

Electromechanical Braking System Functional Safety Design



Sifan You, Hely Zhang

Abstract

The electromechanical brake (EMB) system represents the next generation of vehicle braking technology, replacing traditional hydraulic systems with fully electronic actuation. As a safety-critical system with no hydraulic backup, EMB must be developed to the highest automotive functional safety integrity level, ASIL D, in compliance with ISO 26262:2018. This application note aims to help guide the ASIL D functional safety design process for an EMB system targeting both 12V and 48V automotive platforms. The document covers the complete safety development process from hazard analysis and risk assessment (HARA), safety goal definition, functional safety concept, to system-level safety mechanism design. Key safety challenges including fail-operational architecture, redundant sensing, and multi-level power management are addressed. The proposed design is built around Texas Instruments' automotive-grade device and functional safety compliant product portfolios, including the F29P329SM2-Q1 ASIL D MCU, TPS653880-Q1 ASIL D PMIC, LM78845-Q1 ASIL D DC/DC converter, DRV3263-Q1/DRV3233-Q1 ASIL D gate drivers, DRV8263S-Q1 ASIL B H-bridge driver, WSS001-Q1 ASIL B wheel speed decoder, and TMAG6180-Q1 ASIL B angle sensor. System-level safety mechanisms, including redundant power inputs, dual CAN communication and wake-up paths, redundant position sensing, and ECU-level wheel speed cross-checking, are employed to achieve ASIL D compliance at the system level.

Table of Contents

1 Introduction	2
1.1 Evolution of Braking Systems	2
1.2 Why ASIL D is Required for EMB	3
1.3 How to Develop a Safe EMB System?	3
2 Safety Goal and Safety Concept	5
2.1 EMB System Overview	5
2.2 EMB Safety Goal	6
2.3 EMB Functional Safety Concept	8
3 Proposed Design for ASIL D EMB	12
3.1 EMB System Safety Design Architecture	12
3.2 Hardware Component	13
3.3 Safety Mechanism Design	14
4 Summary	41
5 References	42

Trademarks

C2000™ and E2E™ are trademarks of Texas Instruments.
All trademarks are the property of their respective owners.

1 Introduction

The rapid development of new-energy vehicles is driving continuous evolution of braking systems. The electromechanical brake (EMB) eliminates complex hydraulic or pneumatic pipelines, generating braking force directly through an electric motor. This achieves complete decoupling of the braking system, resulting in a more compact structure, faster response, improved energy efficiency, and better integration with chassis-domain control and advanced driver-assist systems.

1.1 Evolution of Braking Systems

Over the past few decades, the evolution of vehicle braking systems has brought notable shifts across the industry. The main stages are as follows:

- Legacy hydraulic brakes
- Electrical hydraulic brakes
- Electrical mechanical brakes

1.1.1 Legacy Hydraulic Brake

In this braking method, drivers need to push braking pedal. The vacuum booster amplifies push force, pushes the valve of the vacuum pump, and pushes the brake oil onto the calipers of the four wheels. Oil pressure forces the caliper to clamp the disc, creating friction and slowing the vehicle. Legacy hydraulic brakes totally depend on mechanical and hydraulic structure to transmit braking force. Therefore, this system can only provide limited response speed and accuracy for braking.

1.1.2 Electrical Hydraulic Brake (EHB)

Designed with a mechanical fallback, the second-generation EHB system integrates an MCU, pedal and position sensors, a motor, a brake drive unit, and a brake master cylinder into a single braking design. EHBs introduce more electrical devices and sensors into the system than legacy brakes. The pedal signal is sensed and input to the electronic control unit. EHB drive BLDC motor to boost hydraulic pressure to push caliper. The position of BLDC rotor is measured by the sensor and feedback to control unit for control loop. The high-pressure hydraulic control unit automatically adjusts the brake pressure of the wheels according to the driving command. Although braking speed is increased compared to the legacy system, the limitation is that the EHB system still requires hydraulic components, which still require a high-cost and complicated liquid pipeline.

1.1.3 Electrical Mechanical Brake (EMB)

The EMB system is a fully electronic braking system that triggers actuators (motors, sensors, control units) through electrical signals. Each wheel equipped with an EMB system. The EMB system converts the braking intention of the driver directly into mechanical braking. When the brake pedal is pressed by the driver, the sensors transmit signals to the electronic control unit (ECU), which calculates the braking force demand and sends the result to EMB actuator. The control command is sent to the EMB actuator using CAN communication. The caliper is then driven through BLDC motor produced clamping force.

In response to the shortcomings of the legacy and EHB systems, EMB replaces the traditional hydraulic braking system with motor braking, which provides more electronically, precise, and faster braking control than EHB.

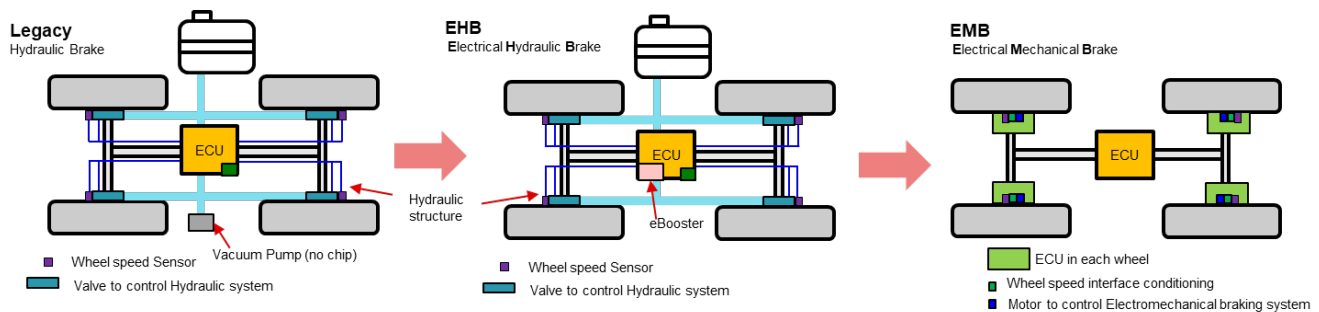


Figure 1-1. Structures of Different Braking System Design

1.2 Why ASIL D is Required for EMB

Correctly braking is the bottom line for safety driving. Brake failure or unexpected braking, especially at high speed, is a life-threatening incident. Because EMB system is a wire-controlled braking system, it completely removes the hydraulic braking, and use electrical signal to control the actuator to brake. Thus, all safety functions rely on the correctness electric signal. The safety requirements for electric signals need to meet a high-level standard, so safety is becoming the decisive factor in the adoption of EMB technology.

In Chinese GB/T 21670-2025, European UN R13-H, American FMVSS, and other standards, EMB system must mandatorily develop the following functional safety requirements and meet the ASIL target. Nowadays, when deciding the ASIL target and safety requirements at the beginning of development according to functional safety standards like ISO 26262 and GB/T 34580, vendors assume EMB malfunction with a more severe consequence and a smaller takeover capability. The analysis result shows that the risk level of an EMB failure is higher than what is considered acceptable. As a result, automotive designers must develop EMB for these critical safety goals with the strictest safety rating: ASIL D.

In addition to fail-safe design, EMB systems must also incorporate fail-operational strategies to provide continuous functionality during a failure. The aim is to make sure that the EMB system can provide the functionality of braking all the time, even if the system fails.

1.3 How to Develop a Safe EMB System?

As required in various standards, EMB system must developed following ISO 26262: 2018. The ISO26262:2018 standard is an international standard functional safety standard that is inspired by and adapted from IEC 61508, and is aimed at automotive E/E systems. [Figure 1-2](#) shows the whole development process to get safety requirements for implementation.



Figure 1-2. Safety Requirement Development Process

- Item Definition: Establish project scope
- Hazard Analysis and Risk Assessment: Identify potential hazards for item, and evaluated based on severity, exposure, and controllability factors, resulting in the definition of safety goals (SG) and assignment of automotive safety integrity levels (ASIL)

- **Functional Safety Concept:** Develop high-level safety strategies, which allocates safety responsibilities across system functions and establishes Functional Safety Requirements (FSR) that define what safety functions are needed
- **Technical Safety Concept:** Translate the functional requirements into specific technical safety requirements (TSR) that detail how the safety design will be implemented in the system architecture
- **Hardware and Software Safety Requirement:** technical requirements are further refined into hardware safety requirements (HSR) and software safety requirements (SSR) that guide the actual implementation
- **Design Implementation:** Implement specific safety functions according to HSR and SSR

In ISO 26262, safety analysis methods such as deductive analysis and inductive analysis are recommended to be adopted for identifying the failures and transform to safety requirements. IC developers and system integrators can select practical analysis methods to identify failures and transform them to adhere to safety requirements.

For example, fault tree analysis (FTA) is a typical top-down deductive analysis method that uses logical reasoning to identify all possible causes and combinations of system failures. FTA uses Boolean logic to describe cause and effect relationships between events. Failure mode and effects analysis (FMEA) is a representative inductive analysis to systematically identify possible failure modes in product designs and evaluate the causes and effects. The safety requirements are defined as the appropriate preventive and control measures targeting for these identified failures.

2 Safety Goal and Safety Concept

2.1 EMB System Overview

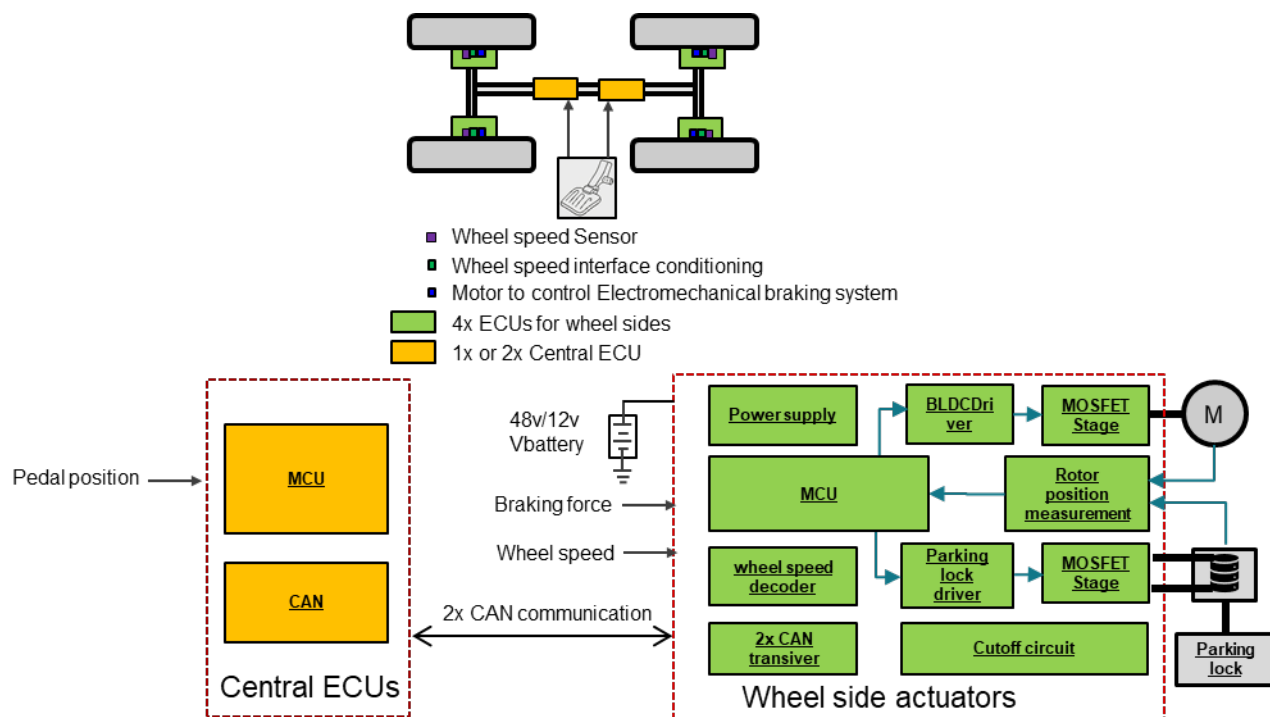


Figure 2-1. EMB System Overview

Figure 2-1 shows a comprehensive EMB system consists of wheel side actuators and central ECU system. Rear-wheel side-systems are typically equipped with electronic parking brakes (EPBs) to provide vehicle parking function. Since the central ECU needs to be developed by system integrators based on individual architecture and functionality, the "EMB system" in the following sections only refers to the wheel-side actuator system. Assume that EMB is adapted to 12V and 48V applications respectively.

The central ECU system is responsible for communicating with the wheel-side MCU and receiving wheel speed, wheel side system fault signal, and so forth. from the wheel-side MCU. These reported signals are sent to the zone controller for signal verification, braking force calculation, and vehicle speed calculation on the application layer for further control command. The pedal position movement signal is also inputted to the central ECU directly. Some system integrators can input the pedal position signal to the wheel-side MCU and send to central ECU by communication.

The wheel-side system is powered by 48V/12V battery due to different systems. The 48V/12V battery input is converted into different power outputs available to the different chips by internal power management circuits. The MCU provides the EMB with central control unit functions, including signal sensing, motor control, communication. After the driver presses the braking pedal, the central ECU generates and sends a braking control command to the wheel-side MCU using CAN communication. The MCU transfers the braking command to the PWM control signal for the gate driver. It triggers motor running in the intended way to output brake function. All sensors provide a runtime system status measurement function for signal control.

The primary scope of this document covers the wheel-side EMB design, including the power management unit, central control unit, communication interface, actuator drive unit, and sensor interface. For safety mechanisms that require aggregation of multi-wheel data, such as the ECU-level wheel speed cross-check (SM_WSS_plausibility check), the safety requirement is allocated to the central ECU. The detailed ECU implementation is outside the scope of this document but shall be developed and verified to ASIL D in accordance with the requirements specified herein.

2.1.1 Item Definition

The item analyzed in this document is the wheel-side EMB system only, including:

- Receiving braking force commands from the central ECU using CAN communication
- Controlling the BLDC motor to generate and release braking clamping force
- Controlling the EPB solenoid lock for vehicle parking function
- Reporting system status and fault information to the central ECU

The item boundary is defined as the wheel-side EMB system, covering:

- Power management unit (PMU)
- Central control unit (MCU)
- Communication interface (CAN transceiver)
- Actuator drive unit (BLDC gate driver + H-bridge driver)
- Sensor interface (angle sensor, wheel speed decoder, pedal position sensor [optional])

ECU-level functions — including braking force calculation, ESC algorithm execution, and vehicle-level fault management — are explicitly excluded from this item scope.

2.1.2 Operational Situations

Table 2-1 shows the operation mode of EMB under different situations.

Table 2-1. EMB Operational Situations

Situation ID	Operational Situation	Vehicle Speed	EMB State
OP1	Normal driving, no braking request	Entire vehicle speed range	Standby
OP2	Normal driving, braking applied	Entire vehicle speed range	Active braking
OP3	Vehicle stationary, parking applied	0km/h	EPB locked
OP4	Vehicle stationary, parking released	0km/h	EPB released
OP5	Power-on initialization	0km/h	Self-test mode
OP6	Degraded fault-operational mode	Entire vehicle speed range: 0km/h to 200km/h	Redundant braking

2.1.3 System Interface

Table 2-2 shows the main interfaces based on the system boundaries.

Table 2-2. EMB System Interface

Interface	Detailed Description
Vbat1 / Vbat2	Dual 48V/Dual 12V battery power inputs
CAN1-H / CAN1-L CAN2-H / CAN2-L	Braking commands from central ECU, system status and fault information report to ECU
Pedal position (optional)	Analog/SENT signal measured by pedal position sensor (front-left wheel EMB only)
Wheel speed	Every wheel deploys with a speed sensor for speed measurement input

2.2 EMB Safety Goal

2.2.1 Application Assumption

To build safety analysis, the following application assumptions are made:

- Assume there are four EMB systems fitted to each of the four wheels of a vehicle. Only the two EMB systems on the rear wheels are embedded with EPB feature.
- Assume the analyzed EMB system is deployed at the rear wheel of vehicle. Therefore, EPB function shall also be considered in the following analysis.
- Assume the EPB function considered in our system is only target for solenoid lock application. BDC motor use case is not covered by this design.
- Assume The key analyzed functions of EMB are limited to:
 - Actuate vehicle EPB motor in apply or release direction

- Actuate vehicle EMB motor in apply or release direction
- Assume there is a central ECU for EMB system sensor signal receive, control signal issue, fault handling, and so forth.
- Assume the central ECU provides valid braking torque commands within the defined message cycle time.
- Assume the battery management system (BMS) is responsible for reverse battery protection on the input power supply.
- Assume the system fault tolerance time interval (FTTI) is less than 100ms.

2.2.2 Hazard Analysis and Risk Assessment

Hazard is the operational situations and operating modes in which the malfunctioning behavior of an item occurs. The hazard events of EMB can be identified by using hazard and operability study (HAZOP), brainstorm, functional hazard assessment (FHA), and other methods. In this paper, take HAZOP as example to show how to derive malfunction behavior with leading words. HAZOP with guide words can easily derive the relevant malfunction, reasonably foreseeable misuse and potential unintended system states.

After all hazardous events are identified, vehicle level risk must be evaluated and classified. For each hazard, evaluate the risk from following aspects:

- Severity (S0-S3): Injury level potential
- Exposure (E0-E4): Probability of occurrence
- Controllability (C0-C3): Ability to control

ASIL ratings are derived from S-E-C scores based on the classification in [Figure 2-2](#). Taking hazard H1 from [Table 2-3](#) as an example: unintended activation of the parking function causes sudden deceleration, leading to potential loss of stability and collisions (Severity: S3). Due to the high operational frequency of the EMB system, the exposure is rated E4. Because the driver cannot easily recover control of the vehicle during such an event, controllability is assigned C3. As a result, H1 is categorized as ASIL D

		Controllability C		
Severity S	Exposure E	C1 Simple	C2 Normal	C3 Difficult
S1 light and moderate injuries	E1 Very low	QM	QM	QM
	E2 Low	QM	QM	QM
	E3 Medium	QM	QM	ASIL A
	E4 High	QM	ASIL A	ASIL B
S2 severe and life threatening injuries	E1 Very low	QM	QM	QM
	E2 Low	QM	QM	ASIL A
	E3 Medium	QM	ASIL A	ASIL B
	E4 High	ASIL A	ASIL B	ASIL C
S3 Life-threatening injuries (survival uncertain)	E1 Very low	QM	QM	ASIL A
	E2 Low	QM	ASIL A	ASIL B
	E3 Medium	ASIL A	ASIL B	ASIL C
	E4 High	ASIL B	ASIL C	ASIL D

Figure 2-2. ASIL Determination List

Table 2-3. HARA Analysis for EMB

ID	Malfunction behavior	Potential vehicle level hazard	S	E	C	ASIL
H1	Unintended actuation of the EPB motor in the apply direction	Unintended actuate parking during vehicle normal operation can cause sudden braking and crash, damage to the body, chassis, and so forth	S3	E4	C3	D
H2	Unintended actuation of the EPB motor in the release direction	Unintended release parking when request enter park can cause roll away and crash other pedestrian and cars.	S2	E4	C3	C
H3	Fail to actuate the EPB motor in the apply direction	Cannot actuate parking when request enter park can cause roll away and crash other pedestrian and cars.	S2	E4	C2	B
H4	Fail to actuate the EPB motor in the release direction	The vehicle cannot start during normal drive-away operation.	S2	E4	C1	A
H5	Unintended actuation of braking motor in apply direction on driving mode	Unintended actuate braking during vehicle normal operation can cause sudden braking and crash, damage to the body, chassis, and so forth	S3	E4	C3	D
H6	Fail to actuate the braking motor in apply direction on driving mode	Cannot actuate braking during vehicle normal operation can cause collision with front vehicle or pedestrian.	S3	E4	C3	D
H7	Actuate braking motor in driving mode more than request	Actuate braking more than request during vehicle normal operation can cause sudden braking and crash.	S3	E4	C2-C3	D
H8	Actuate braking motor in driving mode less than request	Actuate braking less than request during vehicle normal operation can cause collision with front vehicle or pedestrian.	S3	E4	C2-C3	D

2.2.3 Safety Goal

With the HARA above, the safety goal of EMB can be derived as shown in [Table 2-4](#).

Table 2-4. EMB System Safety Goal

Safety Goal		ASIL	Safe State	FTTI
SG1	EMB system shall avoid unintended actuation of the EPB motor in the apply direction	D	Power off	100ms
SG2	EMB system shall avoid unintended actuation of the EPB motor in the release direction	C	Maintain parking state	100ms
SG3	EMB system shall not fail to actuate the EPB motor in the apply direction	B	Actuate redundancy parking motor	100ms
SG4	EMB system shall not fail to actuate the EPB motor in the release direction	A	Power off	100ms
SG5	EMB system shall avoid unintended actuation of braking motor in apply direction on driving mode	D	Power off and report to ECU	100ms
SG6	EMB system shall not fail to actuate the braking motor in apply direction on driving mode	D	Actuate redundancy braking motor	100ms
SG7	EMB system shall avoid inaccurate control braking motor actuation in driving mode	D	Actuate redundancy braking motor/ Power off	100ms

2.3 EMB Functional Safety Concept

2.3.1 Fail Tolerance Strategy

Meeting fail-operational requirements is a key challenge in transitioning from L2 to L3 autonomous driving. EMB, as a key concept for the intelligent drive system design, must be considered in terms of functional architecture with fail-operational.

4-wheel side EMB systems are located diagonally on the vehicle; that is, front left and rear right wheel side systems share the same ECU, as do the front right and rear left wheels, as shown in [Figure 2-3](#). Considering that the vehicle needs to keep balance on four wheels when braking, both EMB system must keep working. The diagonal EMB systems are designed redundant on the entire vehicle. Each system is developed in accordance with the safety goal described above. In addition, the redundant system design is considered on key function modules that affect the brake function output, like power and communication functions, and so forth. Backup modules can immediately take over if the primary fails, which allows the vehicle to continue to operate normally.

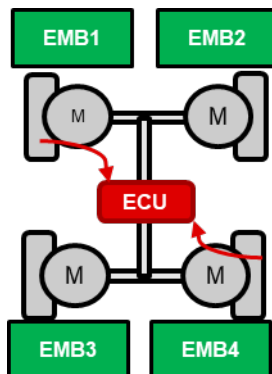


Figure 2-3. Diagonal Allocation of EMB

2.3.2 Functional Safety Concept

Figure 2-4 shows the basic system block diagram of the EMB system.

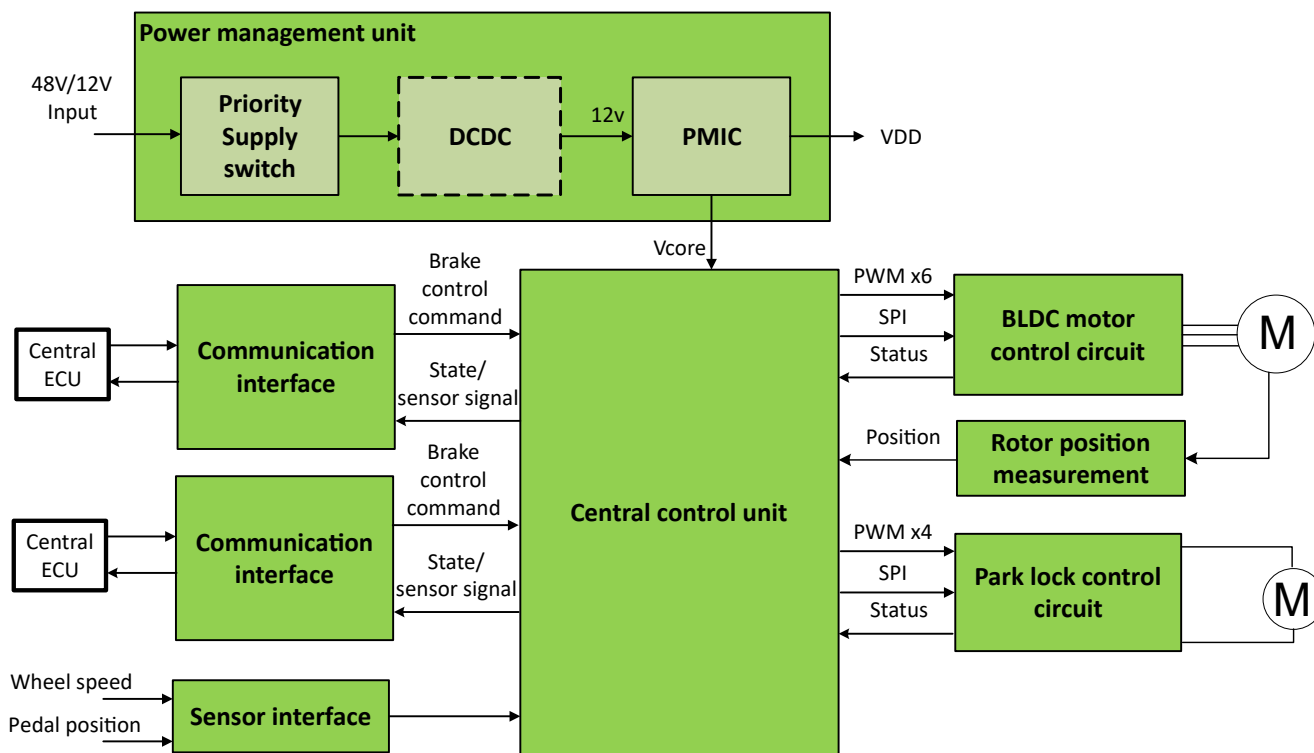


Figure 2-4. Basic System Structure for Wheel-Side EMB System

- Power management unit: Provide whole system power management function for different power output. If system is applied under 48V input, a DCDC must be considered in design.
- Central control unit: Provide central control unit function, including input sensor signals, running software for control algorithm, output PWM control signal, communicate with ECU
- Communication interface: Provide communication interface to receive braking command from other MCU/ECU, and report system status to ECU
- Actuator unit (BLDC/solenoid control circuit): Provide drive function to control motor running in the intended way to output brake/park function, support diversity system architectures
- Sensor interface: Provide system status measurement function for signal control

2.3.3 Functional Safety Requirements

This section identifies the functional safety requirement for each safety goal in Table 2-5 to Table 2-9. There can be multiple functional safety requirements for each safety goal and also, multiple safety goals can have

same functional safety requirement. Each functional safety requirement is derived considering the information like operating modes, fault tolerant time interval, safe state, emergency operation intervals and functional redundancies, and so forth.

Table 2-5. Power Management Function Safety Requirements

FSR ID	Functional safety requirement	ASIL	Safe state	FTTI	SG traced
FSR 1.1	EMB system shall avoid EMB motor voltage out of the maximum relative error of $\pm 10\%$.	D	Reset/switch off	10ms	SG6
FSR 1.2	EPB system shall avoid EPB motor voltage out of the maximum relative error of $\pm 10\%$.	D	Reset/switch off	10ms	SG2, SG3, SG4
FSR 1.3	EMB system shall avoid EMB supply voltage out of the maximum relative error of $\pm 10\%$.	D	Reset/switch off	10ms	SG5-SG7
FSR 1.4	EPB system shall avoid EPB supply voltage out of the maximum relative error of $\pm 10\%$.	D	Reset/switch off	10ms	SG1-SG4
FSR 1.5	The system shall detect and enter safe state within FTTI, without catastrophic failure of any devices	D	Reset/switch off	10ms	SG1-SG7
FSR 1.6	EMB/EPB system shall switch Vbat input when primary power rail fails	D	Switch to another Vbat	10ms	SG2, SG3, SG6
FSR 1.7	When first level safety mechanism fault happens, secondary level safety mechanism shall detect related faults and enter safe state within MPFDI	D	Report to uC	Driving cycle	SG1-SG7

Table 2-6. Central Controller Function Safety Requirement

FSR ID	Functional safety requirement	ASIL	Safe state	FTTI	SG traced
FSR 2.1	EMB system shall output braking control signal correctly.	D	Report to ECU/ drive actuator to inactive mode/reset	5ms	SG1-SG7
FSR 2.2	EPB system shall output parking control signal correctly.	D	Report to ECU/ drive actuator to inactive mode/reset	5ms	SG1-SG7
FSR 2.3	EMB/EPB system shall operating software correctly for control signal generating	D	Enter software process	5ms	SG1-SG7
FSR 2.4	The system shall detect and enter safe state within FTTI, without catastrophic failure of any devices	D	Report to ECU/ drive actuator to inactive mode/reset	5ms	SG1-SG7
FSR 2.5	When first level safety mechanism fault happens, secondary level safety mechanism shall detect related faults and enter safe state within MPFDI	D	Report to uC/ECU	Driving cycle	SG1-SG7

Table 2-7. Communication Functional Safety Requirement

FSR ID	Functional safety requirement	ASIL	Safe state	FTTI	SG traced
FSR 3.1	EMB system shall receive/transit message correctly.	QM(D)	Disable driving function and active braking torque	10ms	SG5-SG7
FSR 3.2	EPB system shall receive/transit message correctly.	QM(D)	Keep parking command	10ms	SG1-SG4
FSR 3.3	EMB/EPB system shall wake up by CAN communication correctly.	D	Enter ECU software process	10ms	SG2, SG3, SG6

Table 2-7. Communication Functional Safety Requirement (continued)

FSR ID	Functional safety requirement	ASIL	Safe state	FTTI	SG traced
FSR 3.4	The system shall detect and enter safe state within FTTI, without catastrophic failure of any devices	D(D)	Enter ECU software process	10ms	SG1-SG7
FSR 3.5	When first level safety mechanism fault happens, secondary level safety mechanism shall detect related faults and enter safe state within MPFDI	D	Report to uC	Driving cycle	SG1-SG7

Table 2-8. Driver and Actuator Functional Safety Requirement

FSR ID	Functional safety requirement	ASIL	Safe state	FTTI	SG traced
FSR 4.1	EMB system shall avoid unintended ON/OFF condition of each of the external gate driver. The system shall detect and enter safe state within FTTI	D	ASC, DRVOFF, cutoff output and brake control by backup system	5ms	SG5-SG7
FSR 4.2	EPB system shall avoid unintended ON/OFF condition of each of the external gate driver. The system shall detect and enter safe state within FTTI	D/B	Park control release Park control by backup system	10ms	SG1-SG4
FSR 4.3	EMB system shall avoid unintended deactivation of the safety switch	D	Report to uC	10ms	SG2, SG3
FSR 4.4	When first level safety mechanism fault happens, secondary level safety mechanism shall detect related faults and enter safe state within MPFDI	D	Report to uC	Driving cycle	SG1-SG7

Table 2-9. Sensor Interface Functional Safety Requirement

FSR ID	Functional safety requirement	ASIL	Safe state	FTTI	SG traced
FSR 5.1	EMB system shall correctly measure braking motor position for braking output control. The system shall detect and enter safe state within FTTI	D	Enter software process	10ms	SG6, SG7
FSR 5.2 (optional)	EMB system shall correctly input pedal position signal for braking output control. The system shall detect and enter safe state within FTTI	D	Enter software process	10ms	SG6, SG7
FSR 5.3	EMB system shall correctly measure wheel speed for braking output control. The system shall detect and enter safe state within FTTI	D	Enter software process	10ms	SG6, SG7
FSR 5.4	When first level safety mechanism fault happens, secondary level safety mechanism shall detect related faults and enter safe state within MPFDI	D	Report to uC	Driving cycle	SG1-SG7

3 Proposed Design for ASIL D EMB

3.1 EMB System Safety Design Architecture

On the basis of FSR proposed in last chapter, [Figure 3-1](#) shows the safety architecture of wheel side EMB.

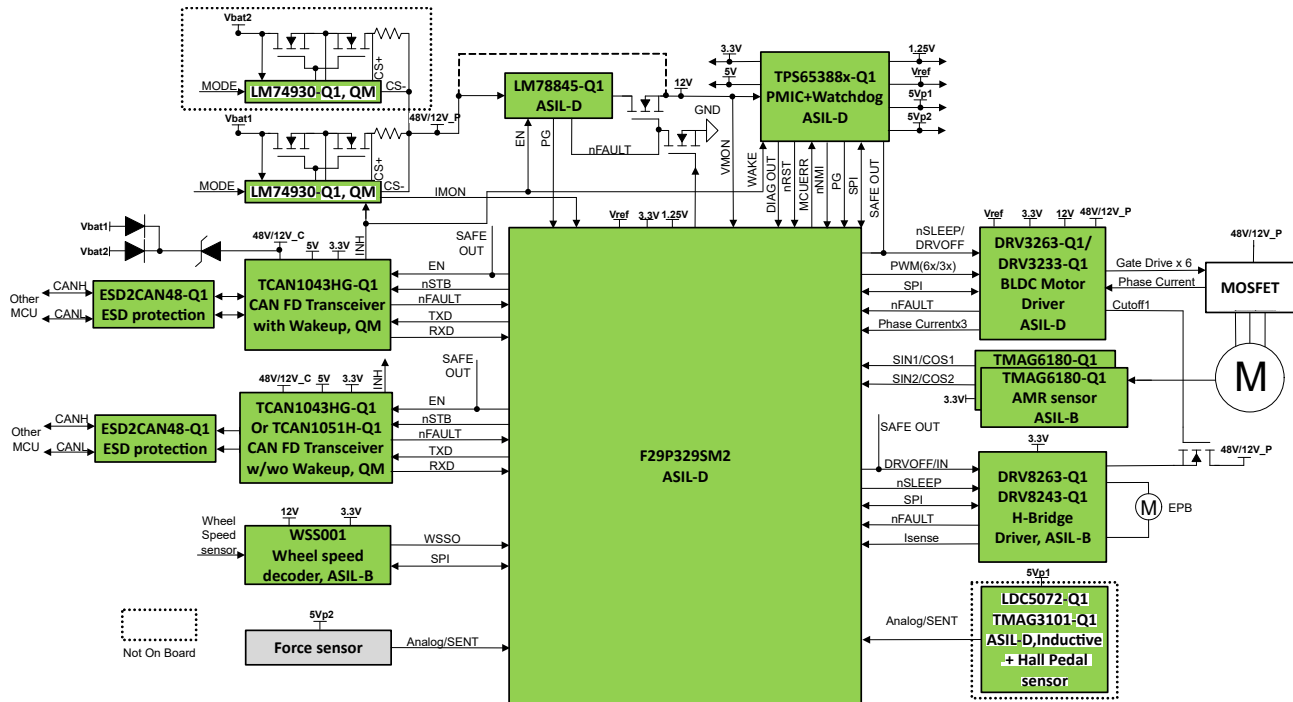


Figure 3-1. Wheel-Side EMB System Safety Design

For the PMU, an independent dual power input structure is adopted to meet the fail-operational strategy. The primary power input is controlled by the first ideal diode controller (LM74930-Q1), followed by the DCDC converter (LM78845-Q1), which steps down the 48V battery voltage to 12V. The PMIC (TPS653880-Q1) further distributes the regulated power to downstream components. In the event of a primary power input failure, the MCU enables the second ideal diode controller to switch to the secondary power path to provide continuous power supply.

For the central control unit, the MCU (F29P329SM2-Q1) serves as the core processor, responsible for braking the car by executing the braking motor algorithm, generating motor control signals, and managing system-level fault handling. The MCU communicates with the ECU via the CAN interface.

For the communication interface, dual CAN transceivers (TCAN1043HG-Q1) are employed to provide redundant communication paths. The primary CAN channel handles normal braking comm and reception and status reporting, while the secondary CAN channel serves as a backup to maintain communication integrity under fault conditions.

For the actuator unit, the gate driver (DRV3263-Q1/DRV3233-Q1) receives PWM signals from the MCU to drive the BLDC motor for braking force generation. The parking driver (DRV8263S-Q1) controls the solenoid lock for the EPB function. Both drivers are equipped with over-current, over-voltage, and under-voltage protections.

For the sensor interface, multiple sensors are integrated to provide real-time system status feedback. The magnetic angle sensor (TMAG6180-Q1) measures the motor rotor position, the wheel speed sensor monitors vehicle speed, WSS001-Q1 decode the wheel speed signal, and the pedal position sensor captures driver braking intent. All sensor signals are fed back to the MCU to close the control loop.

From the point of view of a customer application, we balance the chip safety capability, development complexity, price and other considerations, and then the following ASIL D compliant protocol is proposed. This functional safety reference design thus provides customers with a practical implementation guide for their applications.

3.2 Hardware Component

The following device information are collected from [TI.com](https://www.ti.com). Detailed resources can be referred from chip datasheet, safety manual, or other reference documents.

- **LM74930-Q1:** The LM74930-Q1 is an ideal diode controller that drives and controls external back-to-back N-Channel MOSFETs to emulate an ideal diode rectifier and power path. The LM74930-Q1 provides ON and OFF control over overcurrent and overvoltage protection. The controller can withstand high voltage transients due to its common source topology, and the wide input supply from 4V to 70V allows for the protection and control of 12V, 24V, and 48V automotive battery-powered ECUs.
- **LM78845-Q1:** The LM78845-Q1 is an 80V synchronous buck converter with hardware capability up to ASIL-D. This device supports high 80V rail current up to 4.5A output. The LM78845-Q1 is specifically intended for functional safety-relevant applications. The LM78845-Q1 integrates input/output voltage monitoring, current-limiting, thermal shutdown, redundant bandgap monitoring, redundant output voltage monitoring, redundant temperature sensor, and start-up diagnostics to support ASIL-D random and systematic capability, optimized for 48V battery-powered systems.
- **TPS653880-Q1:** The TPS653880-Q1 is a multi-rail power supply device designed for microcontrollers, sensors, transceivers, and peripherals in safety-relevant applications. This device is equipped with overvoltage, undervoltage, overcurrent protection, soft-start, output-load detection, and watchdog monitoring. Furthermore, the TPS653880-Q1 complies with ISO 26262 and is practical for ASIL D applications.
- **F29P329SM2-Q1:** The F29329SM2-Q1 is a high-performance C2000™ real-time microcontroller designed for automotive and industrial use. The F29329SM2-Q1 utilizes a common safety architecture implemented for multiple products. The F29329SM2-Q1 features a fixed-loop CPU running at 200MHz, 2MB of Flash, and 260KB of RAM, supporting 18 channels of PWM output and various ADCs. The device meets ISO 26262 and IEC61508 standards, providing compliance with safety requirements up to ASIL D/SIL3. With advanced functionalities and extensive connectivity, the F29329SM2-Q1 offers a comprehensive platform for EMB applications.
- **TCAN1043HG-Q1:** The TCAN1043HG-Q1 meets the specifications of the ISO 11898-2 (2016) High Speed controller area network (CAN) physical layer standard. This device provides CAN transceiver differential transmit capability to the bus and differential receive capability from the bus. The TCAN1043HG-Q1 includes multiple protection features to provide CAN bus robustness.
- **DRV3263-Q1:** The DRV3263-Q1 is an integrated smart gate driver for 48V automotive three-phase BLDC motors with support up to ASIL D. The device provides three half-bridge gate drivers, each capable of driving high-side and low-side N-channel MOSFETs to drive a 3-phase brake motor. A wide range of diagnostics and protection features are integrated into the DRV3263-Q1 to enable a robust motor drive system design and eliminate the need for external components.
- **DRV3233-Q1:** The DRV3233-Q1 is an integrated smart gate driver for 12V and 24V automotive three-phase BLDC motors with support up to ASIL D. The device provides three half-bridge gate drivers, each capable of driving high-side and low-side N-channel power MOSFETs to drive a 3-phase brake motor. Integrated diagnostics and protection features enable a robust motor drive system design and eliminate external component requirements.
- **DRV8263S-Q1:** The DRV8263S-Q1 is a wide-voltage, highly integrated H-bridge brushed driver for 24V and 48V automotive applications. The device offers voltage monitoring and load diagnostics, as well as protection against overcurrent and overtemperature, targeting ASIL B/ASIL D parking lock applications.
- **DRV8245-Q1:** The DRV8245-Q1 is a wide-voltage, highly integrated H-bridge brushed driver for 12V automotive applications. The device offers voltage monitoring and load diagnostics, along with protection against overcurrent and overtemperature, targeting ASIL B/ASIL D parking lock applications.
- **WSS001-Q1:** The WSS001-Q1 is a single-channel, ASIL B-targeted wheel-speed sensor interface IC designed for harsh automotive environments. The device supports five decoding modes for 2-Level and 3-Level AK protocol sensors, outputs speed signals through WSS0, and provides decoded results through SPI registers.
- **TMAG6180-Q1:** The TMAG6180-Q1 is an ASIL B AMR-based high-precision angle sensor with integrated signal conditioning. The device provides differential sine/cosine analog outputs and dual Hall sensor outputs (X/Y axes) for full 360° angle measurement.

3.3 Safety Mechanism Design

The safety mechanism is to specify the response of the system or elements to stimuli that affect the achievement of the safety goals. This includes failures and relevant combinations of stimuli in combination with each relevant operating mode and defined system states. In the following section, a system-level safety analysis is performed for each function to show how to propose the safety mechanism for safety design.

In this design, all failure modes of each functional circuit block have been comprehensively considered and incorporated safety mechanisms to address. The failure modes considered in FMEA are from ISO 26262, or "devices' FMEDA", or "devices' Functional Safety FIT Rate, FMD and Pin FMA". These analyses make sure that each functional unit can achieve the ASIL target.

3.3.1 Power Management Safety Design

Figure 3-2 shows the power management safety design.

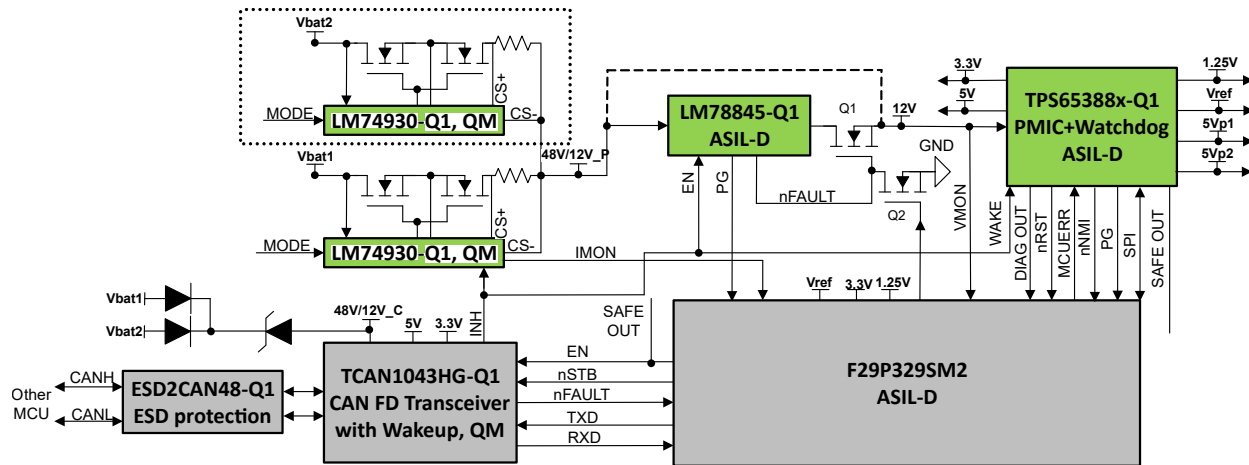


Figure 3-2. Power Management Safety Design Architecture

3.3.1.1 Ideal Diode Safety Analysis

LM74930-Q1 is a functional safety-capable device in TI. Figure 3-3 shows the structure of the LM74930-Q1. The LM74930-Q1 has a simple structure, with only several states and comparators inside. All failure modes are known and limited, and the LM74930-Q1 can be claimed as a class I device according to ISO 26262:8-13 Evaluation of hardware elements. Integrators can use this device into system design directly.



Table 3-1. Power Management System Level FMEA for Ideal Diode

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
DGATE output functional, not in specification voltage or timing	Cannot enable/disable VOUT output or within expected speed, brakes not timely	Single point fault (SPF)	SM_ideal diode_switch over SM_ideal diode_internal VMON SM_ideal diode_external VMON SM_ideal diode_DCDC MON	FSR 1.1 FSR 1.2 FSR 1.3 FSR 1.4 FSR 1.6
DGATE stuck at high	Loss of reverse battery protection	Multiple point fault (MPF)	Considered inside BMS	FSR 1.5 FSR 1.7
DGATE stuck at low	Cannot output power supply for EMB system, loss of brakes function	SPF	SM_ideal diode_switch over SM_ideal diode_internal VMON SM_ideal diode_external VMON SM_ideal diode_DCDC MON	FSR 1.1 FSR 1.2 FSR 1.3 FSR 1.4 FSR 1.5 FSR 1.6
HGATE output functional, not in specification voltage or timing	Cannot enable/disable voltage input or within expected speed, brakes not timely	SPF	SM_ideal diode_switch over SM_ideal diode_internal VMON SM_ideal diode_external VMON SM_ideal diode_DCDC MON	FSR 1.1 FSR 1.2 FSR 1.3 FSR 1.4 FSR 1.6
HGATE stuck at high	EMB system power always on, increase power consumption	Safe fault (SF)	NA	NA

Table 3-1. Power Management System Level FMEA for Ideal Diode (continued)

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
HGATE stuck at low	Cannot output power supply for EMB system, loss of brakes function	SPF	SM_ideal diode_switch over SM_ideal diode_internal VMON SM_ideal diode_external VMON SM_ideal diode_DCDC MON	FSR 1.1 FSR 1.2 FSR 1.3 FSR 1.4 FSR 1.5 FSR 1.6
IMON not in specification - current or timing	Overcurrent reported while no overcurrent, system unintended enter safe state	SF	NA	NA
Overcurrent protection fails to trip or false trip	When overcurrent happens, EMB loss protection	MPF	SM_ideal diode_OCD	FSR 1.5 FSR 1.7
UVLO, OV fails to trip or false trip	When VOUT OV/UV happens, EMB loss protection	MPF	SM_ideal diode_external VMON SM_ideal diode_power-on test SM_ideal diode_DCDC MON	FSR 1.3 FSR 1.4 FSR 1.5 FSR 1.7
Pin-to-pin short	Loss of pin function	SPF	Designed according to Pin FMEA	FSR 1.5

SM_ideal diode_switch over: During power on stage, after first CAN bus receive a wake-up signal, TCAN trigger INH to H for 300ms to enable ideal diode. If ideal diode cannot be enabled or other power rail failure occurs, 1.25V and 3.3V cannot be set up, MCU cannot power up and no nSTB signal is triggered to H to keep continuous INH to high.

During operating, any one of the following shall also initiate switch over:

- The PG pin of LM78845-Q1 asserts low, indicating that the 12V_P rail voltage has fallen outside the normal operating range
- The MCU CMPSS module detects that 48V_P or 12V_P has exceeded the configured threshold (for example, OV > 13.2V or UV < 10.8V for the 12V rail)
- The MCU detects that the primary rail voltage has deviated from the rated value by more than $\pm 5\%$ for three consecutive monitoring cycles (total duration < 10ms)

If ECU detected no communication is built with MCU with the first rail Vbat, it activates the secondary power path by second CAN bus with same sequence. After switchover, the MCU reports the power path switching event to the ECU through CAN message.

SM_ideal diode_internal VMON: LM74930-Q1 provide internal OV/UVLO protection. Using resistor ladder to configure the OV/UV threshold for VOUT monitor. After detect over-threshold matters, disable DGATE output by internal fault logic.

SM_ideal diode_external VMON: LM74930-Q1 VOUT is divided and captured by the CMPSS module inside MCU for monitoring. The threshold can be configured inside CMPSS. If the CMPSS module detects an OV/UV fault, it immediately pulls nSTB low, putting the TCAN1043HG-Q1 into Sleep mode and turns INH_CAN low to disable DGATE output by internal fault logic.

SM_ideal diode_OCD: The voltage across Rsense outside LM74930-Q1 is redundant sampled by MCU ADC. If detected the overcurrent event kept time over OCP delay time inside LM74930-Q1, MCU pulls nSTB low, putting the TCAN1043HG-Q1 into Sleep mode and turns INH_CAN to low to disable LM74930-Q1 output by internal fault logic.

SM_ideal diode_power-on test: After power-on, MCU trigger a power-on test to switch-off for ideal diode. CMPSS detect whether the output voltage is reduced. Once the voltage drop is detected, switched on the ideal diode immediately. If cannot detect the voltage drop, the fault on the OV/UV monitor is detected.

SM_ideal diode_DCDC MON: The 48/12V_P from the LM74930-Q1 controlled output goes to LM78845-Q1. LM78845-Q1 is an ASIL D DCDC with VIN UVLO detection built in, which can be used to detect the unexpected switch off of ideal diode. When the voltage on the VIN pin drops below 2.5V (typical), the device goes into shutdown mode and the PG pin asserts low. MCU will reset after receiving PG low signal.

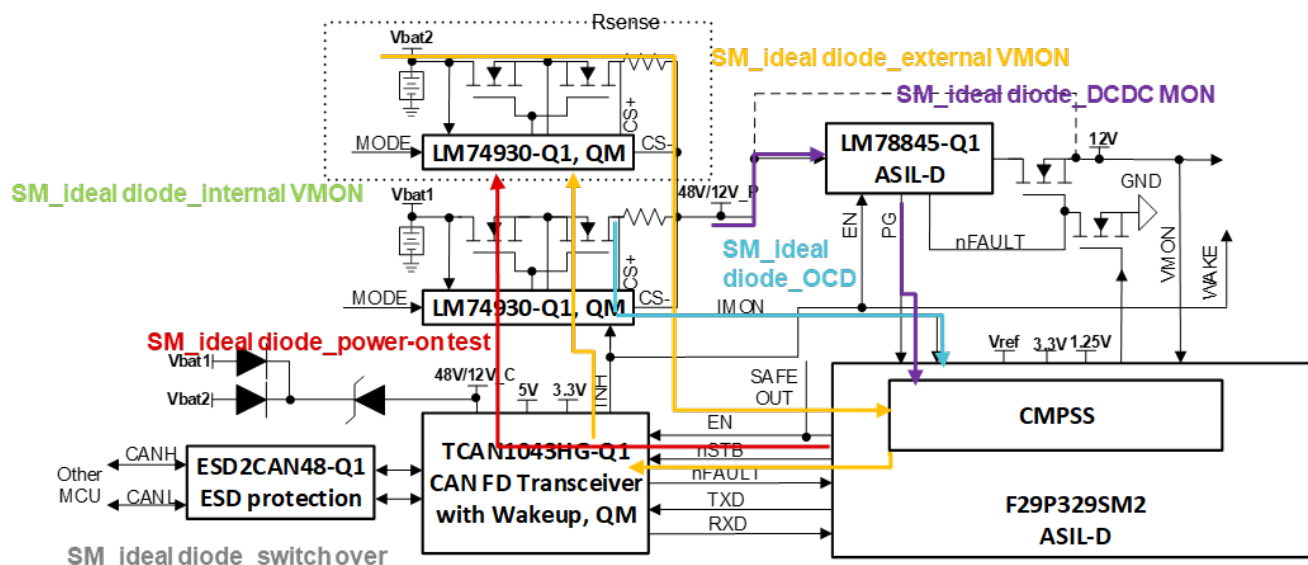


Figure 3-4. Safety Mechanism Design Of Ideal Diode

3.3.1.2 DCDC safety analysis

LM78845-Q1 is applied only for 48V application. For 12V rails, the DCDC does not need to be considered in the system. Figure 3-5 shows the structure of LM78845-Q1. LM78845-Q1 is developed as the SEooC (safety element out of context), target for ASIL D end equipment. Thus, when designing the EMB system, it is only necessary to meet the SA (system assumption) in design specified in the *LM78845-Q1 Safety Manual 4.4 Functional Safety Constraints and Assumptions*.

To meet system assumption, an external MOSFET shall be added to transit system to safe state after receiving nFAULT or PG indication. Other SA are related to operating conditions, shall also be met according to datasheet.

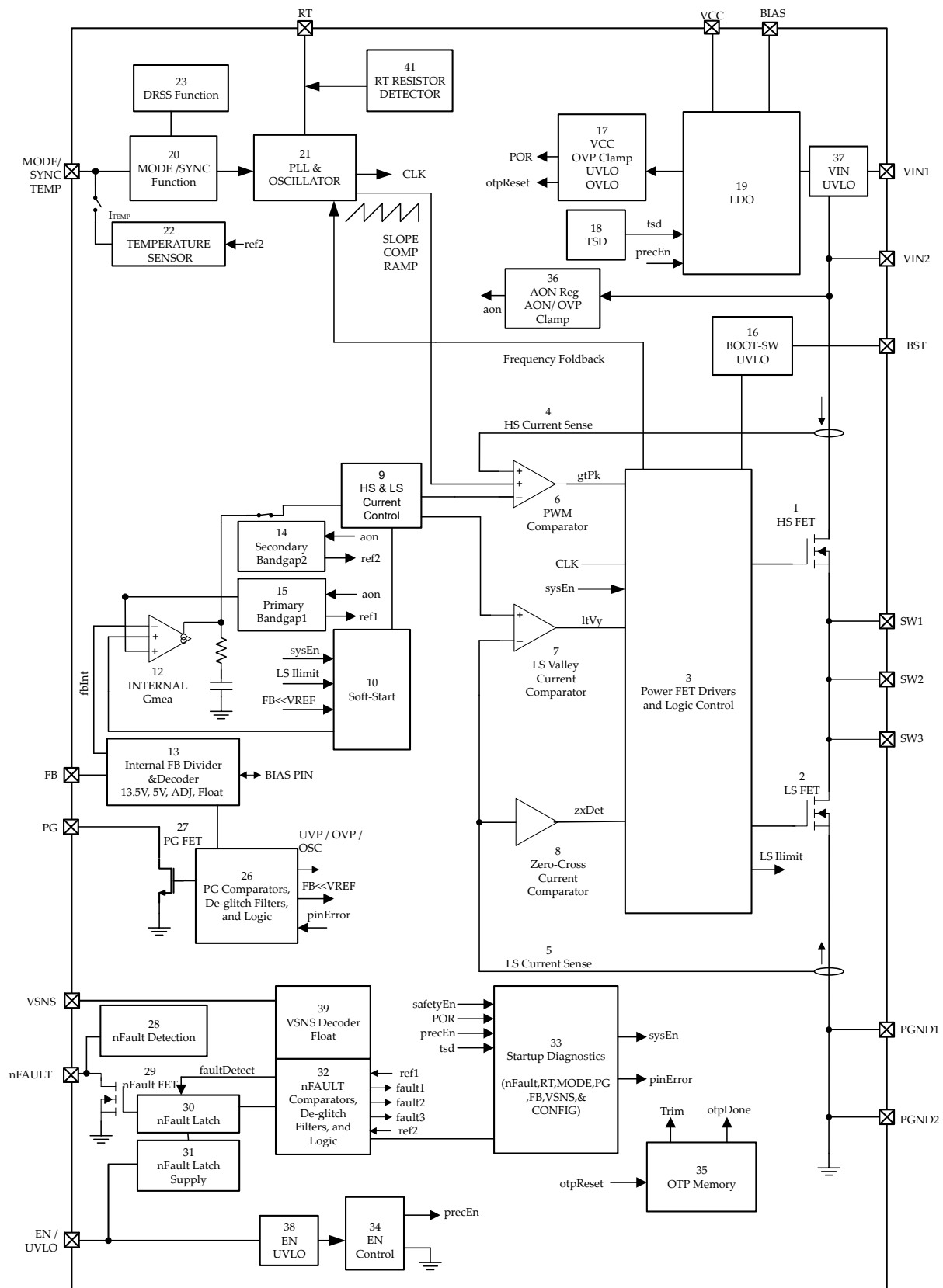


Figure 3-5. LM78845-Q1 Structure

Table 3-2 shows the safety analysis and safety mechanisms proposed for the DCDC application.

Table 3-2. Power Management System Level FMEA for DCDC

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Failure in the supply voltage to the PMIC	Cannot generate 12V output within expected range, brakes not timely	SPF	SM_DCDC_fault indication ⁽¹⁾ SM_DCDC_external VMON SM_ideal diode_switch over	FSR 1.1 FSR 1.3 FSR 1.5
Failure in input supply voltage to the LM78845-Q1	Cannot generate 12V output within expected range, loss of brakes function	SPF	SM_DCDC_fault indication ⁽¹⁾ SM_DCDC_external VMON	FSR 1.1 FSR 1.3 FSR 1.5
Disconnect Switch (Q1) short	Cannot cutoff MOSFET when DCDC output nFault signal	MPF	SM_DCDC_power-on test	FSR 1.5 FSR 1.7
Disconnect Switch (Q1) open	Cannot generate 12V output for EMB system	SPF	SM_DCDC_fault indication ⁽¹⁾ SM_DCDC_external VMON	FSR 1.1 FSR 1.3 FSR 1.5
Test Switch (Q2) short	1 st MOSFET open, system unintended enter safe state	SF	NA	NA
Test Switch (Q2) open	Cannot test 1 st MOSFET at power on stage	SF	NA	NA

(1) Refer to the FMEDA and safety manual of the LM78845-Q1

SM_DCDC_fault indication: When DCDC detect an internal fault, LM78845-Q1 nFAULT pin is latched low and external MOSFET will be switched off.

SM_DCDC_external VMON: LM78845-Q1 VOUT is divided and captured by the CMPSS module inside MCU for monitoring. The threshold can be configured inside CMPSS. The PMIC input can stand 36V maximum. Thus, overvoltage and undervoltage thresholds are set at expected DCDC deviation from the rated voltage respectively. If the CMPSS module detects an OV/UV fault, it immediately pulls nSTB low, putting the TCAN1043HG-Q1 into Sleep mode and turns INH CAN low to disable ideal diode output by internal fault logic.

SM_DCDC_power-on test: After power-on, MCU finish initialization and PMIC rails stable check. Then MCU trigger a power-on test to open Q1 and keep the window duration of 1ms. CMPSS monitors whether the DCDC output voltage drops by more than 10% of the nominal value. Once the voltage drop is detected within time window, immediately restore MOSFET conduction. If cannot detect the voltage drop, MCU restores MOSFET conduction, reports fault and enters safe state.

Note

The PMIC input capacitor shall maintain the downstream load voltage within the test window.

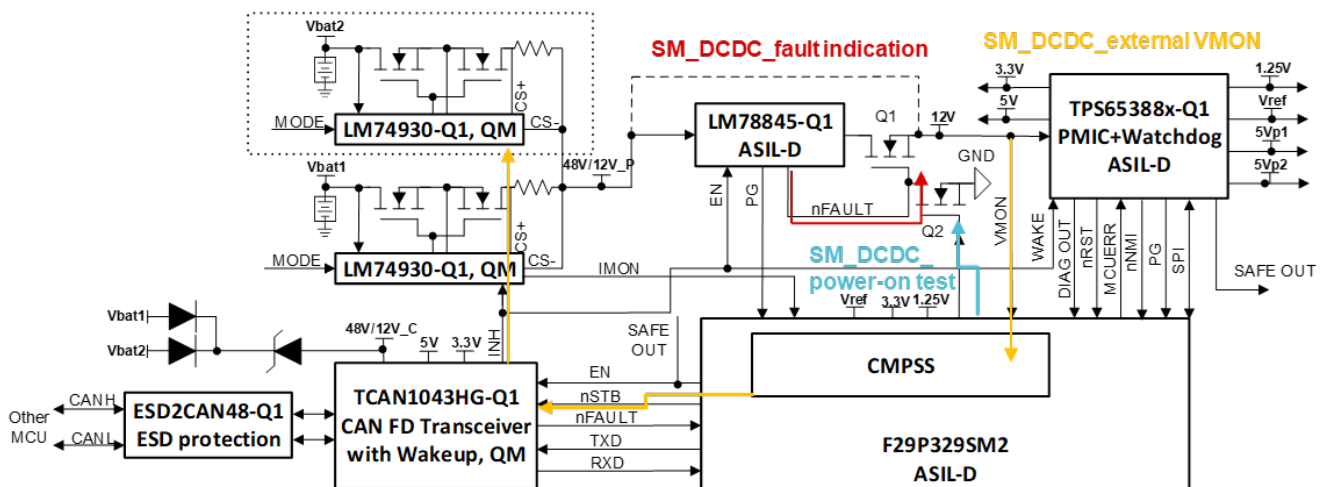


Figure 3-6. Safety Mechanism Design of DCDC

3.3.1.3 PMIC Safety Analysis

TPS653880-Q1 is developed as the safety element out of context (SEooC), target for ASIL D appliance. [Figure 3-7](#) shows the functions and safety mechanisms embedded in this PMIC. When designing the EMB system, it is only necessary to meet the assumption of use (AoU) specified in the *TPS653880-Q1 Safety Manual* in 4.4 *Functional Safety Constraints and Assumptions*.

- To meet system assumption, the safe state of PMIC is considered as disable supply rails to MCU, reset MCU. After receiving GPIOx.nINT, application software checks the fault status and control PMIC and other system part enter safe state.
- E2E™ protection is considered between PMIC and MCU, including CRC, timeout, rolling counter, and so forth, on the safety-related transmission data. When a transceiver has a hardware failure (such as drive failure, parasitic short circuit, and so forth), these errors are reflected at the protocol layer as checksum errors, frame loss, timeout, and so forth, which are captured by MCU and respond safely accordingly.
- After power on, application software shall check the Device ID, Revision, NVM ID with TRIM reference value. If not consist control PMIC and other system part enter safe state.
- MCU application software configure external WDT and ESM timeout threshold, post-reaction, detection protocol, and so forth to PMIC after power on.
- ABIST and LBIST are operated once upon power on. Before enable ABIST/LBIST, check all interrupt event has been cleared. After finish ABIST/LBIST, MCU checks the fault status and control PMIC and other system part enter safe state.
- The application software shall meet above safety requirements. MCU shall trigger an ESM failure signal after power on. Before finish activate, lock any input to configuration register. All configuration registers are protected by CRC. MCU shall finish check within every FTTI.
- Pull-down resistors are added to nRST, Nint, SAFE_OUT pin.
- The SAFE_OUT of PMIC is output to braking and parking motor driving unit, communication interface independently to prevent a single point fault for MCU from causing GDU cannot enter a safe state. After PMIC receive MCU_ERRORSTS, MCU cannot enter post reaction to its failure, PMIC outputs SAFE_OUT to GDUs DRVOFF/ASC/CUTOFF input due to different application requirements.
- The reverse-supply connection is protected by LM74930-Q1, the input-supply, overvoltage, transient protection is implemented by LM78845-Q1. The capacitor on PMIC VIN can protect from transient spike. Every LDO and PLDO output has added redundant protection capacitors.
- Other AoUs are related to operating conditions, and shall also be met according to the datasheet.

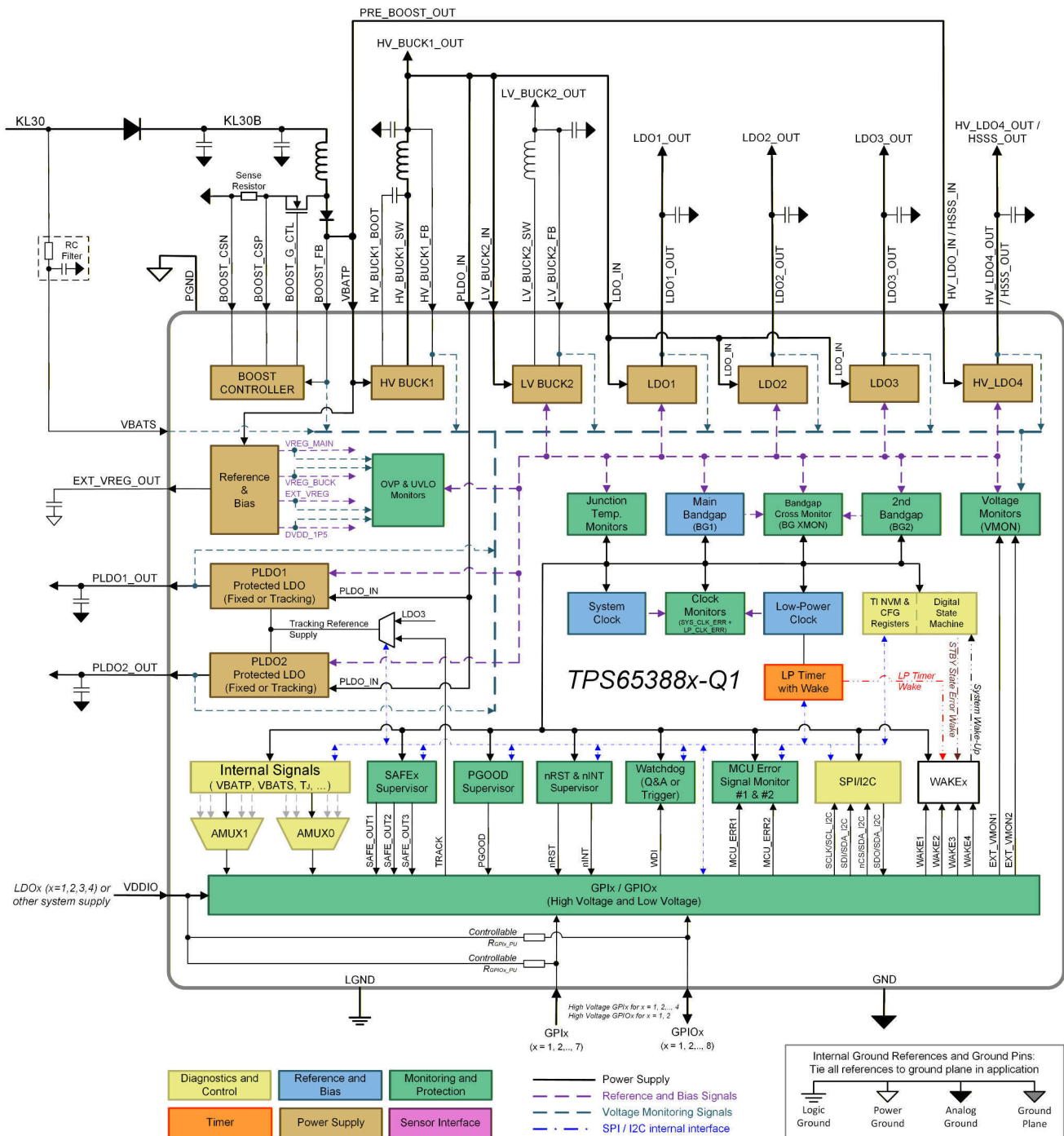


Figure 3-7. TPS653880-Q1 Structure

Table 3-3 shows the safety analysis and safety mechanisms proposed for the PMIC application.

Table 3-3. Power Management System-Level FMEA for PMIC

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Safety MCU supply rails related failure modes	Cannot generate 1.25V and 3.3V output within expected range, loss of brakes function	SPF	SM_PMIC_MCU VMON ⁽¹⁾ SM_ideal diode_switch over	FSR 1.3 FSR 1.4 FSR 1.5 FSR 1.6

Table 3-3. Power Management System-Level FMEA for PMIC (continued)

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Module input supply rail-related failure modes	Cannot generate all power outputs within expected range, loss of brakes function	SPF	SM_PMIC_MCU VMON ⁽¹⁾ SM_ideal diode_switch over	FSR 1.3 FSR 1.4 FSR 1.5 FSR 1.6
Sensor supply rail-related failure modes	Cannot generate 3.3V output within expected range, loss of brakes function	SPF	SM_PMIC_power rail VMON ⁽¹⁾ SM_ideal diode_switch over	FSR 1.3 FSR 1.4 FSR 5.1 FSR 5.4
Safety MCU software or hardware execution-related failure modes	Cannot monitor MCU serious software and hardware failure, do not generate reset signal	MPF	SM_PMIC_power-on test ⁽¹⁾ SM_PMIC_external WDT SM_PMIC_ESM MON	FSR 2.3 FSR 2.4 FSR 2.5 FSR 1.7
Watchdog timeout not triggered	MCU software deadlock undetected	MPF	SM_PMIC_external WDT	FSR 2.3 FSR 2.5
ESM monitoring failure	MCU hardware error not reported	MPF	SM_PMIC_ESM MON	FSR 2.4 FSR 2.5

(1) Refer to the FMEDA and safety manual of TPS653880-Q1

SM_PMIC_MCU VMON: PMIC embedded with input/output UV/OV monitor mechanisms. The abnormal status can be indicated by GPIOx.PGOOD. If multiple MCU power rail exceed programmed threshold, drive GPIOx.nRST to reset MCU. drive GPIOx.SAFE_OUTx to turn off external actuator and communication interface, putting the TCAN1043HG-Q1 into Sleep mode.

SM_PMIC_power rail VMON: PMIC embedded with input/output UV/OV monitor mechanisms. After detect the failure, the abnormal status can be indicated by GPIOx.PGOOD. Drive GPIOx.nINT to MCU for CPU to check fault reasons. Software decide to drive sensors, actuators and communication interface into safe state.

SM_PMIC_power-on test: PMIC activate internal LBIST/ABIST during power up.

SM_PMIC_external WDT: PMIC embedded watchdog supervises the correct operation of the safety MCU hardware and software execution. It has two operating modes:

- Question and Answer (Q&A) Mode
- Trigger Mode

The Q&A Mode uses the SPI to receive the safety MCU watchdog service responses. In Trigger Mode, the MCU applies a pulse signal with a minimum pulse width of t_{WD_PULSE} on the GPI1.WD_IN pin, or GPI4.WD_IN pin, to send the required watchdog trigger.

SM_PMIC_ESM MON: PMIC uses GPI1.ESM_IN input pin to receive the error-signal from the safety MCU. Supervises the correct operation of the safety MCU hardware according to the user-configurable level-mode or PWM-mode.

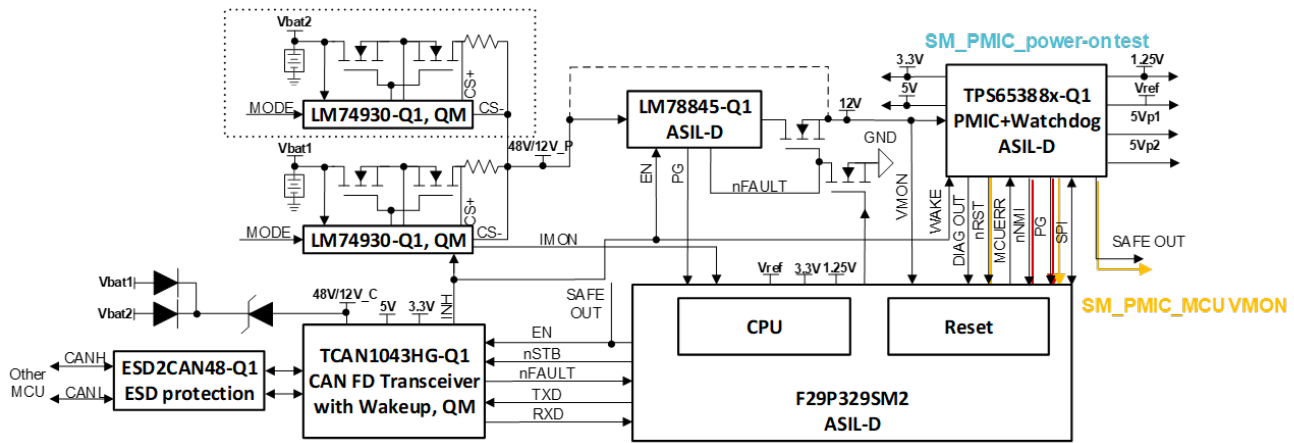


Figure 3-8. Safety Mechanism Design of PMIC

3.3.2 Central Controller Safety Design

F29P329SM2-Q1 is developed as the SEooC, target for ASIL D application. Figure 3-9 shows the functions and safety mechanisms embedded in this MCU. To meet FSR of EMB system, the following requirements (assumed safety requirements in F29P329SM2-Q1 Safety Manual) (at a minimum) must be implemented using external components:

- External voltage monitors to supervise the power supply provided to the MCU

TPS653880-Q1 support voltage OV/UV monitor for output supply and a VMON pin supports input MCU voltage rail monitoring.

- External watchdog timer that can be used for diagnostic purposes

There is an external watchdog embedded in TPS653880-Q1, supporting window watchdog and Q&A mode configuration.

- Components required for taking the system to safe state as per the safe state defined in MCU Safe State.

When HW/SW failure occurs, safety mechanism support put MCU into safe state into one of the following states:

- MCU can trigger ERRORSTS pin output. After receiving this signal, PMIC send nRST signal to MCU, MCU reset can be asserted.
- When PMIC detect there is a failure on the power supply of the MCU, the LDO/BUCK output is disabled.
- The external system is informed using one of the I/O pins of the MCU (for example, ERRORSTS pin is asserted).
- The output of the MCU driving the actuator is forced to inactive mode (for example, the GPIO pins corresponding to the mission function is in a tri-state condition).

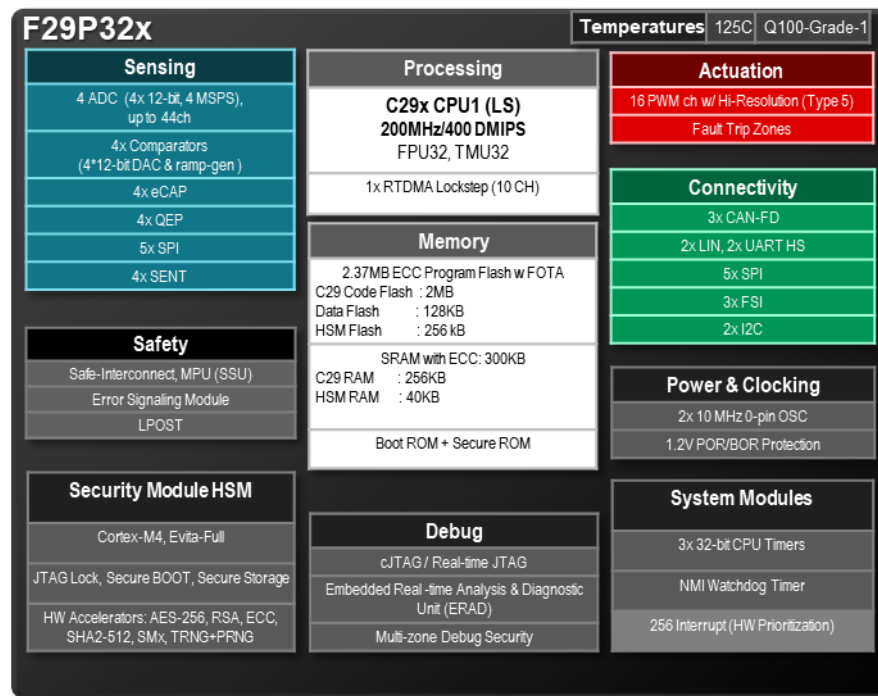


Figure 3-9. F29P329SM2-Q1 Structure

Table 3-4 shows the safety analysis and safety mechanisms proposed for the MCU application.

Table 3-4. Central Controller System Level FMEA for F29P329SM2-Q1

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Processing Units related failure modes	Cannot or incorrect perform software for braking/parking motor control PWM output	SPF	SM_PMIC_external WDT SM_PMIC_ESM MON SM_MCU_ESM signal ⁽¹⁾ SM_MCU_internal MON SM_MCU_SW CHECK	FSR 2.1 FSR 2.2 FSR 2.3 FSR 2.4
Interconnect related failure modes	Cannot or incorrect perform software for braking/parking motor control PWM output	SPF	SM_PMIC_external WDT SM_PMIC_ESM MON SM_MCU_ESM signal ⁽¹⁾ SM_MCU_internal MON SM_MCU_SW CHECK	FSR 2.1 FSR 2.2 FSR 2.3 FSR 2.4
Memories related failure modes	Cannot or incorrect perform software for braking/parking motor control PWM output	SPF	SM_PMIC_external WDT SM_PMIC_ESM MON SM_MCU_ESM signal ⁽¹⁾ SM_MCU_internal MON SM_MCU_SW CHECK	FSR 2.1 FSR 2.2 FSR 2.3 FSR 2.4
Clock and Power related failure modes	Cannot or incorrect perform software for braking/parking motor control PWM output	SPF	SM_PMIC_MCU VMON SM_PMIC_external WDT SM_PMIC_ESM MON SM_MCU_ESM signal ⁽¹⁾ SM_MCU_internal MON SM_MCU_SW CHECK	FSR 1.3 FSR 1.4 FSR 2.1 FSR 2.2 FSR 2.3 FSR 2.4
SM_DCDC_external VMON related failure modes (CMPSS, GPIO, XBAR)	Cannot monitor DCDC output failure, cannot enter safe state	MPF	SM_PMIC_ESM MON SM_MCU_ESM signal ⁽¹⁾ SM_MCU_internal MON SM_MCU_SW CHECK	FSR 1.1 FSR 1.2 FSR 1.3 FSR 1.4 FSR 1.5

Table 3-4. Central Controller System Level FMEA for F29P329SM2-Q1 (continued)

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
PWM generation related failure modes	Cannot output PWM to gate driver for motor control, which lead to loss of torque control	SPF	SM_PMIC_ESM MON SM_MCU_ESM signal ⁽¹⁾ SM_MCU_internal MON SM_MCU_SW CHECK	FSR 2.1 FSR 2.2 FSR 2.4 FSR 4.1 FSR 4.2
Interface related failures (ADC, GPIO, and so forth)	Cannot provide motor position, wheel speed, pedal position, state to uC	SPF	SM_PMIC_ESM MON SM_MCU_ESM signal ⁽¹⁾ SM_MCU_internal MON SM_MCU_SW CHECK	FSR 2.1-FSR 2.4 FSR 5.1- FSR 5.4
Safety mechanism related failures	Cannot monitor MCU software and hardware failure, cannot enter safe state	MPF	SM_MCU_internal MON SM_MCU_SW CHECK	FSR 1.7 FSR 2.5

(1) Refer to the FMEDA and safety manual of F29P329SM2-Q1

SM_MCU_ESM signal: Error Signaling Module (ESM) inside MCU can drive an ERRORSTS signal output to PMIC. Signals external agents when internal chip errors occur. It continuously outputs through a selected GPIO pin, remaining high by default and going low when an error is detected, staying low until the corresponding error status flag is cleared.

SM_MCU_internal MON: The F29P329SM2-Q1 embeds internal safety mechanisms for HW/SW failure detection. Upon detecting a failure, the MCU shall enter a safe state as defined in the system assumptions. The embedded mechanisms shall support, but are not limited to, the following:

- **SM_MCU_CPU lockstep:** Hardware Redundancy implemented by lockstep architecture (two hardware modules executing the same function and the output of the hardware modules are continuously compared) is a proven method for achieving high diagnostic coverage for both permanent and transient faults. Lockstep Compare Module (LCM) is used to implement lockstep compare functionality and indicate an error.
- **SM_MCU_SSU protection:** The SSU (Security and Safety Unit) of the F29P32 is a runtime firewall between the C29x CPU and memory/peripherals, enforcing user access protection policies on every CPU access. It provides 64 memory access protection ranges per CPU with context-sensitive memory and peripheral protection, and supports up to 15 user LINKs and 7 stack pointers per CPU to enable hardware-level code isolation and multi-safety-island execution management.
- **SM_MCU_watchdog monitor:** The internal watchdog supports two modes: normal watchdog (WD) and windowed watchdog (WWD), with only one mode selectable at a time. The WD is a traditional single-threshold watchdog where the user programs a timeout value and must provide a correct WDKEY before expiration; an incorrect WDKEY or timeout triggers an error response, issuing either a warm system reset or a CPU maskable interrupt.
- **SM_MCU_Flash ECC check:** The on-chip flash memory employs SECDED with an 8-bit ECC code word protecting 64-bit data and its address. ECC decoding is performed on every read operation; uncorrectable errors trigger an NMI and assert the ERRORSTS pin, while the corrupted address is logged in the error aggregator registers.
- **SM_MCU_SRAM ECC check:** All SRAMs are ECC-protected, with ECC calculated on a combination of data and address (no separate address ECC). Every 32 bits of RAM data is protected by 7 ECC bits. For sub-32-bit write accesses, the memory controller (MEMSS) performs a read-modify-write operation and generates ECC locally.
- **SM_MCU_BUS signal check:** To cover network elements outside the MCU (wiring, connectors, transceivers), end-to-end safety mechanisms are applied. Common schemes include message checksums, redundant transmissions, and time diversity. Checksums, sequence counters, and timestamps are appended to the payload alongside protocol-level parity, allowing software at both ends to validate the full communication path.
- **SM_MCU_clock frequency check:** DCC validates the PLL output frequency (PLLRAWCLK) within a defined time window, using INTOSC1, INTOSC2, or XTAL as a reference clock. If the PLL frequency deviation exceeds a predefined threshold, DCC asserts an ERROR status flag and notifies the ESM to take appropriate action.

- **SM_MCU_GPIO/XBAR/PWM/CMPSS/CLB/GPIO/ADC redundancy:** Redundancy via multichannel parallel outputs (with internal/external comparators) or input comparison/voting, making sure a single input/output failure does not cause a dangerous state. When servicing redundancy conditions (for example, two sources tripping PWM), always read back status flags to verify both sources are active, providing latent fault coverage.
- **SM_Power On Self-Test:** LPOST performs transistor-level self-testing at startup using on-chip DFT structures, triggered by BootROM based on SECCFG configuration, and requires application code to check and act on its execution status after boot.

SM_MCU_SW CHECK: E-GAS Level 2 Functional Monitoring is applied to address software-level errors:

- An independent monitoring software task verifies the output of the primary control software via a characteristic value check (for example, per-cycle checksum of key output variables).
- The monitoring task executes in a dedicated time slot, isolated from the primary control task.
- Wheel speed and braking torque plausibility checks at the ECU level provide a system-level safeguard against undetected software errors in the wheel-side MCU.

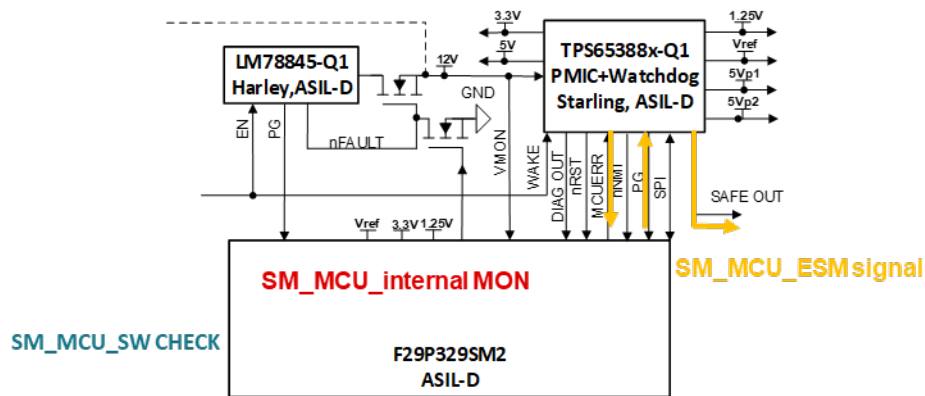


Figure 3-10. Safety Mechanism Design Of Central Controller

3.3.3 Communication Interface Safety Design

TCAN1043HG-Q1 is a functional safety-capable device in TI. Figure 3-11 shows the structure of the TCAN1043HG-Q1. The safety design for communication interface follows ASIL decomposition principle. All failures on the transceiver lead to a communication error is checked by end-to-end mechanism. To achieve an ASIL D target, the check software shall develop as ASIL D and cover all failures on CAN communication. A QM CAN transceiver IC can be selected. To achieve a robust communication, the transceiver shall support fail-safe features that prevents sending data to bus when TXD timeout, RXD short, overtemperature, and so forth. Local failure diagnostics can be implemented by specifically designed output pins for status indication.

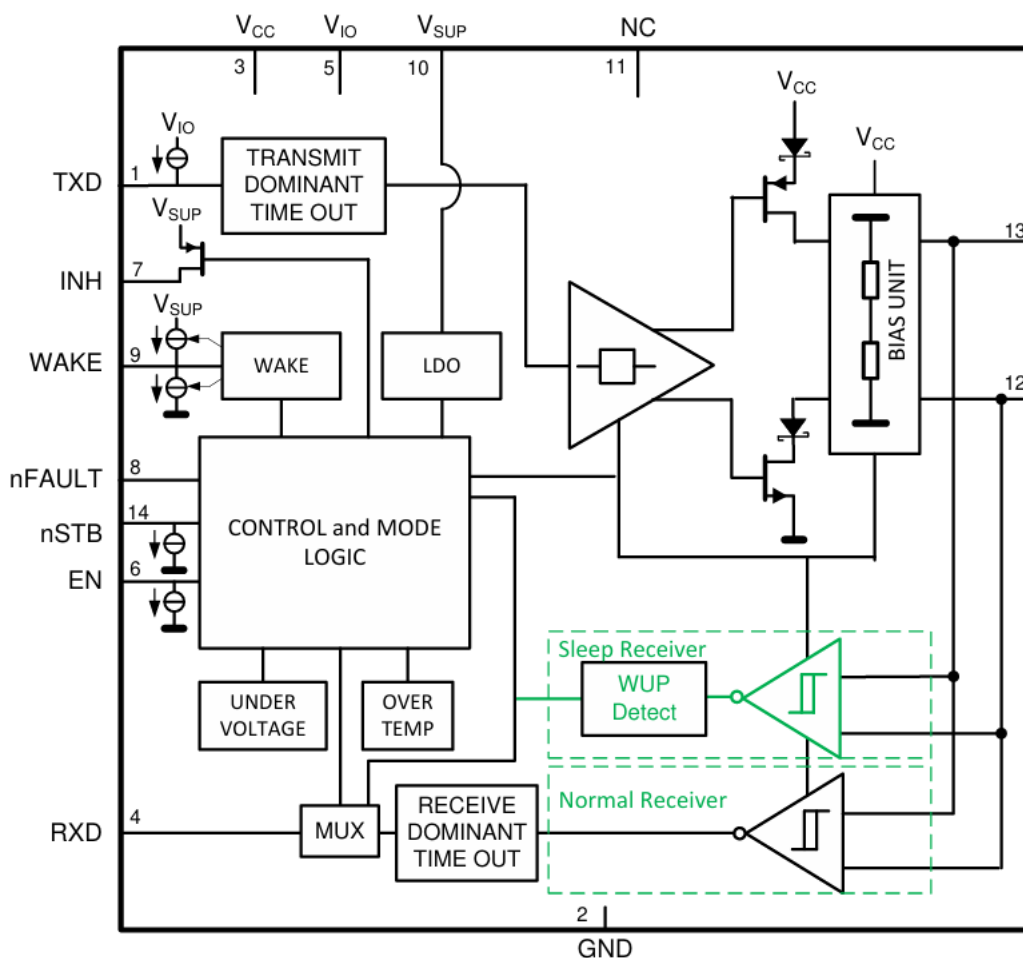


Figure 3-11. TCAN1043HG-Q1 Structure

Table 3-5 shows the safety analysis and safety mechanisms proposed for the ideal diode application.

Table 3-5. System Level FMEA for Communication Interface

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Receiver fail	Cannot receive ECU data, communication fails lead to cannot perform braking control	SPF	SM_TCAN_E2E CHECK SM_TCAN_switch over	FSR 3.1 FSR 3.2 FSR 3.4
Transmitter fail	Cannot transmit pedal, wheel speed, and so forth, message to ECU, cannot generate correct command for braking control	SPF	SM_TCAN_E2E CHECK SM_TCAN_switch over	FSR 3.1 FSR 3.2 FSR 3.4
System stuck in sleep mode	Cannot wakeup MCU for braking control	SPF	SM_TCAN_E2E CHECK SM_TCAN_switch over	FSR 3.3 FSR 3.4
CANL or CANH driver biased dominant indefinitely	ECU cannot communicate with wheel side MCU, cannot receive braking control command	SPF	SM_TCAN_E2E CHECK SM_TCAN_switch over	FSR 3.1 FSR 3.2 FSR 3.4
Short-circuit of any two pins	Loss of pin function	SPF	pin FMEA	FSR 3.4 FSR 3.5
Reports erroneous fault condition	Not used for safety function	NSR	NA	NA

SM_TCAN_E2E CHECK: F29P32 MCU embedded with an ASIL D lockstep core, support end-to-end software running. System integrator shall use ASIL D software for E2E check. The E2E check shall include but not limited to the following items:

- Data CRC for all kinds of message corruption during transmission
- Frame counter for communication frame losses
- Timeout check for message lost detection
- Periodic readback of sent message by MCU or periodic communicate with ECU for communication alive monitor

SM_TCAN_switch over: When detected first TCAN1043HG-Q1 communication failure occurs or cannot wake up the EMB system, MCU switch communication to another TCAN1043HG-Q1 path.

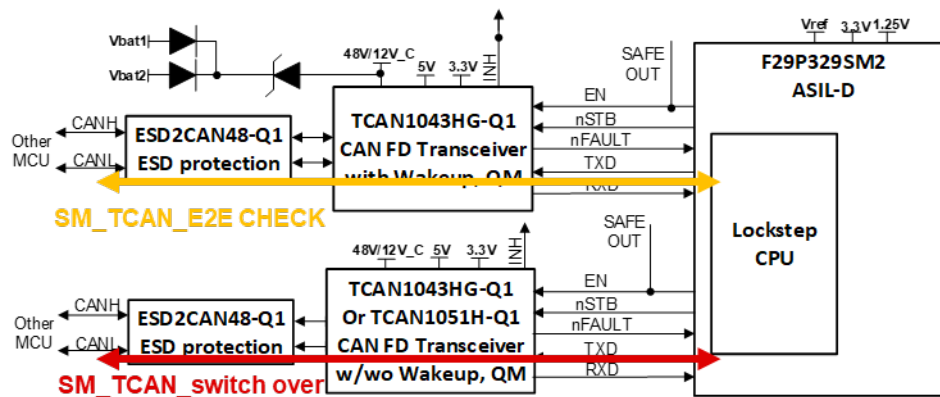


Figure 3-12. Safety Mechanism Design of Communication Interface

3.3.4 Actuator Safety Design

Figure 3-13 shows the EMB and EPB driver and actuator.

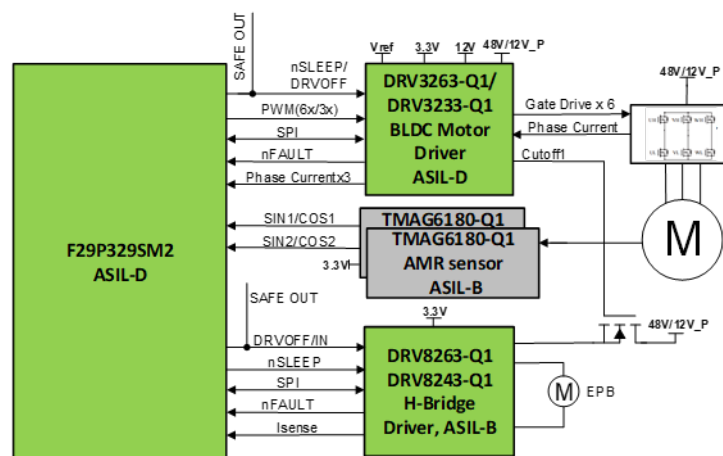


Figure 3-13. Actuator Safety Design Architecture

3.3.4.1 Braking Motor Driver Safety Analysis

The DRV3233-Q1 is designed for 12V rail braking motor systems, whereas the DRV3263-Q1 is utilized for 48V rail braking motor system. The functional design and safety goals of DRV3233-Q1 and DRV3263-Q1 are similar, so take DRV3263-Q1 as the example to show the safety analysis in this section.

Table 3-6. DRV3263-Q1 Functional Safety Requirements

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI
FSR-1	System shall remove motor assist power when unintended assist is detected	ASIL D	10ms

Table 3-6. DRV3263-Q1 Functional Safety Requirements (continued)

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI
FSR-2	System shall detect sudden loss of motor assist	QM	10ms

The DRV3263-Q1 Safety Manual defines two assumed system-level safety requirements as shown in [Table 3-6](#). These device-level FSRs are mapped to the EMB system-level FSRs defined in [Section 2](#).

FSR-1 directly supports EMB system FSR 4.1 and FSR 2.1, and is satisfied through two level detection and reactions. The two levels operate through independent signal paths and power supplies, making sure no single failure defeats both channels simultaneously.

- Device internal detection: DRV3263-Q1 continuously monitors VDS, VGS, phase current, and supply voltage. Upon detection of any fault causing unintended motor torque, nFAULT is asserted and all MOSFETs are turned OFF. This mechanism operates independently of MCU software and achieves ASIL D coverage per the DRV3263-Q1 FMEDA (SM_BLDC_fault indication).
- MCU plausibility check: F29P329SM2-Q1 independently monitors phase current via ADC and compares against the expected value based on the active PWM command. If unintended current is detected, the MCU asserts DRVOFF within FTTI. This check runs on the ASIL D lockstep core (SM_BLDC_current MON).

FSR-2 is rated QM at the device level, as DRV3263-Q1 does not provide a safety-rated loss-of-assist reaction mechanism. The ASIL D requirement for EMB FSR 4.1 is therefore fulfilled entirely at the system level through:

- SM_BLDC_current MON: MCU monitors phase current continuously. Absence of current while PWM is active triggers a fault, ECU notification, and activation of the redundant braking system.
- SM_BLDC_fault indication: MCU periodically reads DRV3263-Q1 fault status via SPI within FTTI, capturing gate driver faults such as UVLO or driver output failure.
- System-level redundancy: Per [Section 2.3.1](#), the diagonal redundant EMB architecture provides a backup braking path, elevating the overall response capability from QM at device level to ASIL D at system level.

DRV3263-Q1 is developed as the SEooC, target for ASIL D application. Thus, when designing the EMB system, it is necessary to meet the assumption of use in design specified in the *DRV3263-Q1 Safety Manual 4.4 Functional Safety Constraints and Assumptions*.

- To meet system assumption, LM78845-Q1 and TPS658880-Q1 provide 12V, 3.3V, Vref supply to DRV3263-Q1 driver.
- TMAG6180-Q1 is used for motor position detection. F29P329SM2 receive TMAG6180-Q1 signal and send three phase control signals to DRV3263-Q1 through 6xPWM wave. F29P329SM2 configure and check status to DRV3263-Q1 through SPI.
- Fault detection is performed via the internal safety mechanism of DRV3263-Q1 and the result is sent through an nFAULT signal to the IO of F29P329SM2. MCU can also make status queries through SPI. If the DRV3263-Q1 enters a safe state, that is, after the six MOSFETs are switched off, the other two EMBs still allow the vehicle to be braked without losing control.
- Other AoUs are related to operating conditions, shall also be met according to datasheet.

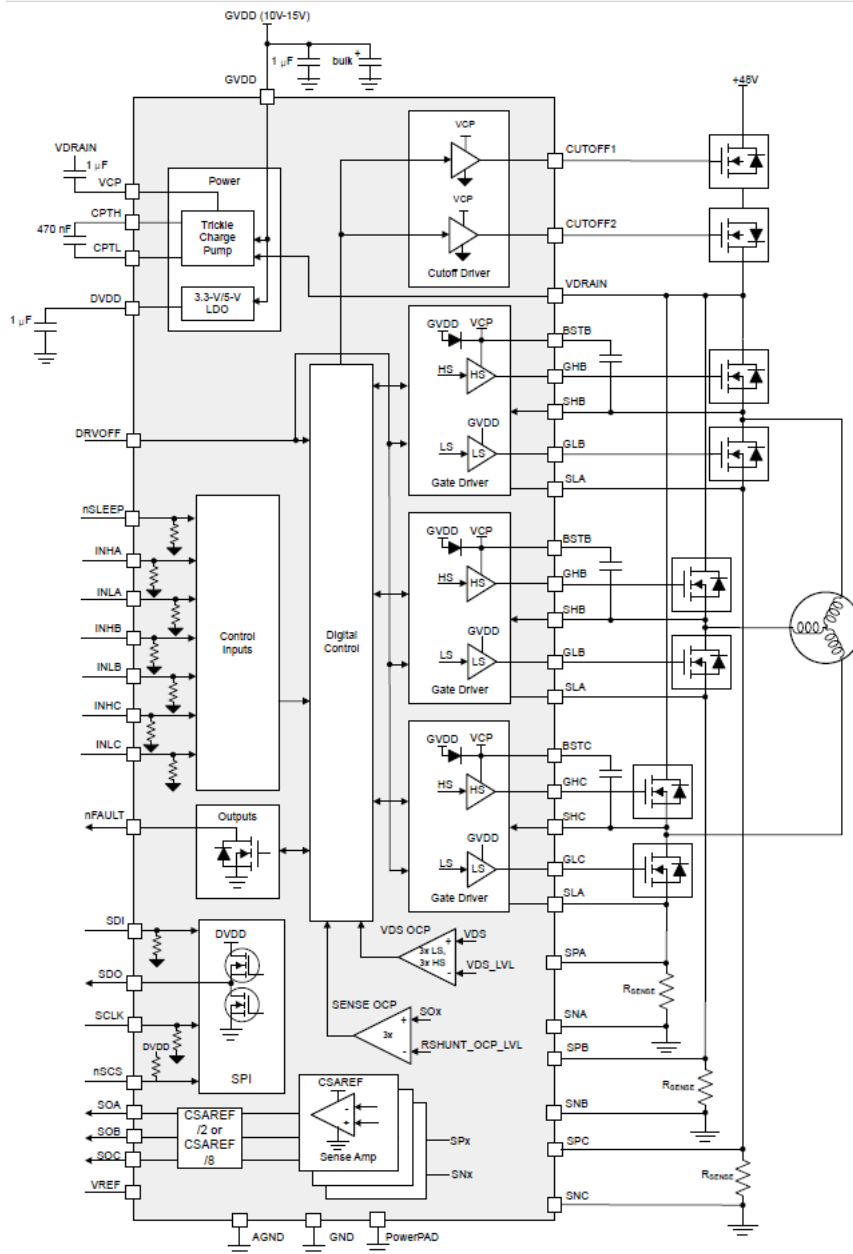


Figure 3-14. DRV3263-Q1 Structure

Table 3-7 shows the safety analysis and safety mechanisms proposed for the BLDC application.

Table 3-7. System-Level FMEA for Braking Motor Drive

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Gate driver output stuck in ON state (one or more phases)	Unintended motor torque output, leads to unintended braking force apply	SPF	SM_BLDC_current MON SM_BLDC_fault indication ⁽¹⁾	FSR 4.1 FSR 2.1 FSR 4.4
Gate driver output stuck in OFF state (one or more phases)	Loss of motor drive capability, leads to loss of braking force	SPF	SM_BLDC_current MON SM_BLDC_fault indication ⁽¹⁾	FSR 4.1 FSR 2.1 FSR 4.4
Turn-on too fast or too slow (shoot-through risk)	Short circuit current through half-bridge, leads to MOSFET damage and loss of motor control	SPF	SM_BLDC_fault indication ⁽¹⁾ SM_BLDC_protection	FSR 4.1 FSR 4.4

Table 3-7. System-Level FMEA for Braking Motor Drive (continued)

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Turn-off too fast or too slow	Voltage spike damage to MOSFETs, leads to abnormal motor behavior	SPF	SM_BLDC_fault indication ⁽¹⁾ SM_BLDC_protection	FSR 4.1 FSR 4.4
Cutoff driver failure (cutoff stuck open)	Cannot cutoff motor output when fault detected, loss of safe state	MPF	SM_BLDC_fault indication ⁽¹⁾	FSR 4.1 FSR 4.4
SPI communication failure between MCU and DRV3263-Q1	Cannot configure or read fault status of gate driver, loss of diagnostic coverage	MPF	SM_BLDC_current MON, SM_BLDC_fault indication ⁽¹⁾	FSR 4.4
Pin-to-pin short	Loss of pin function	SPF	Designed according to Pin FMEA	FSR 4.1 FSR 4.4

(1) Refer to the FMEDA and safety manual of DRV3263-Q1

SM_BLDC_current MON: F29P329SM2-Q1 performs output plausibility check by monitoring phase current via current sense amplifier output through MCU ADC. The measured phase current is compared against the expected value based on the PWM command sent to DRV3263-Q1. If an unintended current is detected (for example, current present when PWM commanded OFF, or no current when commanded ON), the MCU declares a fault, asserts DRVOFF or ASC signal to DRV3263-Q1, and reports to ECU. The MCU also performs periodic SPI readback of DRV3263-Q1 fault status registers within FTTI.

SM_BLDC_fault indication: DRV3263-Q1 embeds internal safety mechanisms including VDS monitor, VGS monitor, shoot-through protection, dead-time control, over-current protection, over-temperature protection, and under-voltage lockout. Upon detection of any internal fault, the nFAULT pin is asserted low to notify F29P329SM2-Q1. The MCU reads the detailed fault status via SPI and drives the gate driver into safe state (all MOSFETs OFF through DRVOFF or ASC). The PMIC SAFE_OUT signal provides an independent path to assert DRVOFF in case MCU itself fails.

SM_BLDC_protection: DRV3263-Q1 integrates programmable dead-time and shoot-through prevention logic. The device monitors both high-side and low-side gate signals and prevents simultaneous turn-on of the same half-bridge leg. This mechanism operates independently of MCU software.

3.3.4.2 Parking Driver Safety Analysis

The DRV8245-Q1 is designed for 12V parking lock systems, while the DRV8263S-Q1 is utilized for 48V parking lock system.. The functional design and safety goals of DRV8245-Q1 and DRV8263S-Q1 are similar, so take DRV8263S-Q1 as the example to show the safety analysis in this section. To achieve ASIL D for FSR 4.2 unintended ON cases, system level mechanisms shall be considered for BDC driver to help achieve ASIL D target.

DRV8263S-Q1 Hardware Safety Mechanisms internal:

- Internal over-current, over-temperature, and under-voltage protection
- IPROPI current sense feedback
- nFAULT status reporting to MCU

F29P329SM2-Q1 Software Safety Mechanisms external:

- Logic plausibility check based on IPROPI current monitoring
- Periodic SPI readback of driver fault status registers within FTTI
- Independent DRVOFF / nSLEEP control path from MCU

The assumed functional safety requirements of DRV8263S-Q1 from safety manual are as followed, which is compliant with the proposed FSR 4.2 unintended OFF cases in [Section 2.3.3](#):

Table 3-8. DRV8263S-Q1 Functional Safety Requirements

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI
FSR-1	Avoid sending current to load when commanded OFF	ASIL B	100ms
FSR-2	Drive motor current when commanded	ASIL B	100ms

DRV8263S-Q1 is developed as the SEooC, target for ASIL B appliance. Thus, when designing the EMB system, it is necessary to meet the assumption of use in design specified in the *DRV8263S-Q1 Safety Manual 4.3 Functional Safety Constraints and Assumptions*.

- In this EMB system, DRV8263S-Q1 is used as a Full H bridge mode.
- To meet FSR 4.4's time interval requirement, run off-state diagnostics within FDTI.
- Before activate parking lock brake, F29P329SM2-Q1 sets S_DRVOFF high and S_IN low, lock SPI and REG to prevent unintended activated.
- The DRV8263S-Q1 internal safety mechanisms detect failure and record the fault flag. F29P329SM2-Q1 read error status within FTTI and pulls nSLEEP low if any faults are detected.
- DRV8263S-Q1 embedded with IPROPI resistor for current sense. F29P329SM2-Q1 shall perform logic plausibility check with IPROPI current sense and SPI command. If unintended driver actuates, MCU trigger nSLEEP or DRVOFF for DRV8263S-Q1.
- Other AoU (Assumption of use) are related to operating conditions, shall also be met according to datasheet.

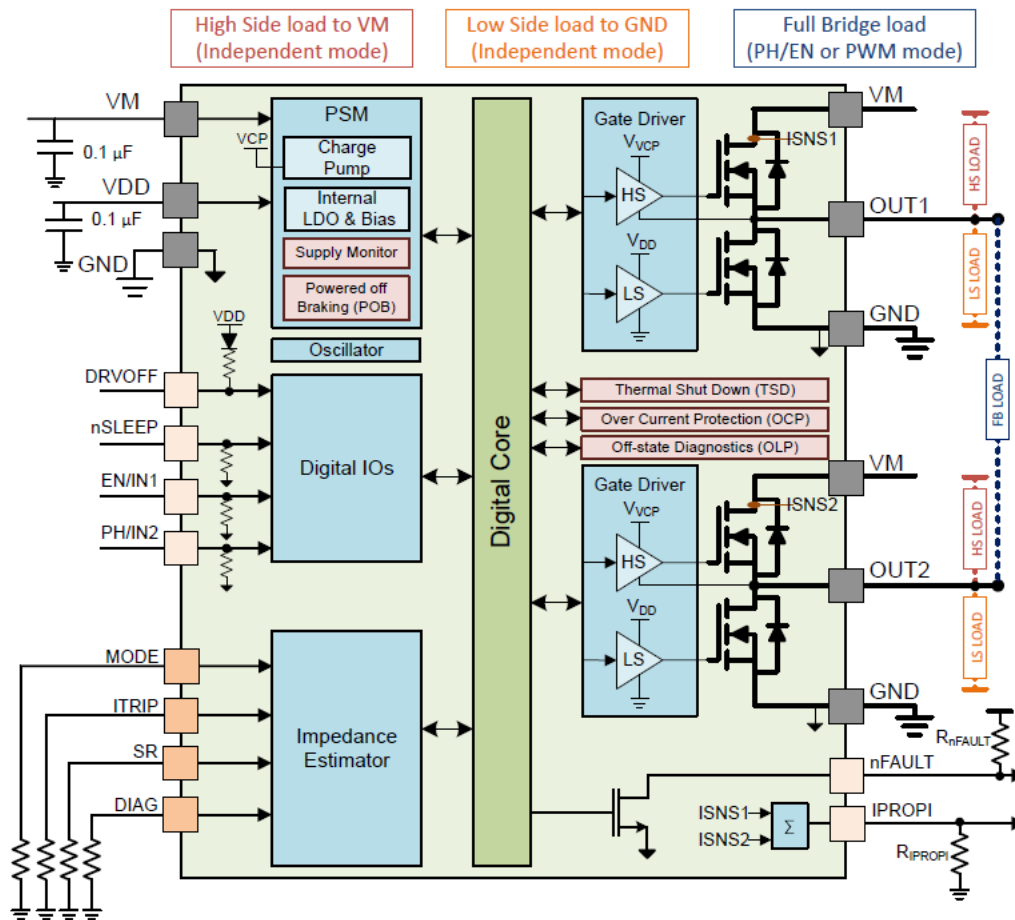


Figure 3-15. DRV8263S-Q1 Structure

The safety analysis and safety mechanisms proposed for the parking lock application is as followed. To achieved ASIL D for FSR 4.2 unintended ON cases, system level mechanisms shall be considered for BDC driver to help achieve ASIL D target.

Table 3-9. System-Level FMEA for Parking Lock Driver

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Failure in the BDC driver cannot drive motor	Cannot activate park lock that vehicle cannot park	SPF	SM_BDC_current MON SM_BDC_fault indication ⁽¹⁾	FSR 4.2 FSR 4.4

Table 3-9. System-Level FMEA for Parking Lock Driver (continued)

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Failure in the BDC driver unintended drive motor	Unintended activate drive park lock that vehicle unintended park	SPF	SM_BDC_current MON SM_BDC_fault indication ⁽¹⁾ SM_BDC_cutoff	FSR 4.2 FSR 4.3 FSR 4.4
Cutoff MOSFET short	Cannot cutoff BDC supply when driver unintended activate	MPF	NA	NA
Cutoff MOSFET open	Cannot activate park lock that vehicle cannot park	SPF	SM_BDC_current MON SM_BDC_fault indication ⁽¹⁾	FSR 4.2 FSR 4.4

(1) Refer to the FMEDA and safety manual of DRV8263S-Q1

SM_BDC_current MON: DRV8263S-Q1 driver embedded with current sense function, when the device is fully turned ON. The load current is reflected on IPROPI pin. F29P329SM2-Q1 ADC monitors the voltage on RIPROPI for current. MCU perform logic plausibility check with IPROPI current sense and MCU. MCU use redundant ADCs input the VOUT of DRV8263S-Q1 for plausibility check with the sent SPI command by CPU. If unintended driver actuates, MCU trigger nSLEEP or DRVOFF for DRV8263S-Q1. If cannot activate driver, another DRV8263S-Q1 operates.

SM_BDC_fault indication: When BDC driver detect an internal fault, DRV8263S-Q1 will record error status. F29P329SM2-Q1 checks the error status through SPI, and trigger DRVOFF signal to DRV8263S-Q1.

SM_BDC_cutoff: If BDC driver cannot be driven off after MCU detected faults, MCU can trigger DRV3263-Q1 output a cut-off signal to the BDC driver power switch for unintended actuating. Independence between SM_BDC_cutoff and Channel 1/Channel 2 is provided by the separate power supply and control signal routing of DRV3263-Q1.

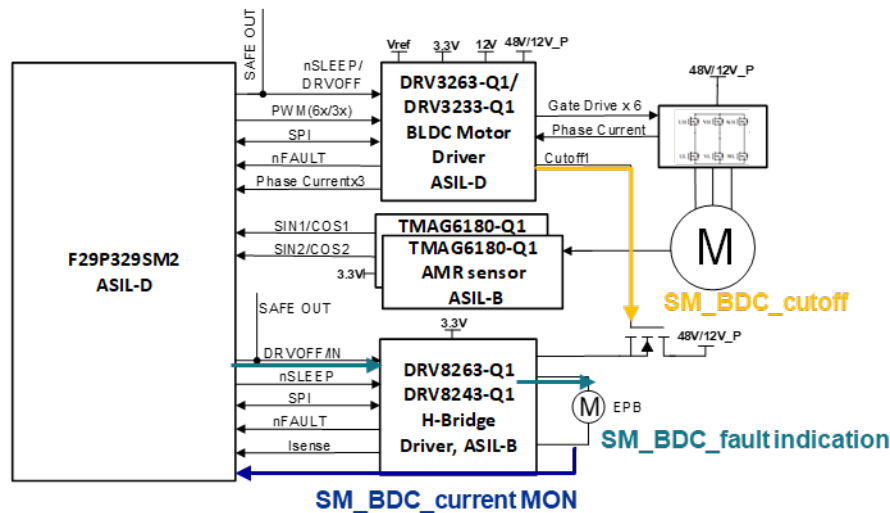


Figure 3-16. Safety Mechanism Design Of Parking Lock Driver

3.3.5 Sensor Interface Safety Design

Figure 3-17 shows the sensor interface safety design.

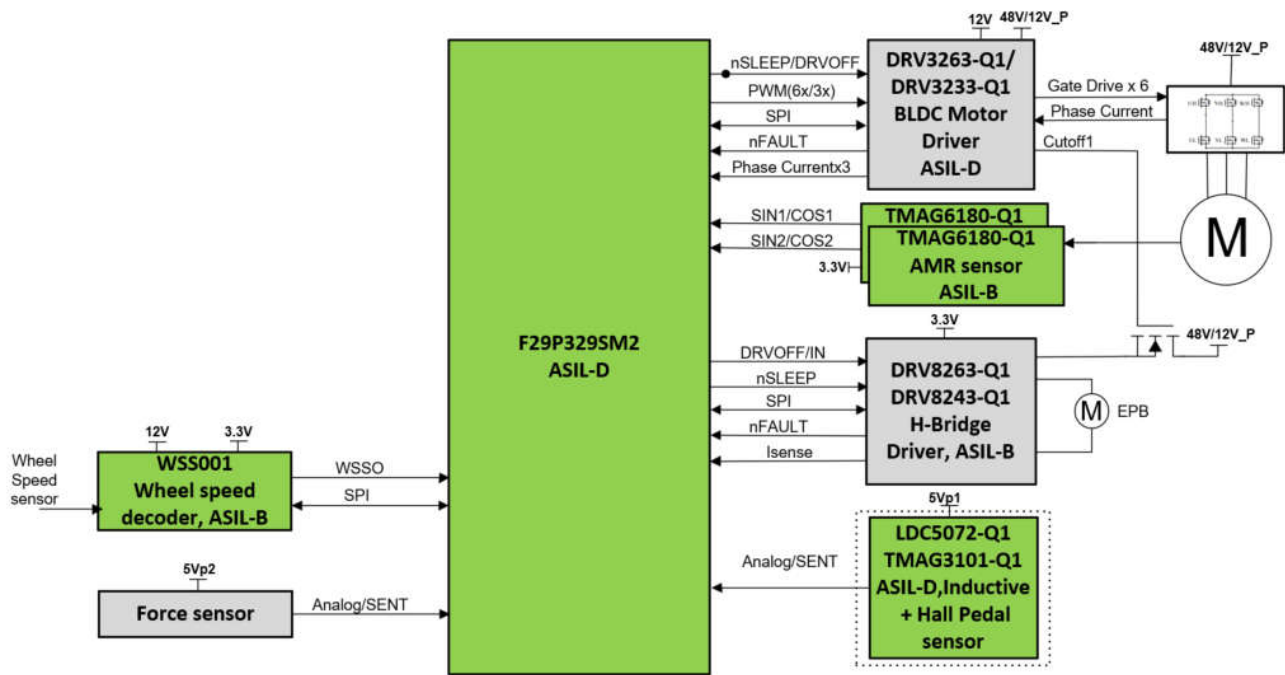


Figure 3-17. Sensor Interface Safety Design Architecture

3.3.5.1 Position Sensor Safety Analysis

TMAG6180-Q1 is developed as the SEooC, ASIL B targeted. The functions and safety mechanisms embedded in this position sensor are shown in [Figure 3-18](#). To meet the ASIL D FSRs of the EMB system, two independent TMAG6180-Q1 sensors are deployed in a redundant configuration. When designing the EMB system, it is necessary to meet the Assumptions of Use specified in the *TMAG6180-Q1 Safety Manual 4.3 Functional Safety Constraints and Assumptions of Use*.

- To meet the above assumptions, F29P329SM2-Q1 enables all internal safety mechanisms of both TMAG6180-Q1 sensors and performs runtime redundancy checks by comparing the outputs of the two sensors (SIN1/COS1, SIN2/COS2). If a discrepancy between the two sensors' signal exceeds the defined threshold, the MCU detects the fault and enters the safe state. All safety mechanisms are executed within FTTI. Other AoUs related to operating conditions shall also be met according to the datasheet.

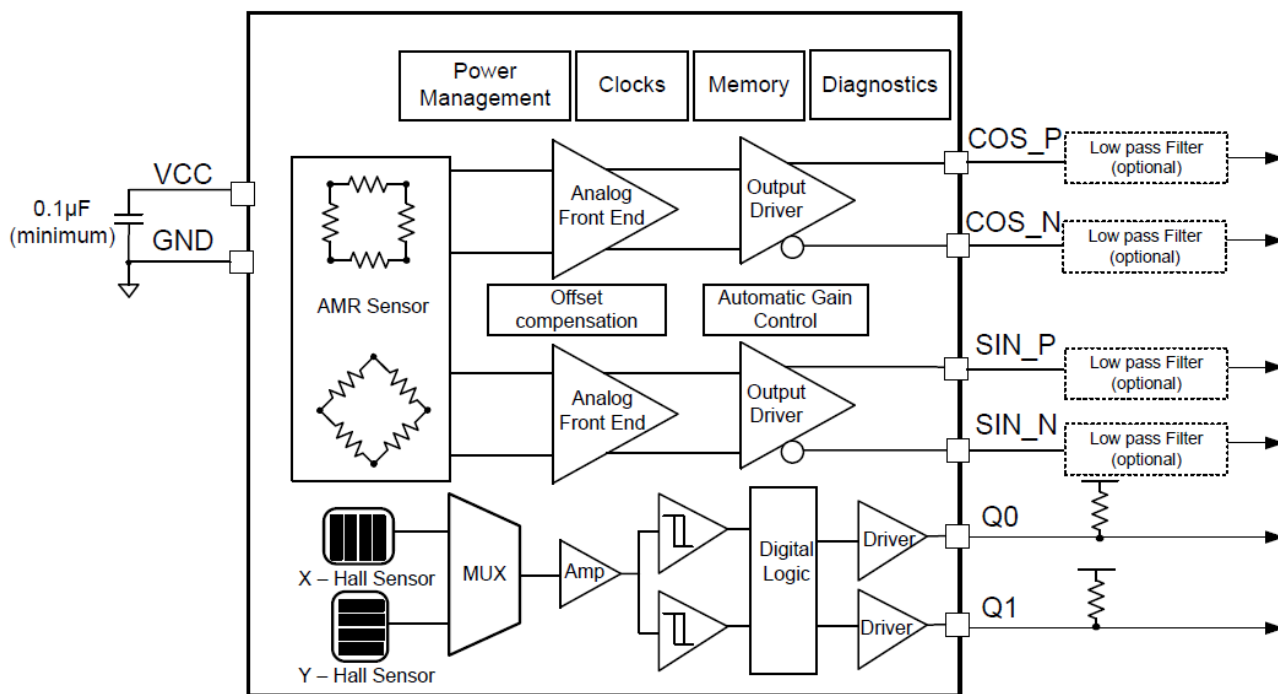


Figure 3-18. TMAG6180-Q1 Structure

The safety analysis and safety mechanisms proposed for the position sensing is as followed.

Table 3-10. System-Level FMEA for Position Sensor

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
Position sensor output out of specification	Incorrect motor position input to MCU, leads to wrong PWM output and inaccurate braking force	SPF	SM_POS_redundant CMP SM_POS_fault indication ⁽¹⁾	FSR 5.1 FSR 2.1 FSR 5.4
Position sensor output offset drift	Incorrect motor position input to MCU, leads to wrong PWM output and inaccurate braking force	SPF	SM_POS_redundant CMP SM_POS_fault indication ⁽¹⁾	FSR 5.1 FSR 2.1 FSR 5.4
Position sensor output stuck	Incorrect motor position input to MCU, leads to wrong PWM output and loss of braking control	SPF	SM_POS_redundant CMP SM_POS_fault indication ⁽¹⁾	FSR 5.1 FSR 2.1 FSR 5.4
Pin-to-pin short	Loss of pin function	SPF	Designed according to Pin FMEA	FSR 5.1 FSR 5.4
Redundant position sensor output out of specification/ offset drift/stuck/short	Incorrect motor position input to MCU, leads to unintended fault signal and enter safe state	MPF	SM_POS_redundant CMP SM_POS_fault indication ⁽¹⁾ Designed according to Pin FMEA	FSR 5.4

(1) Refer to the FMEDA and safety manual of TMAG6180-Q1

SM_POS_redundant CMP: F29P329SM2-Q1 performs runtime redundancy check by continuously comparing the angle results calculated from the two independent TMAG6180-Q1 sensors (SIN1/COS1 and SIN2/COS2). The two sensor outputs are routed to independent ADC modules (ADC-A and ADC-B) on the MCU to verify signal path independence. If the discrepancy between the two results exceeds the defined threshold within FTTI, the MCU declares a fault, reports to ECU, and drives the actuator to inactive mode.

SM_POS_fault indication: Each TMAG6180-Q1 sensor has internal diagnostic mechanisms enabled by the MCU, including signal path diagnostics and supply voltage monitoring. The internal fault flag is monitored by F29P329SM2-Q1 periodically within FTTI. Upon detection of an internal fault, the MCU enters the safe state.

Because two TMAG6180-Q1 devices are used in this design, dependent failure shall be considered. To prevent dependent failures (common cause failures), the following measures have applied to make sure the two sensors remain independent:

- Power supply independence: Sensor's supply voltage is monitored both internally by each sensor and externally by the PMIC.
- Signal path independence: SIN/COS output signals are routed to separate ADC input channels on the MCU to prevent shared signal path failures.
- Physical isolation: The two sensors are physically separated on the PCB to reduce susceptibility to common electromagnetic interference or mechanical stress.
- Other dependent failure initiators (thermal, supply transients, and so forth) are mitigated through independent temperature monitoring on the board and power monitor inside PMIC to make sure the system can maintain necessary safety functions when facing common cause failures.

3.3.5.2 Wheel Speed Decoder Safety Analysis

WSS001-Q1 is an ASIL B compliant wheel speed decoder. The functions and structures are shown in the figure below. Most integrators place an ASIL B wheel speed sensor on each wheel. The captured signals are input to WSS001-Q1 for decoding and output to MCU. Then 4-wheel speed and vehicle speed are sent to ECU for vehicle stability judgment and braking force calculation. Braking force calculation by electrical stability control (ESC) and assignment by ECU. The assumed functional safety requirements of WSS001-Q1 is shown in [Table 3-11](#). A single WSS001-Q1 cannot meet FSR 5.3, system integrator shall do cross check for four received wheel speed signals on system level to meet ASIL D FSR.

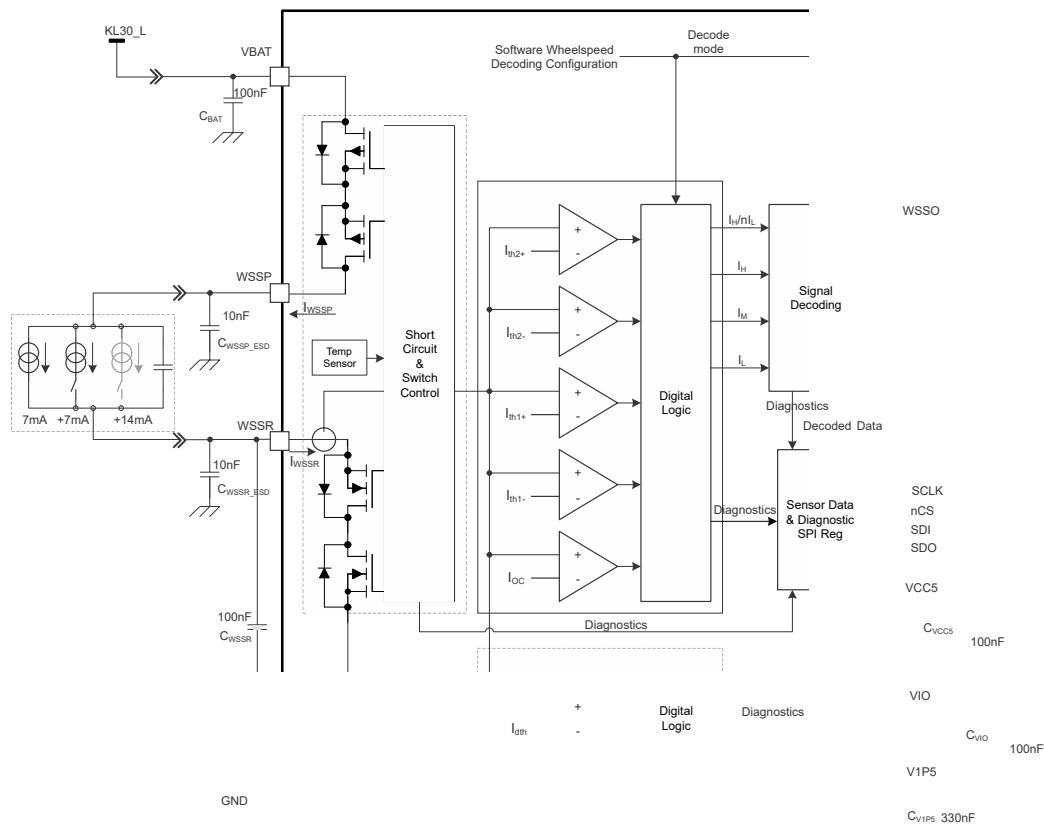


Figure 3-19. WSS001-Q1 structure

Table 3-11. WSS001-Q1 Functional Safety Requirements

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI
FSR-1	No mismatches for one or more speed edges between WSS001-Q1's wheel speed sensor input and its output signal to the MCU.	ASIL B	400ms

The safety analysis and safety mechanisms proposed for the wheel speed decoder is as followed.

Table 3-12. System Level FMEA For Wheel Speed Decoder

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
WSSO output signal loss (no pulse output)	MCU cannot receive wheel speed signal, leads to incorrect vehicle speed calculation and loss of ABS/braking control	SPF	SM_WSS_fault indication ⁽¹⁾ SM_WSS_plausibility check	FSR 5.3 FSR 2.1 FSR 5.4
WSSO output signal stuck-at high or low	MCU receives constant signal level, incorrectly interprets as zero speed or maximum speed, leads to wrong braking control	SPF	SM_WSS_fault indication ⁽¹⁾ SM_WSS_plausibility check	FSR 5.3 FSR 2.1 FSR 5.4
WSS001-Q1 output speed value out of specification (count error / timing error)	Incorrect wheel speed value reported to MCU, leads to inaccurate braking force calculation	SPF	SM_WSS_fault indication ⁽¹⁾ SM_WSS_plausibility check	FSR 5.3 FSR 2.1 FSR 5.4
Pin-to-pin short on WSS001-Q1	Loss of pin function, signal path failure	SPF	Designed according to Pin FMEA	FSR 5.3 FSR 5.4

(1) Refer to the FMEDA and safety manual of WSS001-Q1

SM_WSS_fault indication: F29P329SM2-Q1 periodically reads WSS001-Q1's internal fault status registers via SPI within FTTI. The fault flags monitored include: decoder logic error, OSC failure, VBAT UV/OV, WSSP UV/OV, and BIST result, and so forth. Upon detection of any asserted fault flag, the MCU enters the safe state and reports to ECU.

SM_WSS_plausibility check: An application software-based cross-check running on the 2x independent ECUs. All 4-wheel speed signals decoded by the respective WSS001-Q1 devices are transmitted to both ECUs via CAN. The ECU application software implements the following multi-strategy cross-check:

- Zero-speed plausibility check: Under normal driving conditions, all 4 wheel speed signals shall not simultaneously read zero. If all four signals report zero speed while the vehicle is expected to be in motion (for example, based on IMU data), a fault is declared.
- Outlier rejection: If one wheel speed signal deviates significantly from the other three, that signal is flagged as erroneous and discarded. This strategy excludes extreme but physically valid conditions such as individual wheel slip during ABS activation.
- Temporal plausibility check: Each wheel speed signal is cross-checked against its previously captured value. If an unreasonable data transition or discontinuity is detected (for example,, instantaneous speed jump beyond vehicle dynamics limits), the signal is discarded.
- IMU-based cross-check: Vehicle acceleration integrated from the inertial measurement unit (IMU) is used as an independent reference to validate the wheel speed signals. A significant discrepancy between IMU-derived speed and wheel speed decoder output triggers a fault.

Upon detection of any fault through the above strategies, the ECU enters the defined safe state, disables the affected wheel speed signal, and redistributes braking force calculation accordingly. The cross-check software shall be developed and verified to ASIL D.

3.3.5.3 Pedal Position Sensor Safety Analysis

In this wheel-side EMB system design, pedal position sensor is optional, an interface for the pedal position signal is reserved in case some system integrator input pedal signal to front left EMB directly. This interface is only considered on the left-front EMB. To meet FSR 5.2 (ASIL D), LDC5072-Q1 and TMAG3101-Q1 integrated sensor is implemented.

TMAG3101-Q1 is a low-drift precision 3D Hall-effect sensor with end of line calibration and SENT, triggered SENT, PWM, or analog output interfaces. [Figure 3-20](#) shows the device block diagram. TMAG3101-Q1 includes integrated diagnostic functions to detect and report potential failure modes of the power supply, hall sensor, analog front end, internal oscillators, digital core, and output interface blocks, which provides a SEooC safety rating of ASIL B. [Table 3-13](#) shows the assumed functional safety requirements of the TMAG3101-Q1. A single TMAG3101-Q1 cannot meet FSR 5.3, system integrator shall place another functional safety position sensor LDC 5072-Q1 on system level to meet ASIL D FSR.

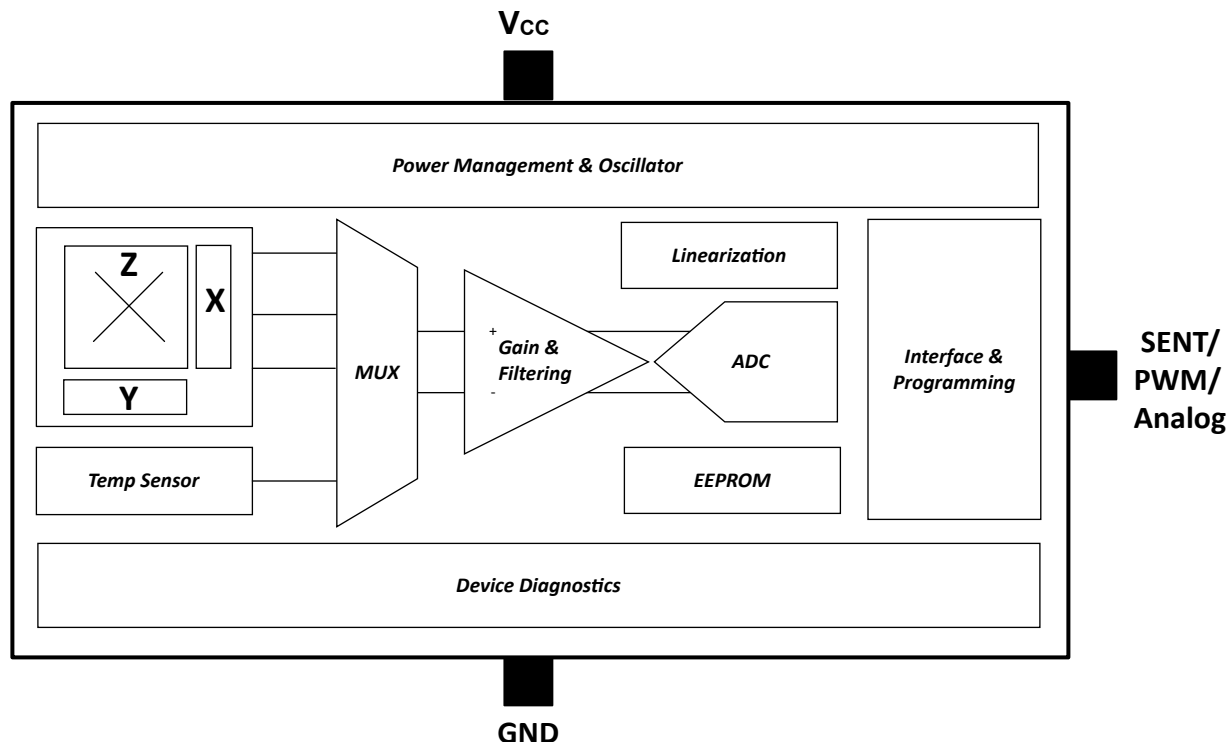


Figure 3-20. TMAG3101-Q1 Structure

Table 3-13. TMAG3101-Q1 Functional Safety Requirements

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI
FSR-4	The braking system uses an alternate sensing method in case of any failure to sense the correct brake pedal position which can lead to unintended brake force.	ASIL D	10ms

LDC5072-Q1 is an inductive position sensor front-end IC with LC oscillator excitation, analog front-end signal processing, and differential analog output interfaces. [Figure 3-21](#) shows the device block diagram. LDC5072-Q1 includes integrated diagnostic functions to detect and report potential failure modes of the power supply, LC oscillator, analog front end, AGC block, internal oscillator, EEPROM memory, digital core, and output driver blocks, which provides a SEooC safety rating of ASIL-C(D). [Table 3-14](#) shows the assumed functional safety requirements of the LDC5072-Q1..

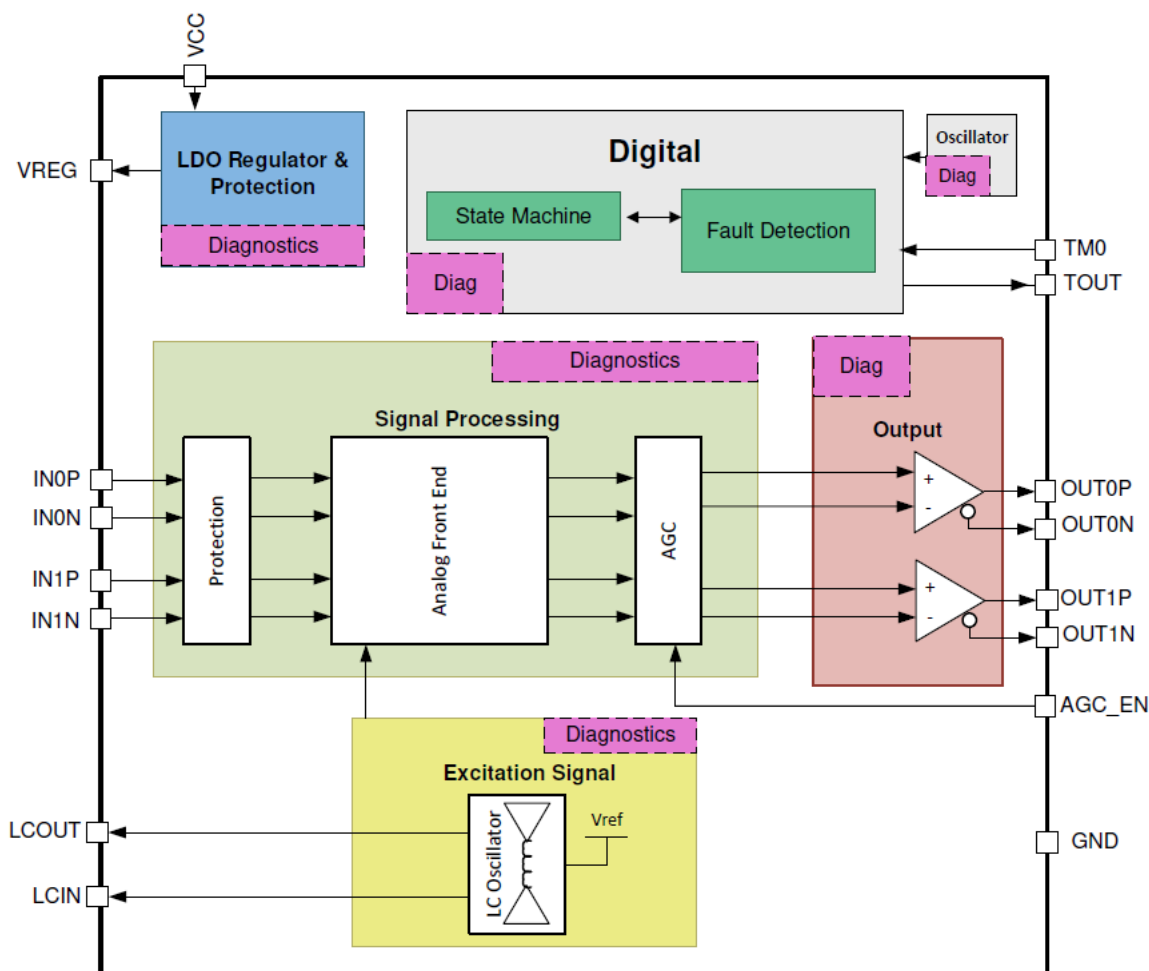


Figure 3-21. LDC5072-Q1 Structure

Table 3-14. LDC 5072-Q1 Functional Safety Requirements

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI
FSR-1	The LDC5072-Q1 shall communicate to the system when there are internal failures that can lead to signal a false but valid angle	ASIL C	2ms

Table 3-15 shows the safety analysis and safety mechanisms proposed for the position sensors.

Table 3-15. System-Level FMEA for Pedal Position Sensors

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
TMAG3101 position sensor output out of specification	Incorrect pedal position to MCU leads to inaccurate or unintended braking force	SPF	SM_PEDAL_redundant comparison SM_PEDAL_TMAG3101 fault indication ⁽¹⁾	FSR 5.2 FSR 2.1 FSR 5.4
TMAG3101 position sensor output stuck	Incorrect pedal position to MCU leads to inaccurate or unintended braking force	SPF	SM_PEDAL_redundant comparison SM_PEDAL_TMAG3101 fault indication ⁽¹⁾	FSR 5.2 FSR 2.1 FSR 5.4
Pin-to-pin short	Loss of pin function	SPF	SM_PEDAL_redundant comparison SM_PEDAL_TMAG3101 fault indication ⁽¹⁾	FSR 5.2 FSR 5.4
LDC5072 position sensor output out of specification	Incorrect pedal position to MCU leads to unintended generate fault signal and enter safe state	SPF	SM_PEDAL_redundant comparison SM_PEDAL_LDC5072 fault indication ⁽¹⁾	FSR 5.2 FSR 2.1 FSR 5.4

Table 3-15. System-Level FMEA for Pedal Position Sensors (continued)

Failure mode	Failure effect	FSR violation	Safety mechanism	FSR traced
LDC5072 position sensor output stuck	Incorrect pedal position to MCU leads to unintended generate fault signal and enter safe state	SPF	SM_PEDAL_redundant comparison SM_PEDAL_LDC5072 fault indication ⁽¹⁾	FSR 5.2 FSR 2.1 FSR 5.4
Pin-to-pin short	Loss of pin function leads to unintended generate fault signal and enter safe state	SPF	SM_PEDAL_redundant comparison SM_PEDAL_LDC5072 fault indication ⁽¹⁾	FSR 5.2 FSR 5.4

(1) Refer to the FMEDA and safety manual of TMAG3101-Q1

SM_PEDAL_redundant comparison: The F29P329SM2-Q1 performs runtime redundancy check by continuously comparing the pedal position results from the TMAG3101-Q1 and the LDC5072-Q1. The two devices feature different measurement technologies (magnetic and inductive) and are routed to independent modules within the MCU. If the discrepancy between the two results exceeds the defined threshold within FTTI, the MCU declares a fault and reports to ECU.

SM_PEDAL_TMAG3101 fault indication: The TMAG3101-Q1 has internal diagnostic mechanisms that can be enabled by the MCU, including:

- VCC and internal LDO checks
- Hall sensor resistance and offset checks
- AFE and ADC integrity checks
- Oscillator integrity check
- EEPROM and RAM ECC checks
- ROM parity check
- Stack overflow and watchdog timer checks
- Output overcurrent protection
- User-configurable magnetic field, angle, and temperature threshold checks

SM_PEDAL_LDC5072 fault indication: The LDC5072-Q1 has internal diagnostic mechanisms that can be enabled by the MCU, including:

- VCC, VREG, and internal supply voltage checks
- LC oscillator amplitude, frequency, and common-mode checks
- Sensor interface pin BIST checks (open/short detection on LC and receiver coil pins)
- Input signal out-of-range and open coil detection checks
- Output signal out-of-range, common-mode, and short checks
- EEPROM CRC, register CRC, and critical registers redundancy checks
- Logic BIST (LBIST) and Analog BIST (ABIST) at power up
- Phase imbalance and frequency imbalance checks (rotation dependent)
- Thermal shutdown check

Because two sensors (TMAG3101-Q1 and LDC5072-Q1) are used in this design, dependent failures shall be considered. To prevent dependent failures, the following measures are applied to make sure the two sensors remain independent:

- **Power supply independence:** Sensors supply voltage is monitored both internally by each sensor and externally by the PMIC.
- **Signal path independence:** Output signals are routed to separate input channels on the MCU to prevent shared signal path failures.
- **Physical isolation:** The two sensors are physically separated on the PCB to reduce susceptibility to common electromagnetic interference or mechanical stress.
- **Other dependent failure initiators** are mitigated through independent temperature monitoring on the board and power monitor inside PMIC to make sure the system can maintain necessary safety functional when facing common cause failures.

4 Summary

This application note presents a functional safety design approach for an electro-mechanical braking system based on TI's automotive-grade device portfolio, targeting ASIL D compliance. Starting from HARA-derived safety goals, the design implements multi-level safety mechanisms across power management, central control, communication, actuation, and sensor interface functional blocks. System-level ASIL D compliance is intended to be achieved through a combination of individually ASIL D certified devices, redundant hardware architecture, and ECU-level software cross-check strategies. This document aims to provide system integrators with a practical implementation reference for EMB development to help facilitate the certification process.

5 References

- International Standard for Organization, [ISO 26262: 2018 Road vehicles — Functional safety](#)
- National public service platform for standards information, [GB/T 34590-2022 《道路车辆 功能安全》](#)
- National public service platform for standards information, [GB21670-2025 《乘用车制动系统技术要求及试验方法》](#)
- Texas Instruments, [TIDA-020106](#), reference design
- Texas Instruments, [LM74930-Q1 Automotive 3-V to 65-V surge stopper with circuit breaker and overvoltage protection](#), product page
- Texas Instruments, [Protection against Unsuppressed Load Dump in Automotive Systems using LM74930-Q1](#), application brief
- Texas Instruments, [Achieving Functional Safety Goals for DC/DC Converters Using F29x](#), application note
- Texas Instruments, <https://www.ti.com/product/LM78845-Q1>, product page
- Texas Instruments, <https://www.ti.com/drr/opn/TPS65388X-Q1-DESIGN>
- Texas Instruments, [F29P329SM-Q1 Automotive C2000 64-bit MCU with C29 200MHz, lockstep, functional safety compliance, 2MB](#), product page
- Texas Instruments, [TCAN1043HG-Q1 Automotive 70-V bus-fault-protected CAN FD transceiver with wake input and 5-Mbps flexible data-rate](#), product page
- Texas Instruments, [DRV3233-Q1 Automotive 12V and 24V battery 3-phase gate driver unit with accurate current sensing](#), product page
- Texas Instruments, [DRV3263-Q1 Automotive, 48V battery three-phase gate driver unit with accurate current sensing](#), product page
- Texas Instruments, [DRV8263S-Q1 Automotive 48V full-bridge motor driver with diagnostics and internal current sense](#), product page
- Texas Instruments, [DRV8245-Q1 Automotive 40-V, 32-A H-Bridge driver with integrated current sensing and feedback](#), product page
- Texas Instruments, [TMAG6180-Q1 Automotive high-precision analog AMR angle sensor with 360° angle range](#), product page
- Texas Instruments, <https://www.ti.com/product/WSS001-Q1>, product page
- Texas Instruments, [LDC5072-Q1 Automotive inductive position sensor front end with sine/cosine interface](#)
- Texas Instruments, <https://www.ti.com/product/TMAG3101-Q1>, product page

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to [TI's Terms of Sale](#), [TI's General Quality Guidelines](#), or other applicable terms available either on [ti.com](#) or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Copyright © 2026, Texas Instruments Incorporated

Last updated 10/2025