Application Note

Towards Functional Safety in On-Board Charger: Design Approach and Component Overview

Forest Fu, Sifan You, Harvey Chen, Mingrui Zhu

ABSTRACT

With functional safety (FuSa) becoming increasingly critical in automotive applications, this document serves as a comprehensive introduction to FuSa implementation in on-board charger (OBC) systems. Section 1 provides foundational knowledge covering background information, applicable standards, and TI's functional safety tools. Section 2 explores general FuSa design principles for OBC applications and demonstrates a practical example of system design approach. Section 3 highlights key TI components for OBC FuSa implementations, featuring chip-level safety features and system-level safety mechanisms. This document aims to equip designers with essential resources for developing FuSa designs.

Disclaimer

The system-level FuSa analysis examples and safety mechanisms presented in this document are intended solely for educational purposes. They should not replace proper engineering analysis and design decisions made by qualified system designers. All described safety measures must be re-evaluated by system integrators within the context of specific system design implementations to verify effectiveness.

Table of Contents

Trademarks

All trademarks are the property of their respective owners.

1 Introduction

1.1 Background

Electric vehicles have experienced rapid growth in recent years due to environmental benefits, including zero emissions and reduced dependence on fossil fuels. As electrification and autonomous driving technologies continue to advance, safety concerns for electric vehicles have become increasingly prominent.

Functional Safety (FuSa) represents a critical component of overall system safety, focusing on ensuring that systems respond predictably to both normal inputs and failure conditions. The primary objective of FuSa is to systematically reduce risks to acceptable levels through the strategic implementation of appropriate safety mechanisms and design methodologies.

ISO 26262: 2018 is the international standard for functional safety of electrical and electronic (E/E) systems in road vehicles. It adapts the generic IEC 61508: 2010 safety-lifecycle framework to the automotive domain. It provides a structured, risk-based approach to verify that failures do not lead to unsafe situations.

Those failures can be classified into systematic faults and random hardware faults. Systematic faults are present in both hardware design and software design, which can be managed and mitigated by a rigorous development process or independent assessment. Random hardware faults are only limited to hardware, which cannot be eliminated, while can be detected and prevented by implementing safety mechanisms. Table 1-1summarizes the difference between systematic and random hardware faults.

Table 1-1. Systematic vs. Random Hardware Faults

Aspect	Systematic Fault	Random Hardware Fault
Definition	Deterministic faults inherent to design, specification, implementation, or operation that manifests consistently under specific conditions	Physical defects or failure occurring unpredictably during hardware operation due to physical phenomena, aging, stress, or environmental factors
Root cause	For example, design errors, incorrect specifications, implementation mistakes	For example, physical deterioration, electrical stress, component aging
Predictability	Deterministic and reproducible, which can be eliminated and permanently fixed	Probabilistic and statistical occurrence, which cannot be eliminated and reproducible
Goal	Eliminate the defect before release.	Detect and mitigate the fault when the fault occurs.
Measures	Functional safety management, development, test, verification, validation activities in full lifecycle.	Safety mechanism design and verification.
Typical metrics	Number of uncovered safety requirements, review coverage, tool confidence level.	Failure rate, Diagnostic Coverage.

Since systematic faults can be prevented and eliminated by ensuring a high-quality development process, this paper will focus on the random hardware fault analysis. Hardware metrics - Single-point fault metric (SPFM), Latent fault metric (LFM), and Probabilistic metric for random hardware failure (PMHF) - are defined to quantitatively assess random hardware failures and determine compliance with automotive safety integrity requirements.

Automotive safety integrity levels (ASIL) range from ASIL A to ASIL D, with ASIL D being the most stringent. Table 1-2 lists the acceptable values of random hardware failure metrics associated with each ASIL level according to ISO 26262.

Table 1-2. Hardware Failure Metrics According to ISO 26262

ASIL Level	SPFM	LFM	PMHF (in FIT; Failures in Time)
ASIL-A	Not relevant	Not relevant	Not relevant
ASIL-B	≥ 90%	≥ 60%	≤ 100 FIT
ASIL-C	≥ 97%	≥ 80%	≤ 100 FIT
ASIL-D	≥ 99%	≥ 90%	≤ 10 FIT

1.2 HW/SW FuSa Analysis Process

ISO26262: 2018 guides manufacturers from initial risk assessment through design, implementation, production, and field operation to ensure that safety goals are achieved and documented throughout the vehicle's life-cycle. Figure 1-1 is general HW/SW safety analysis process according to ISO26262: 2018. [1]

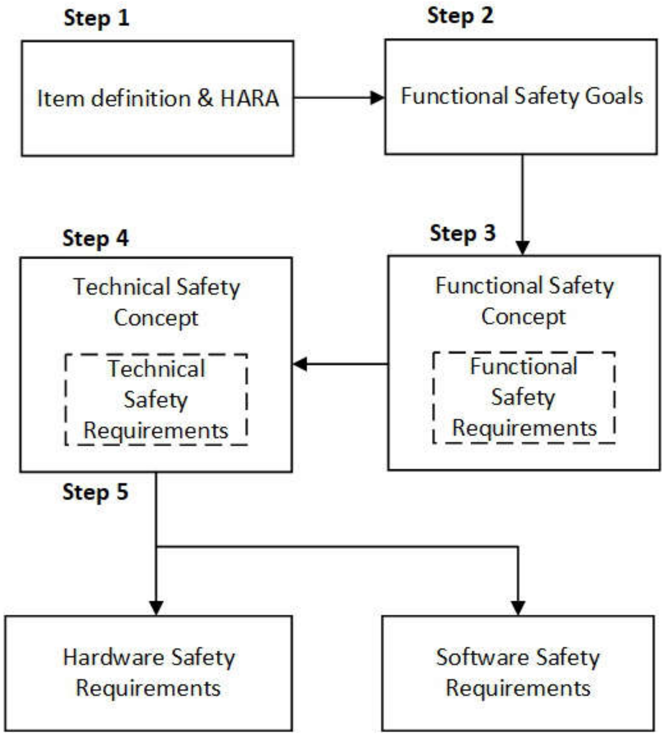

Step 1
Item definition & HARA
Step 2
Functional Safety Goals
Step 3
Functional Safety Concept
Functional Safety Requirements
Step 4
Technical Safety Concept
Technical Safety Requirements
Step 5
Hardware Safety Requirements
Software Safety Requirements

Figure 1-1. Development of SW/HW Requirements

1.2.1 Item Definition

The first step in FuSa design is the item definition. The item is the top-level vehicle function or subsystem that will be the subject of functional-safety analysis. The objectives of item definition are:

- Define and describe the item, its dependencies on, and interaction with the environment and other items.
- Support an adequate understanding of the item so that the activities in subsequent phases can be performed.

This step incorporates hazard analysis and risk assessment (HARA), a systematic methodology that transforms identified functional hazards into quantified Automotive Safety Integrity Levels (ASILs) and corresponding safety goals. The HARA process establishes clear traceability to the item definition while providing a risk-based foundation for all subsequent safety activities. The primary objectives of HARA include:

- Identify all potential hazardous events that could result from the item.
- Rigorous risk assessment through detailed analysis of each hazard's severity, exposure probability, and controllability factors.
- Assignment of appropriate ASIL classifications based on the assessment results.

Hazard identification can be carried out using techniques such as Failure Modes and Effects Analysis (FMEA), Hazard and Operability studies (HAZOP), or lessons learned from past quality problems. Each identified hazardous event is then evaluated for Severity (S), Exposure (E) and Controllability (C) and assigned an ASIL. The appropriate ASIL for each event can be derived from the matrix shown in Table 1-3.

Table 1-3. ASIL Ratings According to ISO 26262

Severity	Exposure	Controllability		
		C1 (Simple)	C2 (Normal)	C3 (Difficult, uncontrollable)
S1 (Light and moderate injuries)	E1 (Very low)	QM	QM	QM
	E2 (Low)	QM	QM	QM
	E3 (Medium)	QM	QM	A
	E4 (High)	QM	A	B
S2 (Severe and life-threatening injuries – survival probable)	E1 (Very low)	QM	QM	QM
	E2 (Low)	QM	QM	A
	E3 (Medium)	QM	A	B
	E4 (High)	A	B	C
S3 (Life threatening injuries – fatal injuries)	E1 (Very low)	QM	QM	A
	E2 (Low)	QM	A	B
	E3 (Medium)	A	B	C
	E4 (High)	B	C	D

1.2.2 Functional Safety Goal

The second step is to formulate the FuSa goal and the corresponding safe state for hazard events. A FuSa goal is a high-level safety requirement that must be satisfied to prevent the occurrence of a hazard identified during the HARA. It is derived from a comprehensive analysis of all possible failure modes of the component or system. For every FuSa goal a corresponding safe state must be specified; the system must transition to that safe state whenever the associated hazard event occurs.

According to Table 1-3, each hazard assigned an ASIL from A through D requires at least one FuSa goal, whereas hazards classified as QM do not require a safety goal. When multiple hazards lead to similar safety goals but have different ASILs, they can be consolidated into a single goal using the highest ASIL among them.

1.2.3 Functional Safety Concept

The third step is to develop the functional safety concept (FSC). FSC provides a high-level, risk-based description of how a vehicle function or subsystem will achieve an acceptable level of safety, which is the bridge between the FuSa goal and the concrete design of safety mechanisms. The objectives of FSC are:

- Derive functional-safety requirements (FSRs).
- Allocate each FSR to the relevant subsystems or to external safety measures that must be added to the architecture.

The ASIL, as an attribute of the safety goal, is inherited by each subsequent safety requirement. In case a single FSR is difficult to meet directly, ISO 26262 permits its ASIL decomposition into multiple redundant FSRs distributed across sufficiently independent design elements. This decomposition typically allocates requirements between primary functional elements and external measures element - additional safety mechanisms such as redundancy implementations, monitoring circuits, or fault detection systems.

If ASIL decomposition is applied, this activity shall follow the permitted ASIL decomposition schemas in accordance with ISO 26262-9, as shown in Table 1-4.

Table 1-4. ASIL Decomposition Schemas

Decomposition	Original requirement			
	ASIL D	ASIL C	ASIL B	ASIL A
Option 1	ASIL B(D)+ ASIL B(D)	ASIL A(C)+ ASIL B(C)	ASIL A(B)+ ASIL A(B)	QM(A)+ ASIL A(A)
Option 2	ASIL A(D)+ ASIL C(D)	QM(C)+ ASIL C(C)	QM(B)+ ASIL B(B)	-
Option 3	QM(D)+ ASIL D(D)	-	-	-

For each FSR, a fault-tolerance time interval (FTTI) must also be specified. FTTI is the maximum time between the occurrence of a fault and the system reaching a safe state before an unacceptable hazard can occur.

1.2.4 Technical Safety Concept

The fourth step is to develop the technical safety concept (TSC), which is the more detailed implementation-level counterpart of the FSC. The objectives of TSC are:

- Derive the technical safety requirement (TSR).
- Demonstrate that the TSRs comply with the corresponding FSRs.

Moving from the FSC to the TSC involves allocating the functional blocks defined in the FSC to concrete physical architecture. In other words, the TSC refines the high-level safety goals and FSRs into specific hardware and software development requirements for the product.

Fault-handling time interval (FHTI) encompasses both the detection time and reaction time, representing the total time available for the safety system to respond to a fault, as illustrated in Figure 1-2. [2]

- Fault Detection Time Interval (FDTI): The time period between the occurrence of a fault and its detection by diagnostic measures. It represents how quickly a system can identify that a fault has occurred.
- Fault Reaction Time Interval (FRTI): The time period between the detection of a fault and the initiation of the specified reaction to that fault. This represents how quickly a system responds after detecting a fault.

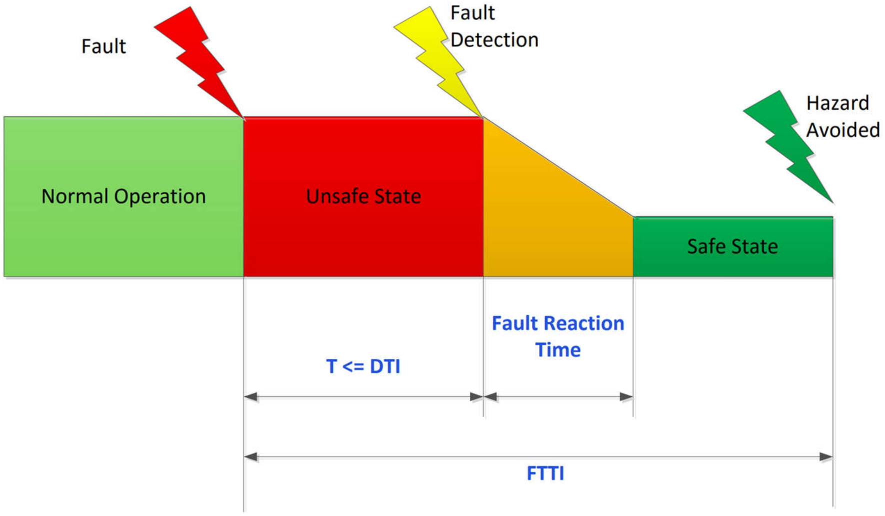


Figure 1-2. Relationship Between FDTI, FRTI and FTTI

TSRs can be obtained through fault-tree analysis (FTA) or failure-mode-effects analysis (FMEA).

- FTA is a top-down method that starts with an undesired top-level event and decomposes it into the underlying causes, providing a systematic view of critical failure paths. This top-down approach is commonly implemented to assess critical failures systematically.
- FMEA is a bottom-up method that examines individual components, identifies their possible failure modes, and evaluates the impact of those failures on the overall system. This bottom-up approach is commonly implemented to assess the potential failures.

1.2.5 HW/SW Safety Requirement

The fifth step is to derive the specification of hardware safety requirement (HSR) and software safety requirement (SSR). Both sets of requirements are traceable from the original functional-safety requirement, carry the same ASIL, and together constitute concrete, verifiable safety features.

HSRs are those TSRs that specify how a hardware element must behave so that the FSR assigned to it is satisfied. This is obtained in the TSC by analyzing the FSR with FTA, FMEDA, or FMEA. The HSR is always traced back to a single FSR and inherits the ASIL.

SSRs are those TSRs that define the behavior, quality, and verification criteria a software unit must satisfy to fulfill the allocated FSR. This is obtained in the TSC by mapping each FSR to software functions and then analyzing the possible software failure modes. The SSR inherits the ASIL of the associated FSR.

Hardware-software interface (HSI) is the set of safety-critical connections that specifies information cross the hardware-software boundary. HSI is introduced in the TSC and then implemented in HSR and SSR, which is important in proving that hardware-software boundary is explicit, deterministic, and independently verifiable.

1.2.6 Dependent-failure Analysis

Dependent-failure analysis (DFA) is a systematic method for identifying and mitigating failures that arise due to dependencies between systems or components that are supposed to be independent, including cascaded failures (CFs) and common-cause failures. (CCFs).

- CF is a failure in one component that triggers a failure in another component, and both failures result from the same root cause. CF is expressed as AND gates in fault tree.
- CCF is a single root cause that disables two or more safety-related items simultaneously.

DFA is applied throughout the FuSa design. It is performed in the concept phase and will be refined through system, hardware and software development. The objectives of DFA are:

- Confirm the required independence or freedom from interference is sufficiently achieved in the design.
- Define safety measures for potential dependent failures.

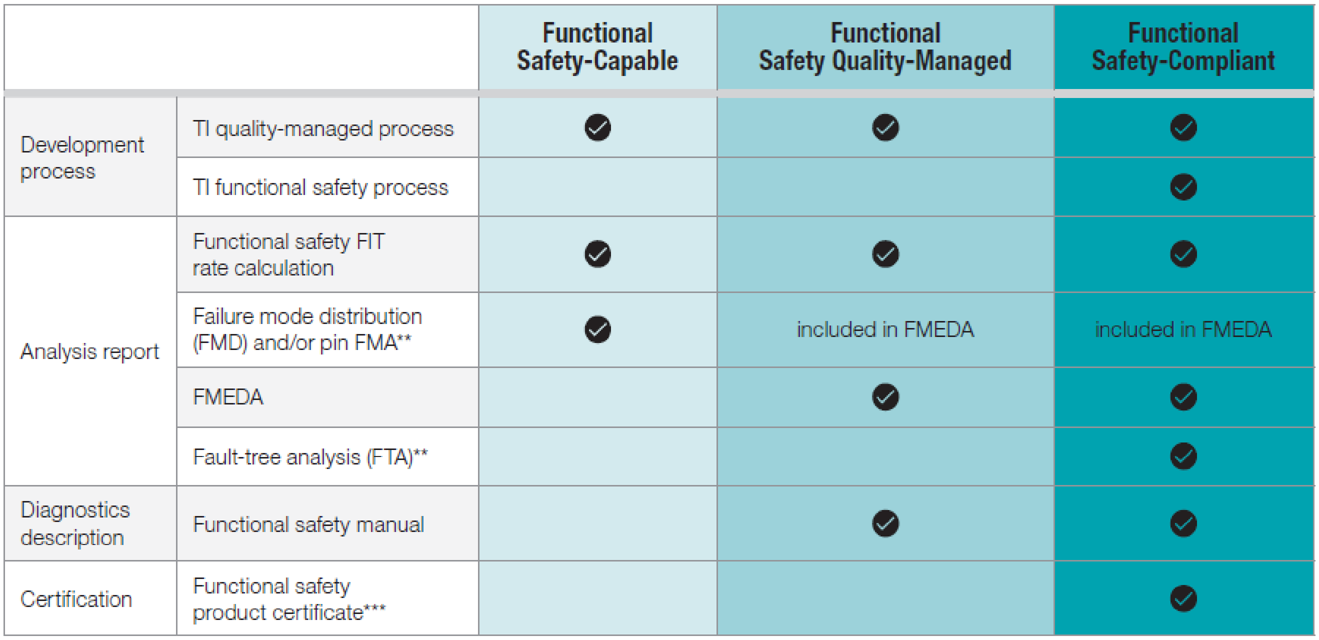
1.3 TI Collaterals

1.3.1 TI Components Category

Although the system integrator is ultimately responsible for carrying out the system-level functional-safety analysis and compliance process, selecting the appropriate components is essential to succeed. Texas Instruments simplifies this task by organizing the offerings into clear functional-safety categories.

As shown in Figure 1-3, TI parts are classified as FunctionalS afety-Capable, Functional Safety Quality-Managed, or FunctionalS afety-Compliant, making it easier for engineers to identify the right products for safety-critical designs.

- Functional Safety-Capable Products:
  - Simpler ICs that are developed using TI's standard quality-managed development flow.
  - Safety functions such as internal monitoring and diagnostics are not always integrated.
  - TI provides FuSa FIT rates calculation, FMD and Pin FMA.
- Functional Safety Quality-Managed Products:
  - Complex products that have internal diagnostic features.
  - Developed using TI's standard quality-managed development flow.
  - Extensive set of documentation: FMEDA analysis, FuSa manual.
- Functional Safety-Compliant Products:
  - The most complex products that can be systems in their own right.
  - Developed according to the certified FuSa development flow prescribed in ISO 26262: 2018.
  - Further extensive documentation: Fault-tree analysis, FuSa product certificate.



		Functional Safety-Capable	Functional Safety Quality-Managed	Functional Safety-Compliant
Development process	TI quality-managed process	✓	✓	✓
	TI functional safety process			✓
Analysis report	Functional safety FIT rate calculation	✓	✓	✓
	Failure mode distribution (FMD) and/or pin FMA**	✓	included in FMEDA	included in FMEDA
	FMEDA		✓	✓
	Fault-tree analysis (FTA)**			✓
Diagnostics description	Functional safety manual		✓	✓
Certification	Functional safety product certificate***			✓

Figure 1-3. TI's Categories for Products in FuSa Design

*** May only be available for analog power and signal chain products.*

**** Available for select products.*

The functional-safety manual [3] describes the safety functions and shows how external components can be employed to obtain the required fault-coverage and diagnostic capabilities. TI's standard quality-managed development flow, also mentioned above, is the company's process for handling both systematic and random faults. More detailed description of this process is shown in [3].

1.3.2 FuSa Collaterals for Safety MCU

TI C2000™ real-time MCUs are independently assessed and certified by TÜV SÜD to meet a systematic capability up to ASIL D and help users build automotive applications requiring functional safety. In addition to the Functional Safety-Compliant collaterals in Figure 1-3, more documentation and software libraries are provided to streamline and speed up the FuSa design. The C2000 safety collateral can be found in [4].

- Development process certificate. TUV-SUD certificate for QRAS-AP00210. FuSa development process for IEC 61508-2 and ISO 26262-5 compliant components.
- C2000 safety package. By request and NDA required. Packages include technical report on random HW capability, technical report on systematic capability, FMEDA, device concept assessment, safety analysis report and device-specific self-test library package.
- Software diagnostic library. A library of modules and examples demonstrating safety features and mechanisms. CPU, memory, clocks, watchdogs, HWBIST, etc.
- FuSa flash APIs. Library is available in C2000Ware. Contact local TI representative for further compliance support package offerings.
- Compiler qualification kit. Compare compiler coverage for customer use cases against coverage of TI compiler release validations.
- Safety certified RTOS. Pre-certified safety real time operating system.
- MathWorks simulation and code generation. IEC certification kit helps you qualify MathWorks code generation and verification tools to streamline certification of your embedded systems.

2 FuSa Concepts of OBC System

This section outlines the overall FuSa design for an on-board-charger (OBC) application and demonstrates how the ISO 26262: 2018 development process can be applied at the system level. The discussion follows the sequence of steps introduced in Section 1.2.

System-level FuSa analysis is strongly dependent on the specific usage scenarios and architecture, and the responsibility rests with the system integrator. The example presented here is intended solely for training purposes and must not be taken as a substitute for a complete, production-grade system design.

2.1 Item Definition

2.1.1 Item Functions

The *item* refers to the highest-level entity that undergoes the safety lifecycle. When defining an OBC, the description must specify what the OBC is, how the OBC functions, and how the OBC interacts with other items. OBC is used to charge the High-voltage (HV) battery from the AC grid while meeting performance, safety, and communication requirements defined by automotive standards.

The OBC architecture has evolved through several generations:

- Early designs were low-power (≤ 3.3kW), uni-directional converters that used a diode rectifier plus boost converter as power-factor-correction (PFC) stage followed by a separate DC-DC stage.
- The next generation increased the rating to 6.6kW and added bi-directional capability, employing a totem-pole PFC stage and a bi-directional DC-DC converter stage. Figure 2-1 shows the typical single-phase dual-stage OBC topology (Left one) and three-phase dual-stage OBC topology (Right one), which are the mainstream topologies in the current market.
- The most recent trend is a single-stage OBC topology, which reduces component count, cost while delivering higher power density. The architecture merges PFC stage and DCDC stage into one high frequency conversion stage. Single-stage OBC topology also has many different variants. Figure 2-2 shows two typical single-stage OBC topologies. Left one is the interleaved totem-pole single-stage topology, and right one is the quasi single-stage topology.

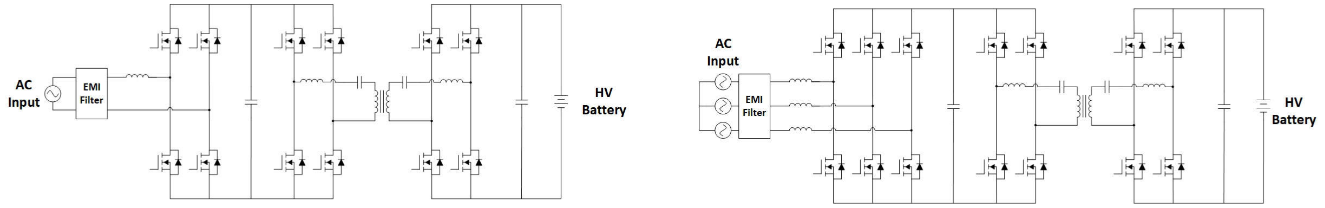


Figure 2-1. Block Diagram of the Dual-Stage OBC

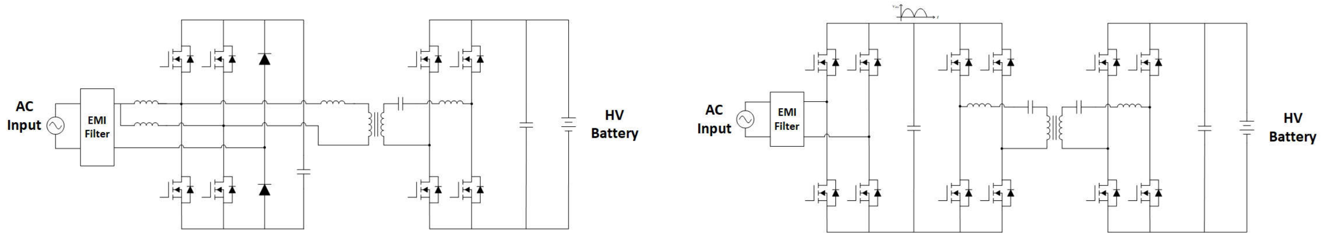


Figure 2-2. Block diagram of the Single-Stage OBC

Despite the single-stage topology in Figure 2-2 gaining notable market interest, the matrix converter is currently the most prominent single-stage topology under discussion. Figure 2-3 shows the block diagram of a matrix converter. This application note takes matrix converters as an example for further FuSa analysis; however, the majority of the analysis is also applicable to single-phase and three-phase dual-stage topologies or other single-stage topologies.

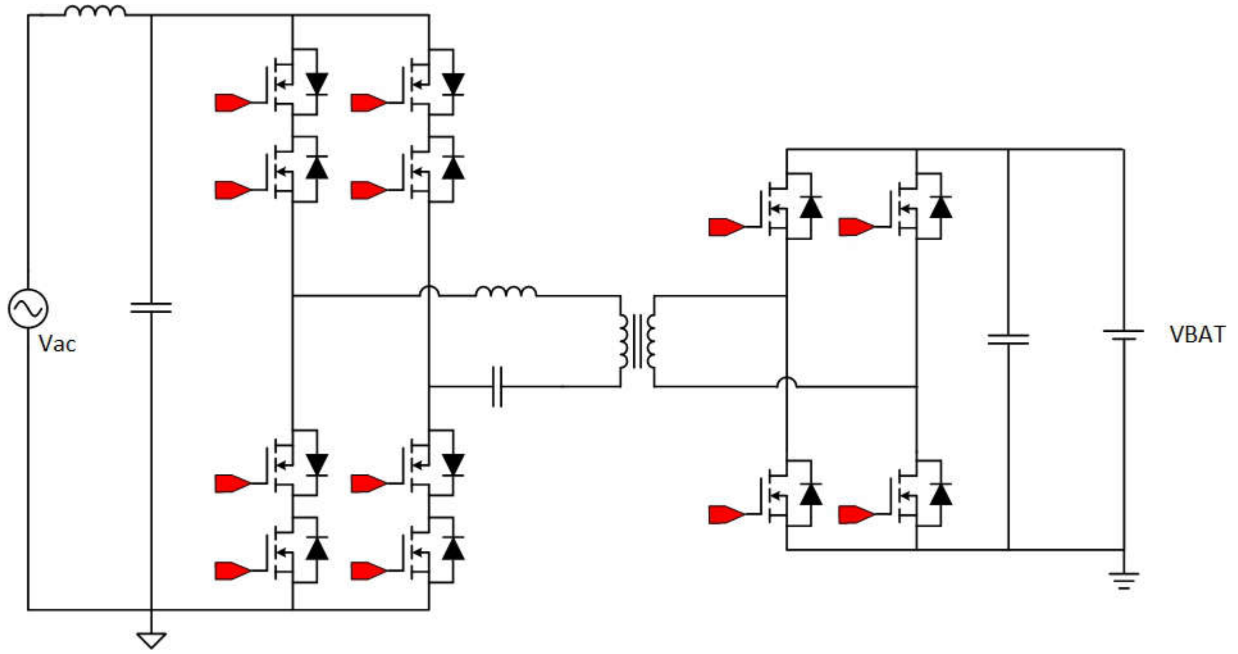


Figure 2-3. Block Diagram of the Matrix Converter

In summary, the OBC performs the following primary functions:

- Power conversion: The OBC performs power conversion with a power level that meets the requirements of the charging station, cables, and the battery.
- Power-factor correction: The OBC shapes input current into a sinusoidal waveform, aligns the input current with the grid voltage and minimizes the harmonics of the input current.
- Output regulation: The OBC performs real-time control of the battery-charging voltage and current according to BMS set-points, temperature limits and state-of-charge limits.
- Vehicle-to-X (V2X): V2X is the umbrella term of OBC operates in reverse mode, and X represents different endpoints in the communication network. Vehicle-to-load (V2L) allows vehicles to serve as mobile power sources to load. Vehicle-to-grid (V2G) allows vehicles to return electricity to the grid. Vehicle-to-vehicle (V2V) enables vehicles to serve as mobile power source to charge another vehicle. Vehicle-to-home (V2H) enables electric vehicles to power homes during outages or high electricity costs.
- Galvanic isolation: Isolation between the AC side and the HV DC bus.
- Protection: Provides comprehensive protection against electrical faults, thermal faults and isolation faults.
- Communication: CC/CP signaling at the AC inlet. CAN communication for charge instruction, mode selection and status reporting.
- Diagnostics: Monitor system status and reports any fault conditions.

Because the topology is matrix converter, the FSC for this safety goal possesses several distinctive characteristics that set it apart from conventional two-stage OBC.

- Overcurrent at the OBC output cannot be handled by simply switching all power devices off. With no free-wheeling path available, turning off every power switch simultaneously generates a tremendous voltage spike that could damage the power switches. Consequently, a sophisticated turn-off sequence for the power switches is required.

- The AC-side current can be used as a plausibility check. Since matrix converter does not include a DC-link capacitor, the transient DC-output current is directly reflected in the AC-side current. In contrast, a conventional two-stage OBC relies on the DC-link capacitor to supply the transient DC current.
- Shorter FTTI. Matrix-transformer topologies operate at much higher switching frequencies, which generally necessitates the use of SiC or GaN devices. Compared with conventional silicon switches, SiC/GaN transistors require a significantly faster current-protection response, thereby shortening the allowable fault-tolerance time interval.

- For gate driver, the interlock feature between two channels must be disabled because back-to-back power switches can be controlled to turn on at the same time. The UVLO feature of the gate driver must not be falsely triggered, as this can also lead to the problem of having no freewheeling path.

2.1.2 System Boundaries

System boundaries define the exact scope of the *item* for which the safety life-cycle is performed. This separates everything that belongs to the safety-relevant system (in-scope) from the surrounding vehicle, infrastructure, or environment (out-of-scope). Table 2-1 summarizes the system boundaries.

Table 2-1. System Boundaries in Item Definition

System Boundaries	In Scope	Out of Scope
Power conversion	Matrix converter Key analog components	Grid side infrastructure External connectors and fuses
Communication	Communication with AC inlet CAN wiring to BMS / VCU	Higher-level vehicle networks in VCU. BMS, E-lock, High-voltage interlock (HVAC, HVDC)
Environment	Ambient temperature Coolant temperature	Mechanical components (Cold plate, Grounding), Humidity, EMC

2.1.3 External Interfaces

The whole process of HV battery charging has been defined in several standards, such as GBT 18487.1 - 2023. This chapter describes the interface between HV battery charging system and other systems beyond the OBC boundary, which can be an input to HARA analysis.

From the system boundaries, the interfaces can be also divided into power interface, communication interface, and environment interface, as shown from Table 2-2, Table 2-3 and Table 2-4.

Table 2-2. Power Interfaces

Power Interface	Connectors	Purpose
AC input	Line, Neutral, PE	Supplies main voltage. Specs: 85V to 265V, 50Hz, maximum 7kW
HV DC output	HV+, HV-	Delivers the regulated DC charging voltage (250V to 460V) and current (Typ. 22A) to battery pack.
Power supply	KL30	Permanent battery positive terminal/connection.

Table 2-3. Communication interface

Communication Interface	Connectors	Purpose
AC inlet	CC, CP, Charging gun temperature	CP carries the 1kHz PWM *pilot* that indicates plug-in status, max-current capability, and vehicle-ready state. CC carries a low-level DC current used for charger-ready and error.
Ignition	KL15	Switched ignition power terminal/connection.
BMS	CAN-H, CAN-L	Exchange battery state, charging limits, and fault codes.
VCU	CAN-H, CAN-L	High-level charging mode commands, charging-set-point commands, safety-state requests, diagnostic requests.
Test pins	Hardwired, JTAG	Used during manufacturing or debug.

Table 2-4. Environment interface

Environment Interface	Connectors	Purpose
Thermal interface	Coolant temperature, Ambient temperature	Provides thermal management for power switches, magnetics, key analog components and other passive components. Coolant temperature: - 40°C to 85°C. Ambient temperature: -40°C to 85°C

2.1.4 Operation Modes

The behavior of single-stage OBC is organized into a small set of operational modes that are selected by the vehicle-level controller (VCU/BMS) or by internal logic when a fault is detected. Table 2-5 lists the key operation modes of single-stage OBC.

Table 2-5. Key Operation Modes of Single-Stage OBC

Operation Modes	Use Case	Status
Stand-by	Normal driving, Vehicle standby	Power converter disabled. Waiting for wake-up.
Derating charging	Battery deeply discharged, Battery low temperature, battery high temperature	Limit charge current to safe value based on the voltage and temperature.
AC charging	Standard charging.	Regulate battery-pack voltage and current to the BMS set-points.
Regenerative	V2G, V2L, V2V, V2H	Reverse the power-stage operation.
Maintenance	Factory diagnostics, Firmware update	Run predefined test patterns.
Emergency	Safety-critical fault is detected, Communication is lost	Stop power conversion. Report fault code to VCU/BMS.

The operating modes also encompass the OBC's usage profile, which varies greatly from one customer to another. This includes factors such as charging frequency, typical charging duration, specific charging scenarios, and average charging power. Assessing the cycle-life is crucial for the HARA. An illustrative mission-profile example is shown in Table 2-6.

Table 2-6. Illustrative Mission-Profile Example of Single-Stage OBC

Profile	Value	Rationale
Daily charging events	1.5	Home charging and workplace charging.
Average charging time	6h	Average of overnight or workhour charging.
Average power	7kW	Typical power for single-phase charging pile
Lifetime	8 years	Typical frequency for updating vehicles
Total cycles	4380 cycles	Rounded 5000 cycles for safety evaluation

Based on the above analysis, Figure 2-4 is the system-level block diagram including major components and interfaces.

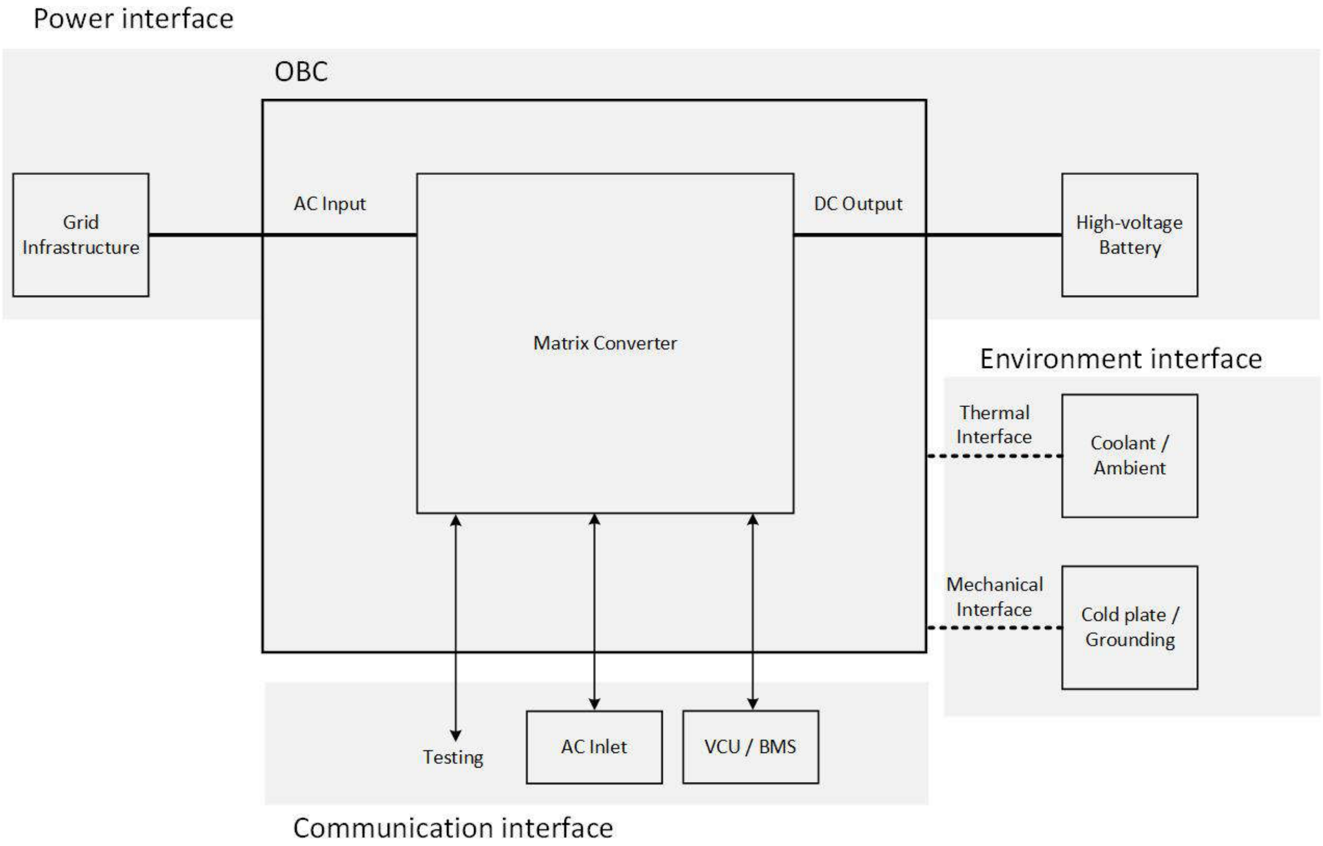


Figure 2-4. Item Definition Level System Block Diagram

2.2 Functional Safety Goal

Prior to conducting the HARA, the following simplifying assumptions are adopted to limit the analysis scope:

- Item functions (Section 2.1.1): The OBC employs a single-stage matrix-converter topology, and primary item functions include power conversion, voltage regulation, galvanic isolation, protection, communication and diagnostics.
- System boundaries (Section 2.1.2): Only the OBC system is in the scope; the HV-LV DC-DC converter, PDU, and any other electronic control units are excluded.
- External interfaces (Section 2.1.3): A single MCU controls the OBC. This MCU is dedicated solely to OBC control and interfaces with the AC inlet as well as the BMS/VCU.
- Operation modes (Section 2.1.4): The main function is to charge the high-voltage battery, and the analysis focuses exclusively on the fast-charge operating mode.

Once the functions, processes, and interactions of each item have been defined, the next phase is the HARA. Using the assumptions and analyses already established, any incorrect behavior in each subsystem can give rise to potential hazard events, such as DC overvoltage, DC bus overcurrent and thermal failure.

Each hazard must be evaluated separately using the ISO 26262: 2018 criteria of Severity (S), Exposure (E) and Controllability (C). Take thermal failure as an example:

- Severity: The worst consequence of a thermal failure is a vehicle fire, which can cause life-threatening or fatal injuries. Consequently, the event is assigned to S3.

- Exposure: In the OBC usage profile, the charger is active for a moderate portion of the vehicle's overall operating time. This corresponds to an exposure rating of E3.
- Controllability: While the vehicle is stationary during charging, the driver can promptly interrupt the charging circuit (e.g., by disengaging the charger or opening the contactors). Therefore, the event is considered C2.

According to Table 1-3, the combination S3 – E3 – C2 corresponds to ASIL-B, so the thermal-failure hazard is assigned ASIL-B.

Regarding DC bus overcurrent, it will not have a significant impact on the high-voltage battery, because the maximum charging current of the high-voltage battery is much higher than the current of AC charging. However, overcurrent can cause the power devices on the OBC output side to overheat and fail due to short circuits. Following a short-circuit failure, the high-voltage battery can create a low-impedance pathway through the OBC, potentially resulting in severe system overheating and, in extreme cases, vehicle fires. The exposure and controllability level are the same as thermal failure. According to Table 1-3, the combination S3 – E3 – C2 corresponds to ASIL-B, so the DC bus overcurrent hazard is assigned ASIL-B.

For DC bus overvoltage, it can cause overvoltage breakdown of the power devices on the OBC output side, and overvoltage is also hazardous to Li-ion cells on high-voltage battery, which can further lead to system overheating or even vehicle fire. The exposure and controllability level are the same as thermal failure. According to Table 1-3, the combination S3 – E3 – C2 corresponds to ASIL-B, so the DC bus overvoltage hazard is assigned ASIL-B.

All hazard events need to be analyzed. Since this assessment is typically performed by the system integrator, the detailed evaluation of every hazard is not presented here. HAZOP is a system hazard analysis method, which can provide 7 guide words. Table 2-7 illustrates an example of the HARA analysis. HAZOP leading word is used in malfunction behavior.

Table 2-7. Example HARA Analysis of the Single-Stage OBC

ID	Malfunction Behavior	Potential Vehicle Level Hazard	S	E	C	ASIL
H1	More thermal than expected	Vehicle fire caused by overheating	S3	E3	C2	B
H2	More DC bus current than requested	Vehicle fire caused by OBC short-circuit	S3	E3	C2	B
H3	More DC bus voltage than requested	Vehicle fire caused by OBC short-circuit	S3	E3	C2	B
H4	More electrical interference	Spurious control signals	S1	E3	C2	QM

For hazard events from ASIL A to ASIL D in Table 2-7, at least one safety goal must be identified. A functional-safety goal is a high-level, technology-independent statement that fulfills the safe state requirement.

Table 2-8 is an example entry of FuSa goal. The FTTI value must be derived from hazard analysis and regulatory requirements. Take SG1 as an example, the operating temperature is 65 °C, and the thermal failure critical temperature is 155 °C. With general temperature rise rate 15 °C / s, the time to critical temperature is 6s. 500ms FTTI time is conservative for early detection to allow early intervention before cascading failure.

Table 2-8. Example FuSa Goal of the Single-Stage OBC

ID	Safety Goal	ASIL	Safety State	FTTI
SG1	Avoid vehicle fire due to thermal failure.	B	OBC shutdown, and switch to emergency operation mode.	Specified by users
SG2	Avoid vehicle fire due to DC bus overcurrent.	B		
SG3	Avoid vehicle fire due to DC bus overvoltage.	B		

The safe state requirement states the system-wide response that must be triggered when the hazard occurs. For example, the safe state of SG1 to SG3 is that OBC shall be switched into emergency operation mode, in which key actions are shown as below. Different from dual-stage OBC, this architecture does not contain a DC-link capacitor, so there is no action on discharging DC-link capacitor.

- Disable gate driver in sequence.
- Open all contactors.
- Discharge OBC output bus into safe voltage.
- Log fault condition.

2.3 Functional Safety Concept

After the FuSa goal has been established, the next phase is to develop the FSC. The system block diagram is shown in Figure 2-5, which is one level deeper than the block diagram in item definition. The objective is to define sub-functional elements and interconnections on preliminary architecture diagrams.

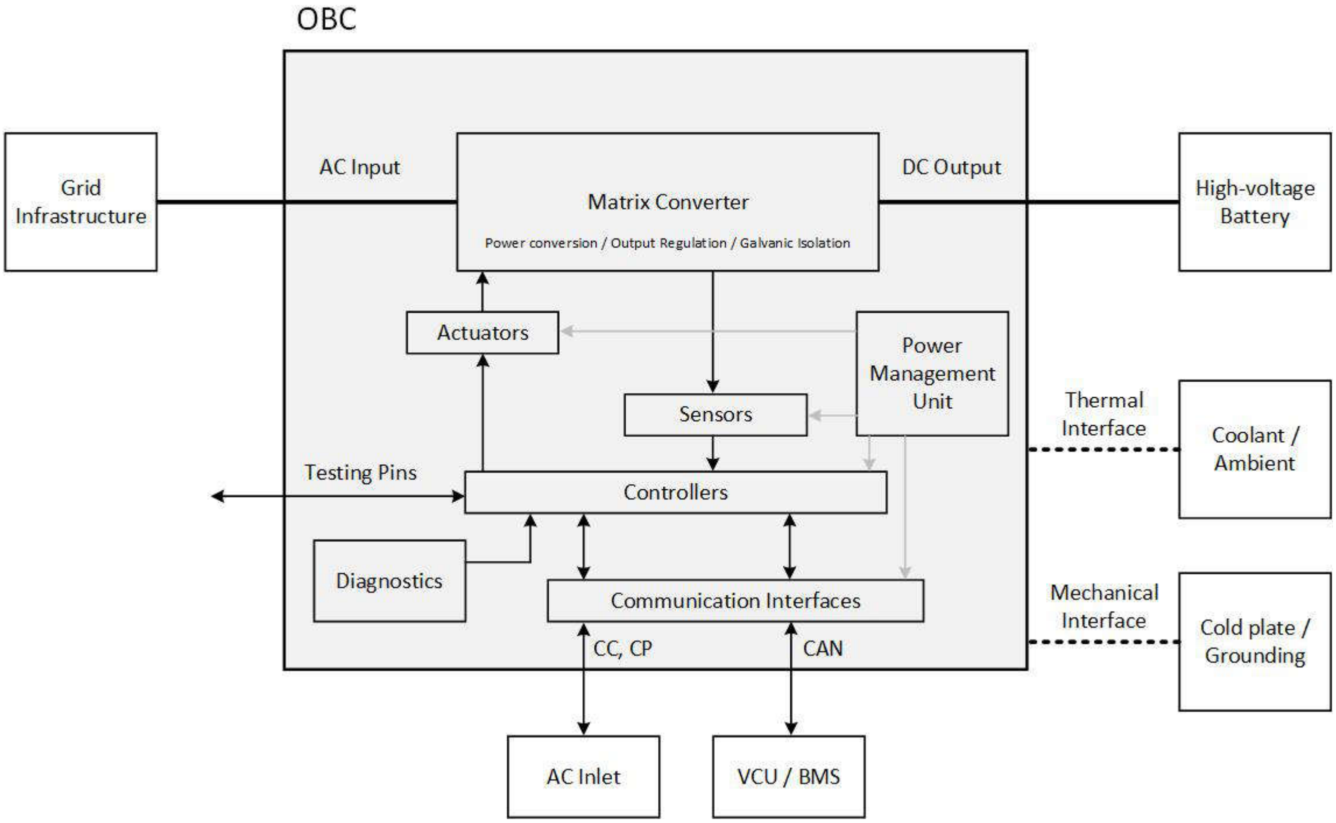


Figure 2-5. FSR Level System Block Diagram

To simplify the analysis, SG2 is chosen as an example. Figure 2-6 is the one level deeper block diagram related to SG2, and related sub-functional elements and interactions are defined in Table 2-9.

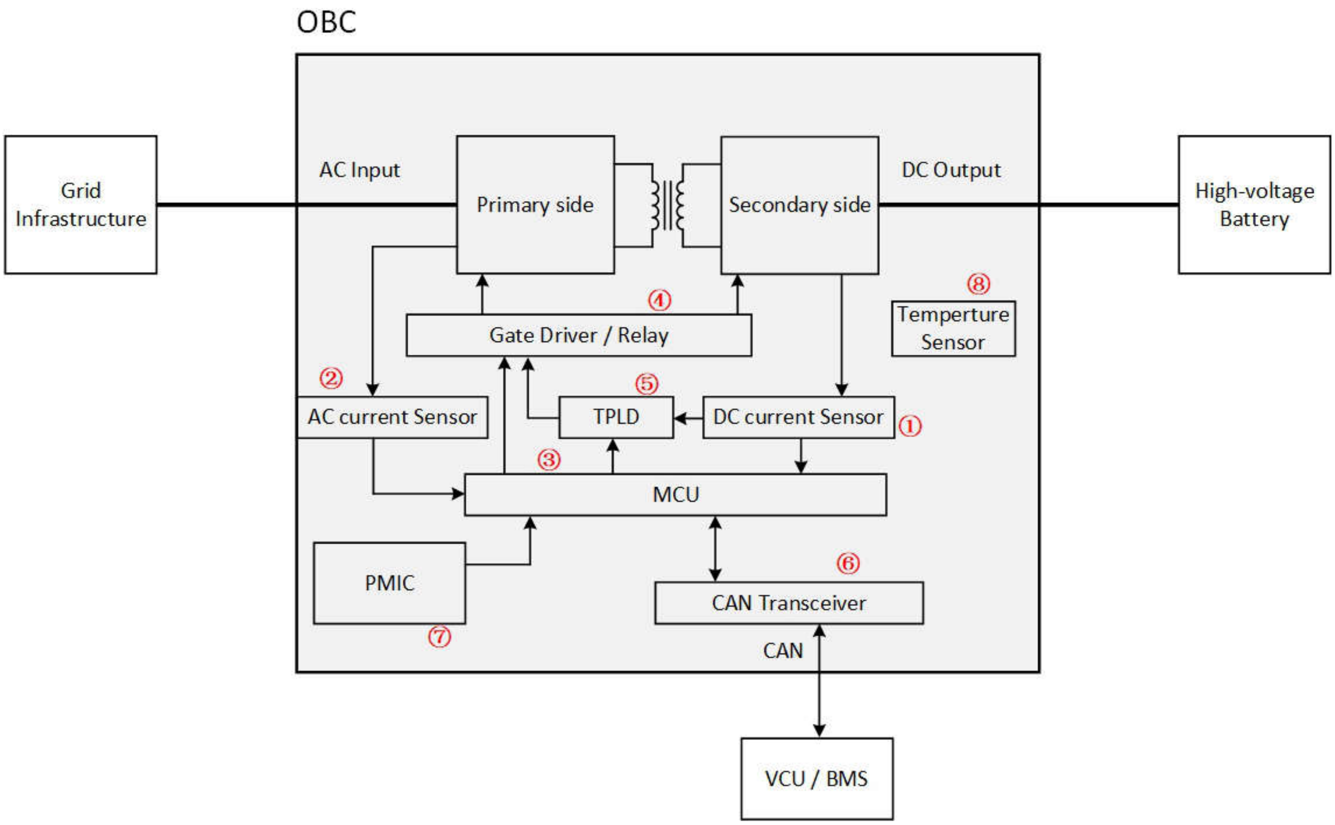


Figure 2-6. FSR Level System Block Diagram of SG2

Table 2-9. Sub-functional Elements and Interactions of SG2

Element ID	Element Name	Description
E1	DC output current measurement circuit	Measure the OBC output current for both constant current control and overcurrent protection.
E2	AC input current measurement circuit	Measure the OBC input current for AC current control and overcurrent protection.
E3	Microcontroller circuit	Executes the charger control algorithm, monitors sensor data, generates PWM signals, and communicates with the vehicle's BMS/VCU.
E4	Gate driver circuit	Provide the required voltage and high-current drive signals of the power switches.
E5	TPLD circuit	Programmable logic device that features power switches switching off sequence with combinational logic.
E6	CAN transceiver circuit	Exchange status and diagnostic information with the BMS/VCU.
E7	PMIC circuit	Provide the power supply to key devices and voltage monitoring for key voltage rails. This also provides an external watchdog and error pin monitor for MCU.
E8	Temperature measurement circuit	Monitors the power switches junction temperature, transformer temperature and the ambient temperature of the converter.

FTA is performed to generate FSRs of SG2. FTA analysis is structured by three steps. The first step is to create the fault tree with SG2 violation as top event, then the second step is to derive each potential malfunction of the defined sub-functional element that leads to top events occur, then the third step is to use logic gates to represent the relationships between events.

Following the above steps, the FTA tree is illustrated in Figure 2-7. Critical failure paths must be identified for cut set analysis. If SPF directly violates the FuSa goal, FSR must be designed; if SPF does not directly violate the FuSa goal, it is necessary to determine whether the dual-point failure system is acceptable and to analyze the independence of dual-point failures.

For the FTA analysis of the SG, in FSR level it can be terminated at the component, while more detailed analysis must be carried out at the TSR level. As shown in Figure 2-7, If there is abnormal current sensing, or a control malfunction, or a power supply issue, SG2 is violated. Then it can be broken down into different components.

- The incorrect current sensing can be caused by the fault on current sensor, or any fault on the discrete comparator used for overcurrent protection.
- The incorrect control command can be caused by many components. It can be caused by communication with VCU (Incorrect charging command or fail to report fault state). It can be caused by incorrect control signals from MCU. It can be caused by the incorrect driving waveform from gate driver. It can be caused by any fault on discrete logic components in the fault reaction path.
- The fault on power supply can cause malfunction of key components, including MCU, gate driver, sensors, voltage references.

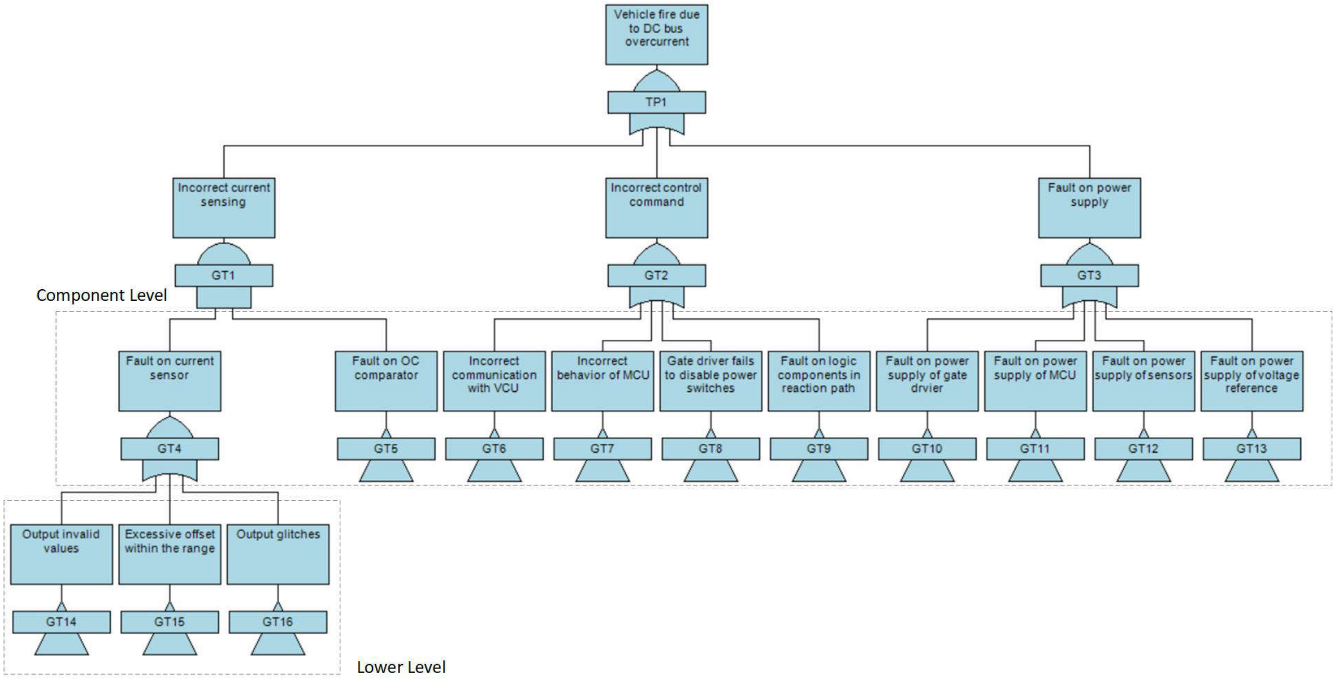

Vehicle fire due to DC bus overcurrent
TP1
Incorrect current sensing
Incorrect control command
Fault on power supply
GT1
GT2
GT3
Component Level
Fault on current sensor
Fault on OC comparator
Incorrect communication with VCU
Incorrect behavior of MCU
Gate driver fails to disable power switches
Fault on logic components in reaction path
Fault on power supply of gate drvier
Fault on power supply of MCU
Fault on power supply of sensors
Fault on power supply of voltage reference
GT4
GT5
GT6
GT7
GT8
GT9
GT10
GT11
GT12
GT13
Output invalid values
Excessive offset within the range
Output glitches
GT14
GT15
GT16
Lower Level

Figure 2-7. The FTA Tree Example of SG2

Cut set is a logical analysis to determine sets of combinations of gate/events which causes the top gate condition to fail.

- 1-order cut set. Only one event can lead the top event occurs. These events are transformed into an FSR with FTTI requirement.
- 2-order cut set. Two events occur at the same time can lead to the top events occurring. These events will be transformed into an FSR with MPFHTI requirement.
- More than 2-order cut set. More than two events occur at the same time can lead to the top events occurring. These events will not be transformed into an FSR.

Each FSR must be assigned to the logical block that is responsible for the implementation. Where an FSR spans more than one block, all relevant subsystems must be listed. Table 2-10 lists the concise set of FSRs that underpin the goal *Avoid vehicle fire due to DC bus overcurrent*.

Table 2-10. Example FSRs for SG2

SG2: Avoid vehicle fire due to DC bus overcurrent.					
ID	**FSR**	**Safe state**	**Allocation**	**ASIL**	**Traced to**
FSR 2.1	DC-bus current sensing system shall perform accurate current measurement.	Assert the OC flag to MCU.	E1 and SW	B	GT4
FSR 2.2	TCAN shall perform correct communication between OBC and VCU.	Transmit OC status to VCU.	E6 and SW	B	GT6
FSR 2.3	MCU shall perform correct control scheme.	Switch to emergency operation mode.	E3 and SW	B	GT7
FSR 2.4	Gate drivers shall drive the power switches correctly.	Disable power switches.	E4	B	GT8
FSR 2.5	Bias supply shall provide reliable voltage to key components.	Provide reliable voltage rail.	E7	B	GT3

2.4 Technical Safety Concept

Once the FSC has been established, the subsequent phase is to create the TSC. The TSC translates the FSCs into concrete TSRs. It is suggested to perform FMEA to generate TSR. For critical components, the analysis confirms:

- Failure modes must be detected by safety mechanisms.
- The response time for fault detection and safe state transition is sufficient.
- The diagnostic coverage meets ASIL requirements.

The TSR level system block diagram of SG2 is shown in Figure 2-8, which is one level deeper than FSC architecture. In Figure 2-8, the sub-functional element design and interconnections are designed. The basic protection path is indicated in red. When an overcurrent occurs, the OC flag from the current sensor is fed to the MCU. Upon detecting the OC flag, the MCU executes a specific shutdown sequence, and the PWM is tripped to verify reliable shutdown.

For each FSR, FMEA must be constructed to identify the failure mode, failure effect and failure cause. Failure paths can be divided into three categories:

- Single-point fault (SPF): Faults directly violate FuSa goal.
- Dual-point fault (DPF): Faults violate FuSa goal when combined with another independent fault.
- Safe fault (SF): Fauls cannot violate FuSa goal, which can be either detected or inherently safe.

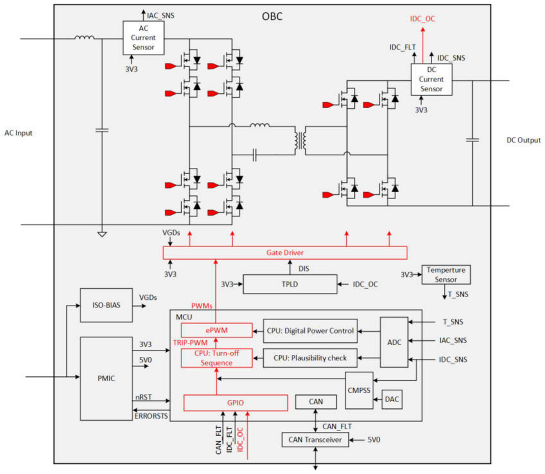


Figure 2-8. TSR Level System Block Diagram of SG2

For each failure that can violate FuSa goal, including SPF and DPF, a safety mechanism is designed. The FMEA table is listed in Table 2-11.

Table 2-11. Example of FMEA Table

System Sub-Element	Main Function	Failure Mode	Failure Effect	SG Violation	Failure Cause	Safety Mechanism
DC output current measurement circuit (E1)	OC Detection	Incorrect asserting OC flag	Fail to identify OC fault	SPF	Fault on OC threshold setting or OC signal chain	Redundant OC flag from MCU CMPSS module.
		Incorrect current sensing	Fail to identify OC fault	DPF	Fault on VOUT signal chain. In this case, the previous SM fails	Plausibility check with AC side current sensor
CAN transceiver circuit (E6)	Report fault status	Communication failure	Fail to report OC fault	SPF	CAN bus failures or local faults	TCAN indicator flags
Gate driver circuit (E4)	Drive power switches	Fail to disable power switches	DC bus short-circuits	SPF	Fault on gate driver or signal chain	Cut-off contactors
Microcontroller circuit (E3)	Execute control and protection	Mismatch switch off sequence	Voltage stress causes failure on power switches	SPF	CPU delayed ISR execution	Independent TLPD circuit to disable gate driver
Microcontroller circuit (E3)	Execute control and protection	Incorrect digital output or PWM signals.	Fail to switch off power switches	DPF	PWM output fault	PWM output redundancy; PWM loop back check
Microcontroller circuit (E3)	Execute control and protection	MCU fails to execute control algorithm.	System failure	SPF	CPU delayed ISR execution	PMIC error pin monitor and reset
PMIC circuit (E7)	Voltage supply	Voltage error	System failure	SPF	Buck/LDO output error	Overvoltage and undervoltage monitoring

From Table 2-11, Safety mechanisms generally can be divided into detection mechanisms and control mechanisms. Detection mechanisms involve but are not limited to plausibility checks, redundant sensing, diagnostic tests and monitoring. Control mechanisms involve but are not limited to safe state transition, fault reaction, warning generation and system shutdown.

For SG2 – *Avoid vehicle fire due to DC bus overcurrent*, take system sub-element DC output current measurement circuit as an example. For current measurement circuit, the current sensor shall have an OC output function that asserts the OC flag when an overcurrent is detected. The sensor must have sufficient bandwidth or response time to capture rapid fault transients.

For SPF on current sensor OC function, it can cause OC to fail to trigger properly. The most straightforward method is to use redundant overcurrent detection circuits. An external isolated comparator can be used as the second signal chain. The output of the isolated comparator can be logically ORed with the OC output of the current sensor, so SPF on current sensing circuit can be covered.

However, additional components leads to an increase in cost. The comparator subsystem (CMPSS) module in MCU can be leveraged as the redundant OC detection. CMPSS provides analog comparison capabilities with digital filtering options. The analog output of the current sensor is fed to the CMPSS module, and after being compared with the voltage threshold inside the MCU, this determines whether the system is in overcurrent status. This safety mechanism is defined as SM1 for the SPF on current measurement circuit.

The premise of SM1 is that the analog output of current sensor is accurate, so the accuracy of current sensor analog output shall be monitored. This can be achieved by plausibility check. Based on the balance of transient power between the input and output of the matrix converter, the DC output current measurement can be compared with the existing current measurement on the AC input of the OBC. Considering the AC voltage drop or low battery voltage, in plausibility check it must compare the input and output power instead of comparing the current. Reactive power and efficiency must also be considered to determine the threshold of plausibility check. The AC-side sensor’s reading provides a secondary verification path without adding an extra DC-bus sensor. This safety mechanism is defined as SM2 for the DPF on the current measurement circuit.

The safety mechanisms on current measurement circuit are illustrated in Figure 2-9.

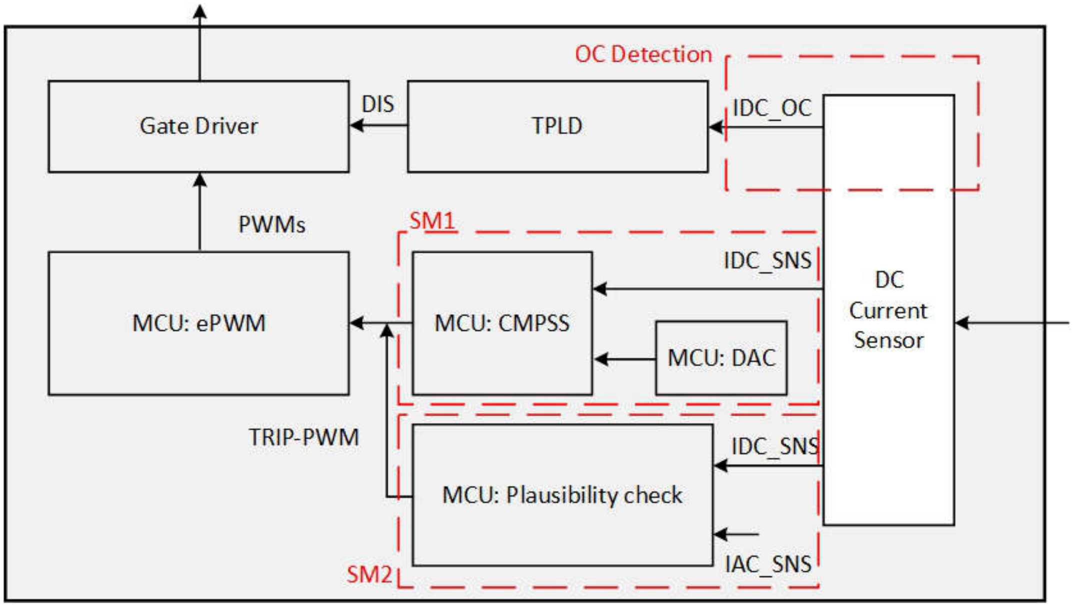


Figure 2-9. Functional Mechanisms on Current Measurement Circuit

For the other system sub-elements in Table 2-11, the detailed analysis is not elaborated here; only some functional safety mechanisms are listed.

- CAN communication with VCU. For the CAN transceiver, it shall establish and maintain reliable bidirectional communication between the OBC and VCU. This critical interface enables the VCU to transmit charging parameters and commands to the OBC while allowing the OBC to report operational status and fault status to the VCU.
  - SM1: Integrated CAN transceiver diagnostics. It enables the microcontroller to continuously assess CAN transceiver health and system integrity. These integrated diagnostic features include undervoltage detection, CAN bus fault identification, software watchdog timer monitoring, battery connection detection, thermal protection, driver dominant state timeout, and comprehensive bus fault protection features.
  - SM2: Advanced end-to-end (E2E) protection features. They are implemented at the protocol level to detect potential communication failures. These techniques include message integrity verification through CRC checksums, sequence counters to detect missing messages, and timestamp to identify communication timing anomalies. This layered approach verifies reliable information exchange even when hardware-level diagnostics cannot directly detect certain fault conditions.
- Driver power switches. For the gate driver, it shall switch off power switches when fault is detected, and system must turn into safe state. Usually for OBC applications, standard isolated gate driver is used, which does not have a self-diagnostic function. If power switches are turned off at the same time, since a single-stage OBC has no freewheeling path, this can result in significant voltage spikes in the power switches.
  - SM1: Independent TLPD circuit to disable gate driver. For the method using PWM shutdown, if there is SPF in the signal chain or the input pin, power switches switching off will violate the specified sequence. TPLD is the programmable logic device that features power switches switching off sequence with combinational logic. This hardware-only path is independent of any software execution. The output of TPLD circuit is connected to the EN pin of gate driver, so the SPF on the PWM signal chain can be covered.
  - SM2: Cut off the contactor as independent fault reaction. If there is an SPF on the secondary side of the driver, power switches cannot be reliably turned off. For this situation, by turning off the contactor on the OBC input and output, the OBC can be disconnected from the input and output interfaces.
- Voltage supply. PMIC provides the voltage supply of key components. Because PMIC is already FuSa compliant components, FuSa mechanisms are elaborated in the safety manual. Some typical voltage supply related FuSa mechanisms are listed below.

- SM1: Redundant OVLO/OVP voltage monitor on VSYS.
- SM2: Output voltage monitor.
- SM3: Residual voltage detection.

- SM4: ABIST during power-up sequence.
- SM5: Redundant UV/OVP voltage monitor on VREG and VDD_1P8.
- SM6: CRC on register map.
- MCU executes control and protection. Because MCU is already FuSa compliant components, FuSa mechanisms are elaborated in the safety manual. Some of the relevant safety mechanisms will be introduced in Section 3.2 of this application note. In addition to the MCU's safety mechanisms, the PMIC also plays a monitoring role for the MCU. Some typical MCU monitoring related FuSa mechanisms are listed below.
  - SM1: MCU error signal monitor.
  - SM2: Readback on digital output pins (nINT/GPIO and GPIO)
  - SM3: Implement the independent watchdog function to detect software execution failures.

In summary, multilayered safety mechanisms are adopted to verify this safety goal is not violated. Plausibility check and redundancy are implemented to provide reliable fault identification. Independent protection paths deliver corrective actions for any over-current event. Comprehensive diagnostics verify early detection of potential faults before they become safety critical.

Safety mechanism for SPF must be transformed as a TSR with FHTI requirement, and safety mechanism for DPF must be transformed into a TSR with MPFHTI requirement. Table 2-12 is the example of TSRs for current-sensor-related FSRs. Where several FSRs call for the same hardware or software capability, the related requirements are combined into a single TSR. Each TSR inherits the ASIL-B of the source FSRs and the FTTI required to satisfy the most stringent timing constraint among the grouped FSRs.

Table 2-12. Example TSRs for FSR 2.1

FSR 2.1: DC-Bus Current Sensing System Shall Perform Accurate Current Measurement					
ID	TSR	Allocation	ASIL	Safe State	Traced to
TSR-CS-1	The DC bus current sensor shall sense the current within 2% accuracy (For SW OCP and plausibility check)	Current sensor Vout pin.	B	Enter user processing SW	FSR2.1 - Current sensing
TSR-CS-2	The DC bus current sensor shall perform self-test and report faults if the test fails.	Current sensor FLT pin.	B	Report FLT to MCU	FSR2.1 - Current sensing, OC detection
TSR-CS-3	The DC bus current sensor shall assert OC pin when current is 20% higher than the overcurrent threshold.	Current sensor OC pin.	B	Report OC to MCU	FSR2.1 - OC detection
TSR-CS-4	The MCU shall perform the plausibility check of two independent current-sensor readings and flag a fault for > 20% error.	MCU ADC module.	B	Stop charging	FSR2.1- Current sensing
TSR-CS-5	The MCU shall perform software OC protection and disable PWM output if OC is detected.	MCU CMPSS module.	B	Stop charging	FSR2.1 - OC detection

All TSRs are traceable to the originating FSRs, carry the same ASIL-B classification, and respect the FTTI required by the safety goal *Avoid vehicle fire due to DC bus overcurrent*.

2.5 HW/SW Safety Requirement

After the TSRs have been established, the next phase is to turn them into HSRs and FSRs. Each HSR/SSR inherits the ASIL-B of its parent TSR and respects the FTTI that is imposed by the most restrictive FSR in the group. The HSR defines the hardware characteristics that must be built into the current-sense front-end; the SSR defines the software actions that must be performed on the measured signal to satisfy the timing and detection criteria.

According to Table 2-12, the current sensor must be able to indicate a short-circuit condition with sufficient bandwidth or response time, and also includes a self-diagnosis function. For these reasons, the TMCS1133-Q1 was selected as the current sensor in OBC application, and it is placed at the input side of PFC stage and the output side of DCDC stage. The pin diagram is shown in Figure 2-10. Alternate shunt-based current sensing method may also be used, but in this case, HSRs and FSRs are different and this is not covered in this document.

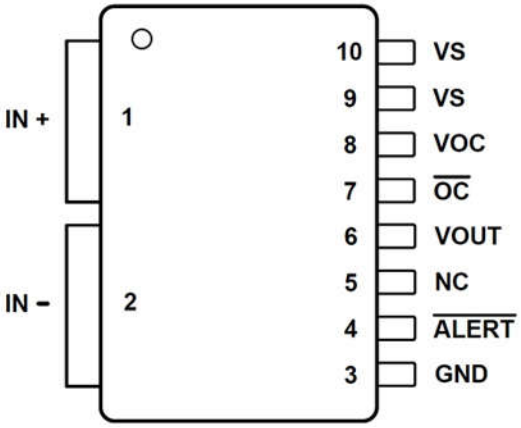


Figure 2-10. Pin Diagram of TMCS1133-Q1

In Table 2-12, TSR-CS-1, TSR-CS-2 and TSR-CS-3 are allocated to current sensor, and TSR-CS-4 and TSR-CS-5 are allocated to MCU. Table 2-13 and Table 2-14 are an example of HSR and SSR that realizes these TSRs traced to FSR 2.1.

Table 2-13. Example of HSR for TSRs Traced to FSR 2.1

ID	HSR	ASIL	Traced to
HSR-CS-1A	Hall sensor shall have > 200 kHz bandwidth, and VOUT filter also shall have > 200kHz cutoff frequency.	B	TSR-CS-1
HSR-CS-1B	Hall sensor shall have at least 40A sensing range.	B	TSR-CS-1
HSR-CS-2A	Hall sensor shall have FLT pin for self-test, and report faults to MCU within 100ms.	B	TSR-CS-2
HSR-CS-2B	Hall sensor FLT pin shall connect to DSP to report faults.	B	TSR-CS-2
HSR-CS-3A	Hall sensor VOC pin shall set the OC threshold to 20% higher than the maximum current.	B	TSR-CS-3
HSR-CS-3B	Hall sensor OC pin shall assert OC flag within 0.5us when overcurrent is detected.	B	TSR-CS-3
HSR-CS-3C	Hall sensor OC filter shall have > 1MHz cutoff frequency	B	TSR-CS-3
HSR-CS-4A	The VOUT of the current sensor in AC side shall be connected to an independent MCU ADC channel.	B	TSR-CS-4

Table 2-14. Example of SSR for TSRs Traced to FSR 2.1

ID	SSR	ASIL	Traced to
SSR-CS-1A	MCU shall sample the hall sensor output at 100kHz.	B	TSR-CS-1
SSR-CS-1B	MCU shall implement power-on hall sensor offset calibration.	B	TSR-CS-1
SSR-CS-2A	MCU shall identify different kinds of alert based on the duty cycle of FLT.	B	TSR-CS-2

Table 2-14. Example of SSR for TSRs Traced to FSR 2.1 (continued)

ID	SSR	ASIL	Traced to
SSR-CS-2B	MCU shall implement plausibility check if sensor alert is detected	B	TSR-CS-2
SSR-CS-4A	MCU shall perform plausibility check algorithm at 10kHz that computes the absolute difference of the two-sensor reading	B	TSR-CS-4
SSR-CS-4B	MCU shall assert the hardware fault within 2ms if the difference > 20 % for three consecutive samples	B	TSR-CS-4
SSR-CS-5A	MCU shall set software OC threshold 10% higher than the maximum current	B	TSR-CS-5
SSR-CS-5B	MCU shall perform OC detection with CMPSS module based on the ADC value.	B	TSR-CS-5
SSR-CS-5C	MCU shall disable PWM output in the specific sequence if OC is detected.	B	TSR-CS-5

These are only a handful of illustrative cases. In a real OBC project, the system integrator must perform a thorough analysis for every TSR and then move on to the subsequent steps.

- Design allocation. Assign each HSR and SSR to the respective team.
- Traceability matrix. Consolidate FTA or FMEA block diagrams to link FuSa goal to FSR, TSR and then HSR and SSR. Each HSR and SSR should be linked to their verification evidence.
- Verification planning. Verification and validation of HSRs and SSRs. Provide the test report that shows the requirement is satisfied and demonstrates the compliance of the ASIL-B safety goal.

In the OBC system, the ASIL level of some analog components is QM. Using QM components in an ASIL-B system is possible but requires hardware element evaluation. Hardware element evaluation demonstrates either the QM component cannot interfere with safety goals or additional safety mechanisms provide sufficient diagnostic coverage to achieve the required ASIL.

For example, TMCS1133-Q1 is FuSa capable component, and it is selected to achieve ASIL-B requirement. Suppose it is used in DC output side for current sensing and overcurrent protection. TI can provide the following content to facilitate customers in hardware element evaluation.

- All failure modes.
- Probability of each failure mode.
- Effect on system safety.

All the above information can be found in the FuSa document of TMCS1133-Q1. Customers shall perform design verification, including analysis and testing. All failures modes include die failure modes and pin failure modes. The total component FIT rate is 62, including die FIT rate 26 and pin FIT rate 36. All die failure modes and distribution are listed in Table 2-15.

Table 2-15. TMCS1133-Q1 Die Failure Modes and Distribution

Die Failure Modes	Failure Mode Distribution (%)
VOUT open (Hi-Z)	5
VOUT stuck (high or low)	30
VOUT functional, not in specification	30
OC false trip, failure to trip	15
ALERT false trip, failure to trip	20

The pin failure modes basically include the typical pin-by-pin failure scenarios:

- Pin short-circuited to ground.
- Pin open-circuited.
- Pin short-circuited to an adjacent pin.
- Pin short-circuit to supply.

Take pin short-circuited to ground as an example, the description of potential failure effects is shown in Table 2-16. Failure effect class indicates how these pins conditions can affect the device:

- Class A: Potential device damage that affects functionality.
- Class B: No device damage, but loss of functionality.
- Class C: No device damage, but performance degradation.
- Class D: No device damage, no impact to functionality or performance.

Table 2-16. Pin FMA for Device Pins Short-circuited to Ground

Pin Name	Pin No.	Description of Potential Failure Effects	Failure Effect Class
IN+	1	For forward current, hall-sensor bypassed, providing no signal to be sensed and amplified. If the IN+ pin is at a large potential above GND, this state results in a large amount of current being sunk. Depending upon layout and configuration, this result can damage the input current system supply, the load device, or the actual device.	A
IN-	2	For reverse current, hall-sensor bypassed, providing no signal to be sensed and amplified. If the IN- pin is at a large potential above GND, this status results in a large amount of current being sunk. Depending upon layout and configuration, this result can damage the input current system supply, the load device or the actual device	A
GND	3	Normal operation.	D
ALERT	4	Alert is not able to trigger since ALERT is shorted to GND	B
NC	5	Normal operation	D
VOUT	6	Output is pulled to GND, and the output current is short circuit limited. When left in this configuration, while VS is connected to a high-load-capable supply and for certain high-load conditions through the IN+ and IN- pins, the die temperature can approach or exceed 150°C.	A
OC	7	Alert is not able to trigger since OC is shorted to GND.	B
VOC	8	The threshold at GND means that all voltages trip the alert. As a result, the alert is stuck in active mode.	B
VS	9	Power supply is short to ground.	B
VS	10	Power supply is short to ground.	B

Based on the safety mechanisms, diagnostic coverage calculation should be implemented to show >90% detection. This evaluation determines that this hardware element can adequately support the safety requirements assigned to it.

Finally, the development team has a complete, traceable, and verifiable set of concrete safety requirements that can be implemented in the single-stage OBC and reviewed during ISO 26262: 2018 audits.

2.6 Dependent-Failure Analysis

DFA should be performed to identify the cascaded failures and common-cause failures that could influence redundancy. Additional TSRs for independence requirement are recognized by DFA analysis. Generally, DFA analysis confirms:

- Physical separation. Redundant components have sufficient physical separation, and different routing for redundant signal paths, and thermal isolation between critical components.
- Diversity. Different technologies are used for redundant functions, and different suppliers for critical components, and different implementation methods for hardware and software protection.
- Independence. Independent power supplies for redundant circuits, and independent processing for redundant functions, and independent activation paths for safety mechanisms.

For example, if the bias supply of MCU is short-circuited to ground, the plausibility check cannot detect the fault, and software-related safety mechanisms also lose its function. In this case, voltage monitoring is the critical safety mechanism to verify the OBC enters safe state.

3 FuSa Components of OBC System

This section aims to provide an overview of all kinds of TI functional safety components in the OBC system, as opposed to designing the minimum system required to meet the specific functional safety goal. Therefore, among the components described below, not all of them will be used simultaneously in the same OBC system.

System-level FuSa analysis is strongly dependent on the specific usage scenarios and architecture. For the following sections, the basic functions of the selected components will be described first, followed by an introduction to the component's safety features.

3.1 Components Overview

Figure 3-1 presents the component-level architecture of the single-stage matrix converter. The diagram is color-coded to make the different design aspects easy to recognize.

- Red text. Example part numbers for the hardware items that are normally selected during the detailed design phase. These identifiers are placeholders only; the actual part numbers must be chosen based on technical requirement, size and cost.
- Blue text. The blue labels highlight the pins that carry safety signals, the redundant components (dual voltage sensors), and the diagnostic interfaces (self-test, watchdog, parity-check). By flagging these pins, the diagram makes it straightforward to trace safety-related signal back to the corresponding FSR.

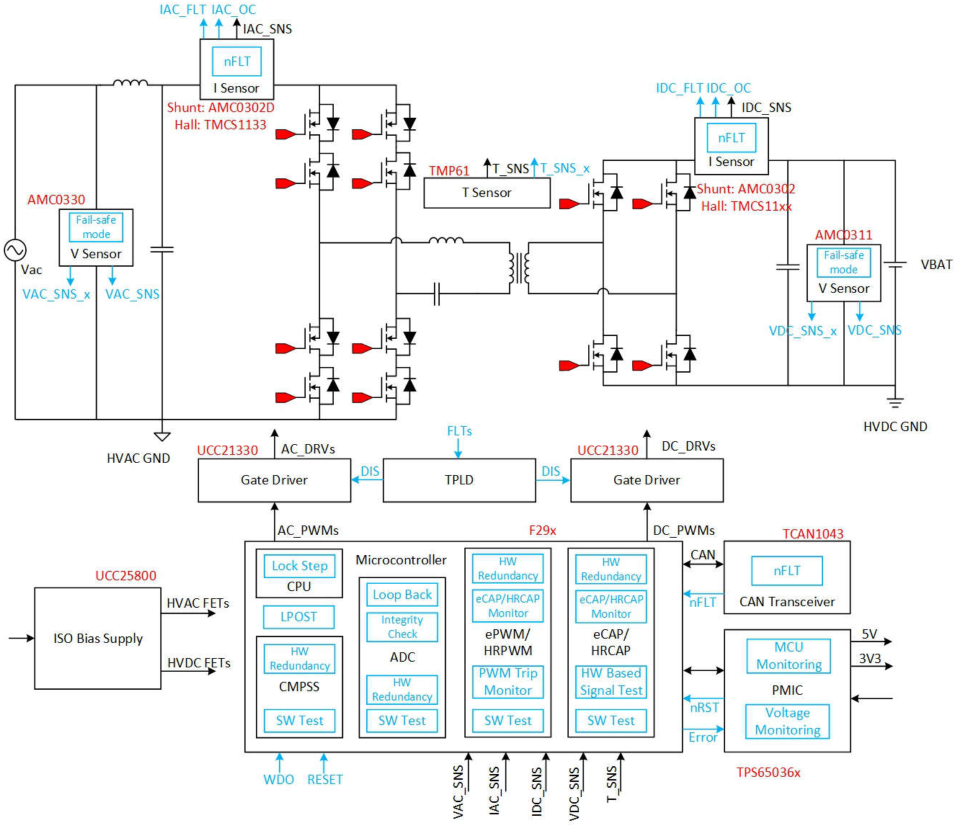


Figure 3-1. Component-Level Architecture of the Single-Stage Matrix Converter

In OBC applications, aside from power switches and passive components, main functional blocks are microcontroller, PMIC, gate driver, voltage sensor, current sensor, temperature sensor, isolated and non-isolated bias supply, communications.

- Microcontroller (MCU). Executes the charger control algorithm, monitors sensor data, and communicates with the BMS/VCU on the vehicle. In safety-critical designs the MCU is typically a dual-core device with a dedicated MCU internal watchdog and self-diagnostic capabilities.
- Power management IC (PMIC). Manages and controls multiple power functions, including voltage conversion, power sequencing, monitoring, protection and communication. The PMIC provides the power

supply to other devices and voltage monitoring for key voltage rails. It also provides an external watchdog and error pin monitor for MCU. When detecting the unrecoverable faults to MCU, PMIC can trigger reset to MCU and cut-off the related control to keep the system enter safe state.
- System basis chips. Exchange status and diagnostic information with the BMS/VCU. Safety-critical messages are transmitted with CRC and message-counter checks to verify integrity.
- Power supply and supervisor. Isolated bias supply generates the gate driver voltage and supplies the high-voltage side of the sensing circuit while maintaining galvanic isolation. Non-isolated bias supply powers the low-voltage components where galvanic isolation is not required.
- Gate driver. Provide the required voltage and high-current drive signals of the power switches. For an isolated gate driver,this also provides galvanic isolation between the low-voltage signal and the high-voltage side. The driver's built-in protection functions are employed to satisfy the FuSa requirements of the system.
- Voltage sensor. Measures the AC input voltage and DC bus voltage with a sufficient resolution to detect over-voltage or undervoltage events. The sensor output can be routed to both the MCU and the safety-monitoring logic.
- Current sensor. Detects AC input current and DC bus current, and also implement overcurrent protections. A typical implementation includes a hall-effect based current sensor with OC pin or shunt-based current amplifier with comparator.
- Temperature sensor. Monitors the power switches junction temperature, transformer temperature and the ambient temperature of the converter. Redundant temperature sensors can be implemented to achieve FuSa requirements.

3.2 Microcontroller

The F29H859TU-Q1 microcontroller belongs to high performance C2000™ real-time microcontroller family. The C2000 product line utilizes a common safety architecture that is implemented for multiple products in automotive and industrial applications. It boasts 3 C29x CPU (supporting lockstep capable) running at 200MHz, 4000kByte flash, 452kByte of RAM, supporting 5 SAR ADCs, up to 36 channels PWM output, and QFP-144/QFP-176/BGA-256 package. It meets ISO 2626 **2** and IEC61508 standards, ensuring compliance with safety requirements up to ASIL-D/SIL3. With advanced functionalities and extensive connectivity options, it offers a comprehensive design. The main safety features in MCU for the OBC applications include the following aspects.

3.2.1 CPU

Embedded CPU supports multiple instruction sizes (16/32/48 bits). The CPU also supports variable instruction packet size, with each packet able to contain up to eight instructions that execute in parallel. For example, the CPU architecture can execute up to eight 16-bit instructions in parallel. This is enabled by multiple functional units inside the CPU which can execute concurrently. Core 1 and Core 2 are capable of independent execution in split-lock mode or lock step mode.

- Hardware Redundancy Using Lockstep Compare Module (LCM). Lockstep Compare Module (LCM) is used to implement lockstep compare functionality and indicate an error.
- Self-test Logic for LCM. The LCM self-test logic is designed for the lockstep comparator. The self-test for the comparator has two different modes – match test and mismatch test. When the self-test is initiated, the two different test modes are executed on the two comparators one after the other.
- Internal Watchdog (WD). Provide watchdog function with two mode selection, which is normal watchdog (WD) and windowed watchdog (WWD).
- Logic Power on Self-Test. LPOST (Logic Power on Self-Test) provides high diagnostic coverage for the device at a transistor level during start-up and application time. LPOST utilizes Design for Test (DFT) structures inserted into the device for rapid execution of high-quality manufacturing tests, but with an internal test engine rather than external automated test equipment (ATE). The LPOST test is triggered by the BootROM based on the SECCFG user input.

3.2.2 ADC Sample

High-performance analog blocks are integrated on the F29H859TU-Q1 MCU to further enable system consolidation. Three separate 12-bit SAR ADCs and Two separate 16-bit/12-bit selectable SAR ADCs provide precise and efficient management of multiple analog signals, which ultimately boosts system throughput. Four analog comparator modules provide continuous monitoring of input voltage levels for trip conditions. The main supported safety mechanisms for ADC are as follows.

- DAC to ADC Loopback Check. Integrity of ADC can be checked by monitoring the DAC output using ADC. A set of predetermined voltage levels can be configured and output by DAC. These voltage levels can be measured by the ADC and cross checked against the expected value to verify the ADC are functioning properly.
- ADC Input Signal Integrity Check. ADC input signal integrity can be checked using a mix of hardware and software runtime diagnostic on ADC conversions. A plausibility check of the input signal can be checked with the help of built-in hardware mechanisms and software configurable thresholds. The plausibility check of converted results can be checked by using an ADC post processing block.
- Hardware Redundancy with ADC Safety Checker. Using multiple instances of the ADC to sample the same input and simultaneously perform the same operation followed by cross check of the output values. The hardware-based result safety checker module that automatically compares the results from primary and redundant ADCs once both the results are available.
- Software Test of Function Including Error Tests. Support run functionality test or fault injection test on the ADC module and post processing block. A set of predetermined voltage levels can be provided on the ADC input pin by external circuit or internal DAC. The conversion result can be compared with expected value to check the functional correctness of ADC module and post processing block.
- Logic Power on Self-Test. LPOST (Logic Power on Self-Test) provides high diagnostic coverage for the device at a transistor level during start-up and application time. LPOST utilizes Design for Test (DFT) structures inserted into the device for rapid execution of high-quality manufacturing tests, but with an internal test engine rather than external automated test equipment (ATE). The LPOST test is triggered by the BootROM based on the SECCFG user input.

3.2.3 PWM Generation

The F29H859TU-Q1 devices contain industry-leading control peripherals with 36 Enhanced Pulse Width Modulator (ePWM) channels, all with high-resolution capability (HRPWM). Enhanced Capture (eCAP) module allows for a best-in-class level of control to the system. The built-in Sigma-Delta Filter Module (SDFM) allows for seamless integration of an oversampling sigma-delta modulator across an isolation barrier.

- Hardware Redundancy. For PWM, hardware redundancy can be implemented by having multichannel parallel and comparing the outputs by internal or external comparators. For eCAP, SDFM, hardware redundancy can be implemented by having multiple instances of the peripheral sample the same input and simultaneously perform the same operation followed by a cross check of the output values.
- Monitoring ePWM/HRPWM by eCAP/HRCAP. The ePWM/HRPWM outputs can be monitored for proper operation by input capture peripheral, such as the eCAP/HRCAP. The captured pulse width can be used to build additional diagnostics for user implemented to detect rising and falling edges of the PWM and the timestamping information. eCAP/HRCAP can be tested by periodically measuring ePWM/HRPWM pulse width when used as diagnostic for PWM.
- Online MINMAX monitoring of TRIP events. Support detects the occurrence of a trip event in a configured time window. The window is configured by MIN and MAX values configured in the XMINMAX register sets.
- Fault avoidance using Minimum Dead Band logic. The Minimum Dead Band logic can be configured to verify a minimum inactive gap (dead band) between the active pulse phases of the two PWM channels and across PWM instances.
- Hardware Redundancy and comparison of outputs using WADI. The waveform analyzer and diagnostic (WADI) peripheral consists of many useful built in signal analysis support and provides a safety mechanism for the signals. WADI is able to perform the following checks on individual signal or perform checks between two signals: Pulse width measurement, Frequency measurement, Phase Overlap measurement, Dead-band measurement.
- Software Test of Function Including Error Tests. Support running functionality test or fault injection test on the ePWM module. The individual submodules can be tested by providing appropriate stimulus using PWM and observing the response using one of the captures (timestamping) modules (eCAP) to check the functional correctness of eCAP or ePWM module.
- Error Detection using Signal Monitoring. A hardware-based signal monitoring unit has the ability to measure edge, pulse width, and period of eCAP input signals to check whether this event happens within the programmable expected range.
- Logic Power on Self-Test. LPOST (Logic Power on Self-Test) provides high diagnostic coverage for the device at a transistor level during start-up and application time. LPOST utilizes Design for Test (DFT) structures inserted into the device for rapid execution of high-quality manufacturing tests, but with an internal

test engine rather than external automated test equipment (ATE). The LPOST test is triggered by the BootROM based on the SECCFG user input.

3.2.4 CMPSS

CMPSS consists of analog comparators and supporting components that are combined into a topology that is useful for power applications such as peak-current mode control, switched- mode power, power factor correction, and voltage trip monitoring. With ePWM for active synchronous rectification, active synchronous rectification enables higher efficiency.

- Hardware Redundancy. For CMPSS, hardware redundancy can be implemented by having multichannel parallel outputs or input comparison.
- Software Test of Function Including Error Tests. Support running functionality test or fault injection test on the CMPSS critical registers or critical features. A set of predetermined patterns can be written to the registers, after that the user read back the register value and compared with expected value. Through adjusting the filter thresholds, check whether the output is followed with the filer changes to achieve the key CMPSS function detection.
- Logic Power on Self-Test. LPOST (Logic Power on Self-Test) provides high diagnostic coverage for the device at a transistor level during start-up and application time. LPOST utilizes Design for Test (DFT) structures inserted into the device for rapid execution of high-quality manufacturing tests, but with an internal test engine rather than external automated test equipment (ATE). The LPOST test is triggered by the BootROM based on the SECCFG user input.

3.2.5 Data Transmission

Data transmission is supported through various industry-standard communication ports, such as Serial Peripheral Interface (SPI); Serial Communication Interface (SCI); Inter-integrated Circuit (I2C); and Controller Area Network (CAN) and offers multiple multiplexing options for optimal signal placement in a variety of applications.

- Information Redundancy Techniques Including End-to-End Safing. The module communication transceivers or physical layers are considered a 'black box' and any communication transceiver or physical layer related fault can be detected indirectly by communication protocol E2E protection, including additional message checksums, sequence counter, and timestamp and so forth. Information redundancy techniques can be applied using software as an additional runtime diagnostic. Many techniques that can be applied by software, such as a readback of written values and multiple reads of the same target data with a comparison of results.
- Logic Power on Self-Test. LPOST (Logic Power on Self-Test) provides high diagnostic coverage for the device at a transistor level during start-up and application time. LPOST utilizes Design for Test (DFT) structures inserted into the device for rapid execution of high-quality manufacturing tests, but with an internal test engine rather than external automated test equipment (ATE). The LPOST test is triggered by the BootROM based on the SECCFG user input.

3.2.6 Fault Signal Monitor and Safe State Control

The safety MCU checks the integrity of the remote sensor data, controls the battery charge. When an abnormal situation is detected, the system will enter a safe state.

3.3 Power Management IC

The TPS650365-Q1 device is a highly integrated power management IC. This device combines three step-down converters and one low-dropout (LDO) regulator. All converters can operate in a forced fixed-frequency PWM mode or in Auto-PFM mode and support optional spread-spectrum modulation (SSM) for EMI reduction. The TPS650365-Q1 also supports low power mode. These flexible features suit MCU power applications. It meets ISO 26262: 2018 and IEC61508: 2010 standards, ensuring compliance with safety requirements up to ASIL-B/SIL2. Available in VQFN-24 package. The main safety features in PMIC for the OBC applications include the following aspects.

3.3.1 MCU Monitor

The TPS650365-Q1 component monitors the module safety MCU hardware and software operation. In case of the safety MCU hardware and/or software execution failure modes, PMIC generates different reactions depending on the severity rating of the detected fault, including interrupting to MCU, turning off external power stages and module communication interfaces, and if the fault continues to exceed the threshold, re-boot the safety MCU.

- Watchdog. Provides external watchdog function with three selectable modes: Input trigger mode, software trigger mode and question and answer (Q&A) mode.
- Error Signal Monitor (ESM). TPS650365-Q1 device can monitor the MCU error output signal through nERR input pin after MCU configured the ESM and enabled this with the start bit. ESM supports two operating modes: Level mode and PWM mode.

3.3.2 Shutdown Sequence

The TPS650365-Q1 component can provide a shutdown sequence when detecting unrecoverable faults in PMIC or MCU. The component enters RESET-MCU state and drives the RESET pin output to MCU, then controls the safety MCU in reset state. The MCU-output controls are cut off accordingly.

3.3.3 Power Supply

The TPS650365-Q1 component monitors PMIC internal voltages, input and output voltages, and provides internal diagnostics.

- Voltage Monitor. TPS650365-Q1 input supply voltage and internal regulated output voltage are continuously monitored for undervoltage and overvoltage events by comparing with the reference voltage. When the voltage is outside the range, regulators is shut off and state machine jumps to a fault handling state. Note: All regulators include a current-limit circuit to protect the internal power MOSFETs from an over-current event.
- ABIST. Provide an Analog Built-in-Self-Test (ABIST) at power-up and on demand on the under/over-voltage monitors for all regulated supplies if they are enabled.

As outlined in Power Management IC, PMIC represents a fully integrated design that delivers both power supply and voltage monitoring capabilities for the OBC system. Alternatively, a discrete approach can be implemented where no PMIC is utilized. In discrete configurations, system basis chips or individual LDO regulators supply power to the MCU, while separate supervisor circuits or watchdog devices handle system monitoring functions. Section 3.4 covers system basis chips, and Section 3.5 will discuss power supply units and supervisory circuits.

3.4 System Basis Chips

The TCAN1164-Q1 is a high-speed Controller Area Network (CAN) system basis chip (SBC) that meets the physical layer requirements of the ISO 11898-2:2016 CAN flexible date-rate (FD) specification. The transceiver supports both classical CAN and CAN FD networks up to eight megabits per second (Mbps). The TCAN1164-Q1 supports a wide input supply range and integrates a 5V LDO output. The 5V LDO output (VCCOUT) supplies the CAN transceiver voltage internally as well as additional current externally.

The TCAN1164-Q1 was developed using Texas Instruments Incorporated Quality Managed product development process and qualified according to AEC Q100 Grade 1. The process falls under TI's Functional Safety Quality-Managed. TI recommends that this component is integrated into the system through the strategy of *evaluation of hardware element* (ISO 26262-8: 2018 clause 13).

The TCAN1164-Q1 interfaces with the system as described below:

- The TCAN1164-Q1 receives 5V power from the Non-ISO Bias Supply on the VSUP pin.
- The TCAN1164-Q1 integrates a 5V LDO (VCCOUT) to supply internal CAN transceiver and external devices.
- The TCAN1164-Q1 connects to the MCU through the four SPI pins. The host MCU uses these pins to configure the TCAN1164-Q1 and to periodically service the watchdog.
- The TCAN1164-Q1 connects to the external CAN bus via the CANH and CANL pins, and connects to the MCU via the TXD and RXD pins for CAN bus communication.

Therefore, the potential failure points and safety mechanisms are focused on CAN communication, supply voltage rail monitoring, SPI/processor communication, as well as internal memory to fulfill the functional safety application.

3.4.1 CAN Communication

The following are functional safety mechanisms that cover the CAN communication.

- CAN protocol: CAN protocol with CRC checksums implemented in the MCU detects and handles any communication errors
- CAN bus fault diagnostics: The TCAN1164-Q1 provides advanced bus fault detection circuitry to monitor the CANH and CANL pins and determine if there is a short circuit to battery, short to ground, short to each other or open faults.
- TSD: The TCAN1164-Q1 has thermal shutdown warning and thermal shutdown (TSD) protection to disable the CAN transceivers.
- CAN bus short circuit limiter: this device limits the short-circuit current when a CAN bus line is shorted.

CAN TXD pin dominant state timeout: The device supports dominant state time out (DTO); the device prevents the local node from blocking network communication in the event of a hardware or software failure where TXD is held dominant (LOW) longer than the time out period.

3.4.2 Supply Voltage Rail Monitoring

There are two voltage rails monitored in the TCAN1164-Q1: VSUP and VCCOUT. VSUP is an input source for the TCAN1164-Q1, and VCCOUT is the LDO output that is used for the CAN transceiver as well as external power sourcing. Once a power fault is detected, the device enters standby mode or fail-safe state. Safety mechanisms that cover the supply voltage rails including:

- VCCOUT LDO short circuit current protection
- VSUP supply undervoltage detection (UVSUP)
- VCCOUT undervoltage detection (UVCCOUT)
- VCC overvoltage detection (OVCCOUT)

3.4.3 SPI/Processor Communication

The TCAN1164-Q1 has several ways to determine if communication between the processor and the device is functioning correctly.

- Watchdog: The devices provide a default window-based watchdog as well as a selectable time-out and question and answer (Q&A) watchdog using the SPI interface.
- SPI communication error indicator: If the correct number of clock cycles and data are not shifted in during one SPI transaction, interrupts at dedicated register are set.
- Scratchpad write/read: The device provides a dedicated register that can be written and read back to verify the SPI interface to register space.

3.4.4 Device Internal EEPROM

The TCAN1164-Q1 uses an internal EEPROM for certain performance trimming. Upon power up, the device loads an internal register from the EEPROM and performs a CRC check. The CRC_EEPROM interrupts are set when the internal EEPROM used for trimming has a CRC error.

3.5 Power Supply and Supervisor

This section describes the TI design leveraging two TI Functional Safety-Capable devices – the LM5155-Q1 boost controller combined with the TPS3850-Q1 supervisor – to meet system ASIL-B requirement.

LM5155-Q1 is used to output 3.3V power supply for safety MCU. Keeping the power supply of MCU within the recommended operating range is essential to prevent the MCU from running into an unsafe state. Therefore, the 3.3V power output needs to be monitored for faults such as supply undervoltage or overvoltage. If either OV or UV occurs, resetting the MCU to switch off and transition the system into safe state is required.

To detect the 3.3V power OV/UV failure modes, the recommended design is to use an external supervisor to monitor the power-supply output. The supervisor is independent of the power-supply output, so there is no common-cause failure. Given the supervisor's high performance and accuracy, the diagnostic coverage for power-supply over- and undervoltage is high.

In this OBC system, the TPS3850-Q1 - a window voltage supervisor with an integrated window watchdog is used to monitor the 3.3V power rail. This resets the safety MCU to a safe state upon detection of a power fault.

3.6 Gate Driver

In a typical OBC application, gate drivers are required to prevent unintended turn-on events and direct shoot-through in the high side and low side switches. UCC21330-Q1 is an isolated dual-channel gate driver with 4A peak-source and 6A peak-sink current to drive power MOSFET, SiC, GaN, and IGBT transistors.

The protection features of UCC21330-Q1 include resistor programmable dead time, disable feature to shut down both outputs simultaneously, and integrated de-glitch filter that rejects input transients shorter than 5ns. All supplies have UVLO protection. The internal weak pull down on both INA and INB pin can verify the output will be low at default as a safe state. DIS pin disables both driver outputs if asserted high, enable both outputs if set low. In case of the detected failure state, a global DIS asserted by the microcontroller or other analog comparators disables all drivers at once.

To prevent direct shoot-through of the high side and low side FET during dynamic switching, the interlock function can be enabled by placing 0Ω to 150Ω resistor, or short DT pin to GND to have two outputs interlocked. If both inputs are high simultaneously, both outputs are immediately be set low. Figure 3-2 can illustrate this functionality.

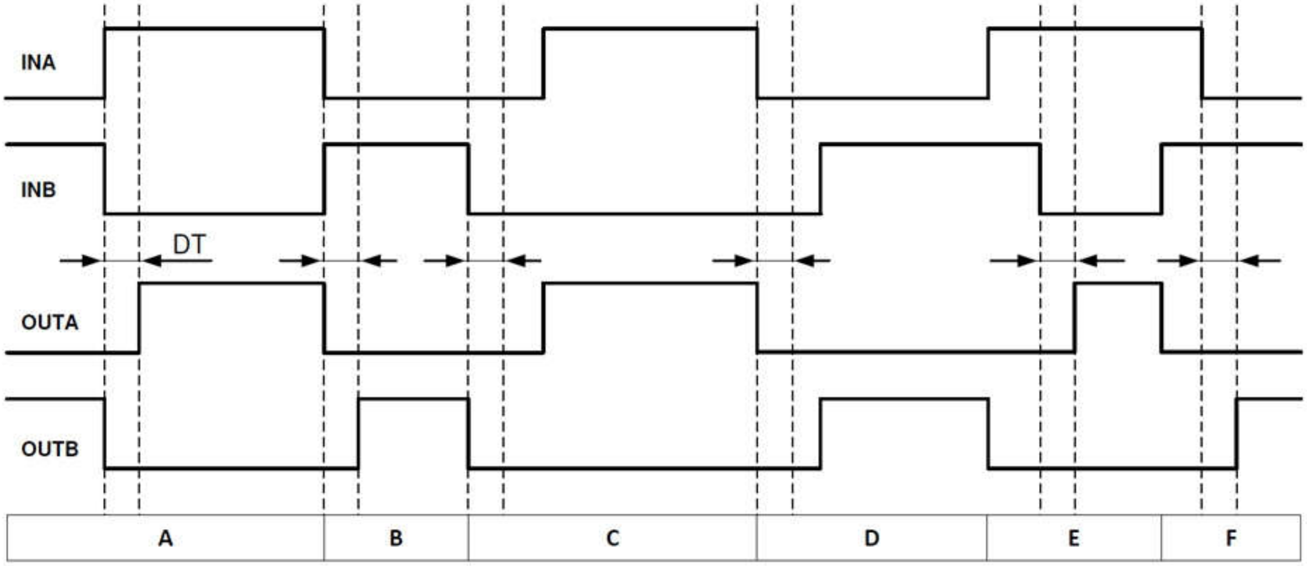


Figure 3-2. Input and Output Logic Relationship With Input Signals

Condition A: INB goes low, INA goes high. INB sets OUTB low immediately and assigns the programmed dead time to OUTA. OUTA is allowed to go high after the programmed dead time.

Condition B: INB goes high, INA goes low. Now INA sets OUTA low immediately and assigns the programmed dead time to OUTB. OUTB is allowed to go high after the programmed dead time.

Condition C: INB goes low, INA is still low. INB sets OUTB low immediately and assigns the programmed dead time for OUTA. In this case, the dead time of the input signal is longer than the programmed dead time. Thus, when INA goes high, this immediately sets OUTA high.

Condition D: INA goes low, INB is still low. INA sets OUTA low immediately and assigns the programmed dead time to OUTB. INB's own dead time is longer than the programmed dead time. Thus, when INB goes high, this immediately sets OUTB high.

Condition E: INA goes high, while INB and OUTB are still high. To avoid overshoot, INA immediately pulls OUTB low and keeps OUTA low. After some time OUTB goes low and assigns the programmed dead time to OUTA. OUTB is already low. After the programmed dead time, OUTA is allowed to go high.

Condition F: INB goes high, while INA and OUTA are still high. To avoid overshoot, INB immediately pulls OUTA low and keeps OUTB low. After some time OUTA goes low and assigns the programmed dead time to OUTB. OUTA is already low. After the programmed dead time, OUTB is allowed to go high.

To verify robust and reliable operation of gate drivers, pay special attention to the minimum pulse width. The minimum input pulse width is dictated by the deglitch filter present in the driver IC, which determines the shortest pulse that will be transmitted to the output in an unloaded driver.

Under voltage lockout (UVLO) is implemented in gate drivers to monitor the gate voltage and prevent it from dropping below a specified threshold. The UVLO rating is an important consideration in high-power applications that use Si & SiC MOSFETs or IGBTs.

- UVLO is a key feature to verify the system is protected in case of a bias supply failure.
- High UVLO is required for SiC MOSFETs and IGBTs in high power applications due to the device characteristics and high-power system. The efficient switching of these devices is critical to prevent destruction or reduced lifetime.

For high switching frequency or hard-switching applications, to prevent false turn-on of the gate driver, miller clamp is preferred to increase overall system robustness. The UCC5350-Q1 is a single-channel, isolated gate driver with 10A source and 10A sink typical peak current, which has the option for Miller clamp or Split Outputs.

- Vds dv/dt results in current through Cgd, also known as the miller capacitance. This Miller current induces a voltage at the gate

- The Miller Clamp introduces a low-impedance path to bypass the Miller current and prevent false turn-on when the gate driver is OFF.

This single-channel gate driver integrates specific logic to prevent shoot through. Interlock can be achieved by simply connecting IN+ and IN- respectively into 1-ch devices. If both high-side and low-side gate drivers are sent an input high, the drivers disable the output to prevent shoot-through. The logic table is listed in Table 3-1.

Table 3-1. Device Functional States

IN+	IN-	OUTH/OUTL	Functional States
0	0	LO	System off
0	1	LO	Normal low
1	0	HI	Normal high
1	1	LO	Prevents shoot through

If additional advanced protection feature is desired, UCC218200-Q1 is an isolated gate-driver with overcurrent and short circuit detection, controlled soft shutdown after a fault, fault reporting, active Miller clamp, input and output side power supply UVLO to optimize SiC and IGBT switching behavior and robustness, output voltage gate monitoring, and built-in self-test during startup.

Output voltage gate monitor checks to make sure gate voltage reaches > VDD - 3V when PWM is high and < VEE + 3V when PWM is low.

- RDY is pulled low when a gate monitor fault is detected.
- OUT_FB on LV side provides real time feedback output.

During the initial startup the driver runs a series of checks to verify the following comparators are not stuck high or low:

- DESAT/OC.
- VCC, VDD, and VEE UVLO.
- VDD-3V and VEE+3V gate monitors.
- Miller Clamp Threshold.

3.7 Voltage Sensor

In OBC applications, voltage sensing is crucial for closed-loop control, fault detection and following protection. Isolated amplifier is the commonly used design for voltage sensing with isolation barrier. The isolation barrier separates parts of the system that operate on different common-mode voltage levels and protects the low-voltage side from voltages that can cause electrical damage or be harmful to an operator.

The AMC0311D-Q1 is a precision, isolated amplifier with an output separated from the input circuitry by a capacitive isolation barrier that is highly resistant to magnetic interference. The high-impedance input is optimized for connection to high-impedance resistive dividers or any other high-impedance voltage signal source. The excellent DC accuracy and low temperature drift support accurate, isolated voltage sensing and control in closed-loop systems. Figure 3-3 shows the block diagram.

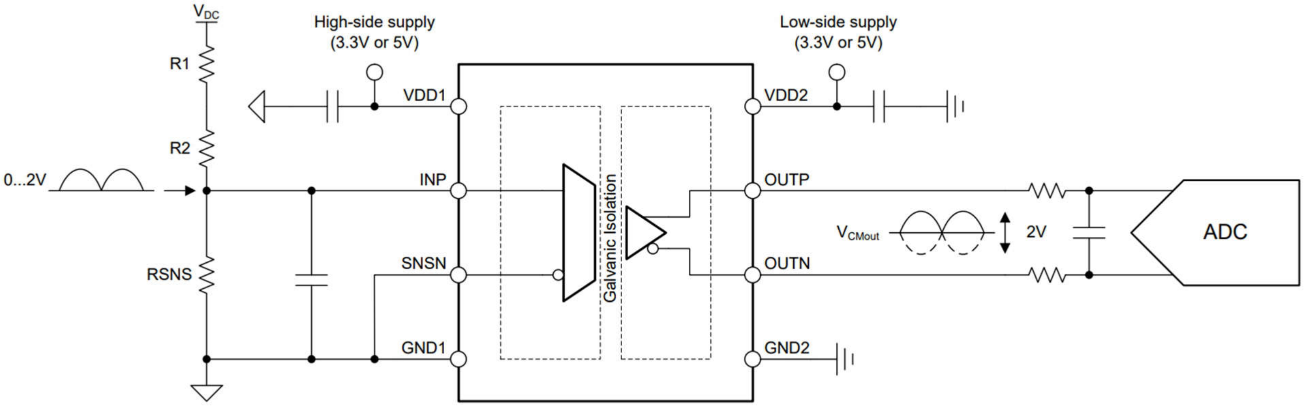


Figure 3-3. Block Diagram of AMC0311D-Q1

The integrated missing high-side supply voltage detection feature simplifies system-level design and diagnostics. Figure 3-4 shows the fail-safe mode, in which the AMC0311D-Q1 outputs a negative differential output voltage that does not occur under normal operating conditions.

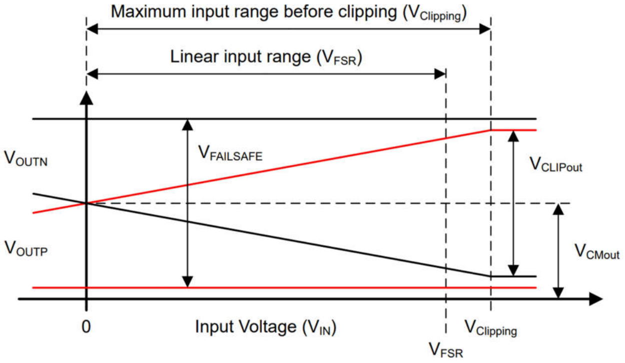


Figure 3-4. Output Behavior of the AMC0311D-Q1

Use the maximum fail-safe voltage as a reference value for fail-safe detection on system level. The fail-safe output is active in three cases:

- When the high-side supply VDD1 of the AMC0311D-Q1 device is missing.
- When the high-side supply VDD1 falls below the undervoltage threshold VDD1 UVLO threshold.

In the actual application, two separate sampling channels can be used for redundant voltage sensing to verify that the MCU has reliable voltage information.

3.8 Current Sensor

In a typical OBC application, current sensors are required for close-loop control and overcurrent or short-circuit protection. Hall-effect based components are one option, which can be used for both AC and DC current measurements. Hall-effect based features low-ohmic lead frame path reducing power dissipation, and does not require any external passive components, isolated supplies, or control signals on the HV side.

TMCS1133-Q1 is a galvanically isolated hall-effect current sensor providing high levels of reliable reinforced isolation working voltage, ambient field rejection and high current carrying capability. Industry leading accuracy was achieved with a factory-trimmed sensitivity error 0.4% at 25°C and sensitivity error 0.5% over the full operating temperature. The function block diagram is shown in Figure 3-5.

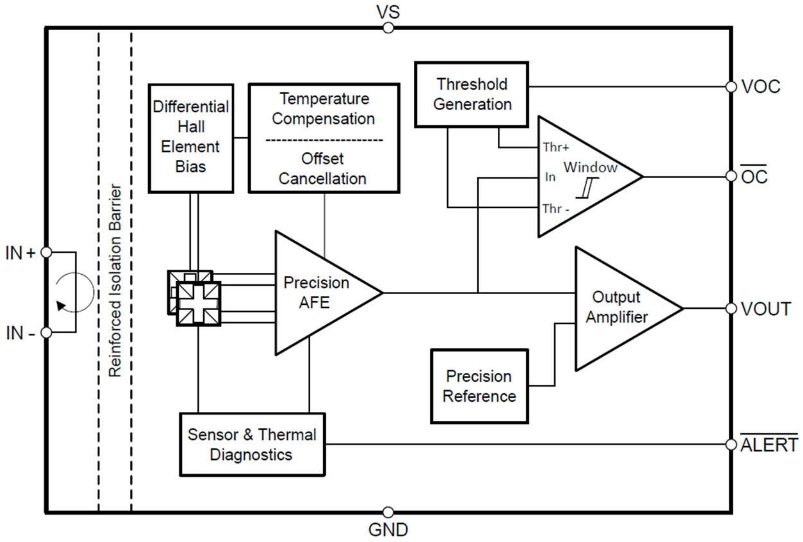


Figure 3-5. Function Block Diagram of TMCS1133-Q1

TMCS1133-Q1 offers a fast digital overcurrent detection response. This can be used to trigger a warning or initiate a system shutdown to prevent damage from excessive current flow caused by short circuits or other unintended system conditions. The OC threshold can be configured on both bidirectional and unidirectional devices to assert based on a signal from half to over twice the full-scale analog measurement range.

The benefits of using OC output instead of VOUT to detect overcurrent events are higher dynamic range with higher sensitivity and lower overall signal noise from lower analog signal bandwidth. However, VOUT pin can also be used as a redundant OC protection feature by using CMPSS module of MCU. For VOUT pin OC protection, lower OC threshold can be set to cover the event with a smaller current but a longer duration. It can also cover the OC events when the SPF occurs in the OC pin path.

Built-in self-diagnostic features are incorporated in the TMCS1133-Q1 to warn when operating conditions invalidate current sensor measurements. Two critical conditions being monitored are sensor temperature and sensitivity.

- High input currents, coupled with elevated ambient temperatures and printed circuit board thermal design can cause the TMCS1133-Q1 to overheat and be permanently damaged by exceeding maximum allowed junction temperatures. A thermal alert occurs when the internal temperature approaches the maximum allowed junction temperature.
- Sensor sensitivity and offset are constantly monitored inside TMCS1133-Q1. A sensor alert occurs in the unlikely event hall sensor sensitivity or offset is out of range compared with factory set limits.

The active-low ALERT output signal can be used to decipher which of four diagnostic states the TMCS1133-Q1 resides. The duty cycle of the 8kHz PWM output signal indicates which, neither, or both thermal and sensor operating condition warnings exist.

Shunt-resistor based designs are the alternative in current sensing. The AMC0302D-Q1 is a precision, isolated amplifier with an output separated from the input circuitry by an isolation barrier that is highly resistant to magnetic interference. The input of the AMC0302D-Q1 is optimized for direct connection to a low-impedance shunt resistor or other low-impedance voltage source with low signal levels. The excellent DC accuracy and low temperature drift supports accurate current control in OBC application. Figure 3-6 shows the block diagram.

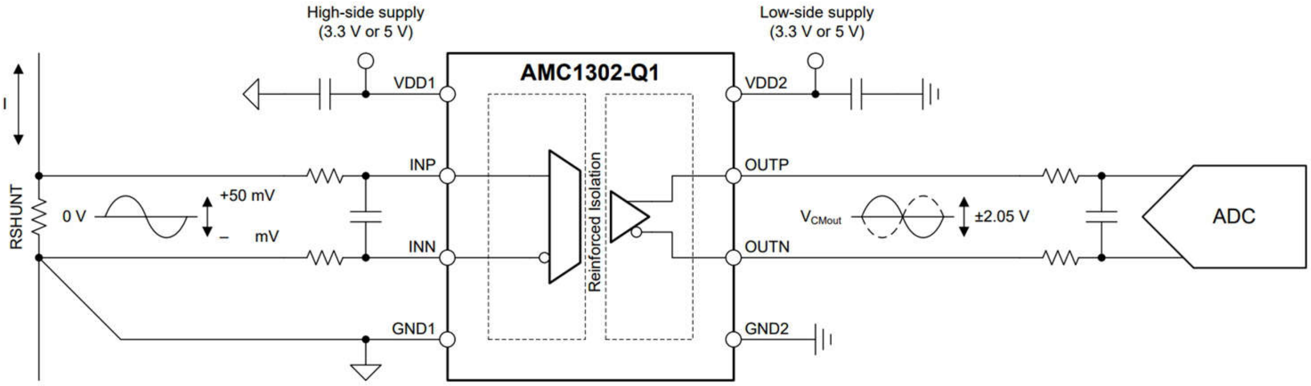


Figure 3-6. Block Diagram of AMC0302D-Q1

The integrated missing-shunt and missing high-side supply detection features simplify system-level design and diagnostics. Figure 3-7 shows the fail-safe mode, in which the AMC0302D-Q1 outputs a negative differential output voltage that does not occur under normal operating conditions.

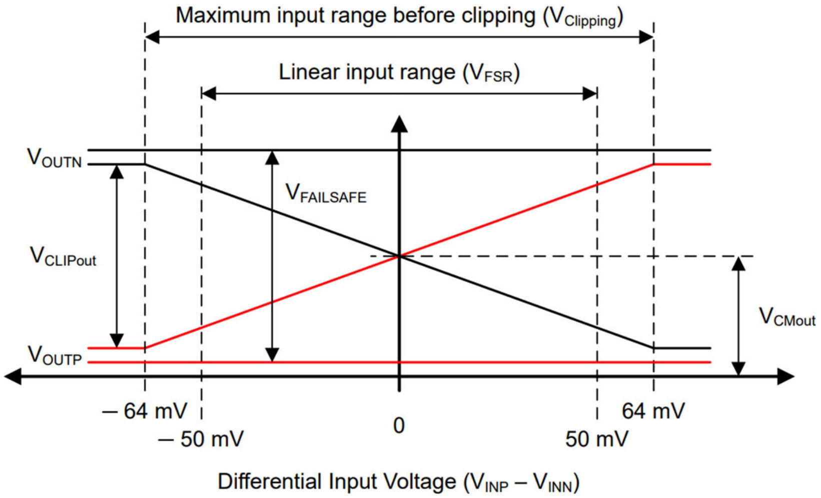


Figure 3-7. Output Behavior of the AMC0302D-Q1

Use the maximum fail-safe voltage as a reference value for fail-safe detection on system level. The fail-safe output is active in two cases:

- When the high-side supply is missing or below the VDD1 UVLO threshold.
- When the common-mode input voltage, that is VCM = (VINP + VINN) / 2, exceeds the common-mode overvoltage detection level.

If the current sensing circuit is only used for overcurrent protection and not for current control, an isolated comparator is a very suitable solution. Generally, it can be regarded as the second chain of redundant sensing for FuSa. The AMC23C12-Q1 is an isolated window comparator with a short response time. The comparison window is centered around 0V, meaning that the comparator trips if the absolute value of the input voltage exceeds the trip threshold value. The block diagram is shown in Figure 3-8.

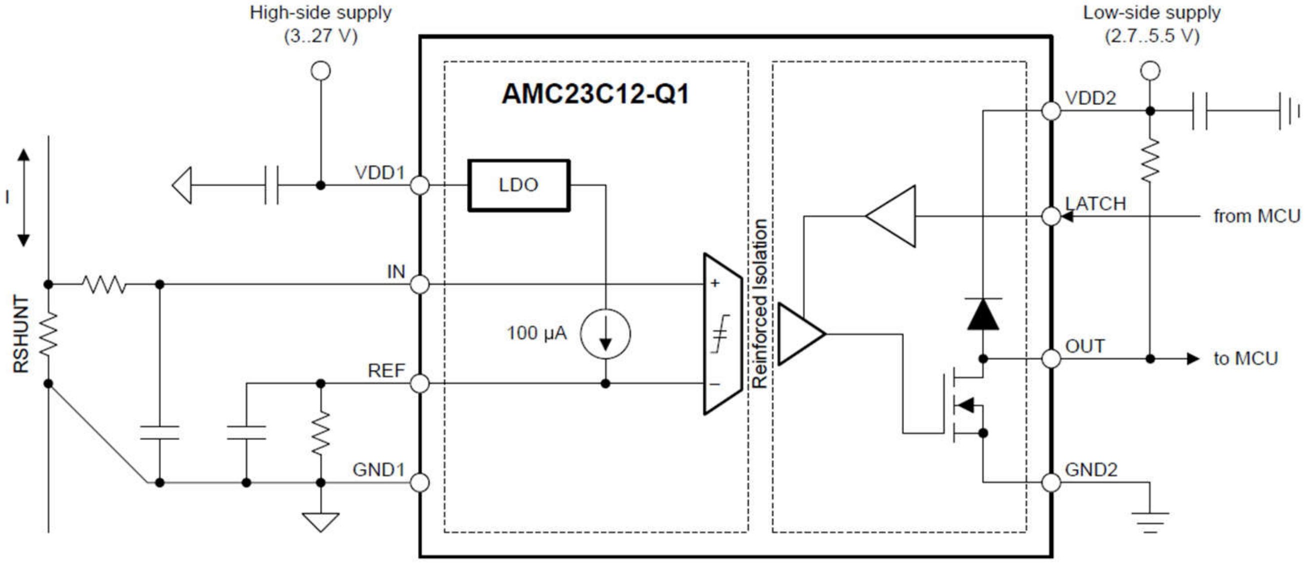


Figure 3-8. Block Diagram of the AMC23C12-Q1

3.9 Temperature Sensor

In the OBC system, temperature sensors are also critical for control and safety monitoring, so this also requires careful consideration. It is usually implemented by an analog device, such as a negative temperature coefficient (NTC) resistor. TMP61-Q1 is the silicon-based thermistor with a positive temperature coefficient (PTC).

Accuracy is the most critical factor for temperature sensors. The TMP61-Q1 provides excellent linearity and consistent sensitivity across the operating range, enabling simple and accurate temperature conversion methods. The high linearity enables users to calculate temperature without using piecewise fitting or lookup tables in the software. The sensor maintains consistent sensitivity with a 6400ppm/°C Temperature Coefficient of Resistance (TCR) at 25°C and a typical TCR tolerance of just 0.2% across the entire temperature range. Figure 3-9 shows the typical resistances versus ambient temperature.

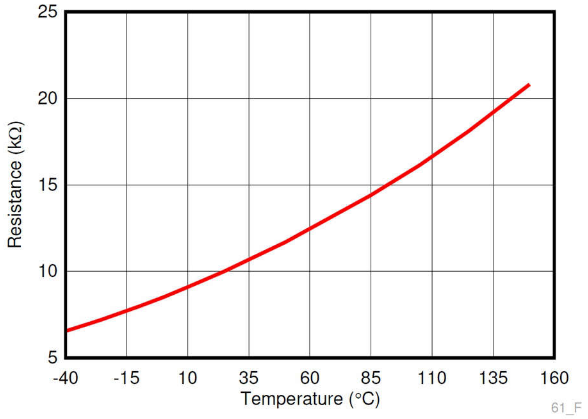


Figure 3-9. TMP61-Q1 Typical Resistances versus Ambient Temperature

TMP61-Q1 is designed for a long lifetime of high performance. It features built-in fail-safe behavior in case of short-circuit failures at high temperatures. With exceptional resistance to environmental fluctuations, this maintains a typical long-term sensor drift of only 0.5%. The device responds rapidly to temperature changes with a quick thermal response time of just 0.6 seconds.

Available in a compact 0402 package, the TMP61-Q1 can be positioned in close proximity to heat sources and serves as a direct replacement for conventional NTC resistors. For applications requiring higher temperature tolerance, the ELPG package option extends the operational range up to 170°C.

The reliability of temperature sensing depends not only on the thermistor but also on the pull-up resistor and the power supply. The TMP23x-Q1 devices are a family of automotive grade precision CMOS integrated-circuit linear analog temperature sensors with an output voltage proportional to temperature. Figure 3-10 shows the block diagram.

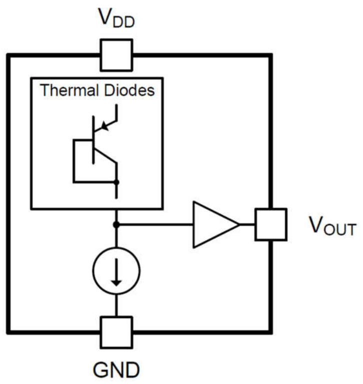


Figure 3-10. Block Diagram of TMP23x-Q1

The TMP235-Q1 device provides a positive slope output of 10mV/°C over the full –40°C to +150°C temperature range and a supply range from 2.3 V to 5.5 V. The higher gain TMP236-Q1 sensor provides a positive slope output of 19.5 mV/°C from –10°C to +125°C and a supply range from 3.1 V to 5.5 V. By eliminating the need for external pull-up resistors, it achieves enhanced reliability. Furthermore, it provides built-in protection for downstream components—when exposed to power supply overvoltage conditions, the device prevents these abnormally high voltages from being proportionally transmitted to the backend ADC, effectively safeguarding the MCU from potential damage.

If the thermistor cannot be placed close the hotspot (e.g. FETs / Transformer / Shunt resistor), the accuracy and response time are usually compromised. For OBC applications, since electrical clearance and creepage distance need to be considered, sometimes the placement of the thermistor is a trade-off. To solve this problem, The ISOTMP35-Q1 is the industry's first isolated temperature sensor IC, combining an integrated isolation barrier, up to 3000VRMS withstand voltage, with an analog temperature sensor featuring a 10mV/°C slope from –40°C to 150°C. Figure 3-11 shows the block diagram.

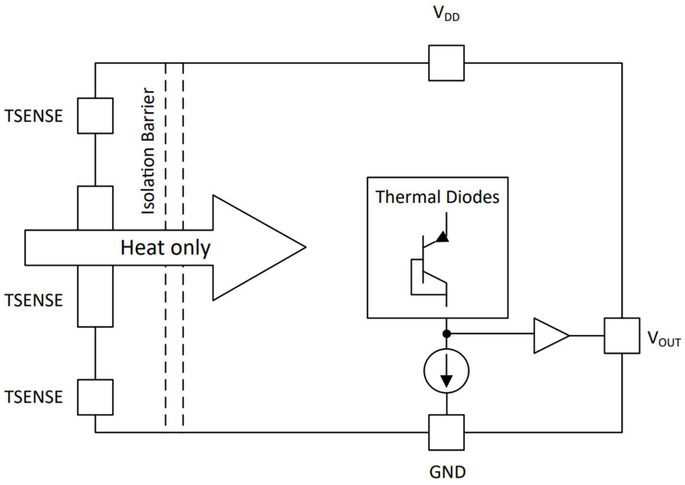


Figure 3-11. Block Diagram of ISOTMP35-Q1

This integration enables the sensor to be co-located with high voltage heat sources without requiring expensive isolation circuitry. Direct contact with the high-voltage heat source also provides greater accuracy and faster thermal response compared with approaches where the sensor is placed further away to meet isolation requirements.

In addition to the above-mentioned device-level designs, redundant temperature sensor and plausibility check are also common approaches to improving system functional safety.

4 Summary

This paper presents the FuSa analysis for OBC. Section 1 outlines the FuSa basics, general ISO 26262: 2018 workflow, and the TI tools that support FuSa development. Section 2 walks through the FuSa analysis example of single-stage OBC, starting with the item definition, deriving the safety goal, and then developing the FSRs, TSRs, and finally the HSRs and SSRs. Section 3 provides an overview of the key OBC elements and the safety functions, including MCU, gate driver, sensors and bias supply. The document is intended to give designers the essential information and resources needed to create OBC designs with FuSa.

5 References

1. TUV SUD, *Understanding the ISO 26262 Standard: What you need to know | TÜV SÜD PSB*
2. Texas Instruments, *Understanding Functional Safety FIT Base Failure Rate Estimates per IEC 623801 and SN 29500*, technical white paper.
3. Texas Instruments, *Streamlining Functional Safety Certification in Automotive and Industrial*, functional safety manual.
4. Texas Instruments, *Designing a Power Supply for a Safety MCU to Meet Functional Safety ASIL B*, technical white paper.
5. Texas Instruments, *TMCS1123-Q1, TMCS1126-Q1, TMCS1127-Q1, and TMCS1133-Q1 Functional Safety FIT Rate, FMD and Pin FMA (Rev. A)*, functional safety information.
6. Texas Instruments, *Automotive Functional Safety for C2000™ Real-Time Microcontrollers (Rev. F)*, functional safety manual.
7. Texas Instruments, *C2000™ Safety Mechanisms (Rev. B)*, functional safety manual.

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.

Last updated 10/2025