, the below main safe state are defined for each application function handle by the X-in-1 ECU.

Table 9. FSC safe state of X-in-1

ID	Main functional safety concept	Main safe sates
FSC1	Insure integrity of e.motor drive	Send warning and stop providing torque to the e.motor **[SS_ APPLY _ZERO_TORQUE]**
FSC2	Insure integrity of HV battery charging	Send warning and stop current flow to the HV battery **[SS_STOP_CHARGE_HV_BAT]**
FSC3	Insure integrity and availability of LV generation	Send warning and stop current flow to the LV battery **[SS_STOP_LV_GENERATION]**
FSC4	Insure HV protection against electrocution	Send warning and discharge any residual HV potential **[SS_DISCHARGE_HV_BUS]**
FSC5	Insure integrity and availability of communication	Send warning and maintain communication with redundant path **[SS_CAN_DEGRADED]**

Depending on the functional state mode (driving or charging) and on the failure criticality, a succession of safety reactions under responsibility of X-in-1 ECU, are defined in addition to the above safe state in order to achieve a vehicle system safe-state.

3.4.2 Functional safety reaction in Driving mode

During Driving mode, a failure of one of these systems HV/LV battery, LV generation and e.motor drive could result in hazard. Therefore safety measures will be implemented to mitigate/avoid the risk of the failed one.

3.4.2.1 Communication failure

Table 10 lists the generic FSR reaction in case of CAN communication failure.

Table 10. Communication failure

ID	Description	ASIL
FSR001	In case of the communication failure with Zonal powertrain ECU, X-in-1 shall apply **SS1**: • Send warning request to driver **[SS_WARN_CAN_COM]** • Maintain communication by redundant CAN path **[SS_CAN_DEGRADED]**	B

3.4.2.2 HV isolation failure

The safe state, the degraded mode and the safety timing will be different from one fault to another as described in the following figures:

Table 11 lists the generic FSR reaction in case of HV isolation failure.

- It is assumed that HV isolation failure will be detected by BMS and notify from the zonal powertrain ECU to the X-in-1 in order it can take safety reaction accordingly.
- It is assumed that the BMS will disconnect HV from the X-in-1 in case of HV Isolation failure.

Table 11. HV isolation failure

ID	Description	ASIL
FSR002	In case of the HV isolation failure notify by Zonal powertrain ECU, X-in-1 shall apply **SS2**: • Send warning request for load shedding on LV BUS **[SS_ LOAD SHEDDING]** • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Stop LV generation **[SS_STOP_LV_GENERATION]** • Disconnect LV generation from LV battery **[SS_DISCONNECT_LV BAT]** • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]** • Insure 0 torque apply to the e.motor **[SS_ APPLY _ZERO_TORQUE]** • Wait warning message HV contactor are open **[SS_DISCONNECT_HV_BATTERY]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	B

3.4.2.3 HV battery failure

Table 12 lists the generic FSR reaction in case of HV battery failure in charging mode.

- It is assumed that HV battery failure will be detected by BMS and notify from the zonal powertrain ECU to the X-in-1 in order it can take safety reaction accordingly.
- It is assumed that the BMS will disconnect HV from the X-in-1 in case of HV battery failure.

Table 12. HV battery failure

ID	Description	ASIL
FSR003	In case of the HV battery failure notify by Zonal powertrain ECU, X-in-1 shall apply **SS3**: • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]** • Insure 0 torque apply to the e.motor **[SS_ APPLY _ZERO_TORQUE]** • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Stop LV generation **[SS_STOP_LV_GENERATION]**	B

Table 12. HV battery failure

ID	Description	ASIL
	• Disconnect LV generation from LV battery **[SS_DISCONNECT_LV BAT]** • Wait warning message HV contactor are open **[SS_DISCONNECT_HV_BATTERY]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	

3.4.2.4 E.motor drive failure

Table 13 lists the FSR for safety reaction in case of EV propulsion function failure.

Table 13. E.motor drive failure

ID	Description	ASIL
FSR004	In case of the sudden loss of propulsion, X-in-1 shall apply **SS4**: • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]** • Insure 0 torque apply to the e.motor **[SS_ APPLY _ZERO_TORQUE]** • Wait warning message HV contactor are open **[SS_DISCONNECT_HV_BATTERY]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	D
FSR005	In case of the unintended acceleration or braking, X-in-1 shall apply **SS4**: • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]** • Insure 0 torque apply to the e.motor **[SS_ APPLY _ZERO_TORQUE]** • Wait warning message HV contactor are open **[SS_DISCONNECT_HV_BATTERY]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	D
FSR006	In case of the over/under acceleration or braking, X-in-1 shall apply **SS5**: • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]** • Ramp down of torque and speed of the e.motor : **[SS_TORQUE & SPEED_RAMP_DOWN]** • Wait warning message HV contactor are open **[SS_DISCONNECT_HV_BATTERY]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	D

3.4.2.5 LV battery failure

Table 14 lists the generic FSR reaction in case of LV battery failure.

- It is assumed that LV battery failure will be detected by BMS and notify from the zonal powertrain ECU to the X-in-1 in order it can take safety reaction accordingly.

Table 14. LV battery failure

ID	Description	ASIL
FSR007	In case of the LV battery failure notify by Zonal powertrain ECU, X-in-1 shall apply **SS6**: • Send warning request for load shedding on LV BUS **[SS_ LOAD SHEDDING]** • Apply e.motor torque and speed limitation : **[SS_LIMIT_TORQUE & SPEED]** • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]**	C

3.4.2.6 LV generation failure

Table 15 lists the generic FSR reaction in case of LV generation function failure.

- It is assumed that zonal powertrain ECU will send warning to the driver dashboard to require vehicle stop for final safe state reaction in case of LV generation failure notification from X-in-1 ECU.

Table 15. LV generation failure

ID	Description	ASIL
FSR008	In case of the LV generation critical failure (leading to loss of LV domain), X-in-1 shall apply **SS7**: • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Stop LV generation **[SS_STOP_LV_GENERATION]** • Disconnect LV generation from LV battery **[SS_DISCONNECT_LV BAT]** • Send warning request for load shedding on LV BUS **[SS_LOAD SHEDDING]** • Apply E.motor torque and speed limitation : **[SS_LIMIT_TORQUE & SPEED]** • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]**	C
FSR009	In case of the LV generation failure (leading to lower energy provided), X-in-1 shall apply **SS8**: • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Apply LV generation output limitation **[SS_LV_GENERATION_DEGRADED]** • Send warning request for load shedding on LV BUS **[SS_LOAD SHEDDING]** • Apply E.motor torque and speed limitation : **[SS_LIMIT_TORQUE & SPEED]** • Send warning request to driver **[SS_WARN_E_MOTOR_DRIVER]**	C

3.4.3 Functional safety reaction in Charging mode

During Charging mode, a failure in HV/LV battery, HV battery charging and LV generation could result in hazard. Therefore safety measures will be implemented to mitigate/avoid the risk of the failed one.

3.4.3.1 HV battery failure

The safe-state, the degraded mode and the safety timing are described in the following figure. Table 16 shows the generic FSR reaction in case of HV battery failure in charging mode.

- It is assumed that HV battery failure will be detected by BMS and notify from the zonal powertrain ECU to the X-in-1 in order it can take safety reaction accordingly.
- It is assumed that the BMS will disconnect HV from the X-in-1 in case of HV battery failure.

Table 16. HV battery failure

ID	Description	ASIL
FSR010	In case of the HV battery failure notify by Zonal powertrain ECU, X-in-1 shall apply **SS9**: • Send warning request to driver **[SS_WARN_HV_CHARGER]** • Stop HV charge **[SS_STOP_CHARGE_HV_BAT]** • Disconnect X-in-1 from Grid **[SS_DISCONNECT_GRID]** • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Stop LV generation **[SS_STOP_LV_GENERATION]** • Disconnect LV generation from LV battery **[SS_DISCONNECT_LV BAT]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	B

3.4.3.2 HV battery charging failure

Table 17 lists the generic FSR reaction in case of HV battery failure in Charging mode.

- It is assumed that the BMS will disconnect HV from the X-in-1 in case of HV battery charging failure is reported from the X-in-1 ECU.

Table 17. HV battery charging failure

ID	Description	ASIL
FSR011	In case of the HV battery charging failure, X-in-1 shall apply **SS9**: • Send warning request to driver **[SS_WARN_HV_CHARGER]**	B

Table 17. HV battery charging failure

ID	Description	ASIL
	• Stop HV charge **[SS_STOP_CHARGE_HV_BAT]** • Disconnect X-in-1 from Grid **[SS_DISCONNECT_GRID]** • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Stop LV generation **[SS_STOP_LV_GENERATION]** • Disconnect LV generation from LV battery **[SS_DISCONNECT_LV BAT]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	

3.4.3.3 LV battery or LV generation failure

Table 18 lists the generic FSR reaction in case of LV battery failure.

- It is assumed that LV battery failure will be detected by BMS and notify from the zonal powertrain ECU to the X-in-1 in order it can take safety reaction accordingly.

Table 18. LV battery or LV generation failure

ID	Description	ASIL
FSR012	In case of the LV generation or LV battery failure , X-in-1 shall apply **SS10**: • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Stop LV generation **[SS_STOP_LV_GENERATION]** • Disconnect LV generation from LV battery **[SS_DISCONNECT_LV BAT]** • Send warning request to driver **[SS_WARN_HV_CHARGER]** • Stop HV charge **[SS_STOP_CHARGE_HV_BAT]** • Disconnect X-in-1 from Grid **[SS_DISCONNECT_GRID]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	B

3.4.3.4 HV isolation failure

Table 19 lists the generic FSR reaction in case of HV isolation failure.

- It is assumed that HV isolation failure will be detected by BMS and notify from the zonal powertrain ECU to the X-in-1 in order it can take safety reaction accordingly.
- It is assumed that the BMS will disconnect HV from the X-in-1 in case of HV isolation failure.

Table 19. HV Isolation failure

ID	Description	ASIL
FSR013	In case of the HV isolation failure notify by Zonal powertrain ECU, X-in-1 shall apply **SS11**: • Send warning request for load shedding on LV BUS **[SS_ LOAD SHEDDING]** • Send warning request to driver **[SS_WARN_LV_GENERATION]** • Stop LV generation **[SS_STOP_LV_GENERATION]** • Disconnect LV generation from LV battery **[SS_DISCONNECT_LV BAT]** • Wait warning message HV contactor are open **[SS_DISCONNECT_HV_BATTERY]** • Discharge HV DC link **[SS_HV_DISCHARGE]**	B

3.5 Functional safety state machine

A safety system life cycle is modeled by the state machine bellow. The state machine of X-in-1 is decomposed into two main states :

- Power OFF
- POWERED that includes Charging mode, Standby, Driving mode

The operating Charging and Driving mode are decomposed into sub-states which describe a specific behavior of X-in-1 at a given change . In case of failure, the safe state of charging / driving will be reached to prevent any occurrence of physical injury or damage to the health of persons.

- It is assumed that the Zonal Powertrain ECU is waking up the X in 1 when needed.
- It is assumed that the status “Charger connected (true/false)” is received from the Zonal powertrain ECU.
- It is assumed that the status “Ignition ON/OFF” is received by the Zonal owertrain ECU.

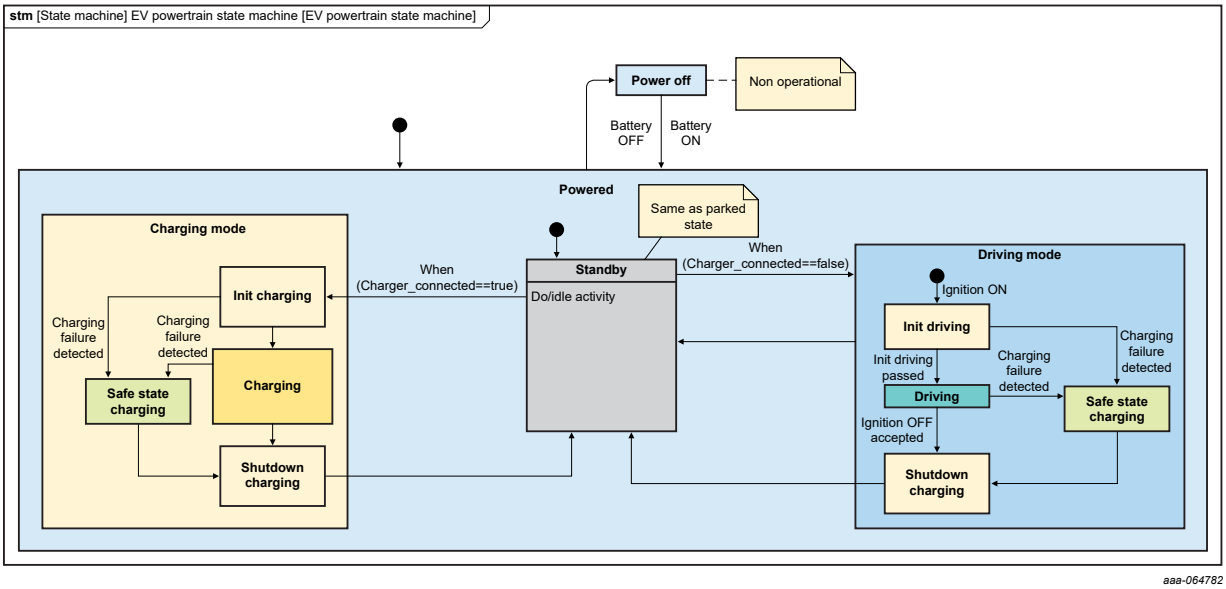

Figure 5. X-in-1 state machine

Table 20. Description of operational states

System state	Description
Power OFF	The vehicle is in non-operational state; There is no power from the LV battery
Charger connected	The charger has been plugged inby the user; The vehicle enters the charging state
Init charging	Charging Initialization - The integrated OBC module starts all the internal power supplies and runs all the start-up tests
Charging	The internal components of charging function are ready; And the charge-module is charging the HV battery
Charging safe-state	Charging functions doesn’t charge the HV battery i.e. no current flow to the batteries after the system has incurred a critical failure
Shutdown charging	Charging of HV batteries complete
Charger disconnected	The charger has been plugged out by the user; Only after that the ignition is possible and the vehicle can enter the driving mode; Drive function is waiting for the ignition signal i.e. Ignition-ON
Init driving	Driving initialization – The integrated OBC module starts all the internal power supplies and runs all the start-up tests
Driving	All the start-up tests are successful; Drive system is ready to provide torque to motor on request.
Degraded mode	Fault detected in the Drive module; Limit the torque to motor; (thereby by limiting max speed of the car) Vehicle can move aside/Vehicle to next service station

Table 20. Description of operational states*...continued*

System state	Description
Driving safe-state	Critical fault detected in the Drive module and no torque is applied to the motor
Shutdown driving	Vehicle is at standstill

The standard way to comeback from a safe state for the charging functionality is to unplug the charger and restart the system.

The standard way to comeback from a safe state for the drive functionality is to restart the system.

3.6 Functional safety concept for the 3-in-1 use case (OBC, DCDC, PIM)

The FSC for the X-in-1 must implement several safety measure and safety mechanism, to detect and control each failure mode of all system functions.

The safety concept shall implement a safety manager function which will insure in case of failure, to bring the system into safe state to avoid violation of any safety goal which could lead to a critical hazard.

3.6.1 FSC1 - Insure integrity of e.motor propulsion concept

Insure safe e.motor propulsion mean that the torque apply to the motor shall be the same as the torque requested by the driver, any deviation between torque command and torque apply to the motor shall be detected and appropriate safety reaction shall be taken.

The principal functions in Driving mode for e.motor drive are:

- The X-in-1 shall provide internal supplies DC voltage using the HV and LV battery inputs.
- The X-in-1 shall compute and provide torque propulsion according to Zonal ECU torque request.
- The X-in-1 shall convert HV DC energy into e.motor torque.
- The X-in-1 shall sense e.motor state.
- The X-in-1 shall charge HV battery from regenerative braking.
- The X-in-1 shall communicate with Zonal ECU to receive torque request and transmit status.

3.6.1.1 Functional safety architecture of e.motor propulsion

Figure 6 represents the functional safety architecture block of e.motor propulsion and regenerative braking during Driving mode.

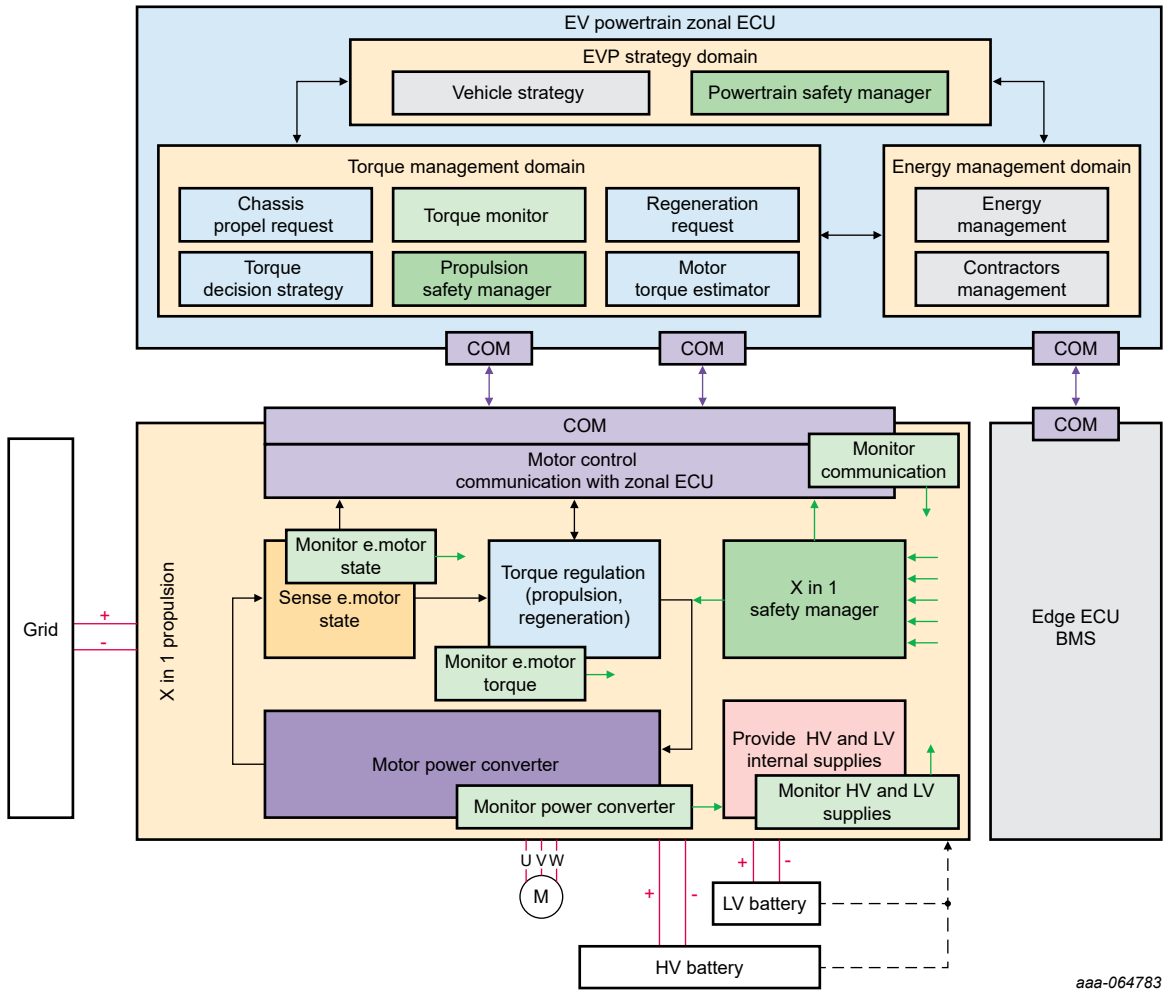

Figure 6. Functional safety architecture of e.motor propulsion concept

3.6.1.2 Driving and regenerative braking assumptions

The regenerative breaking offers a great advantage in conserving energy by charging the HV battery which gives the ability to increase the driving range. However, the mechanical braking system takes over in the event of a regenerative braking failure.

In EV system, there is an algorithm that measure the pedal sensor and calculate the amount of the braking that needs to be done from regenerative braking and mechanical braking, this algorithm could be part of an energy optimization strategy in Zonal powertrain ECU.

The X-in-1 are some assumptions that are taken into account during Driving mode:

- It is assumed that the Zonal ECU ensure that the charger is disconnected from the vehicle before sending driving mode activation request.
- It is assumed that the Zonal ECU ensure the ignition signal from chassis has been received before sending driving mode activation request.
- It is assumed that the Zonal ECU periodically send to X-in-1 the requested propulsion torque base on propel information, energy optimization, regeneration, and torque limiter functions.

3.6.1.3 FSR allocated to e.motor propulsion

Table 21. FSR allocated to e.motor propulsion 100-103

FR	Provide internal supplies DC voltage using the HV and LV battery inputs	ASIL
FSR100	X-in-1 shall monitor and detect failure of internal HV power supply.	D
FSR101	In case of HV power supply failure is detected the X-in-1 shall apply zero torque to the motor following **SS4 or SS5** reactions	D
FSR102	X-in-1 shall monitor and detect failure of the LV internal power supplies.	D
FSR103	In case of LV internal power supplies failure is detected the X-in-1 shall apply zero torque to the motor following **SS4 or SS5** reactions	D

Table 22. FSR allocated to e.motor propulsion 104-106

FR	Compute and provide torque propulsion according to Zonal ECU torque request.	ASIL
FSR104	X-in-1 shall monitor and detect failure of torque applied to the e.motor	D
FSR105	X-in-1 shall compare the torque applied to the e.motor with the torque requested from the Zonal ECU in order to detect mismatch failure.	D
FSR106	In case of e.motor torque failure is detected the X-in-1 shall apply zero torque to the motor following **SS4 or SS5** reactions	D

Table 23. FSR allocated to e.motor propulsion 107-108

FR	Convert HV DC energy into e.motor torque	ASIL
FSR107	X-in-1 shall monitor DC / AC converter to detect torque conversion failure.	D
FSR108	In case of e.motor torque conversion failure is detected the X-in-1 shall apply zero torque to the motor following **SS4 or SS5** reactions	D

Table 24. FSR allocated to e.motor propulsion 109-110

FR	Sense e.motor state (current , position , temperature)	ASIL
FSR109	X-in-1 shall monitor and detect the e.motor state failure (3 phase currents ,position or temperature).	D
FSR110	In case of e.motor state failure is detected the X-in-1 shall apply zero torque to the motor following **SS4 or SS5** reactions	D

Table 25. FSR allocated to e.motor propulsion 111-113

FR	Charge HV battery from regenerative braking	ASIL
FSR111	X-in-1 shall monitor and detect failure of regenerative braking torque from the e.motor.	D
FSR112	X-in-1 shall compare the regenerative braking torque with the braking torque requested from the Zonal ECU in order to detect mismatch failure.	D
FSR113	In case of e.motor regenerative braking torque failure is detected the X-in-1 shall apply zero torque to the motor following **SS4 or SS5** reactions	D

Table 26. FSR allocated to e.motor propulsion 114-115

FR	Communicate with Zonal ECU to receive torque request and transmit status	ASIL
FSR114	X-in-1 shall detect failure of the torque request received from Zonal ECU.	D
FSR115	X-in-1 shall protect the regenerative torque feedback send to Zonal ECU.	D

Table 27. FSR allocated to e.motor propulsion 117-116

FR	Communicate with Zonal ECU to receive torque request and transmit status	ASIL
FSR116	In case of Torque communication failure is detected the X-in-1 shall use the redundant communication pass following **SS1** reactions.	D
FSR117	In case the second communication path still reporting failure on charging request, the X-in-1 shall apply zero torque to the motor following **SS4 or SS5** reactions.	D

3.6.2 FSC2 - Insure integrity of HV battery charging concept

The principal functions in this mode are:

- The X-in-1 shall acquire AC energy from the grid.
- The X-in-1 shall provide DC energy to the HV battery according to Zonal ECU request.
- The X-in-1 shall convert AC energy to DC energy to charge the HV battery.
- The X-in-1 shall communicate with Zonal ECU to receive charge request and transmit status.

3.6.2.1 Functional safety architecture of OBC

Figure 7 represents the functional safety architecture block of On-board charging HV battery during Parking mode .

A safety manager presented in this figure aims to gather, report fault and to react with all the activities necessary to achieve a safe state to prevent a risk due to hazard in case of malfunctioning behavior while charging the HV battery.

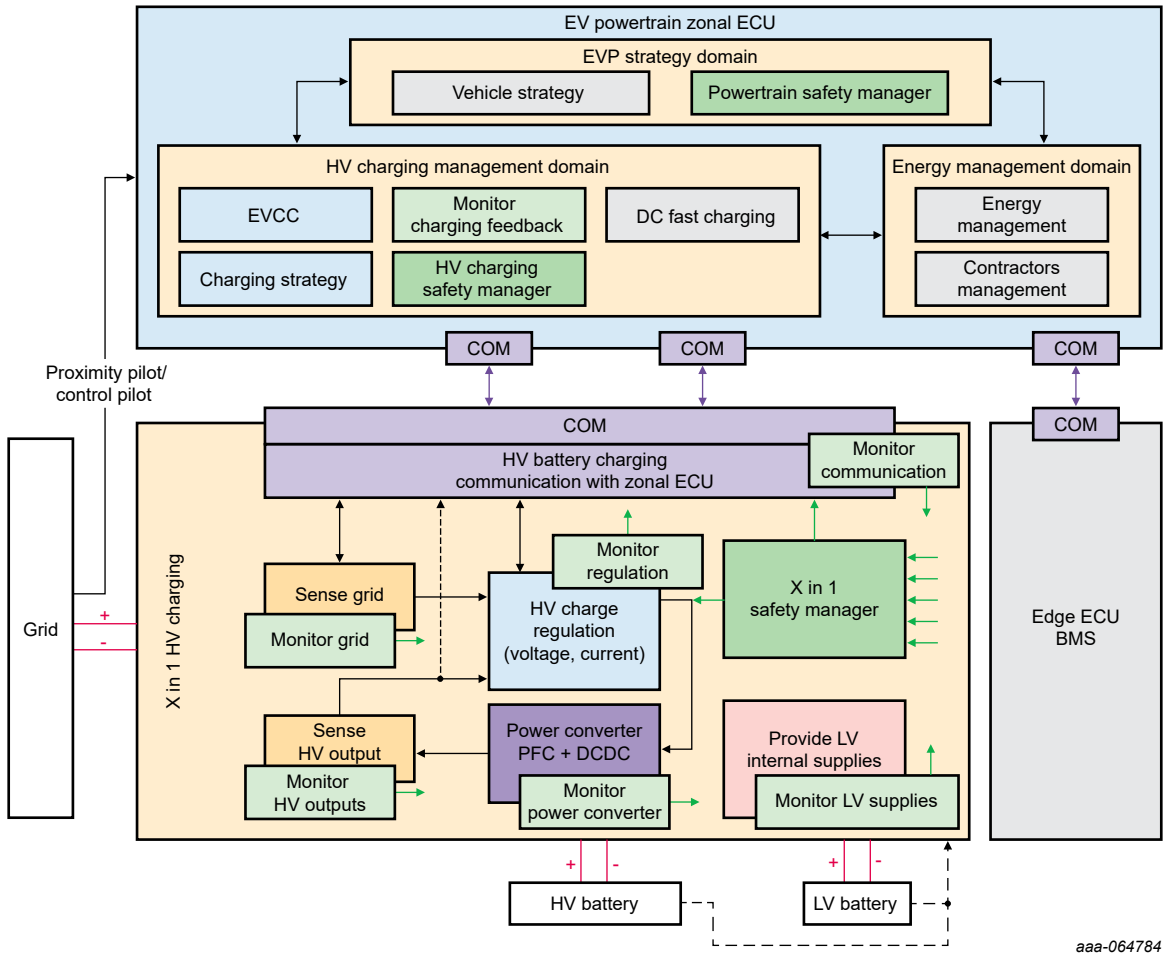

Figure 7. Functional safety architecture of On-board HV battery charging concept

3.6.2.2 HV Battery charge assumptions

- It is assumed that the Zonal ECU ensure that vehicle is in ‘parked’ state before charging request.
- It is assumed that the Zonal ECU disengage the motor while charging.
- It is assumed that the Zonal ECU ensure correct and locked connection to the grid (to protect user from the HV potential).
- It is assumed that the Zonal ECU is in charge of connecting and disconnecting the HV battery to the X-in-1 ECU base on vehicle state or safety issue.
- It is assumed that the Zonal ECU is informed by BMS about SoC and SoH of the HV battery thus it provides to X in1 correct charging voltage and current target.
- It is assumed that the X-in-1 is a three phase unidirectional isolated OBC for a single 400 V battery.
- It is assumed that the fast DC charging mode is not handle by the X-in-1 ECU.
- It is assumed that the EVCC function is handled by the Zonal ECU which provide charging request to the X-in-1 ECU.

3.6.2.3 FSR allocated to HV battery charge function

Table 28. FSR allocated to HV battery charge function FSR200-FSR201

FR	Acquire AC energy from Grid	ASIL
FSR200	X-in-1 shall monitor and detect overvoltage and overcurrent failures of the 3 grid input phases of the OBC Converter	B
FSR201	In case of OBC inputs voltage/current failure is detected, the X-in-1 shall stop the charge of HV battery following **SS9** reactions	B

Table 29. FSR allocated to HV battery charge function FSR202-FSR204

FR	Provide DC energy to charge HV battery	ASIL
FSR202	X-in-1 shall monitor and detect overvoltage and overcurrent failures of the OBC HV outputs to HV battery.	B
FSR203	X-in-1 shall compare the OBC output current and voltage with the voltage and current target received from Zonal ECU.	B
FSR204	In case of OBC HV outputs voltage/current failure is detected, the X-in-1 shall stop the charge of HV battery following **SS9** reactions	B

Table 30. FSR allocated to HV battery charge function FSR205-FSR207

FR	Convert AC power to DC power to charge the HV battery	ASIL
FSR205	X-in-1 shall monitor AC / DC converter to detect power conversion failure (short).	B
FSR206	X-in-1 shall monitor and detect overtemperature failures of the AC / DC converter	B
FSR207	In case of OBC converter (short or temperature) failure is detected, the X-in-1 shall stop the charge of HV battery following **SS9** reactions.	B

Table 31. FSR allocated to HV battery charge function FSR208-FSR212

FR	Communicate with Zonal ECU to charge request and transmit status	ASIL
FSR208	X-in-1 shall detect failure of the target voltage and current request received from Zonal ECU.	B
FSR209	X-in-1 shall protect the OBC output voltage and current feedback send to Zonal ECU.	B
FSR210	X-in-1 shall monitor and detect failure of the charge request status received from Zonal ECU.	B
FSR211	In case of OBC charge target or request failure is detected the X-in-1 shall use the redundant communication pass following **SS1** reactions and continue operation.	B
FSR212	In case the second communication path still reporting failure on charging request, the X-in-1 shall stop the charge of HV battery following **SS9** reactions.	B

3.6.3 FSC3 – Insure integrity and availability of LV generation concept

The principal functions in this mode are:

- The X-in-1 shall acquire DC energy from the HV battery.
- The X-in-1 shall convert HV DC energy to LV DC energy to charge LV battery
- The X-in-1 shall provide LV energy to the LV network of the vehicle.
- The X-in-1 shall convert LV DC energy to HV DC energy to precharge DC link.

- The X-in-1 shall provide HV energy (reverse mode) for DC link precharge.
- The X-in-1 shall communicate with Zonal ECU to receive charge request and transmit status.

3.6.3.1 Functional safety architecture of provide energy to LV Bus

Figure 8 represents the functional safety architecture block of charging LV battery.

A safety manager presented in this figure aims to gather, report fault and to react with all the activities necessary to achieve a safe state to prevent a risk due to hazard in case of malfunctioning behavior while controlling the LV battery.

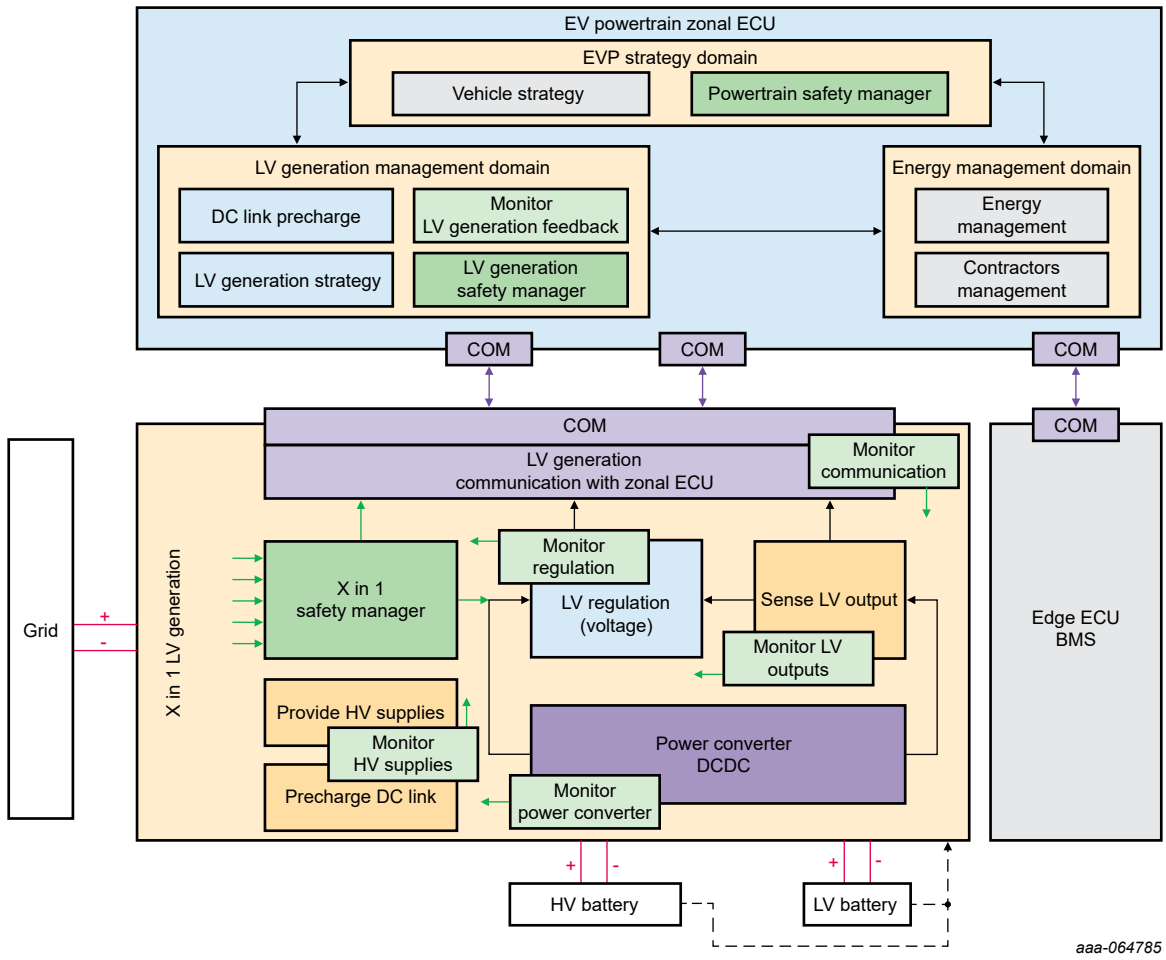

Figure 8. Functional safety architecture of LV generation concept

3.6.3.2 LV generation assumptions

- It is assumed that the LV battery is the last LV source of energy in case of LV generation faut.
- It is assumed that the LV battery energy is sufficient to ensure safety reaction to reach vehicle safe state.
- It is assumed that the Zonal ECU is informed by BMS about SoC and SoH of the LV battery and will notify X-in-1 in case of LV battery failure.
- It is assumed that the Zonal ECU notify the X-in-1 in order to start or stop LV generation.
- It is assumed that the Zonal ECU notify the X-in-1 in order to start or stop Boost mode to precharge DC link.
- It is assumed that the X-in-1 regulate itself the voltage and current to maintain correct LV voltage at its output.
- It is assumed that the X-in-1 regulate itself the voltage and current to precharge HV DC link.

3.6.3.3 FSR allocated to LV battery

Table 32. FSR allocated to LV battery FSR300-FSR303

FR	Acquire DC energy from the HV battery	ASIL
FSR300	X-in-1 shall monitor and detect loss of HV supply failure in the input of DCDC conversion.	B
FSR301	X-in-1 shall monitor and detect overcurrent failure in the input of DCDC conversion.	B
FSR302	In case of DCDC Input failure is detected, the X-in-1 shall stop the LV generation power output following **SS7** reactions while in Driving mode.	B
FSR303	In case of DCDC Input failure is detected, the X-in-1 shall stop the LV generation power output following **SS10** reactions while in Charging mode.	B

Table 33. FSR allocated to LV battery FSR304-FSR310

FR	Convert HV DC energy to LV DC energy to charge LV battery	ASIL
FSR304	X-in-1 shall monitor DC / DC converter to detect power conversion failure (short to ground). // Requirement decomposed with the UV detection of LV output.	B (C)
FSR305	X-in-1 shall monitor and detect overtemperature failures of the DC / DC converter.	B
FSR306	X-in-1 shall compare the DCDC conversion voltage set point received from Zonal ECU to LV generation output while in LV generation.	B
FSR307	In case of DCDC voltage set point plausibility failure is detected, the X-in-1 shall derate the LV generation output following **SS8** reactions while in Driving mode.	B
FSR308	In case of DC/DC converter (short) failure is detected, the X-in-1 shall stop the LV generation following **SS7** reactions while in Driving mode.	C
FSR309	In case of DC/DC converter overtemperature failure is detected, the X-in-1 shall derate the LV generation power output following **SS8** reactions while in Driving mode.	B
FSR310	In case of DC/DC converter (short) failure is detected, the X-in-1 shall stop the LV generation following **SS10** reactions while in Charging mode.	B

Table 34. FSR allocated to LV battery FSR311-FSR318

FR	Provide LV energy to the LV network of the vehicle	ASIL
FSR311	X-in-1 shall monitor and detect undervoltage (<9 V) failure on the LV output of DCDC conversion while in LV generation.	B
FSR312	X-in-1 shall monitor and detect overcurrent failure on the LV output of DCDC conversion while in LV generation.	B
FSR313	X-in-1 shall monitor and detect overvoltage (>17 V) failure on the LV output of DCDC conversion while in LV generation.	C
FSR314	X-in-1 shall monitor and detect sudden loss of LV generation failure (short to ground due to converter failure) on the LV output of DCDC conversion while in LV generation. // Requirement decomposed with the short to ground detection of LV converter	A (C)
FSR315	X-in-1 shall monitor and detect Reserve current (negative) failure on the LV output of DCDC conversion while in LV generation.	B
FSR316	In case of DCDC LV generation output critical failure (short or OV) is detected, the X-in-1 shall stop the LV generation power output following **SS7** reactions while in Driving mode.	C
FSR317	In case of DCDC undervoltage or overcurrent failure on LV output generation is detected, the X-in-1 shall derate the LV generation power output following **SS8** reactions while in Driving mode	B

Table 34. FSR allocated to LV battery FSR311-FSR318*...continued*

FR	Provide LV energy to the LV network of the vehicle	ASIL
FSR318	In case of DCDC LV generation output failure is detected, the X-in-1 shall stop the LV generation power output following **SS10** reactions while in Charging mode.	B

Table 35. FSR allocated to LV battery FSR319-FSR321

FR	Convert LV DC energy to HV DC energy to precharge DC link	ASIL
FSR319	X-in-1 shall inhibit the Reverse mode of DCDC conversion while in LV generation mode.	B
FSR320	X-in-1 shall compare the DCDC conversion voltage set point received from Zonal ECU to HV generation output (reverse mode) while in HV DC link precharge.	B
FSR321	In case of DCDC voltage set point plausibility failure is detected, the X-in-1 shall stop the LV generation following **SS7 or SS8** reactions while in Driving mode.	B

Table 36. FSR allocated to LV battery FSR322-FSR324

FR	Provide HV energy (reverse mode) for DC link precharge	ASIL
FSR322	X-in-1 shall monitor and detect overcurrent failure on the HV output of DCDC conversion while in Reverse mode.	B
FSR323	X-in-1 shall monitor and detect overvoltage failure on the HV output of DCDC conversion while in Reverse mode.	B
FSR324	In case of DCDC HV output (OC, OV) failure is detected, the X-in-1 shall stop the DCDC reverse mode power output following **SS7** reactions while in Driving mode.	B

Table 37. FSR allocated to LV battery FSR325-FSR329

FR	Communicate with Zonal ECU to receive voltage set point and mode and transmit status	ASIL
FSR325	X-in-1 shall detect loss or failure of the voltage set point request received from Zonal ECU.	B
FSR326	X-in-1 shall detect loss or failure of the DCDC mode request received from Zonal ECU.	B
FSR327	X-in-1 shall protect the DCDC output voltage and current feedback send to Zonal ECU.	B
FSR328	In case of DCDC voltage set point failure is detected the X-in-1 shall use the redundant communication pass following **SS1** reactions.	B
FSR329	In case of DCDC request mode failure is detected the X-in-1 shall use the redundant communication pass following **SS1** reactions.	B

3.6.4 FSC4 - Insure HV protection against electrocution concept

The principal functions for isolation and HV protection are:

- The X-in-1 shall Isolate LV domain from HV domain.
- The X-in-1 shall Isolate AC Grid domain from LV domain.
- The X-in-1 shall protect human from electrocution in case of maintenance, charge, drive or crash situation.

3.6.4.1 Functional safety architecture of insulation

Figure 9 represents the functional safety architecture block of insulation.

A safety manager presented in this figure aims to gather, report fault and to react with all the activities necessary to achieve a safe state to prevent a risk due to hazard in case of malfunctioning behavior of insulation.

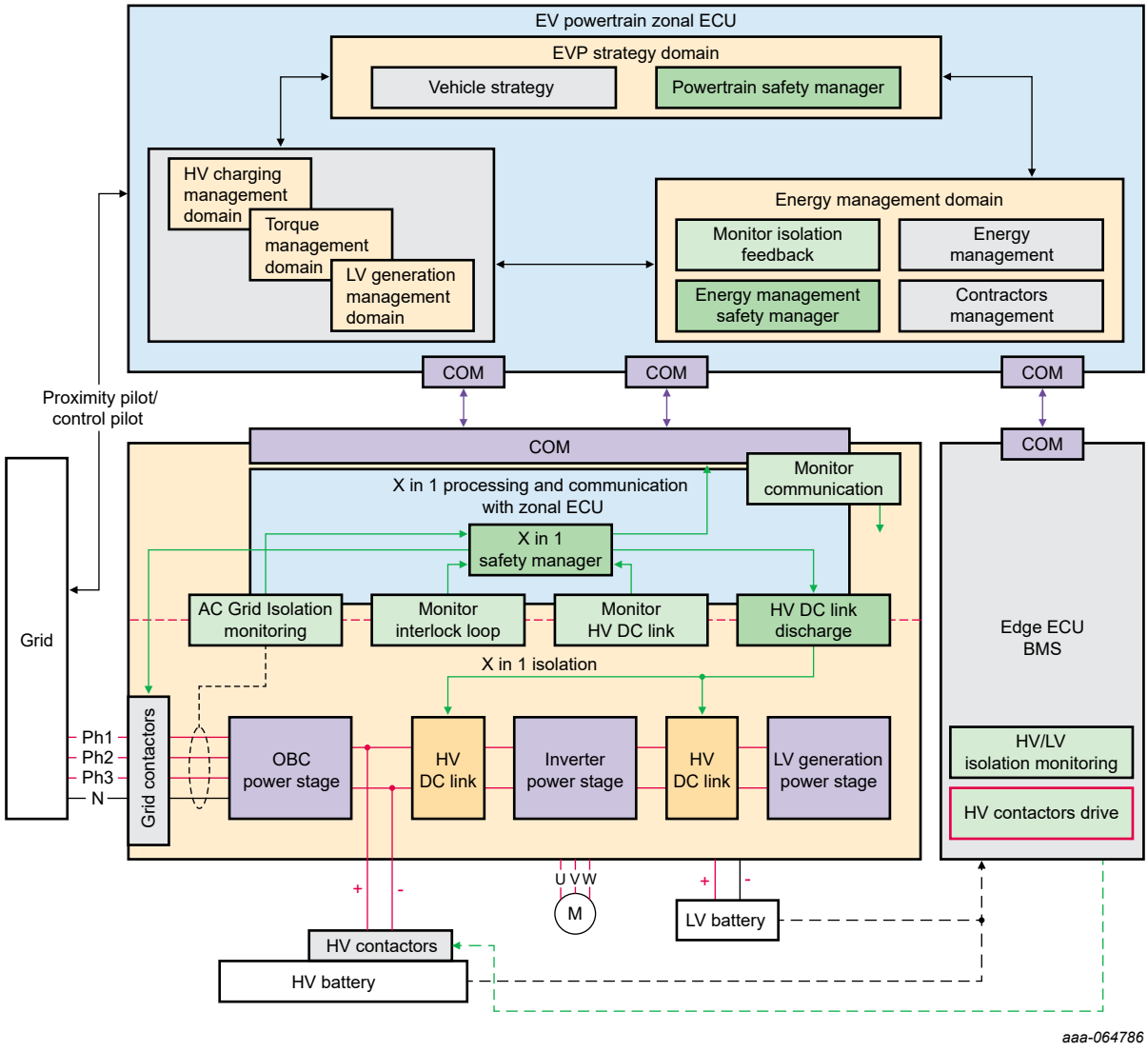

Figure 9. Functional safety architecture of HV protection and isolation concept

3.6.4.2 HV protection and isolation assumptions

The HV leakage current is by definition an unwanted current that will flow in unintended paths like to LV domain ground from vehicle Chassis which can be touch by users. It is found that those leakage currents could rise to dangerous levels and cause potential electric shocks. Therefore it is important that the different high voltage domain of the integrated X-in-1 are sufficiently isolated from the human/user during charging, driving or in case of a crash or maintenance. Online monitoring of isolation integrity is also required to achieve functional safety.

- It is assumed that the charging station used the CCS type 2 plug with the PE (protective Earth) connection.
- It is assumed that the X-in-1 system has the charging plug with the PE (protective Earth) connection.
- It is assumed that the BMS system is in charge of isolation monitoring between HV domain (HV battery) and the LV domain (Chassis Ground).

- It is assumed that the Zonal ECU will inform the X-in-1 system if HV isolation failure as been detected by the BMS system.
- It is assumed that the BMS system is in charge of monitoring the Hv Interlock loop.
- It is assumed that the Zonal ECU will inform the X-in-1 system in case of crash or maintenance detection by BMS Interlock monitoring.
- It is assumed that the X-in-1 system is in charge of isolation monitoring between HV Grid domain and the LV domain (Chassis Ground).
- It is assumed that the Zonal ECU is in charge of the charging plug detection and report status to the X-in-1 periodically.

3.6.4.3 FSR allocated to insulation

Table 38. FSR allocated to insulation FSR400-FSR401

FR	Human protection and isolation from HV Bus to LV Bus	ASIL
Info	HV LV isolation failure are detected outside the X-in-1 (See Section 3.6.4.2).	NA
FSR400	In case of HV to LV isolation failure is notified from Zonal ECU, the X-in-1 shall be isolated (from HV) and discharge any HV potential in less than 5s following **SS2** reactions while in Driving mode.	B
FSR401	In case of HV to LV isolation failure is notified from Zonal ECU, the X-in-1 shall be isolated and discharge any HV potential in less than 5s following **SS11** reactions while in Charging mode.	B

Table 39. FSR allocated to insulation FSR402-FSR403

FR	Human protection and AC Grid domain isolation from LV domain (Chassis)	ASIL
Info	AC Grid isolation detection is done by measuring AC and DC leakage current flowing to the chassis. This is done by so call “Residual current sensor”.	NA
FSR402	X-in-1 shall monitor the Grid phases and neutral in order to detect isolation failure (AC and DC leakage current) between AC Grid and LV domain.	B
FSR403	In case of AC Grid to LV isolation failure is detected, the X-in-1 shall isolate the grid and discharge any HV potential in less than 5s following **SS9** reactions while in Charging mode.	B

Table 40. FSR allocated to insulation FSR404

FR	Human protection in case of crash or maintenance	ASIL
Info	Crash or maintenance is detected by interlock loop which is open.	NA
FSR404	In case of crash or maintenance is notified from Zonal ECU, the X-in-1 shall be isolated (from HV and AC Grid) and discharge any HV potential in less than 5 s following.	A

3.6.5 FSC5 - Insure integrity and availability of communication concept

The principal functions in Driving mode are:

- The X-in-1 shall communicate with Zonal ECU to receive charge request and transmit status.
- The X-in-1 shall communicate with Zonal ECU to receive drive request and transmit status.
- The X-in-1 shall communicate with Zonal ECU to receive safety reaction request and transmit status.

3.6.5.1 Functional safety architecture of communication

Figure 10 represents the exchange of information between the X-in-1 and the Zonal ECU powertrain domains, HV charge management, torque management, LV generation management, energy management.

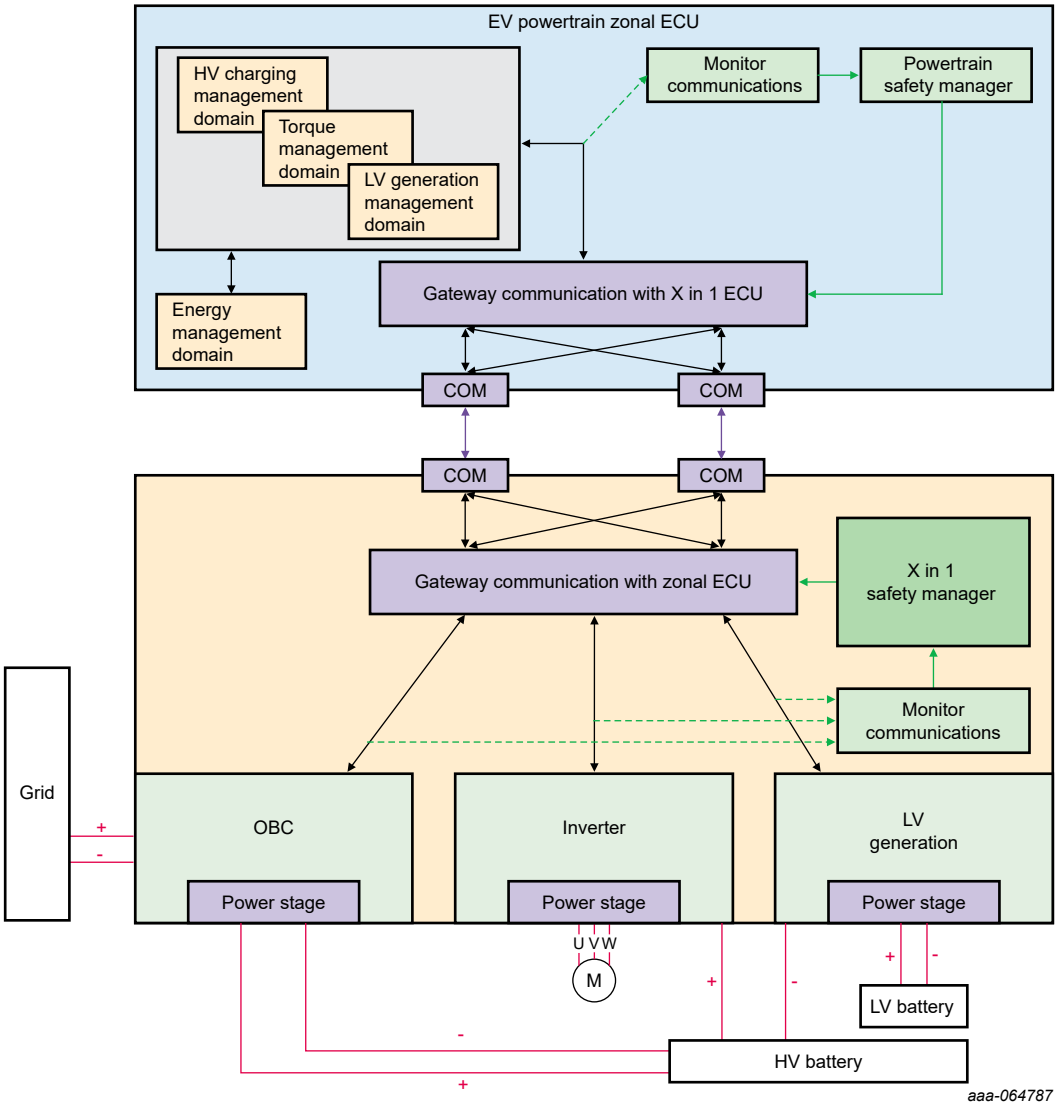

Figure 10. Functional safety architecture of X-in-1 communication concept

3.6.5.2 Fault tolerant communication assumptions

- It is assumed that the Zonal ECU handle fault communication reported by BMS, EVCC, Chassis to the X-in-1 system.
- It is assumed that the Zonal ECU handle charge or drive request communication from EVCC and torque management to the X-in-1 system.
- It is assumed that the Zonal ECU handle safety reaction request communication from BMS , EVCC, torque management or higher vehicle level to the X-in-1 system.
- It is assumed that the Zonal ECU receive charge, drive, LV generation, or safety status and information reported from the X-in-1 system.

3.6.5.3 FSR allocated to communication

Table 41. FSR allocated to communication FSR500-FSR501

FR	Receive charge request and transmit status	ASIL
FSR500	X-in-1 shall implement a communication end to end integrity check to control the charging request communication with Zonal ECU.	B
FSR501	If the communication integrity check failure is detected while charging, the X-in-1 shall continue operation using the redundant communication pass following **SS1** reactions.	B

Table 42. FSR allocated to communication FSR502-FSR503

FR	Receive drive request and transmit status	ASIL
FSR502	X-in-1 shall implement a communication end to end integrity check to control the propel or regeneration request communication with Zonal ECU.	D
FSR503	If the communication integrity check failure is detected while driving, the X-in-1 shall continue operation using the redundant communication pass following **SS1** reactions.	D

Table 43. FSR allocated to communication FSR504-FSR505

FR	Receive safety reaction request and transmit status.	ASIL
FSR504	X-in-1 shall implement a communication end to end integrity check to control the safety reaction request communication with Zonal ECU.	D
FSR505	If the communication integrity check failure is detected while charging or driving, the X-in-1 shall continue operation using the redundant communication pass following **SS1** reactions.	D

4 Revision history

Table 44. Revision history

Document ID	Release date	Description
AN14911.v.1.0	24 April 2026	Initial version.

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents