

2.1 Preliminary Architecture of the Item

The system under consideration is an electrical powertrain of the pure electric vehicle with all-wheel drive is shown in Figure 1.[2]

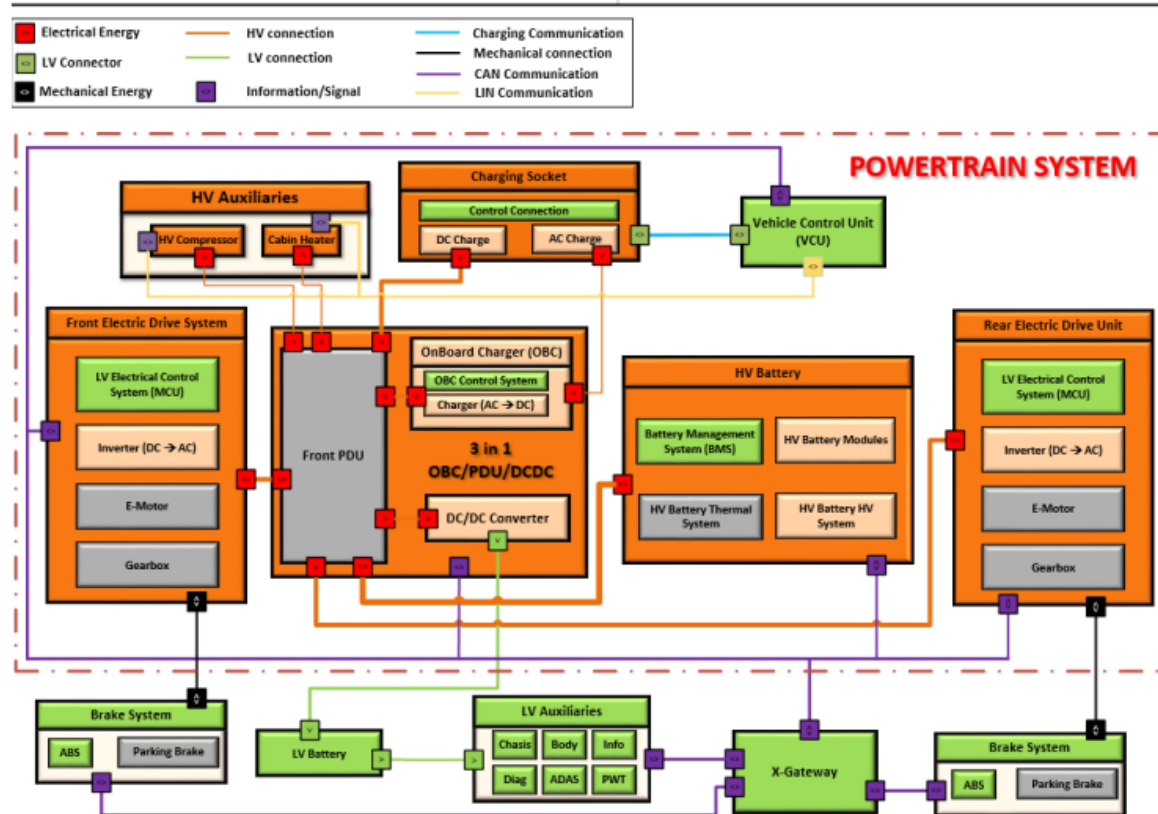


Figure 1 High-Level System Overview

The considered functions are described as below:

- Pedal Acquisition Function
- Driver Interpretation
- High Voltage System Coordination
- Torque Management
- Charge Management
- Energy Management
- High Voltage Safety
- Thermal Management
- Creep Control
- Cruise Control
- Vacuum Booster Pump Control
- Fault Diagnostics

2.2 Operating Modes

Operating modes for VCU are defined as state diagram in Figure 2.

Blue dashed line is represented FEV responsibility area. Red dashed line is represented BOSCH responsibility area.

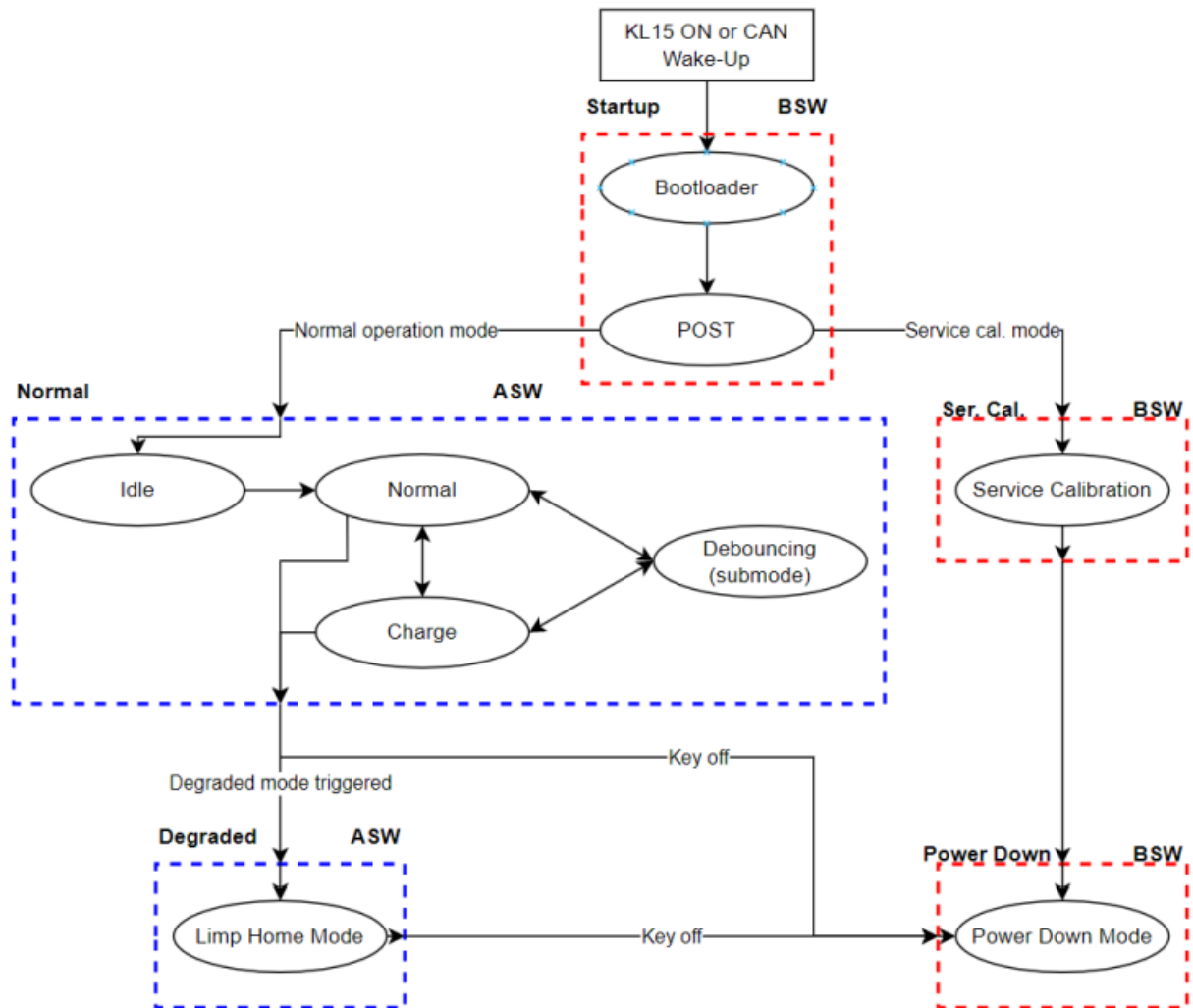


Figure 2 VCU operation mode

Table 5: Summary of Hazards, Safety Goals, ASIL and FTTI's for the Item under consideration

Safety Goal ID	Safety Goal	ASIL Rating	FTTI
SG1	Prevent Unintended acceleration (without destabilization) of $> 1.5 \text{ m/s}^2$ of the drivers intended path within 400 ms	ASIL C	0.4 sec.
SG2	Prevent Unintended rotational motion (vertical axis) --> Yaw of 3 degrees/sec of the drivers intended path within 1s	ASIL C	1 sec.
SG3	Prevent Motion in incorrect direction of the drivers intended path within 400 ms	ASIL A	0.4 sec.
SG4	Prevent unintended jerk $> 2.5 \text{ m/s}^3$ within 200ms	ASIL C	0.2 sec.
SG5	Prevent Undemanded vehicle movement of 0.5m with 200 ms	ASIL B	0.2 sec.
SG6	Prevent Insufficient deceleration $< 0.3G$ within 400ms	QM	0.4 sec.
SG7	Prevent Unintended release of thermal energy that may cause burns or fire within 2s	ASIL C	2 sec.
SG8	Prevent exposure to high voltage $> 60V \text{ DC}$ within 300ms	ASIL B	0.3 sec.
SG9	Prevent loss of LV system supply resulting in Loss of primary vehicle functions within 200ms	ASIL B	0.2 sec.
SG10	Prevent insufficient acceleration $< 2 \text{ m/s}^2$ within 500 ms	ASIL A	0.5 sec.
SG11	Prevent loss of acceleration within 1s	ASIL C	1 sec.
SG12	Prevent Missing/loss of brake lights when braking within 400 ms	ASIL B	0.4 sec.

4.1 Scope of Technical Safety Concept

This Technical Safety Concept covers possible hazards within the scope of ISO 26262 caused by malfunctioning behavior of the VCU. The TSRs defined in this document shall only ensure technical safety of the E/E-system with regards to the Safety Goals corresponding to Table 5. The nominal performance of the E/E-system is not within the scope of this document.

4.2 Basic Principles and Assumptions

As a basis for the definition of the Technical Safety Concept, some general assumptions are made. These assumptions are treated as basic principles and guidelines for all development activities in the lifecycle of the item (Concept Phase, System Design and HW-/SW-Development).

- Protection of life (of driver/passenger or other parties) has the highest priority.
- Reliability has higher priority than backup functions.
- The safety functions and mechanisms shall be as far as possible independent of the driver reaction.
- Safety related functions, in particular for system monitoring and error reactions shall be simple, manageable and robust.
- The system shall be designed so that single errors and single errors in combination with latent errors lead to controllable system reactions. The corresponding signal paths (sensors, actuators, functions) shall be monitored.
- The system shall be designed so that double and dual faults lead to controllable system reaction as required by the ISO and to achieve state-of-the-art.
- In terms of a high system availability, staged error reactions shall be strived.
- A signal path shall be classified as "confirmed error", after an explicit detection (E.g. after debouncing event or time) and before the reaction shall be activated. Previously the defect shall be classified as "unconfirmed error".
- Appropriate reaction mechanisms shall be defined according to the function in the cases of an "unconfirmed error" and a "confirmed error".
- The reset, e.g. going from a limited operating mode to unlimited operating mode, of fault reactions shall be determined in individual cases and shall be performed controllable. Non-continuous transitions shall be avoided.
- Disable of powertrain is permitted when no other controllable system reaction can be ensured.

- Any control unit transmitting safety critical/related signals are responsible for the validity of the content (information) of these signals. i.e. responsibility of the subsystem to provide reliable information
- All safety requirements with QM ASIL will not be considered for L2 and shall be considered by L1 functions.
- There are two-channel independent accelerator pedal sensors in the vehicle, no common cause failure and dependent failure between them.
- The driving Style Mode switch is QM in the TSC phase since torque change is very smooth when changing the "Driving Style Mode". Torque Filter in the L2 SW can cover the hazards of "Unintended change Driving Style Mode".
- "Creep ON/OFF" signal and "KL15" signal are QM level in the TSC phase. Since the safety mechanism in the VCU L2 SW can avoid the hazards caused by them.
- "ESP torque intervention" signals are the inputs of TSC-SM7 (Torque management). Torque calculation module in the VCU L2 SW is ASIL C, but "ESP torque intervention" signals are ASIL B. Logically ASIL B signal shall not influence the ASIL C SW. While the VCU L2 SW will only use absolute value smaller between "Drive torque request" and "ESP torque intervention". So, even though "ESP torque intervention" signals are ASIL B, "ESP torque intervention" signals do not influence the VCU L2 SW, which means they will not lead vehicle excessive/unintended acceleration.
- The mechanical design of charge socket can ensure
 - No direct contact with conducting parts of DC+ and DC-
- The safety software shall be executed once in less than 10ms

4.4 Informal Description of Technical Safety Concept

This chapter describes the Technical Safety Concept in an informal manner. The TSC is a collection of Safety Mechanisms that are derived from the FSC. A list of Safety Mechanisms is shown in Table 6: Refined Safety Mechanism. The first 2 columns of the table indicate the ID and the name of the Safety mechanisms. The description of each safety mechanism is provided in subsequent chapters. This informal description is converted into formal TSRs in Chapter 6. Columns 3 and 4 in Table 6: Refined Safety Mechanism refers to the ID and the name of the Safety Mechanism implemented in the L2 Software.

4.4.1 Refined Safety Mechanism

In TSC phase, the safety mechanisms in the FSC have been merged to reduce the number of safety mechanisms as shown in Table 6. The safety mechanisms in L2 SW can cover all the safety goals listed in chapter 3.

Table 6: Refined Safety Mechanism

TSC-SM ID	Technical Safety Concept - Safety Mechanism Name	SM ID	Safety Mechanism Name	ASIL
TSC-SM1	Accelerator pedal monitor	SM1	Plausibilize Accelerator Pedal Value	C
TSC-SM2	Brake pedal monitor (Not valid for HaBang)	SM2	Plausibilize Brake Pedal Status	C
TSC-SM3	E2E check for CAN input signals	SM3	Determine Brake Pedal Status	C
		SM4	Determine Gear Lever Status	
		SM7	Determine ESP Input Values	
		SM8	Determine ADAS Input Values	

		SM9	Determine Front MCU Input Values	
		SM10	Determine Rear MCU Input Values	
		SM11	Determine Park Lock Input Values	
		SM13	Determine BMS Input Values	
		SM15	Determine DCDC Input Values	
TSC-SM4	Vehicle speed determination	SM81	Determine Vehicle Speed	C
TSC-SM5	Powertrain status monitor	SM80	Determine and Broadcast Vehicle Crash	C
		SM50	Monitor Powertrain Activation/Deactivation	
TSC-SM6	Gear management monitor	SM51	Gear Shift Monitoring	C
		SM82	Park Lock Request Monitoring	
		SM83	Park Lock Engagement Monitoring	
TSC-SM7	Torque management monitor	SM52	Driver Torque Demand Determination	C
		SM53	Follow ESP Torque Reduction	
		SM54	Determine Actual Torque	
		SM60	Avoid Unint. Acc/Dec	
		SM61	Avoid unint. Yaw	
		SM62	Avoid unint. Movement	
TSC-SM8	12V battery voltage monitor	SM86	LV network voltage monitor	C
TSC-SM9	Plug-in charge monitor	SM5	Determine Charge Plug Status	B
		SM87	Charging plug monitoring	
		SM88	Charging lock monitor	
		SM89	DC charge relay monitor	
TSC-SM10	Vacuum pump control monitor	SM90	Vacuum pressure monitor	B
TSC-SM11	Error reaction	SM85	Powertrain error management and warning degradation	C

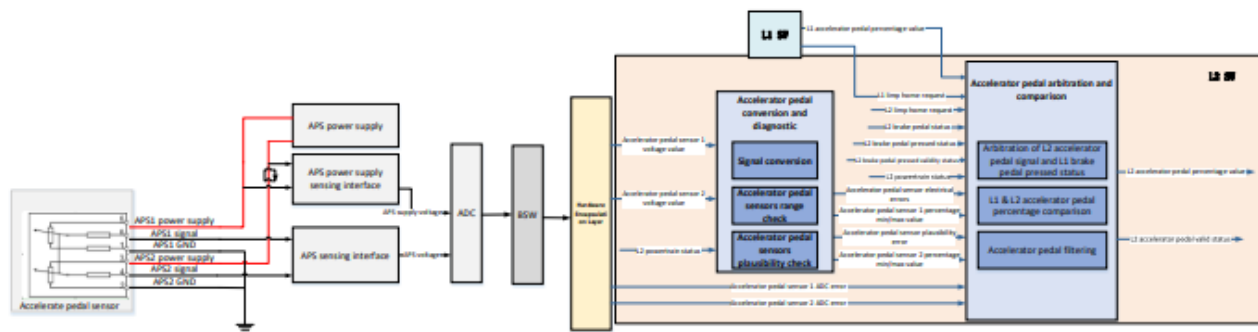


Figure 4 Accelerator pedal monitor

The TSC-SM1 is to monitor the accelerator pedal position, which is one of the most important inputs of driver. To avoid excessive accelerator pedal position signal which can lead to unintended/excessive vehicle acceleration, the accelerator position signals received from accelerator pedal sensors, and all the failures of accelerator pedal sensor itself and ADC path.

There are several methods for accelerator pedal signal monitoring

- Range check: the monitor compares the nominal value with the actual value collected in real time, if the actual value is higher than the upper limit or lower than the floor of nominal value, and last for a predefined time, then an out-of-range failure is determined.
- Synchronization check: Normally, there is a quantitative relationship between the signals from two paths. If the actual values of the two signals do not meet this relationship and last for a predefined time, then a synchronization failure is determined.

If the failure of APS signals is detected, VCU shall enter limp home mode (limit vehicle speed and vehicle torque) or degradation mode (replacement value and invalid status).

The L2 software monitors the APS percentage value from Level1. If the L1 APS value is within the L2 limit range, the VCU forwards the APS percentage value from Level1 to rest of the APSW. Otherwise, the VCU forwards the upper/lower limit value to rest of the APSW.

There are several methods for brake pedal signal monitoring

- Range check: the monitor compares the nominal value with the actual value collected in real time, if the actual value is higher than the upper limit or lower than the floor of nominal value, and last for a predefined time, then an out-of-range failure is determined.
- Synchronization check: Normally, there is a quantitative relationship between the signals from two paths. If the actual values of the two signals do not meet this relationship and last for a predefined time, then a synchronization failure is determined.

If any failure of brake pedal sensor is detected and confirmed, VCU shall disable regeneration torque output till the end of drive cycle.

The L2 software will monitor the BPS value from level1. If the L1 BPS value is within the L2 limit range, the VCU will forward the BPS value from level1 to continue calculation. Otherwise, the VCU will forward the upper or lower limit value to continue calculation.

The L2 also determines the brake pedal status based on the brake pedal percentage calculated by L2 and the brake pedal status from L1, according to the strategy in the related requirement.

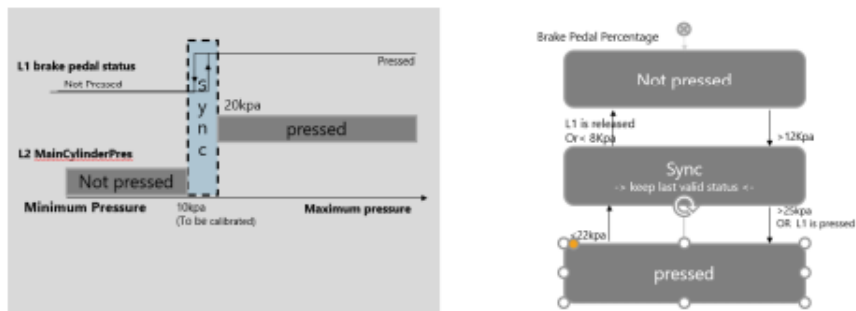


Figure 7-Main cylinder evaluation algorithm

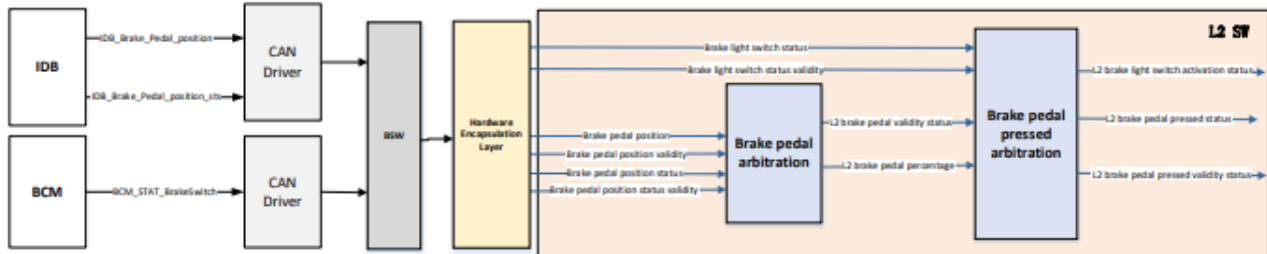


Figure 8-HaBang project brake pedal monitor

If any failure on the brake pedal position status and percentage value that come from IDB is detected, VCU disables regeneration torque and VCU shall enter limp home mode.

The L2 APSW monitors the brake light switch status from BCM to determine the brake pedal pressed status and the brake pedal pressed valid status. If the failure of the brake light switch status is detected, the VCU forwards the pressed valid status as invalid. The brake pedal pressed status is determined based on the brake pedal position percentage value or brake light switch pressed status.

hardware, communication peripherals, transceivers, communication lines, or other communication infrastructure.

E2E communication protection works as follow:

- Sender: addition of control fields like CRC or counter to the transmitted data.
- Receiver: evaluation of the control fields from the received data, calculation of control fields (e.g. CRC calculation on the received data), and comparison of calculated control fields with an expected/received content.

The VCU HEL is responsible for E2E check, and forward the error status to level2.

All the fault status and error confirmed status will be forwarded to signal processing unit of level2. Then the level2 will do the arbitration according the failure type and status. If one or more CAN failures are detected, VCU shall set a replacement value for the safety-related signals (E.g. last cycle value) to support the normal operation. After the failure being confirmed, the replacement value shall not lead any violation of safety goals.

4.4.5 Informal Description of TSC-SM4 (Vehicle speed determination)

The TSC-SM4 is shown in Figure 10.

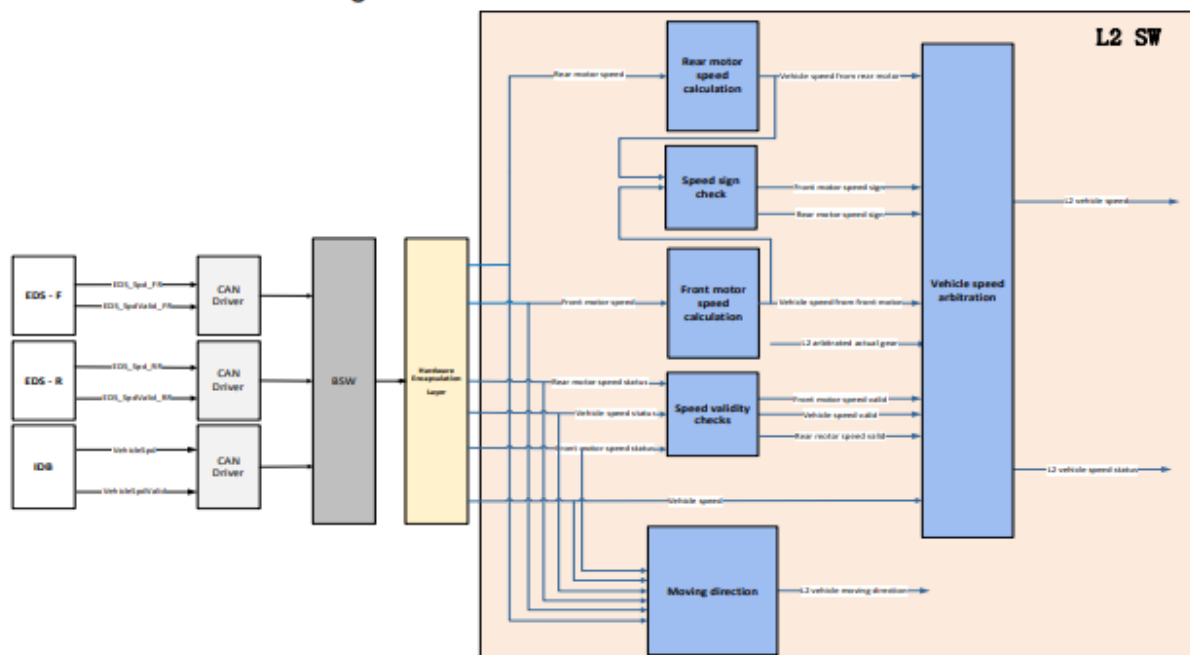


Figure 10-Vehicle speed determination

Vehicle speed is one of the most important signals in torque management. To calculate the driver torque request, and support other functions like gear shifting monitoring, the VCU shall calculate correct vehicle speed signal with ASIL C.

To improve the robustness of powertrain, the vehicle speed signal is calculated based on three signals, the motor speed signal of front motor, the motor speed signal of rear motor

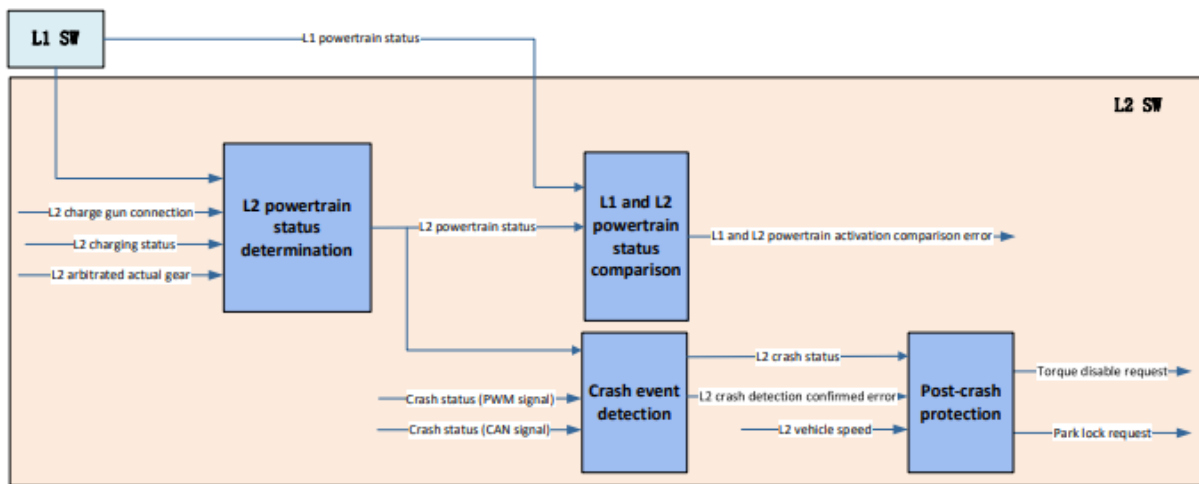


Figure 11-Powertrain status monitor

The powertrain status monitor concept is about the method to determine the activation/deactivation of powertrain and to detect the crash status.

The L2 APSW determine the powertrain status based on the following conditions:

- Charging status
- Actual gear
- Charge gun connection status

After determining the powertrain status, the L2 software shall compare it to the L1 powertrain status.

For the crash status detection, the CAN signal and PWM signals are used. To prevent vehicle acceleration after crash to prevent the secondary damage, the post-crash protection like torque disable request and park lock request will be triggered once the crash event is determined.

4.4.7 Informal Description of TSC-SM6 (Gear management monitor)

The TSC-SM6 is shown in Figure 12.

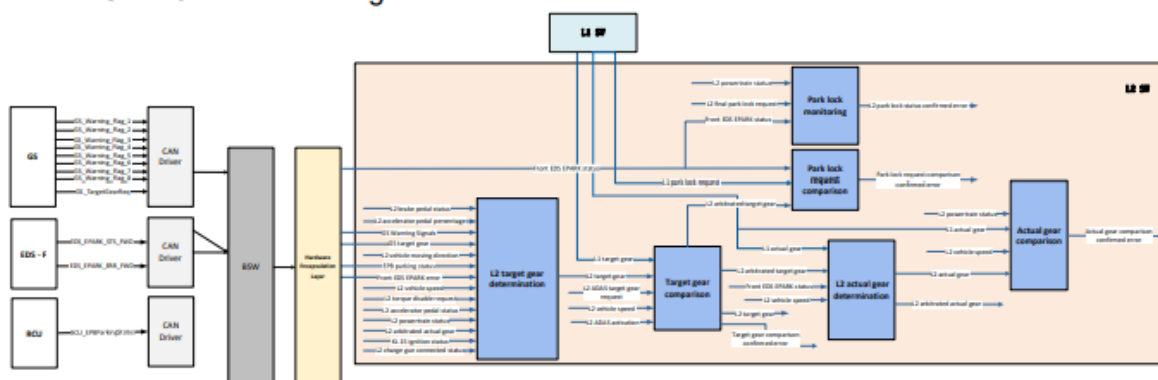


Figure 12-Gear management monitor

The TSC-SM6 consists of two parts, one is the independent gear calculation, the other one is the park lock engagement monitoring.

The safety concept of “independent gear calculation” is to prevent gear calculation fault since gear calculation fault will lead to below hazards directly.

- Unintended vehicle movement
- Take off in wrong direction

For Manual Shifting, the L2 APSW shall calculation the gear according to following conditions

- Shifting request (P/R/N/D)
- Brake pedal status
- Vehicle speed (including moving direction)
- Key ignition status

The L2 APSW shall compare “L2 target gear” with “L1 target gear” and determine L2 actual gear according to the table in the REQ_001549 and REQ_001538.

The safety concept of “park lock engagement monitoring” is to prevent unintended vehicle rolling away in case of park lock system failure. The potential hazard “Rolling vehicle due to malfunction of park lock function” can occur due to the following malfunctions:

- Unintended shifting gear from P to R/N/D
- Unintended release of park lock in P gear
- Request P gear but Park lock does not engage

Park lock functionality can be realized using manual park request from driver or by automatic park function requesting park lock, hence term “park lock request” shall be understood for both manual and automatic park request if not stated explicitly otherwise.

The “unintended shifting gear from P to R/N/D” is covered with “independent gear calculation”. While the “park lock engagement monitoring” is only used for preventing rolling vehicle when driver selected P gear, but park lock does not engage.

VCU shall continuously detecting the P gear status after VCU sent P gear engaging request to EDS. If the VCU requests park lock to engage but the park lock feedback status from the EDS is not park lock engaged within a certain amount of time, VCU shall send a driver warning message to the dashboard.



Figure 13-Detailed Pressed Gear Management Description

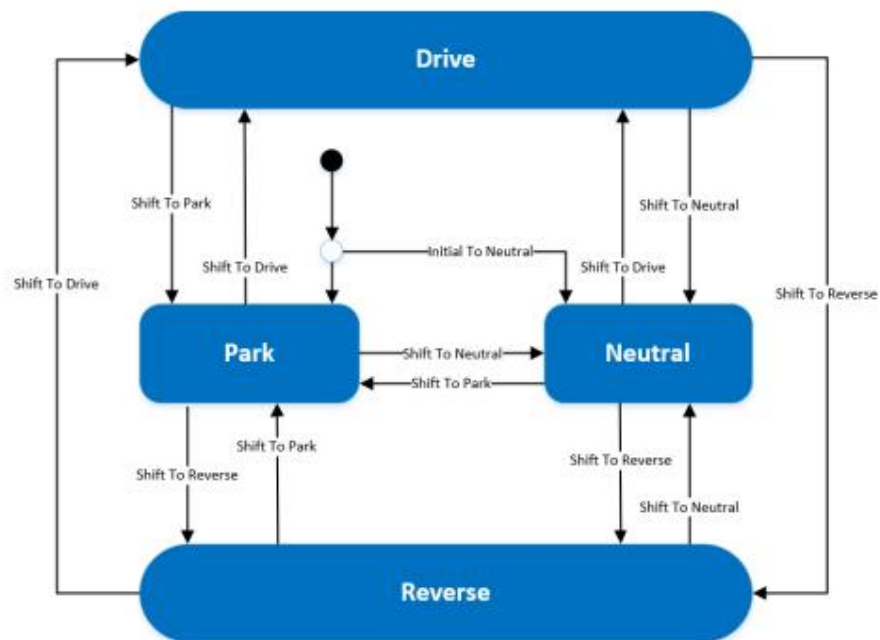
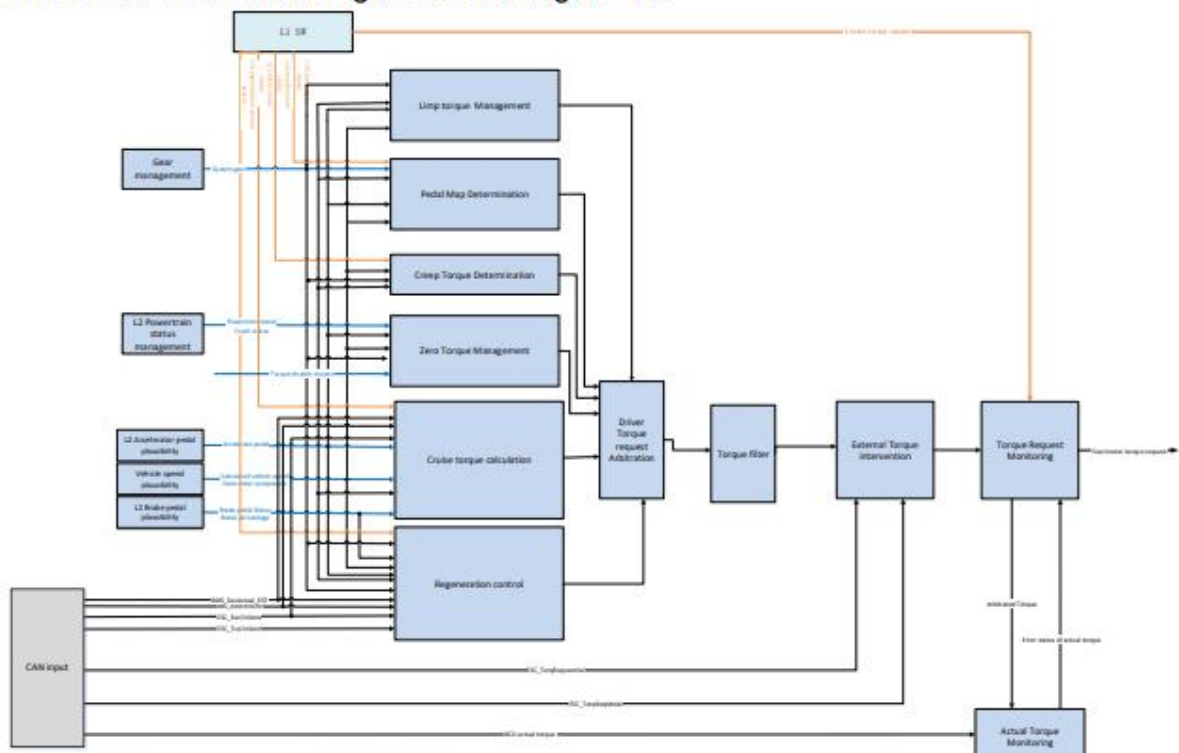


Figure 14-Gear Transition Diagram

4.4.8 Informal Description of TSC-SM7 (Torque management monitor)

The TSC-SM7 is shown in Figure 15 and Figure 16.



The system architectural design is the selected system-level solution that is implemented by a technical system. The system architectural design aims to fulfil both, the allocated technical safety requirements and the non-safety requirements. System Architecture is shown in following figure. Figure 23 is derived from FSC [5].

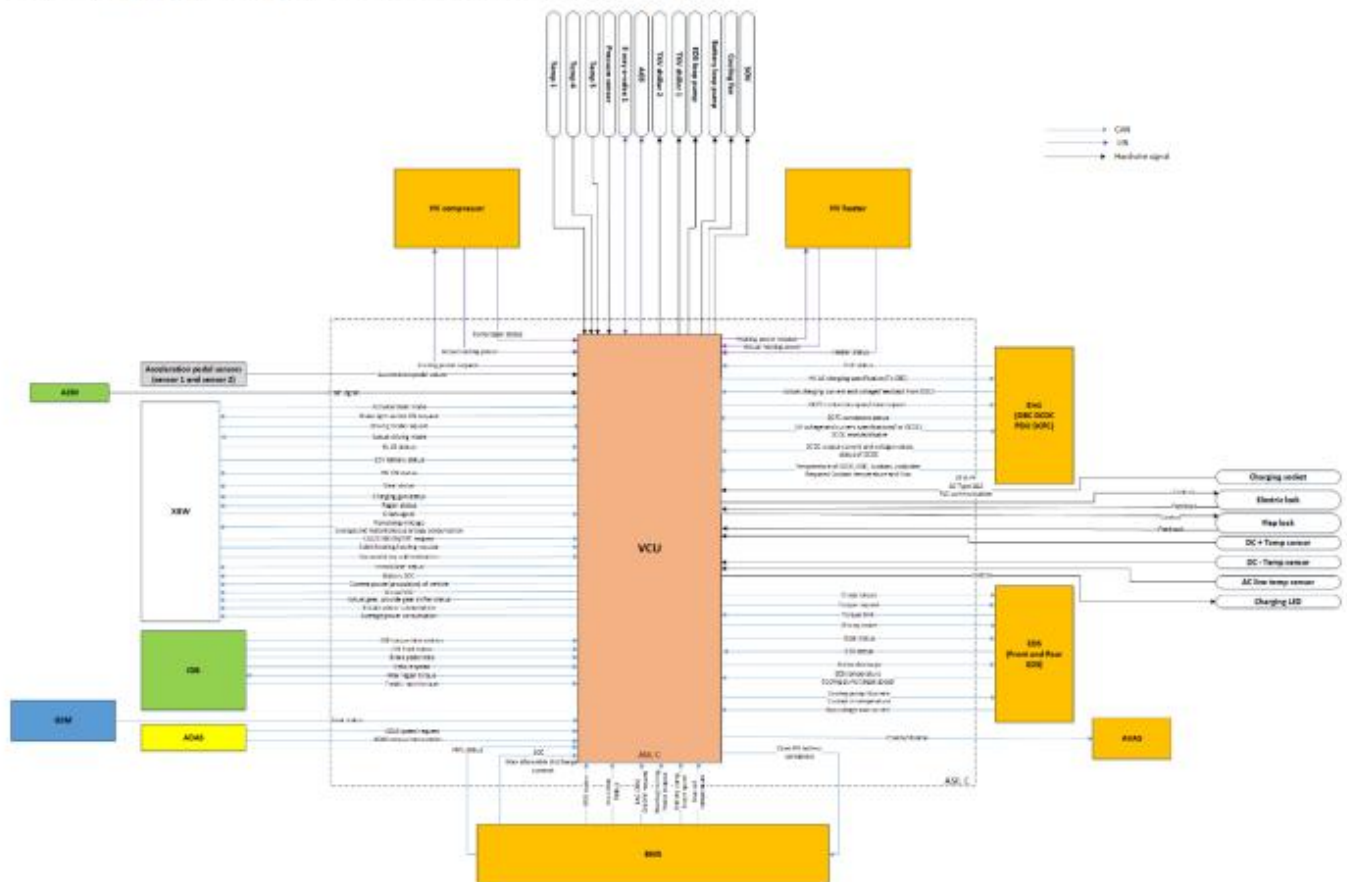


Figure 23-Habang 4WD system Architecture

Software level detailed structures are demonstrated in software architectural design document [8].