Application Note

Towards Functional Safety in Traction Inverter: Design Approach and Component Overview

Yuxin Liu, Sifan You, Lars Lotzenburger

ABSTRACT

With functional safety (FuSa) becoming increasingly critical in automotive electrification, this document serves as a comprehensive introduction to FuSa implementation in traction inverter systems for hybrid electric vehicles (HEV) and electric vehicles (EV). Section 1 provides foundational knowledge covering the importance of functional safety in traction inverters, applicable international and regional standards, and the ISO 26262 V-model development process. Section 2 explores the systematic FuSa requirements derivation process for traction inverter applications, demonstrating practical examples of safety goal definition, Fault Tree Analysis (FTA), and Failure Mode and Effects Analysis (FMEA) to derive functional and technical safety requirements. Section 3 highlights key Texas Instruments components for traction inverter and technical safety requirement implement, featuring chip-level safety mechanisms and system-level safety design strategies for critical subsystems including microcontrollers, gate drivers, position sensors, current sensors, power management ICs, and so on. This document aims to equip designers with essential resources for developing FuSa designs.

Table of Contents

Trademarks

1 Introduction

1.1 End-Equipment Traction Inverter

The traction inverter is a critical system in hybrid electric vehicles (HEV) and electric vehicles (EV) that controls the motor to generate traction torque based on commands from the driver and Vehicle Control Unit (VCU). The traction inverter also manages regenerative braking to charge the high-voltage battery. Figure 1-1 illustrates the structure of a traction inverter.

Upon receiving commands from the VCU and processing measured signals, the Microcontroller Unit (MCU) executes the field-oriented control (FOC) algorithm to generate appropriate PWM signals for the power module. This modulates the DC input into symmetric three-phase AC current to drive the motor. Torque commands originate from two sources: driver inputs through the acceleration or braking pedals, and Advanced Driver Assistance Systems (ADAS) during autonomous driving or emergency braking situations.

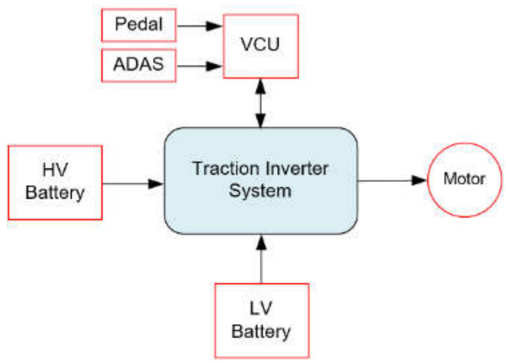

Figure 1-1. The Structure of a Traction Inverter

1.2 Why is Safety Needed in Inverter?

As electrification and autonomous driving technologies continue to advance, safety concerns for HEV and EV have become increasingly prominent. Critical failures can create hazardous conditions—for example, a malfunctioning rotor position sensor may output incorrect signals, causing erroneous FOC modulation and generating unintended motor torque. Similarly, a communication interface failure may prevent proper transmission of torque commands, resulting in motor performance that doesn't match driver requirements. Such malfunctions pose significant risks to vehicle occupants.

Functional Safety (FuSa) represents a critical component of overall system safety, focusing on verifying 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.

Consequently, FuSa has been incorporated into international standards and local regulatory frameworks worldwide. ISO26262:2018, the international standard for road vehicles FuSa, is the most authoritative reference in automotive FuSa globally. This comprehensive standard defines a complete FuSa development process for automotive electrical/electronic systems—from concept design to decommissioning—including core elements such as safety management, risk assessment, ASIL classification, and verification methods. The standard has become a mandatory compliance requirement in the global automotive market, with virtually all mainstream OEMs and suppliers required to strictly adhere to it. Building on this foundation, several region-specific standards address traction inverter FuSa, including China's GB/T 43254-2023, Europe's EU 2019/2144, America's SAE J2980, and so on. These standards propose typical safety goals for traction inverter driving and braking torque functions, formally establishing design and verification requirements for safety features. Additionally, for regenerative braking functionality, system structure and safety requirements are specified in GB21670-2025. As can be foreseen, FuSa is gradually becoming a mandatory requirement for inverters.

1.3 FuSa Development Flow

1.3.1 V-Model Development

The classic FuSa development process, known as the V-Model, serves as a core framework for many safety-critical systems. Figure 1-2 illustrates the automotive FuSa V-Model from ISO26262:2018. This structured approach divides the entire development lifecycle into two main phases: the left arm (requirements analysis and design) and the right arm (integration and verification).

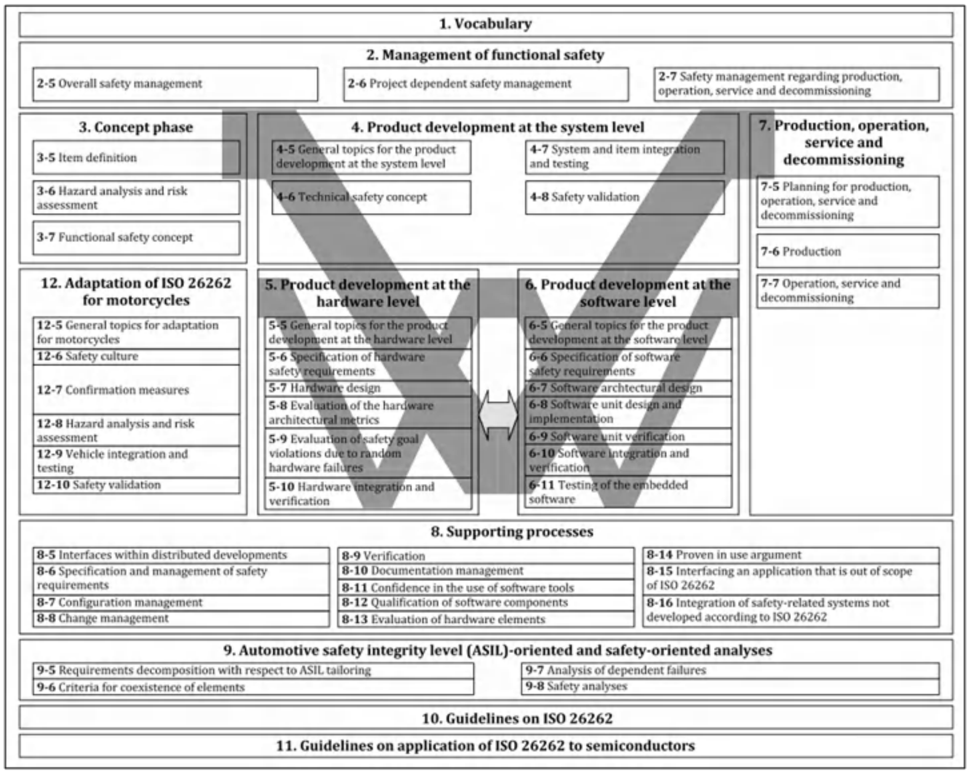

Figure 1-2. V-Module Process from ISO26262:2018

The Left Arm of V-Model shows the decomposition and design phase in FuSa development, encompassing the following detailed activities:

- **Item Definition:** Establishes the project scope and boundaries.
- **Hazard Analysis and Risk Assessment:** Identifies potential hazards for the item and evaluates them based on severity, exposure, and controllability factors, resulting in the definition of Safety Goals (SG) and assignment of Automotive Safety Integrity Levels (ASIL).
- **FuSa Concept:** Develops high-level safety strategies that allocate safety responsibilities across system functions and establishes FuSa Requirements (FSR) that define what safety functions are needed.
- **Technical Safety Concept:** Translates the functional requirements into specific Technical Safety Requirements (TSR) that detail how safety design is implemented in the system architecture.
- **Hardware/Software Safety Requirement:** Further refines technical requirements into Hardware Safety Requirements (HSR) and Software Safety Requirements (SSR) that guide the actual implementation.
- **Design Implementation:** Implements specific safety functions according to HSR and SSR

The Right Arm of V-Model shows the integration and verification phase in FuSa development, which contains the following detailed activities:

- **Software Testing & Verification:** Verifies the smallest software testable units.
- **Hardware Testing & Verification:** Verifies the smallest hardware testable units.
- **Integration Testing:** Verifies interactions between components.
- **System Testing:** Validates complete system functionality.
- **Vehicle Integration Testing:** Verifies performance in the actual vehicle environment.
- **Safety Confirmation:** Confirms achievement of safety goals.
- **FuSa Assessment:** Provides final safety confirmation.
- **Production release:** Approves the system for production.

The V-Model emphasizes that each development stage has corresponding verification activities, verifying that safety requirements are effectively transmitted and verified throughout the entire development process, thereby meeting the stringent requirements of automotive FuSa standards.

1.3.2 Inverter Safety Lifecycle

To provide a functionally safe traction inverter system, TI and system integrators must follow the ISO26262:2018 safety lifecycle in addition to the FuSa development process. This comprehensive approach verifies systematic risk reduction from concept to decommissioning.

The process begins with safety planning and management to define objectives. Through hazard analysis and risk assessment, the appropriate Automotive Safety Integrity Level (ASIL) is identified and established. These safety goals are then refined into detailed safety requirements specifications that guide all subsequent development activities.

Technical safety concepts are implemented during the design and implementation phases and validated through integration and testing. Safety requirements are methodically refined into specific hardware safety designs and software safety designs, which are developed and verified separately in accordance with hardware and software FuSa processes.

Finally, quality control during the production and operation phases is defined, while maintenance and decommissioning mechanisms are planned – from the end of the sale to the end of life – to make sure that the traction inverter maintains the FuSa throughout the life cycle.

2 FuSa Requirements for Traction Inverter

2.1 Traction Inverter Structure and Function Introduction

The primary goal of the traction system is to efficiently drive the traction motor, typically the permanent magnet synchronous motor (PMSM), with high control bandwidth. The Field-Oriented Control (FOC) algorithm is implemented in the Microcontroller Unit (MCU) to generate corresponding PWM signals, which control the gate driver to preciously switch the power module, converting the DC input voltage from the high-voltage (HV) battery into three-phase symmetric AC currents to drive the PMSM. Figure 2-1 shows the block diagram of a traction inverter.

For the FOC algorithm, the system requires real-time measurement of phase currents, rotor position, and DC-link input voltage. This requires high-accuracy, low-latency sensors within the traction inverter. Additionally, high-reliability power management components are essential to supply all elements in the system.

Since the isolation is required between the HV side and low-voltage (LV) side, isolated gate drivers with reliable isolated power supply circuits are necessary elements. Through CAN transceivers, the traction inverter accurately receives command of driving torque and reports any potential fault information to the Vehicle Control Unit (VCU). During braking operations, the traction inverter can operate in regeneration mode to charge the battery while simultaneously generating braking torque.

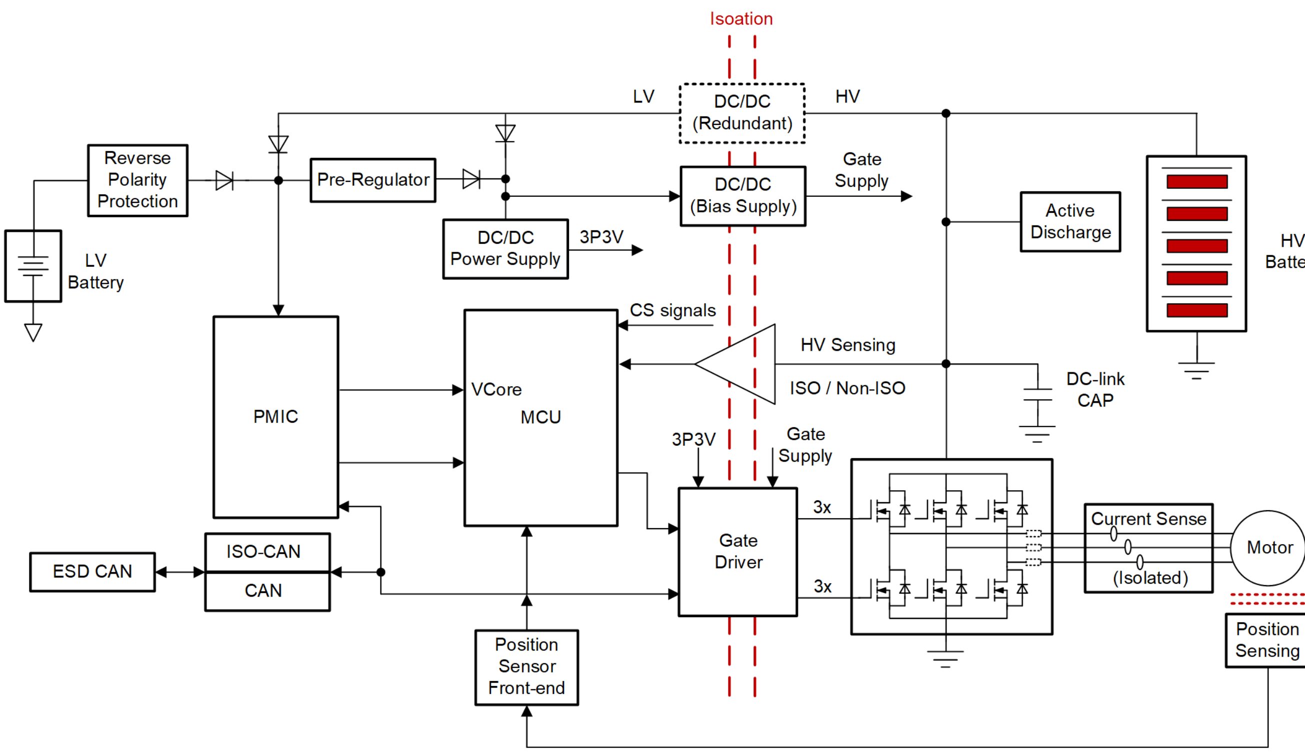

Figure 2-1. Block Diagram of a Traction Inverter

2.2 FuSa Requirements Derivation Process

The following system safety designs are applied on the basis of TIDM-02014, one TI traction inverter reference design, and all safety requirements are derived following the sequence outlined in Section 1.3. More system FuSa requirement analysis steps can be referred to "Towards FuSa in On-Board Charger: Design Approach and Component Overview".

In the following analysis, we have collected common customer safety requirements and standard-based safety requirements from standards outlined in Section 1.2 as the safety goals for our traction inverter safety design. The resources provided by the inverter in both drive and brake functions have been considered, and have proposed the safety goals of the system accordingly.

Using Safety Goal 1 (SG1) as an example, this document demonstrates how to build a Fault Tree Analysis (FTA) with this top-level safety goal in detail. Then, the derived FSR 1.6 serves as a new safety goal input to the Failure Mode and Effect Analysis (FMEA). The FMEA analysis on the position sensing system has been performed, illustrating an example of the TSR derivation process.

2.3 Safety Goal

Traction inverter's safety goals are vehicle-level safety requirements for the whole system. It shall be defined with consideration of undesirable hazard events and the safe state once a critical situation occurs. The safety goals in this analysis are derived as shown in Table 2-1. The Fault Tolerant Time Internal (FTTI) value should be provided by OEM or regulatory requirements depending on the specific system operating needs. The ASIL ratings indicate the level of rigor required in the safety processes, with ASIL-D representing the highest safety criticality level.

Table 2-1. Example FuSa Goals of the Traction Inverter

ID	Safety Goal	ASIL	Safe State	FTTI
SG1	Avoid unintended acceleration torque that exceeds the expected value.	ASIL-C/D	1. Alert and report failure. 2. Block torque output.	750ms (Specified by users)
SG2	Avoid unintended braking torque that exceeds the expected value.	ASIL-C		
SG3	Avoid inability to output drive torque.	ASIL-A	Alert and report failure.	

2.4 FuSa Concept

After establishing safety goals, a FuSa Concept (FSC) is developed, which contains safety requirements for sub-functional elements. ISO26262:2018 recommends safety analysis methods such as deductive analysis and inductive analysis to identify failures and transform them into safety requirements. In this chapter, FTA is taken, a typical deductive analysis method, to derive FuSa requirements from safety goals. Taking *SG1-Avoid unintended accelerating torque than expected* as an example, this document demonstrates the process of constructing an FTA to derive FSR.

FTA is a top-down deductive analysis method that uses logical reasoning to identify all possible causes and combinations of system failures. The method employs Boolean logic to describe cause-and-effect relationships between events. All the possible causes that can directly lead to the top event can be identified through an FTA. This is where safety requirements are established for the basic events or gates, constituting the derivation process for FSRs.

The FTA methodology allows users to systematically break down the high-level safety goal into more specific functional requirements that address individual failure modes. By analyzing the logical combinations of events that can lead to unintended acceleration torque, critical areas requiring safety mechanisms can be identified and appropriate functional requirements to mitigate these risks can be established.

2.4.1 FSC Design Architecture

Figure 2-2 shows the FSC level traction inverter system block diagram. FTA is performed according to the system architecture illustrated in this figure. The functions of each element are listed in Table 2-2.

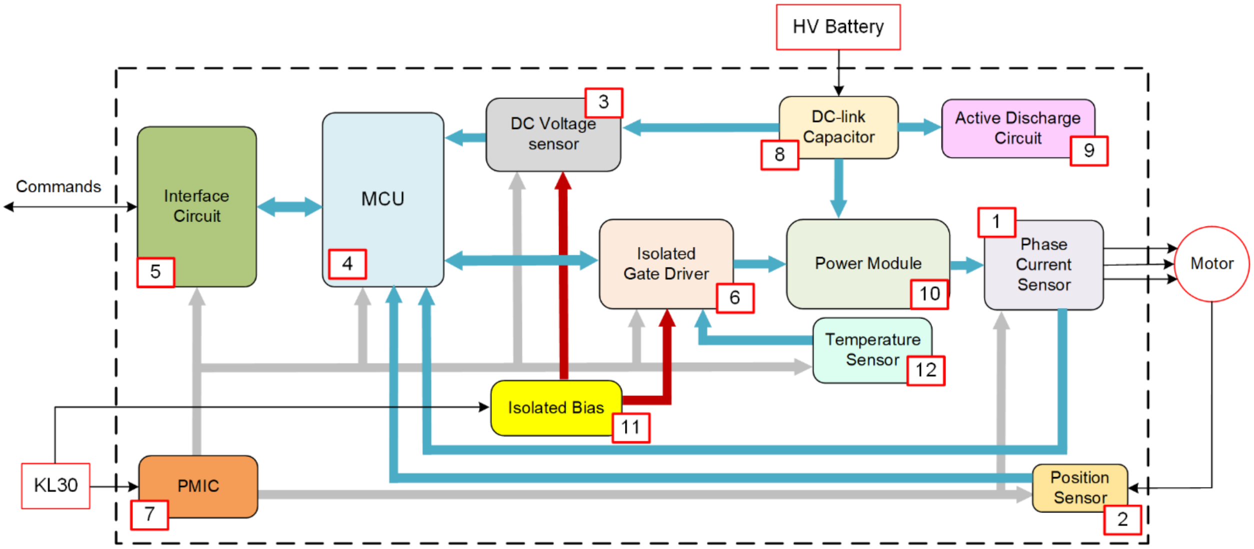

Figure 2-2. FSR Level Traction Inverter System Block Diagram

Table 2-2. Key Elements in Traction Inverter

Element ID	Element Name	Description
E1	Motor phase currents measurement circuit	Measures the inverter phase currents at power stage and transmits to MCU for FOC and operating condition monitoring.
E2	Rotor position measurement circuit	Measures the motor rotor position and transmits to MCU for FOC and operating condition monitoring.
E3	DC Voltage sensor	Measures the inverter power supply at the power stage for FOC and operating condition monitoring.
E4	Microcontroller circuit	Executes the FOC algorithm, monitors sensor data, generates PWM signals, and communicates with external systems.
E5	Interface circuit	Provides communication transceiver functionality between the inverter and external systems.
E6	Gate driver circuit	Provides the required voltage and driving current for the power module according to input PWM signals
E7	Power management circuit	Provides power supplies to key devices in the inverter on the LV side; also provides external watchdog and error monitoring for the MCU.
E8	DC-Link Capacitor	Capacitor for the power stage to stabilize and maintain the HVDC input voltage.
E9	Active discharge circuit	Provides active discharge for the DC-link capacitor during power-off or repair operations.
E10	Power module	Generates required modulated motor phase currents from the HV battery under the control of the gate driver circuit
E11	Isolated bias supply	Provides HV side isolated power supply for the gate driver circuit and voltage sensing circuit.
E12	Temperature measurement circuit	Measures the power stage temperature for operating condition monitoring.

2.4.2 Fault Tree Analysis

The FTA for SG1 is illustrated in Figure 2-3. The top event is defined as *providing unintended accelerating torque of the inverter during driving conditions*. The functional element structure within the system is then systematically analyzed to determine how various components can contribute to the occurrence of this top event. These failure events are associated with different logic gates in the fault tree diagram, representing AND or OR relationships between potential failure modes.

A cut-set analysis was performed for the basic events or gates in the FTA. The purpose of this analysis is to identify which elements or combinations of elements are included in the cut-set that could cause the top event to occur, and to determine the number of elements within each cut-set. The smaller the number of cut-set events, the more likely they are to directly lead to an SG violation. Therefore, propose FSR for the first order and second order cut-sets to prevent direct violation. This approach corresponds to addressing single point faults and multiple point faults in ISO26262: 2018. For cut-sets of third order or larger, we consider them as safe fault. These combinations of failures are sufficiently unlikely that they do not require additional safety requirements beyond those already established for lower-order cut-sets.

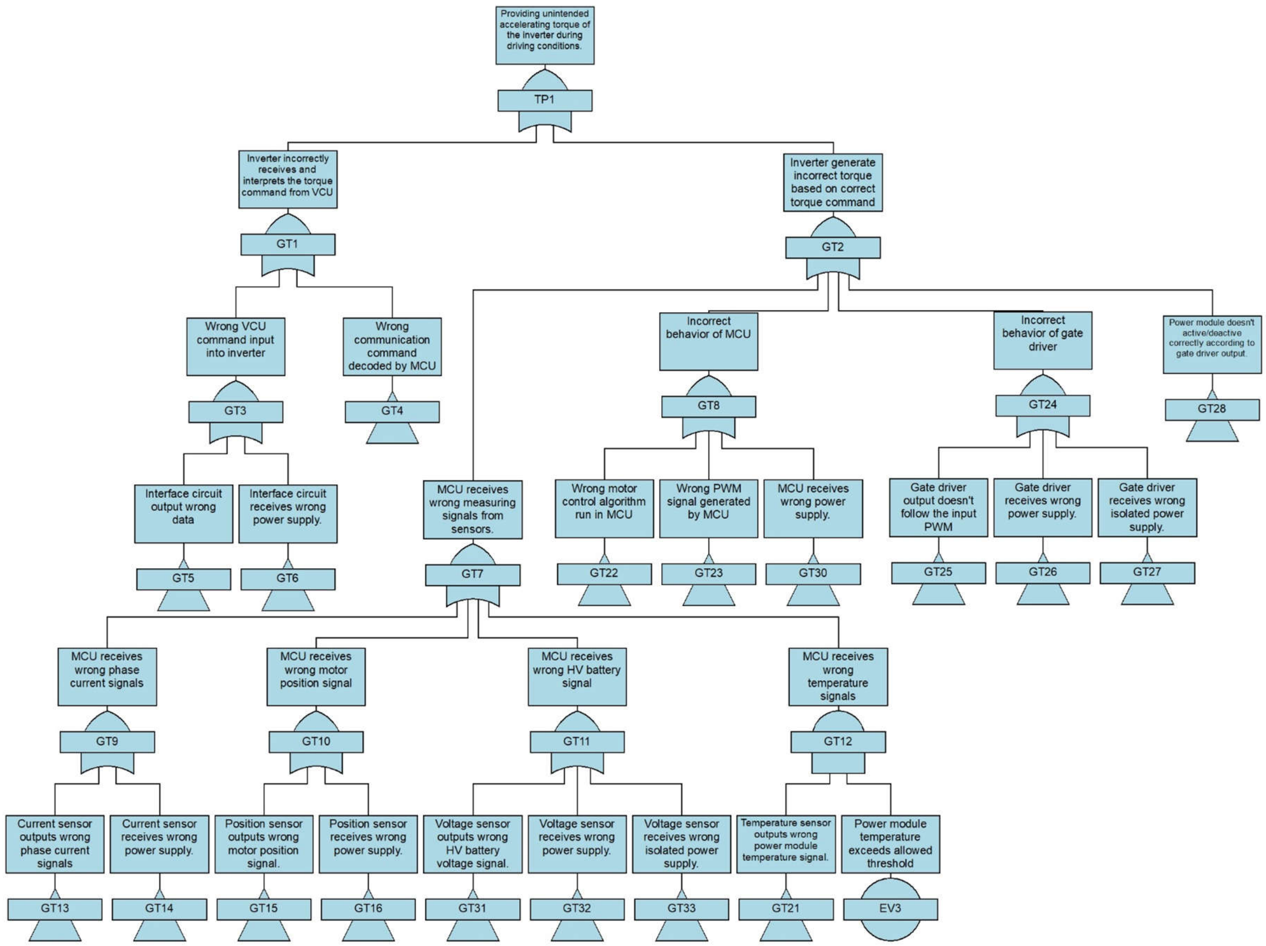

Figure 2-3. FTA Tree Example of SG1

2.4.3 FuSa Requirement

From the FTA results, certain failures were identified as first-order cut-sets that directly violate the top safety goal, causing unintended torque and potential damage. For example, if *GT15 – the motor position sensor output a wrong position signal* is TRUE, the MCU will receive incorrect position signal from sensor for FOC control, triggering events GT10 and GT7. This will cause the FOC algorithm to output incorrect PWM signals, generating wrong AC current and torque, ultimately leading to the top event *TP1-provide unintended accelerating torque than expected.*

Based on this analysis, the user can propose an FSR such as *Inverter shall correctly measure rotor position by position sensor* and assign this requirement to the motor position sensor implementation. Using this methodical approach,all first order and second order cut-sets into FSRs under the safety goal *Avoid unintended accelerating torque than expected* have been derived, as listed in Table 2-3.

Table 2-3. Example FSRs for SG1

FSR ID	FuSa Requirement	Safe State	Allocation	ASIL	FTTI	Traced to
1.1	Inverter shall correctly transfer the communication data from VCU to MCU with the interface circuit.	Generate alert to MCU. Enter 0-torque control.	HW, E5 SW, E4 HW&SW	D	FTTI	GT5

Table 2-3. Example FSRs for SG1 (continued)

FSR ID	FuSa Requirement	Safe State	Allocation	ASIL	FTTI	Traced to
1.2	Inverter shall correctly provide the power supply for the interface circuit.	Enter 0-torque control.	HW, E7, E5 SW, E4 HW&SW	D	FTTI	GT6
1.3	Inverter shall correctly perform communication command decode from VCU by MCU.	Discard torque command and enter 0-torque control.	HW, E4, E5 SW, E4 HW&SW	D	FTTI	GT4
1.4	Inverter shall correctly measure motor phase currents by current sensor.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E1 SW, E4 HW&SW	D	FTTI	GT13
1.5	Inverter shall correctly provide the power supply for current sensor.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E7 SW, E4 HW&SW	D	FTTI	GT14
1.6	Inverter shall correctly measure rotor position by position sensor.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E2 SW, E4 HW&SW	D	FTTI	GT15
1.7	Inverter shall correctly provide the power supply for position sensor.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E7 SW, E4 HW&SW	D	FTTI	GT16
1.8	Inverter shall correctly measure the HV battery voltage by voltage sensor.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E3 SW, E4 HW&SW	D	FTTI	GT18
1.9	Inverter shall correctly provide the power supply for voltage sensor.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E7 SW, E4 HW&SW	D	FTTI	GT19
1.10	Inverter shall correctly provide the isolated power supply for voltage sensor.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E7, E11 SW, E4 HW&SW	D	FTTI	GT20
1.11	Inverter shall correctly perform power module temperature measurement.	Generate alert to MCU. Limit the maximum torque.	HW, E12 SW, E4 HW&SW	D	MPFDTI	GT21
1.12	Inverter shall correctly support motor control software algorithm run in MCU.	Block MCU output. Enter ASC or freewheeling.	HW, E4, E5 SW, E4 HW&SW	D	FTTI	GT22
1.13	Inverter shall correctly provide PWM control signal output from MCU.	Block MCU PWM output. Enter ASC or freewheeling.	HW, E4, E5 SW, E4 HW&SW	D	FTTI	GT23
1.14	Inverter shall correctly provide the power supply for MCU.	Reset MCU. Enter ASC or freewheeling.	HW, E7, E5 SW, E4 HW&SW	D	FTTI	GT30
1.15	Inverter shall correctly amplify the PWM signal into driving signal in gate driver.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E6 SW, E4 HW&SW	D	FTTI	GT25
1.16	Inverter shall correctly provide the power supply for the gate driver.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E7, E6 SW, E4 HW&SW	D	FTTI	GT26
1.17	Inverter shall correctly provide the isolated power supply for the gate driver HV side.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E7, E6 SW, E4 HW&SW	D	FTTI	GT27
1.18	Inverter shall correctly perform activation/ deactivation control by power stage.	Generate alert to MCU. Enter ASC or freewheeling.	HW, E6, E10 SW, E4 HW&SW	D	FTTI	GT28

As shown in Table 2-3, there are several failure modes that directly violate the top safety goal. The system needs to be forced into a safety state after a failure occurs. Considering the traction inverter with PMSM, which generates a significant back-EMF at high speed. We have defined four possible safe states:

- **Degrade to 0-torque mode**

This is the safe state when the traction inverter can still provide fully motor control and sensing functions. The MCU continues to run the FOC algorithm based on sensing signals with iq = 0 for zero torque output. This safe state is appropriate for communication failures, such as receiving incorrect VCU commands or harness disconnection. Since other parts of the inverter remain operational, normal function can be easily restored when the failure is resolved.

- **Freewheeling**

This is the safe state when the traction inverter cannot generate correct AC currents and torque following commands at low speed. All power switches are turned off in this safe state to disconnect all three phases. At low motor speed, the PMSM will only generate back-EMF lower than the HV battery voltage.

- **Active short circuit (ASC)**

This is the safe state when the traction inverter cannot generate correct AC current and torque following commands at high speed. At high speeds, the PMSM generates back-EMF greater than the HV battery voltage, causing significant regeneration current, excessive braking torque, and potential battery damage. Therefore, the inverter should enter ASC at high speeds by turning on either all three high-side power switches or all three low-side power switches to short the three phases. This limits the phase current to a constant value with low braking torque.

- **Limit torque output**

This is a degraded fail-operational strategy implemented when the power module temperature exceeds an alert threshold. If the temperature continues to rise above the shutdown threshold despite running in this degraded mode, the traction inverter enters either ASC or freewheeling mode.

2.5 Technical Safety Concepts

Once the FSC has been established, the subsequent phase is to create the Technical Safety Concept (TSC). The TSC translates the FSCs into concrete TSRs. FuSa analysis is used to derive these technical safety requirements from FSRs.

In the previous chapter, this document showed how to perform FTA for the traction inverter system. This chapter uses FMEA, a representative inductive analysis method, to illustrate the safety analysis process and how to derive TSRs. This chapter uses *FSR1.6 – Inverter shall correctly measure rotor position by position sensor* as the example for this demonstration.

FMEA is a systematic methodology that identifies possible failure modes in product designs, evaluates their effects and causes, and develops appropriate preventive and control measures targeting each specific failure. Unlike FTA, which works top-down from a defined hazard, FMEA works bottom-up by examining individual components and their potential failure modes, then tracing the consequences up to system-level effects.

2.5.1 TSC Design Architecture

Figure 2-4 shows the TSC level traction inverter system block diagram and the safety path for FSR1.6, which is one level deeper than FSC level block diagram. For critical components, the analysis aims to provide:

- Propose valid safety mechanisms for safety-violated failure modes that are not affected by dependent failures
- Create safe state entrance path for the system that can meet detection/reaction time interval requirements.
- Provide safety mechanisms with appropriate diagnostic coverage without over-design.
- Transfer TSR to hardware/software level implementations.

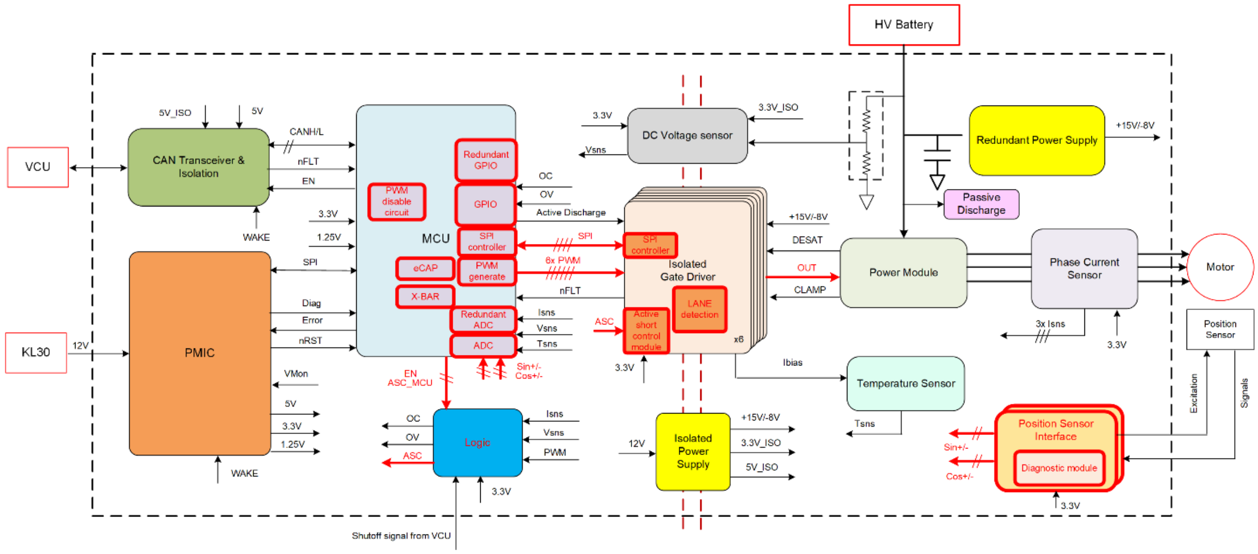

Figure 2-4. TSR level traction inverter system block diagram of with FSR1.6 safety path

2.5.2 Failure Mode and Effect Analysis

For each FSR, an FMEA must be constructed to identify the failure mode, failure effect and failure cause. For the failure mode, Each failure mode must be classified according to the safety goal violation type, which can be divided into three categories:

- **Single-point fault (SPF):** Faults that directly violate the FuSa goal.
- **Multi-point fault (MPF):** Faults that violate the FuSa goal only when combined with another independent fault.
- **Safe fault (SF):** Faults that cannot violate FuSa goal, which can be either detected or inherently safe.

Additionally, some elements may be non-safety related, where the function of each element does not impact the safety goal.

For each failure that can violate an FSR (including both SPF and MPF), appropriate safety mechanisms must be designed. These safety mechanisms are considered in the following aspects, but are not limited to:

- **Detection Mechanisms** (as referenced in ISO26262-Part5/Part11: 2018):

- Plausibility Checks: Value range, rate of change, signal correlation
- Redundancy Monitoring: Comparison between redundant channels
- Diagnostic Tests: Built-in self-test, periodic functional tests
- Watchdog Monitoring: Program flow, timing supervision

- **Control Mechanisms** (as referenced in ISO26262-Part5/Part11: 2018):

- Safe State Transition: Graceful degradation to safe operation
- Fault Reaction: Immediate response to detected faults
- Warning Generation: User notification of system status
- System Shutdown: Controlled system deactivation

Table 2-4 shows part of the FMEA for FSR1.6. (Inverter must correctly measure rotor position by position sensor).

Table 2-4. Example of a Portion of FMEA Table

System Element	System Sub-Element	Main Function	Failure Mode	Failure Effect	SG Violation Types	Failure Cause	Safety Mechanism
Rotor position measurement circuit (E2)	Rotor position measurement sensor	Measure the rotor position for FOC algorithm for motor speed and torque control	Cannot provide motor position measurement	Cannot measure the motor position which leads to wrong motor speed and torque control	SPF	Position sensor output short/ open circuit	1. Tri-state output and run output out of range check. 2. Position sensor output out of range check. 3. Redundant position sensor measurement circuit.
					SPF	Position sensor excitation circuit no output or output drift.	1. Excitation circuit output plausibility check. 2. Tri-state output and run output out of range check. 3. Redundant position sensor measurement circuit.
					SPF	Position sensor input short/open circuit	1. Input signal plausibility check. 2. Tri-state output and run output out of range check. 3. Redundant position sensor measurement circuit.
			Providing motor position mismatch the actual position.	Incorrectly measure the motor position which lead to wrong motor speed and torque control	SPF	Position sensor output drift	1. Output phase & gain imbalance check. 2. Tri-state output and run output out of range check. 3. Redundant position sensor measurement circuit.
	Rotor position measurement sensor redundant circuit	Provide redundant rotor position to MCU for FOC	Cannot provide motor position measurement	Incorrect/no input value to MCU and unintended enter safe state when main rotor position sensor without malfunction	MPF	Position sensor output open/short circuit or no output for excitation / AFE / amplifier circuit.	Redundant position sensor measurement circuit.
			Providing motor position mismatch the actual position.	Inaccurate input value to MCU and cannot detect the main rotor position sensor failure	MPF	Position sensor output drift	1. Tri-state output and run output out of range check. 2. Redundant position sensor measurement circuit.

Table 2-4. Example of a Portion of FMEA Table (continued)

System Element	System Sub-Element	Main Function	Failure Mode	Failure Effect	SG Violation Types	Failure Cause	Safety Mechanism
MCU (E4)	PWM generation circuit	Generate PWM signal based on FOC.	Unintended generating PWM signal	Unintended PWM causing unintended torque, and fail to enter safe state.	SPF	Unintended PWM signal generation.	PWM trip zone circuit to disable or program PWM to respond accordingly. eCAP for PWM level detection.
	eCAP circuit	Capture the rising or falling edges	Cannot capture the edges.	Cannot correctly capture the ePWM edge for ePWM diagnostics	MPF	Cannot capture the edges.	BIST
	PWM trip zone circuit	Disable or program PWM when faults occur	Cannot operate as required	Cannot disable or program PWM to safe state.	MPF	Trigger circuit fault.	BIST
			Unintended operate with no trip requirement.	Unintended triggered and enter safe state	SF	Unintended trigger without the trigger signal	NA
	ADC circuit	A to D converter for sensing	Cannot measure the analog input signal correctly	Cannot get the correct position sensor output signals.	SPF	ADC converter failure or pins open circuit	Redundant ADC with HW comparator mechanism.
	Redundant ADC circuit	Redundant A to D converter.	Cannot measure the analog input signal correctly	Cannot get the correct position sensor output signals.	MPF	ADC converter failure or pins open circuit	Redundant ADC with HW comparator mechanism.
	GPIO circuit	Generate the ASC related signal to help system enter the safe state	Unintended trigger the GPIO output.	Unintended enter the safe state.	SF	GPIO output wrong	NA
				Enter the wrong safe state.	SPF	GPIO output wrong	GPIO Readback and Comparison. Block GPIO output and rely on external logic circuit to enter safe state while readback comparison is wrong.
	GPIO Readback and comparison	Read the GPIO status to detect if safe state output is correct.	Unintended trigger the wrong signal	Unintended Enter sate state without GPIO output wrong.	SF	GPIO readback circuit wrong	NA

Table 2-4. Example of a Portion of FMEA Table (continued)

System Element	System Sub-Element	Main Function	Failure Mode	Failure Effect	SG Violation Types	Failure Cause	Safety Mechanism
Gate driver circuit (E6)	Active short circuit part	Perform ASC for motor to enter the corresponding safe state.	Cannot block PWM output with related ASC command.	Cannot enter the safe state while failure occurring.	MPF	ASC logic circuit or transmission circuit failed.	BIST Isolation Lane Diagnostics
			Output wrong safe state with related ASC command.	Enter the wrong state, which is not safe.	MPF	ASC logic circuit or transmission circuit flip.	BIST Isolation Lane Diagnostics
	Isolation lane detection circuit	Detect the wrong signal on isolation lane.	Cannot detect the isolation lane error.	Cannot enter the safe state while failure occurring.	MPF	Isolation lane detection circuit failed.	BIST
			Unintended report isolation lane failure.	Unintended enter the safe state.	SF	Isolation lane detection circuit failed.	NA

2.5.3 Technical Safety Requirements

From the FMEA results, the proposed safety mechanisms are directly proposed in the form of TSR. For some SPF/MPF faults where we cannot propose practical safety mechanisms at the system level, the safety requirements are passed down to the hardware/software level for implementation within semiconductor components. Based on Table 2-4, the related TSR for FSR1.6 can be found in Table 2-5.

Table 2-5. TSR for FSR1.6

TSR ID	Technical safety requirement	Allocation	ASIL	Safe State	FTTI (Specified by users)
1.6.1	The rotor position sensing circuit shall measure rotor position correctly.	Position sensor ADC	ASIL B(D)	Position sensor tri-state output. MCU blocks position sensor signals and route the redundant position sensor signals.	FTTI_PS
1.6.2	The rotor position sensing circuit shall run input and output amplitude and phase plausibility check correctly.	Position sensor ADC	ASIL B(D)	Position sensor tri-state output. MCU blocks position sensor signals and route the redundant position sensor signals.	FTTI_PS
1.6.3	The rotor position sensing circuit shall run excitation amplitude and frequency plausibility check correctly.	Position sensor ADC	ASIL B(D)	Position sensor tri-state output. MCU blocks position sensor signals and routes the redundant position sensor signals.	FTTI_PS
1.6.4	The rotor position sensing circuit shall block output into tri-state with sensor plausibility check failure.	Position sensor ADC	ASIL B(D)	MCU blocks position sensor signals and routes the redundant position sensor signals.	FTTI_PS
1.6.5	Redundant rotor position sensing circuit shall run plausibility check and enter tri-state if fails.	Position sensor ADC	ASIL B(D)	MCU abandons redundant position sensor signal.	FTTI_PS

Table 2-5. TSR for FSR1.6 (continued)

TSR ID	Technical safety requirement	Allocation	ASIL	Safe State	FTTI (Specified by users)
1.6.6	MCU shall force the inverter entering safe state when the 2x position sensor outputs are valid but mismatched.	ADC SW MCU CPU Position sensor	ASIL-D	MCU enter ASC or freewheeling.	FTTI_MCU
1.6.7	MCU shall run the sensor output range plausibility check correctly with sensor tri-state output.	ADC SW MCU CPU Position sensor	ASIL D	MCU abandons sensor signal and read the redundant sensor signal	FTTI_MCU
1.6.8	MCU shall check if the PWM output matches the intended logic.	PWM eCAP	ASIL-D	MCU block output and enter ASC or freewheeling	FTTI_MCU
1.6.9	MCU shall check ADC comparator output.	ADC Redundancy ADC ADC HW Check	ASIL-D	MCU block output and enter ASC or freewheeling	FTTI_MCU
1.6.10	Gate driver shall block PWM output with ASC signal input.	PWM disable circuit PWM Lane check ASC Circuit Output stage MCU CPU	ASIL-D	Gate driver will cutoff output stage and enter safe state leveraging other 5x gate drivers	FTTI_GD
1.6.11	Gate driver shall output correct safe state voltage level.	ASC Circuit Isolation lane check Output stage	ASIL-D	Gate driver will cutoff output stage and enter safe state leveraging other 5x gate drivers	FTTI_GD
1.6.12	Gate drive shall check if the signal transferred on isolation lane is correct.	Isolation lane check	ASIL-D	Gate driver will block PWM output and enter ASC or freewheeling.	FTTI_GD

These Technical Safety Requirements define specific measures to make sure that the rotor position sensing function operates correctly and safely. They address various aspects including measurement accuracy, plausibility checks, redundancy management, fault detection, and safe state transitions. Each requirement is allocated to specific components, assigned an appropriate ASIL rating, and linked to defined safe states and fault tolerant time intervals.

3 Safety Design Implementation on Inverter

3.1 TI FuSa Product

Texas Instruments provides various discrete device options, allowing customers to build safety systems tailored to their specific application requirements. TI also offers comprehensive and flexible FuSa solutions that fully comply with ISO26262: 2018 requirements, helping customers achieve FuSa goals in automotive electronics and safety-critical applications. Additionally, TI provides complete product FuSa documentation and technical support to assist integrators with their design processes and simplify safety certification procedures.

TI's products are categorized into "FuSa-Capable", "FuSa Quality-Managed", "FuSa-Compliant" to meet different ASIL requirements. The detailed development process and deliverables are shown in Figure 3-1.

		Functional Safety-Capable Low-complexity products that can be evaluated for use in a functionally safe system	Functional Safety Quality-Managed Previously-released, complex products that have had additional documentation developed to enable their use in functional safety applications.	Functional Safety-Compliant Products specifically developed to be compliant to functional safety standards that can be used in functional safety applications
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**			✓

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

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

- **FuSa-Capable products**

These products are non-FuSa compliant but are developed following TI's quality-managed process. TI provides assistance documentation including "Failure Mode Distribution (FMD)" and/or "Pin FMA" to help customers complete evaluation of hardware elements when using these products in safety applications. TI also provides FuSa-capable device failure rate information for system FMEDA (Failure Modes, Effects, and Diagnostic Analysis). These products are suitable for medium to low safety integrity level applications or as auxiliary components in high-safety systems in automotive environments.

- **FuSa Quality-Managed products**

These products are also non-FuSa compliant but are developed following TI's quality-managed process. TI provides detailed failure mode types, distribution, and failure rate information. This information is included in device FMEDA, which helps customers complete hardware evaluation of hardware elements when using these products in safety applications. These products are delivered with a safety manual, and system integrators can enable or disable embedded safety mechanisms depending on their specific needs. They are suitable for medium to low safety integrity level applications or as auxiliary components in high-safety systems in automotive environments.

- **FuSa-Compliant products**

These products are the only type of FuSa compliant. They are developed following both TI's quality-managed process and also TI's FuSa process. TI has the FuSa-certificated FuSa development process for both hardware and software. TI provides a complete FMEDA and safety manual for this type of product. System integrators can enable/disable embedded safety mechanisms depending on their needs. These products are suitable for direct use in safety-related applications and can meet safety targets in automotive environments. TI also provides FuSa certificates or assessment reports to assist integrators with system-level FuSa certification.

For information about TI FuSa devices, customers can easily find the related information in www.ti.com/technologies/functional-safety/overview.html. By selecting the FuSa category, all safety-related devices will be selected as shown in Figure 3-2. In the device detailed pages shown in Figure 3-3, users can access critical FuSa documentation through a straightforward process. By clicking on the technical documentation section, the FuSa report can be downloaded directly, providing essential safety-related information about the device. For more detailed analysis documents such as FMEDA, these must be requested separately due to Non-Disclosure Agreement (NDA) requirements.

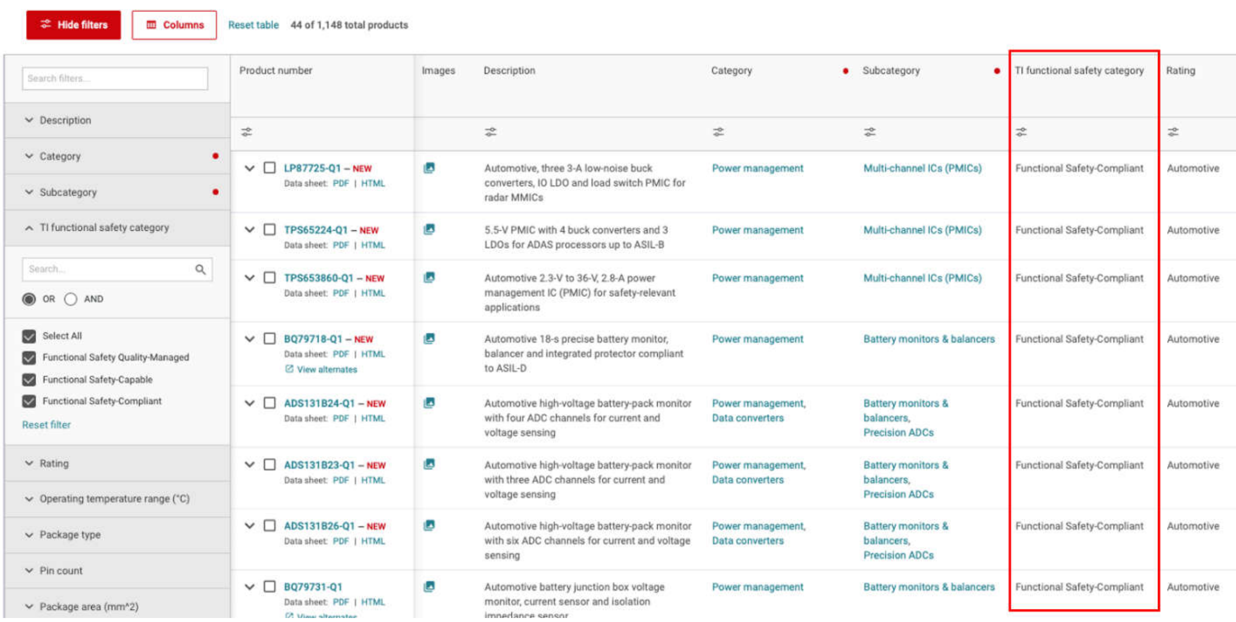

Figure 3-2. TI Devices FuSa Category on TI.com

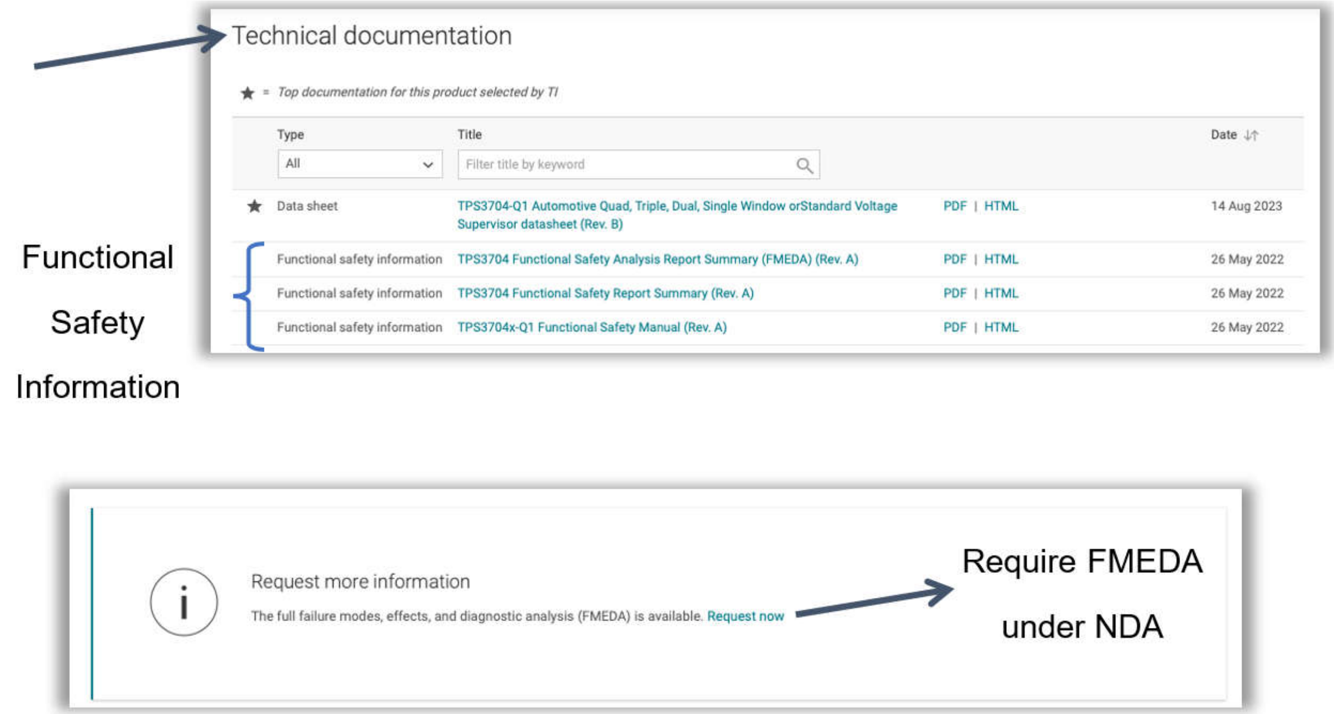

Figure 3-3. Requesting FuSa Related Documents From Ti.com

3.2 How Does TSR Implement?

Taking the TSR in section 2.5.3 as an example, this part shows the TSR implementation with position sensor output failure based on TI safety position sensor AFE LDC5072/3-Q1, safety MCU F29H859-Q1, smart gate driver UCC5881-Q1, and TI programmable logic device TPLD1201-Q1. Figure 3-4 shows the detailed safety path with the related devices.

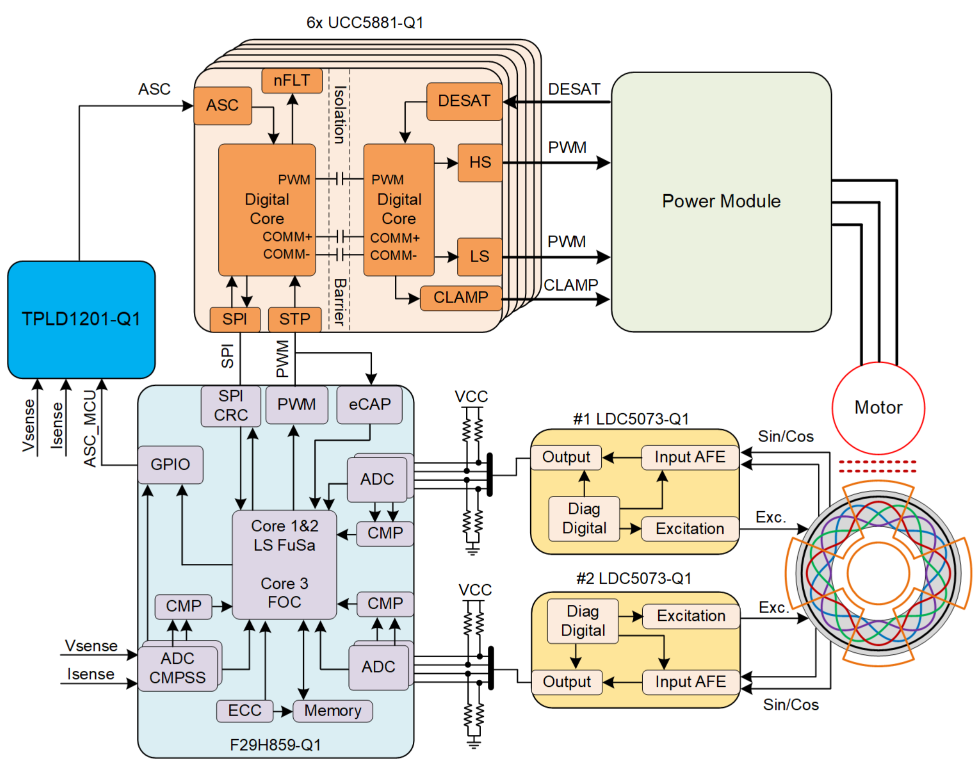

Figure 3-4. Safety Path Regarding TSR on Position Sensor Output Failure

3.2.1 Position Sensor

The LDC5073-Q1 is an inductive resolver analog front-end for motor position sensing, which is developed following the ISO26262: 2018 with the hardware capability up to ASIL-C compliance. The inductive sensor, built using PCB technology and sharing the same board as the LDC5073-Q1, consists of stator coils and a conductive target. The target is mounted to the motor's rotor and positioned over the stator coils, which are traces on the PCB. The LDC5073-Q1 drives the excitation coil, creating eddy currents in the target which then induces voltages in the stator sense coils. The MCU attached to the harness uses these two signals to estimate the angle. The LDC5073-Q1 generates the excitation signal, and then filters, demodulates, and amplifies the COS and SIN signals. The block diagram of the inductive sensor with LDC5073-Q1 is shown in Figure 3-5.

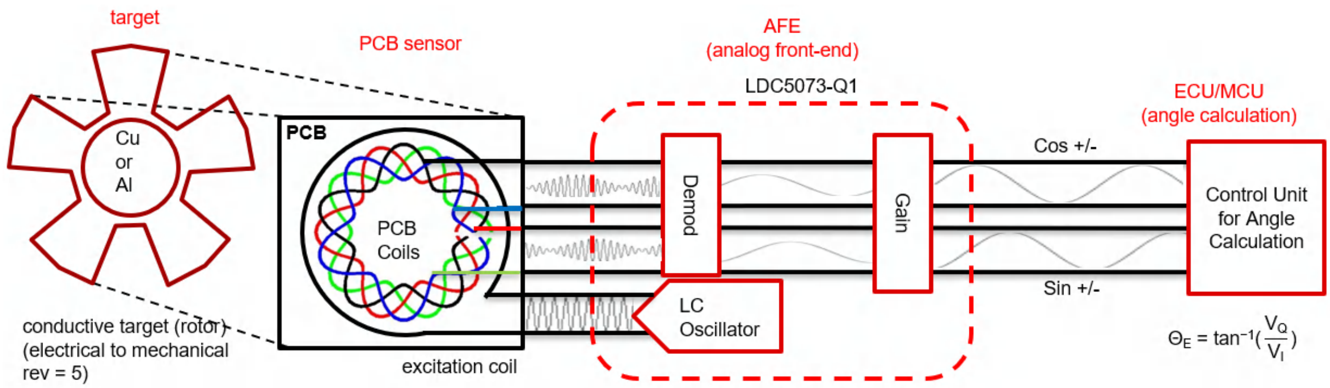

Figure 3-5. Inductive Position Sensor Block Diagram With LDC5073-Q1

The LDC5073-Q1 provides full support for On-Board-Diagnostics II (OBD2) and enables the controller to distinguish sensor and harness failures. The device communicates fault conditions to the controller by forcing fault state voltages on the outputs without requiring additional pull-ups or pull-downs on the sensor board. Using End-of-Line (EOL) programming, the fault state voltages are configured according to the controller board pull-up and pull-down configuration. With any sensor failure or harness failure, the MCU ADC will read the pin voltage out of range and directly detect the failure. The OBD2 can be configured for both fail-operational mode and fail-safe mode cooperating with MCU. When experiencing excitation signal fault, sensor input signal fault, LDC5073-Q1 internal gain/offset fault, or LDC5073-Q1 output stage fault, the LDC5073-Q1 will enter diagnostics mode, and the MCU will read the failure mode based on OBD2 voltage on the ADC. At the same time, the fail-operational mode allows continuous reporting of angle information during safety faults to continue vehicle operation, while informing the user of a need for service.

The LDC5073-Q1 is also equipped with numerous diagnostics features to detect, monitor, and report failures that occur either before power-on or during normal operation. The diagnostics includes UV/OV monitoring, BIST, EEPROM ECC check, excitation/sensing input/output integrity check, thermal shutdown, etc. The configurable output mode of LDC5073-Q1 supports 3.3V SIN/COS output with a 5.0V supply along with traditional SIN/COS output matching supply at 5.0V or 3.3V enables advancing MCU/ADCs to 3.3V while still operating the sensor board at 5V. LDC5073-Q1 is a more predictable high speed angle sensor in the market with less than 100nS of delay uncertainty and 0.05 degrees of 3 sigma repeatability.

To cover scenarios where the sensor output angle is incorrect but valid, and to meet the systematic ASIL-D level design requirements, two LDC507x-Q1 devices with redundant sensing coils can be implemented without significantly increasing PCB size, as shown in Figure 3-6. If the two sensor outputs mismatch, the MCU will abandon both sensor outputs and force the system to enter a safe state. Additionally, the system can operate in failure operational mode when one sensor output is out of range. With this method, fewer safety mechanisms can be selected for each LDC5073-Q1, since two ASIL-B designs can achieve ASIL-D through decomposition.

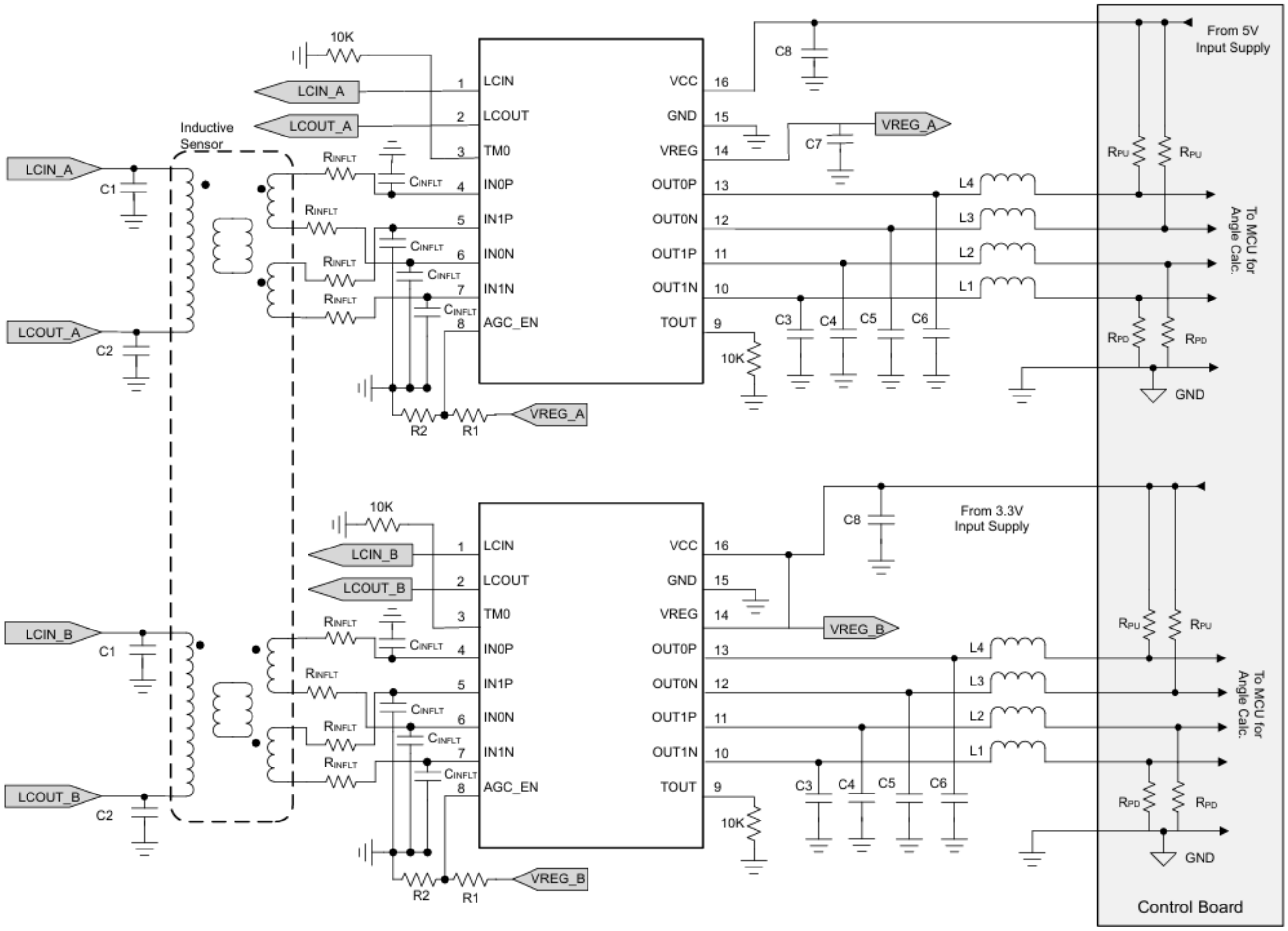

Figure 3-6. 2x LDC507x-Q1 Path as Redundancy to Achieve Systematic ASIL-D

3.2.2 MCU

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 three C29x CPU (supporting lockstep capable) running at 200 MHz, 4000 kByte flash, 452 kByte of RAM, supporting 5 SAR ADCs, up to 36 channels PWM output, and QFP-144/QFP-176/BGA 256 package. It meets ISO26262 and IEC61508 standards, ensuring compliance with safety requirements up to ASIL-D/SIL3, which also support HSM for cyber-security. With advanced functionalities and extensive connectivity options, it offers a comprehensive solution.

In traction inverter application, one pair of lockstep (LS) cores can be dedicated to FuSa operations, while another core can be used for main FOC motor control algorithms. The LS cores run identical FuSa code to detect any failures in program execution or memory integrity. If the MCU detects an out-of-range signal from the ADC, it will mark the position sensor as failed and automatically switch to reading the redundant position sensor output. If the MCU detects mismatched outputs from the two position sensors, it will send an ASC command via GPIO to an external logic circuit, which then triggers the ASC function in the smart isolated gate driver. The MCU will also transmit corresponding state information through SPI to correctly configure the gate driver for ASC mode.

Hardware redundancy for the ADC is implemented by having multiple instances of the peripheral sample the same input and simultaneously performing the same operation, followed by a cross-check of the output values. By cross-checking the ADC conversion data simultaneously across different ADC instances, the hardware ADC checking circuit can detect and address ADC conversion failures. The PWM output can be readback by (enhanced Capture) eCAP with crossbar (XBAR) to detect if PWM output is correct or has been successfully disabled with PWM Trip Zone (TZ) following an ASC command. A similar safety mechanism can be implemented for ASC (GPIO output) to verify the correct output for safe state command.

These comprehensive safety features ensure that the MCU can reliably detect sensor failures, process safety-critical signals, and initiate appropriate safe states when necessary, maintaining the FuSa integrity of the traction inverter system.

3.2.3 Logic Circuit

The TPLD1201-Q1 is TI's programmable logic device that integrates a substantial array of logic resources, including Look-Up Tables (LUTs), D-flip-flops, counters, edge detectors, and oscillators. It also incorporates several analog macro-cells including analog comparators and voltage references. The detailed resources available in the TPLD1201-Q1 are illustrated in Figure 3-7.

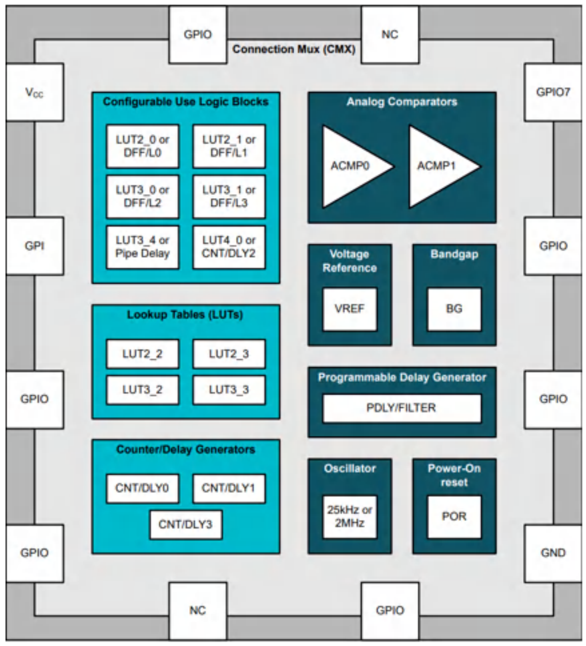

Figure 3-7. Resources in TPLD1201-Q1

The device can be easily configured with TI ICS GUI and can be permanently configured as a fixed-function device. With dedicated digital circuit design, the TPLD1201-Q1 can function as a redundant safe state entering circuit to help the system enter the correct safe state when the MCU fails. The block diagram of this implementation can be found in Figure 3-8.

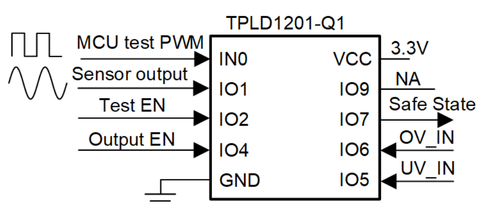

Figure 3-8. TPLD1201-Q1 Connection for Motor Speed Detection Design

With this TPLD1201-Q1 logic circuit design, when MCU is failed, PMIC triggers the Output_EN signal to the TPLD1201-Q1, and the safe state output pin will respond according to sensor output signal frequency, OV_IN and UV_IN. During an overvoltage event, the TPLD1201-Q1 will output ASC command, while during an undervoltage event, it will output freewheeling command. When the voltage is within the normal range, the TPLD1201-Q1 will output either ASC command or freewheeling command based on the sensor output frequency. The threshold frequency can be flexibly adjusted by modifying the counter data inside the device during the configuring stage.

This design also supports power-on Built-In Self-Test (BIST) with the MCU sending out the TEST_EN signal and test PWM to further decrease the latent failure metric. If no failure is detected in the MCU, the TPLD1201-Q1 output will be masked, and the MCU will send out the corresponding safe state. All functions and safety mechanisms design inside the TPLD1201-Q1 can be flexibly modified by users in ICS GUI according to their specific requirements.

TPLD1201-Q1 Functional Safety FIT Rate, FMD and Pin FMA document is also available now. For any FuSa calculation requirement, this document can be used as a reference for any data.

The TPLD1201-Q1 serves as a critical component in the safety architecture, providing an independent monitoring and control path that can maintain system safety even in the event of MCU failure. This redundancy is essential for achieving high safety integrity levels in traction inverter applications.

3.2.4 Smart Isolated Gate Driver

The UCC5881-Q1 is an isolated, highly configurable adjustable drive strength gate driver targeted to drive high power SiC MOSFETs and IGBTs. It is a TI FuSa-Compliant device developed with ISO26262:2018 and is fully validated. Documentation is available to aid ISO26262: 2018 system design up to ASIL-D with numerous integrated safety mechanisms.

UCC5881-Q1 features dedicated hardware ASC pins on both primary side and secondary side. This active short circuit function allows the system to force the state of the power transistor regardless of the PWM input. For cases where the main MCU is unavailable due to fault or other reasons, a secondary control circuit drives the ASC_EN input high to force the output of the device to the state defined by the ASC pin input. Figure 3-9 illustrates the typical ASC implementation diagram with the UCC5881-Q1. The ASC circuit is also detected by BIST to ensure its proper functioning.

Table 3-1 presents the input truth table for the safe state pins, showing how different combinations of inputs determine the output state. Beyond these basic functions, the ASC can be flexibly configured as a high-priority event that overrides certain other failures (such as DESAT, shoot-through, SPI fault, etc.). The secondary side ASC can also force the system to enter a safe state regardless of UCC5881-Q1 primary side power faults and other PWM/communication-related faults. More detailed information is available in the UCC5881-Q1 datasheet.

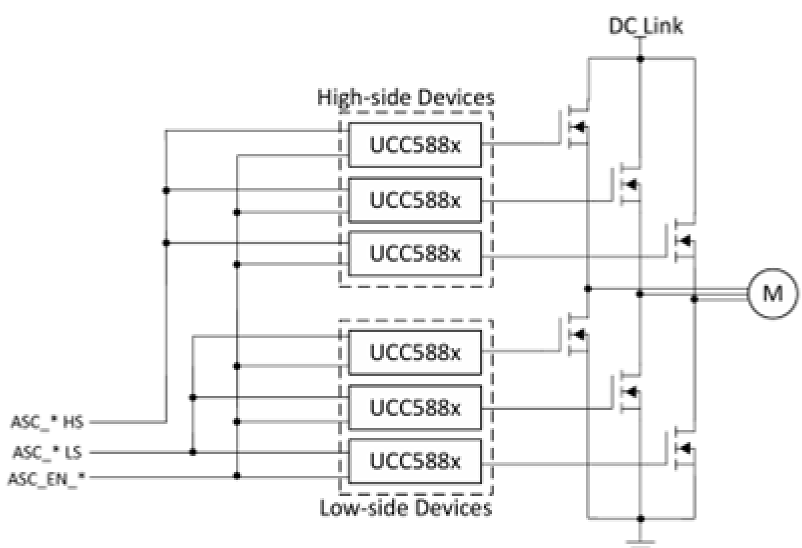

Figure 3-9. ASC Implementation with UCC5881-Q1

Table 3-1. Truth Table of the UCC5881-Q1 Safe State Pins

INP	INN	ASC_EN_SEC	ASC_SEC	ASC_EN_PRI	ASC_PRI	Output State
0	0	0	x	0	x	Low
1	0	0	x	0	x	High
x	1	0	x	0	x	Low
x	x	1	0	x	x	Low
x	x	1	1	x	x	High
x	x	0	x	1	0	Low
x	x	0	x	1	1	High

The shoot-through protection (STP) function of the UCC5881-Q1 provides an additional layer of protection against shoot-through conditions that might arise from incorrect PWM commands from the MCU. If an over-current or power module short-circuit event occurs despite this protection, the UCC5881-Q1 will report it through the DESAT signal, which is also monitored by BIST.

In traction inverter safety design applications, the external ASC signal (from both the MCU and external logic circuits) is routed to either the UCC5881-Q1 primary side ASC pin or the secondary side ASC pin. This configuration ensures that the gate driver output operates independently from the PWM input when necessary, generating the appropriate safe state output to the power module. Both the PWM signal and ASC signal are protected with isolation lane detection safety mechanisms to address potential isolation lane failures. Based on these FuSa features, the system can meet the TSR related to FSR 1.6 using TI's safety-oriented devices.

3.3 Dependent Failure Consideration

Dependent Failure Analysis (DFA) is a systematic safety analysis methodology designed to identify and evaluate common cause failures or cascading failures that could lead to simultaneous failures of multiple components within a system. The core principle of DFA involves analyzing interdependence within the system to identify initiators that can cause multiple safety functions fail simultaneously, such as environmental factors, design flaws, manufacturing process issues, external interference, etc.

The main process of DFA follows four key steps:

- **Step1:** list the architecture elements and identify dependent pairs
- **Step2:** identify Dependent Failure Initiators (DFIs) which can lead dependent failure that violate a safety goal
- **Step3:** identify necessary safety measures to control or mitigate dependent failures. Define additional measures if independence is insufficient
- **Step4:** evaluate the effectiveness of measures to control or to avoid dependent failures

Due to space limitations, Table 3-2 shows only a portion of the DFA analysis for the traction inverter system, focusing on the position sensor subsystem.

Table 3-2. Example of Traction Inverter DFA Table

Element	Dependent Element	DFI Type	DFI Root Cause	DFI Effect	Fault Prevention Measures	Fault Control Measures
#1 LDC5073-Q1	#2 LDC5073-Q1	Failure of shared resources	Shared power	The share 3.3V power can lead #1 LDC5073-Q1 and #2 LDC5073-Q1 loss of function at the same time	PMIC TPS65386x-Q1 3.3V LDO embedded with output voltage monitoring for UV, OV, SC events.	• PMIC IC level verification & testing • Integration testing by customers
			Shared power supply elements	The failure of PMIC can lead #1 LDC5073-Q1 and #2 LDC5073-Q1 loss of function at the same time	TPS65386-Q1 equipped with multiple safety mechanisms like BIST, UVLO, VMON, CRC, etc. can cover the failures of PMIC	• PMIC IC level verification & testing • Integration testing by customers
		Single physical root cause	Cross talk	The location of position sensor can affect by cross talk and lead #1 LDC5073-Q1 and #2 LDC5073-Q1 loss of function at the same time	NA	Simulation and validation testing to verify performance.
			Local heating	The location of position sensor can affect by heating and lead #1 LDC5073-Q1 and #2 LDC5073-Q1 loss of function at the same time	NA	• Ambient temperatures are defined in spec. The device is designed/ simulated and tested to these conditions • AEC-Q100 High Temperature Operating Life qualification is performed on this device.
		Environmental faults	EMI	For some application scenarios, both #1 LDC5073-Q1 and #2 LDC5073-Q1 can be affected and loss of function at the same time	NA	Integration testing by customers
			ESD	The position sensor location can be affected by ESD and lead #1 LDC5073-Q1 and #2 LDC5073-Q1 loss of function at the same time	ESD protection design for specific boundaries.	ESD limits are defined in spec and ESD tests are performed on all pins according to the ESD standard

In our traction inverter system FuSa design, DFA analysis methodology has been comprehensively implemented. As a result, diversified redundancy, physical isolation, independent monitoring, and other protective measures have been implemented in our design to make sure the system can maintain necessary safety functions when facing common cause failures. These measures significantly enhance the FuSa level and reliability of the traction inverter system.

The systematic approach to dependent failure analysis makes sure that potential common cause failures are identified early in the design process and appropriate countermeasures are implemented, preventing simultaneous failures that can compromise the overall safety of the traction inverter system.

3.4 Detailed FuSa Design Structure for Traction Inverter

Using the methodology discussed in Section 2, this section provides an overview of the various TI FuSa components used in traction inverter safety design. System-level FuSa analysis is highly dependent on specific usage scenarios and architecture. For the following sections, the basic functions of the selected components are described, followed by an introduction to the FuSa mechanisms of each component. Figure 3-10 presents the component-level architecture of the traction inverter.

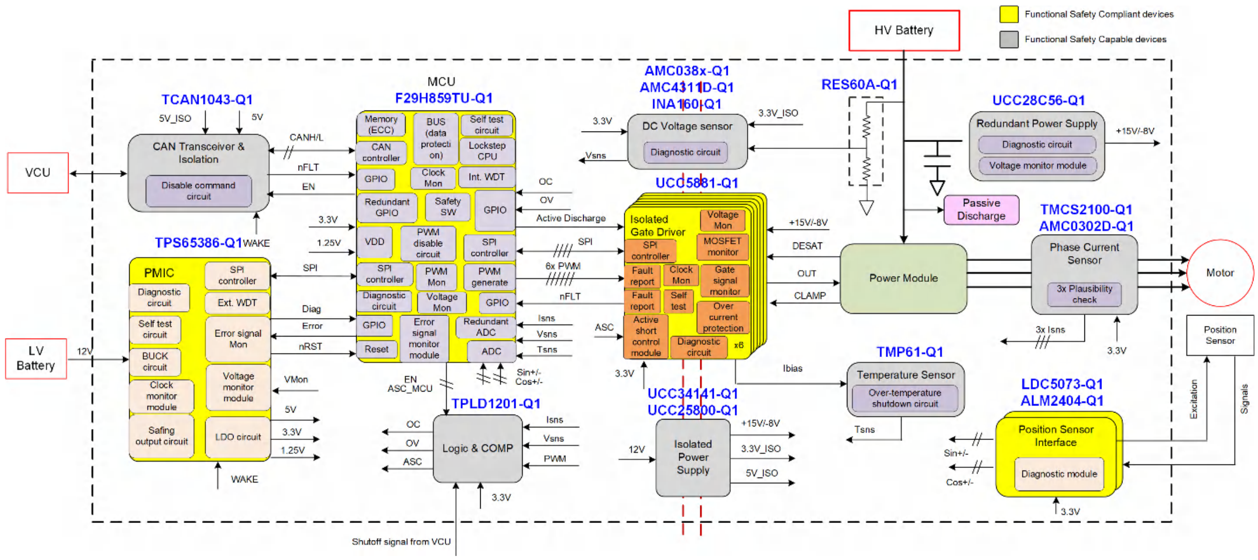

Figure 3-10. Component Level Architecture of Traction Inverter

In a traction inverter, aside from power switches and passive components, the main functional blocks include microcontroller, gate driver, isolated bias supply, power management IC, position sensor, current sensor, voltage sensor, temperature sensor, communication interface, and logic circuits:

- **Microcontroller (MCU)**. Executes the motor control FOC algorithm, monitors sensor data, protects the system, and communicates with the VCU. In safety-critical designs, the lockstep cores are essential, along with dedicated MCU internal watchdog and self-diagnostic capabilities.
- **Gate driver**. Provides the required voltage and high-current drive signals of the power module. Isolated gate drivers also provide reinforced galvanic isolation between the low-voltage side and the high-voltage side. To satisfy the FuSa requirements of the system, isolated gate drivers incorporate numerous safety mechanisms such as BIST, DESAT, clamp circuit, ASC, gate monitor, PWM lane detection, etc.
- **Isolated power supply**. Isolated bias supply generates the gate driver voltage and supplies the high-voltage side sensing circuits while maintaining galvanic isolation. To drive SiC and IGBT, both positive and negative isolated bias supplies are required. Separating the bias supply for different gate drivers will support higher FuSa level design.
- **Power management IC (PMIC)**. Manages and controls multiple power functions, including protected voltage conversion, power sequencing, voltage monitoring and diagnostics, protection, watchdog, and communication. It 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 the MCU. When detecting unrecoverable faults in the MCU, the PMIC can trigger an MCU reset and cut off related control signals to make sure the system enters a safe state.
- **Position sensor**. Measures the motor rotor position and speed for FOC control. The typical position sensing solution in traction inverter will be resolver and inductive sensor. Traction inverter will generate the excitation signal into resolver/inductive sensor and receive the sensor feedback signal for decoding. Since the signal wires are connected to the sensor outside the main board, protection on short-to-battery/GND is required.
- **Current sensor**. Measures three-phase AC motor currents for FOC control and implements overcurrent protection. Typical implementations include Hall-effect based current sensors with overcurrent pins or shunt-based current amplifiers with comparators.
- **Voltage sensor**. Measures the HV battery DC input voltage for FOC and modulation, and also to detect over-voltage or undervoltage events for protection.
- **Temperature sensor.** Monitors the power module junction temperature and the ambient temperature of the board, reporting to the MCU. Redundant temperature sensors can be implemented to achieve FuSa requirement. It can be measured by simply connecting the NTC or PTC to the MCU ADC or gate driver ADC with a bias current.

- **Communication interface**. Receives torque commands and other instructions from the VCU, and reports status and fault signals back to VCU. In traction inverter, 2x CAN transceiver channels are typically implemented. Safety-critical messages are transmitted with Cyclic Redundancy Check (CRC) and message-counter checks to verify data integrity.
- **Logic**. Logic circuits are used for FuSa design and providing protection, such as PWM feasibility check, safe state entering circuit, redundant motor speed detection, and so on.

3.5 Achieving FuSa Requirements with TI Safety Devices

As described in Section 2.4, any failure events in traction inverter system must be detected or mitigated, and the system must enter the appropriate safe state when failure occurs. This section demonstrates how TI devices can be effectively implemented in traction inverter for FuSa purposes, with particular emphasis on designs that help the system enter ASC or freewheeling states when required.

3.5.1 MCU

The F29 series devices are powerful MCUs that feature C29x CPU designed for real-time control in automotive and industrial applications. C29x CPU is a Very Long Instruction Word (VLIW) architecture with a fully protected pipeline and supports multiple instruction sizes. The device consists of up to three 200MHz C29x cores supporting 32-bit and 64-bit floating and fixed-point signal processing running from on-chip flash or RAM. The C29x CPU is enhanced by trigonometric math instructions, speeding up common algorithms key to real-time control systems.

As mentioned in Section 3.2.2, several key features are particularly valuable for traction inverter FuSa design, including the lockstep capability, Error-Correcting Code (ECC) protection, redundant ADC with cross-check functionality, and GPIO/PWM readback features. Beyond these previously mentioned safety mechanisms, the F29 MCU offers additional functions, peripherals, and numerous safety mechanisms suitable for FuSa system design:

- **Logic Power-On Self-Test (LPOST).** Verifies the integrity of critical logic circuits during system startup
- **Memory Power-On Self-Test (MPOST).** Ensures memory contents are valid at system initialization
- **Error and Signaling Module (ESM).** Centralizes error detection and handling for the entire device
- **Dual-clock Comparator (DCC).** Monitors clock frequencies to detect clock failures
- **Context-sensitive Memory and Peripheral Protection with Safety and Security Unit (SSU)**. Supports safe Live Firmware Update (LFU) and FOTA for application firmware updates with A/B swap and rollback control.
- **Safety Interconnect (SIC).** Provides protected communication paths between safety-critical components
- **Hardware Security Module (HSM)** with ECC-protected for cybersecurity.
- **Configurable Logic Block (CLB).** Offers programmable logic functionality for custom safety mechanisms
- **Embedded Pattern Generator (EPG)**. Generates test patterns for diagnostic purposes
- **Windowed watchdog timer module**
- **Missing clock detection circuitry.** Identifies clock failures that could compromise system timing
- **Real-Time Direct Memory Access (RTDMA) controllers with Memory Protection Unit (MPU).**

These comprehensive safety features make the F29 series MCUs particularly preferred for implementing the complex FuSa requirements of modern traction inverter systems, enabling them to detect failures and transition to appropriate safe states when necessary.

3.5.2 Gate Driver

In traction inverter systems, the gate driver is assigned a high FuSa level to prevent unintended torque and over-current/shoot-through conditions in the power module. The UCC5881-Q1 is an isolated, highly configurable gate driver with adjustable drive strength specifically designed to drive high-power SiC MOSFETs and IGBTs. The ASC feature for entering safe state has been mentioned in Section 3.2.4.

Beyond ASC functionality, the UCC5881-Q1 incorporates numerous protection features including gate driver output state monitoring, soft turn-off during failure conditions, power module threshold voltage detection, overvoltage/undervoltage lockout (OV/UVLO), and shoot-through protection. The UCC5881-Q1 also supports active Miller clamp functionality to prevent unintended turn-on of the power module during high dv/dt events. Additionally, the device provides two external ADC channels to support multiple DC link voltage and power module temperature sensing paths, which is beneficial for implementing measurement redundancy while optimizing system cost.

Figure 3-11 illustrates the block diagram of the UCC5881-Q1 in a typical traction inverter application. The key protection features and safety mechanisms are listed below.

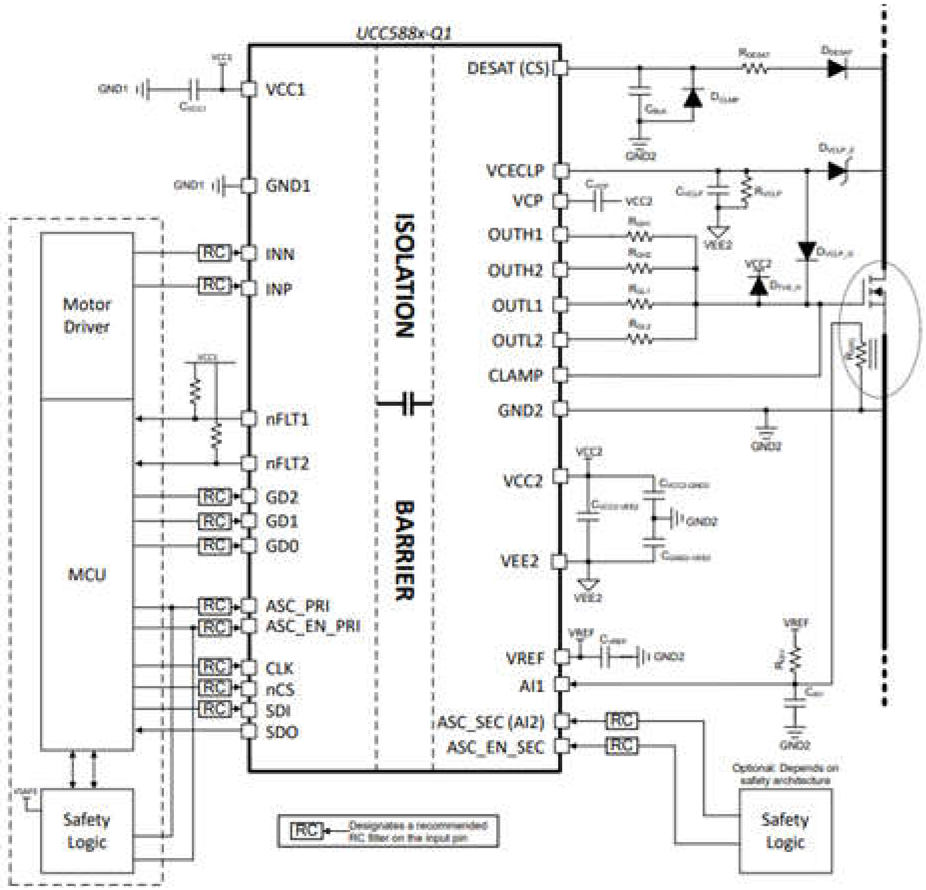

Figure 3-11. Block diagram of UCC5881-Q1 used in a typical traction inverter

3.5.2.1 Gate Monitor Circuit and Over Current Protection

To properly enter ASC safe state, a traction inverter must be able to reliably turn on either all three high-side power switches or all three low-side power switches, while keeping the opposite legs off. The UCC5881-Q1 integrates a gate monitor circuit that detects whether the gate driver output voltage level matches the input PWM signal from the MCU. This circuit provides rapid detection of gate driver output failures or power switch short circuit/open circuit conditions. By monitoring the health status of each gate driver and power switch, the MCU can make informed decisions about which power legs should be turned on during a transition to a safe state. The gate monitor circuit block diagram is illustrated in Figure 3-12.

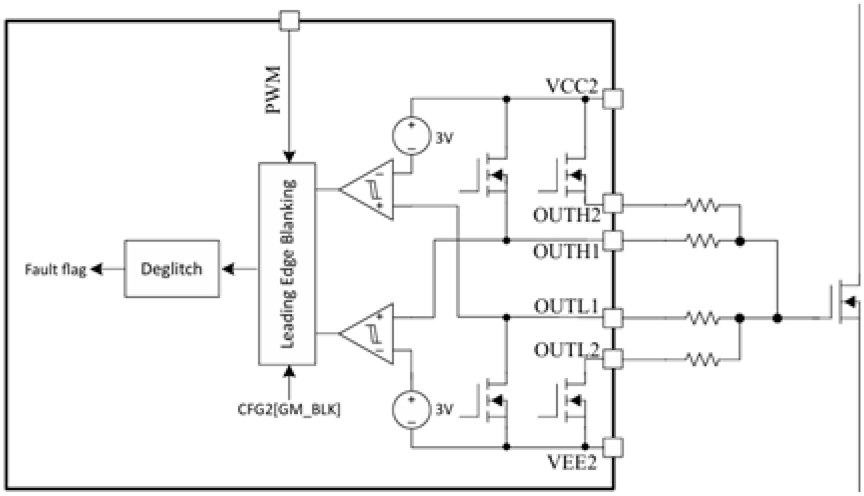

Figure 3-12. Gate Monitor Circuit in UCC5881-Q1

Over-current protection is a critical safety function in traction inverters, as unmitigated over-current conditions can cause severe damage if not addressed within 2-3 microseconds (typical for SiC devices). The UCC5881-Q1 integrates a DESAT circuit for fast over-current protection. The DESAT input monitors the collector-emitter saturation voltage (VCEsat) for IGBTs or the drain-source on-state voltage (VDSon) for MOSFETs through an external resistor and diode network, as shown in Figure 3-13.

While the power FET is ON, an internal current source, I_{CHG}, forward biases the DESAT diode and sinks into the collector/drain of the external power switch. Once the voltage on the DESAT input charges up to the threshold, a DESAT fault is detected. The UCC5881-Q1 reports the fault and soft turn off the power module to minimize voltage spikes during shutdown. The MCU then forces the system enter the appropriate safe state based on the DESAT and gate monitor information from 6x gate drivers.

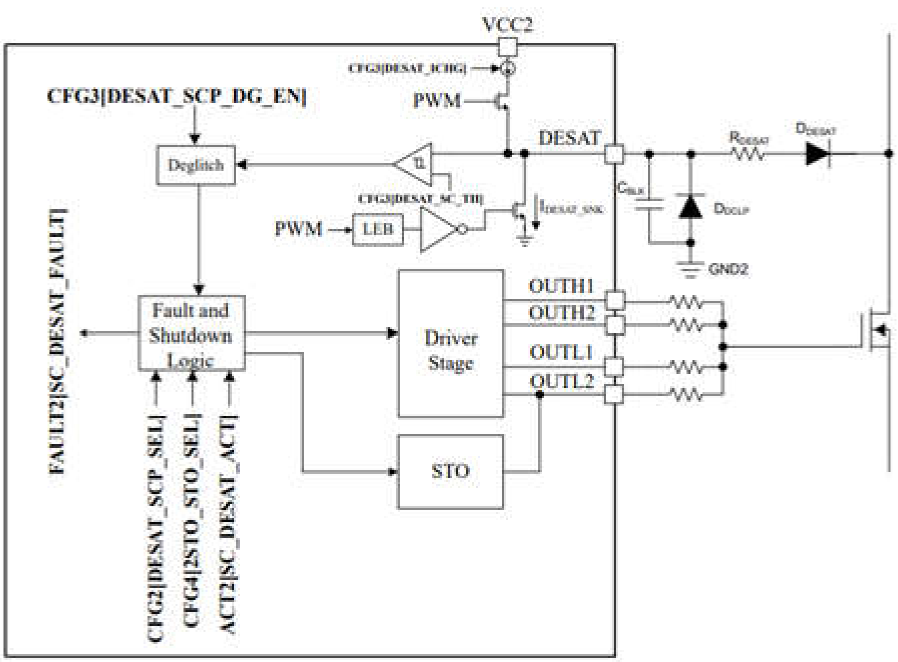

Figure 3-13. DESAT Circuit Block Diagram of UCC5881-Q1

This combination of gate monitoring and fast over-current protection verifies that the traction inverter can quickly detect abnormal operating conditions and transition to a safe state before damage occurs to the power components or unintended torque is generated at the motor.

3.5.2.2 Other Safety Mechanisms in UCC5881-Q1

Beyond the gate monitoring and over-current protection features, the UCC5881-Q1 incorporates numerous additional safety mechanisms designed to enhance traction inverter protection and fault reporting capabilities:

- Vgs(th) power module healthy status checking at start-up state.
- Undervoltage and overvoltage monitoring on VCC1, VCC2, and VEE2 power supplies
- Undervoltage and overvoltage monitoring on internal power supplies used for its supporting circuits
- Clock monitor on logic clock
- Configuration Data Cyclic Redundancy Check (CRC)
- SPI CRC
- Internal NVM (non-volatile memory) CRC
- Built-in self-test (BIST) diagnostics for VCC1, VCC2, VEE2, and internal regulator UV/OV monitoring functions, and main clocks
- Power transistor high voltage clamping circuit detection and function diagnostics
- Active Miller clamp diagnostic.

3.5.3 Isolated bias supply

In traction inverter systems, the isolated power supply serves the critical function of providing the required power to gate drivers while maintaining galvanic isolation between the low-voltage control circuitry and high-voltage power stage. Due to its role in ensuring proper gate driver operation, the isolated power supply is assigned a high FuSa level to prevent unintended torque generation. Based on different architectural approaches, there are three primary types of isolated power supply structures implemented in traction inverter systems: Centralized power supply; Fully distributed power supply; and Semi-distributed power supply.

3.5.3.1 Centralized LV Isolated Power Supply Architecture

Figure 3-14 illustrates the centralized power supply architecture in traction inverter. All high-side and low-side gate drivers are supplied using a single isolated bias power supply device. This approach offers significant cost advantages through component reduction. However, the centralized architecture introduces critical safety concerns. Most notably, a failure in this single power supply device constitutes a single point of failure—if it malfunctions, all gate drivers simultaneously lose power, potentially preventing the traction inverter from entering the required safe state during fault conditions. Another significant challenge with the centralized approach is the complexity of designing a transformer with six secondary windings (Primary : Secondary ratio of 1:6) to supply all gate drivers. This design requires specialized transformer construction and results in complex PCB layout with long PCB traces to reach all gate drivers.

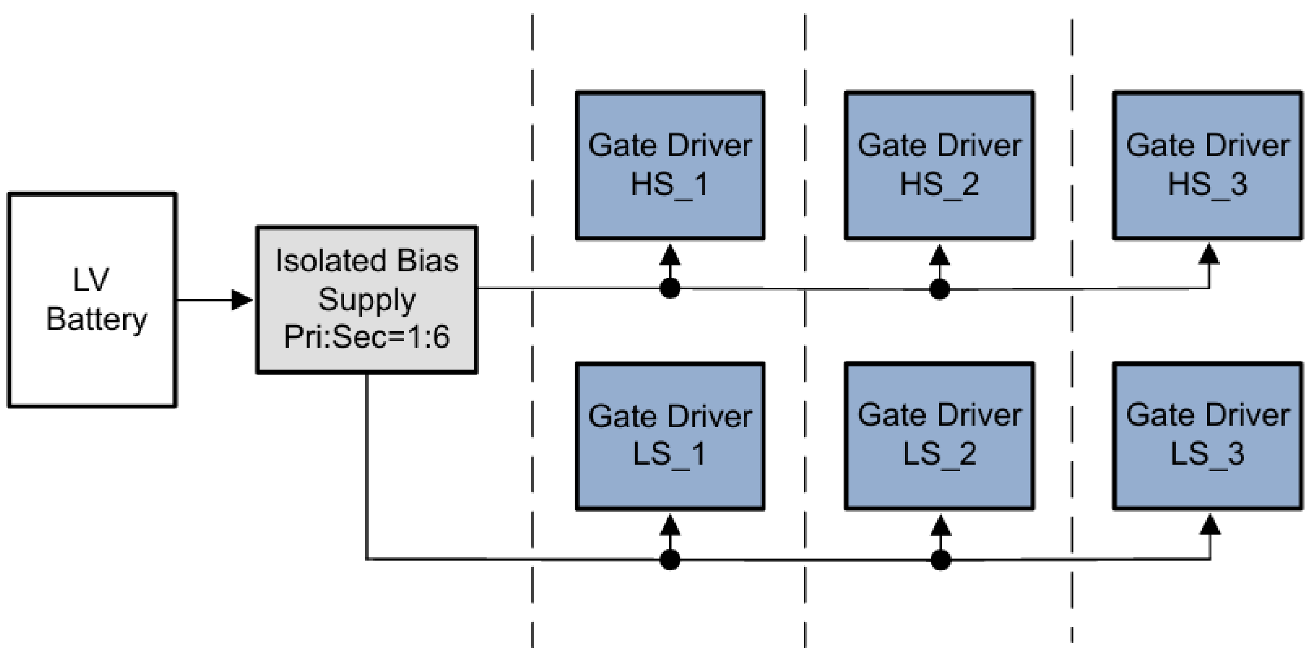

Figure 3-14. Centralized Isolated Power Supply Architecture

3.5.3.2 Fully Distributed LV Isolated Power Supply Architecture

Figure 3-15 illustrates the fully distributed power supply architecture in traction inverter. In this configuration, each gate driver is powered by its own individual isolated bias power supply device. This approach requires six separate isolated bias supply devices to power the six isolated gate drivers in a three-phase inverter. The primary advantage of this fully redundant solution is its enhanced fault tolerance: the system can still enter the appropriate safe state even if any individual bias power supply circuit fails. This eliminates the single point of failure concern present in centralized architectures, making the fully distributed approach particularly suitable for high ASIL applications where fault tolerance is critical.

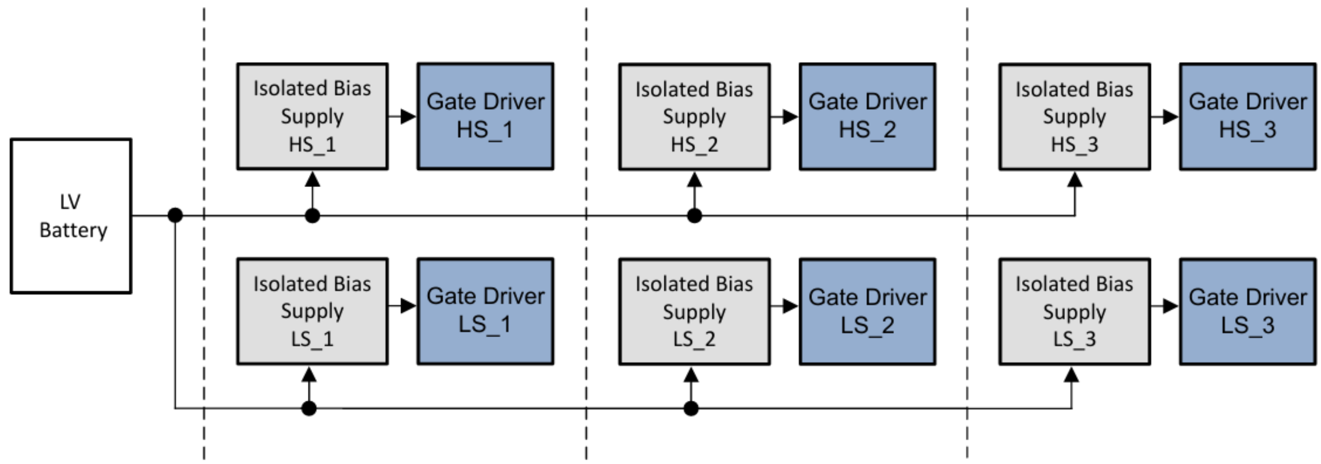

Figure 3-15. Fully Distributed Isolated Power Supply Architecture

3.5.3.3 Semi-Distributed LV Isolated Power Supply Architecture

Figure 3-16 illustrates the fully distributed power supply architecture in traction inverter, which represents a strategic compromise between the centralized and fully distributed approaches. In this configuration, multiple gate drivers share power from a single isolated bias power supply device, but the system employs more than one power supply unit overall. This hybrid approach enables cost savings compared to the fully distributed architecture by reducing the total number of isolated power supply devices required. It also avoids the total shutdown vulnerability inherent in the centralized approach. If one power supply fails, only a subset of gate drivers loses power, while others remain operational. This partial redundancy ensures the inverter maintains the capability of entering a safe state even during power supply failures.

The flexibility of this architecture allows system designers to tailor the power distribution strategy to their specific application requirements and safety goals, making it a versatile solution for modern traction inverter designs.

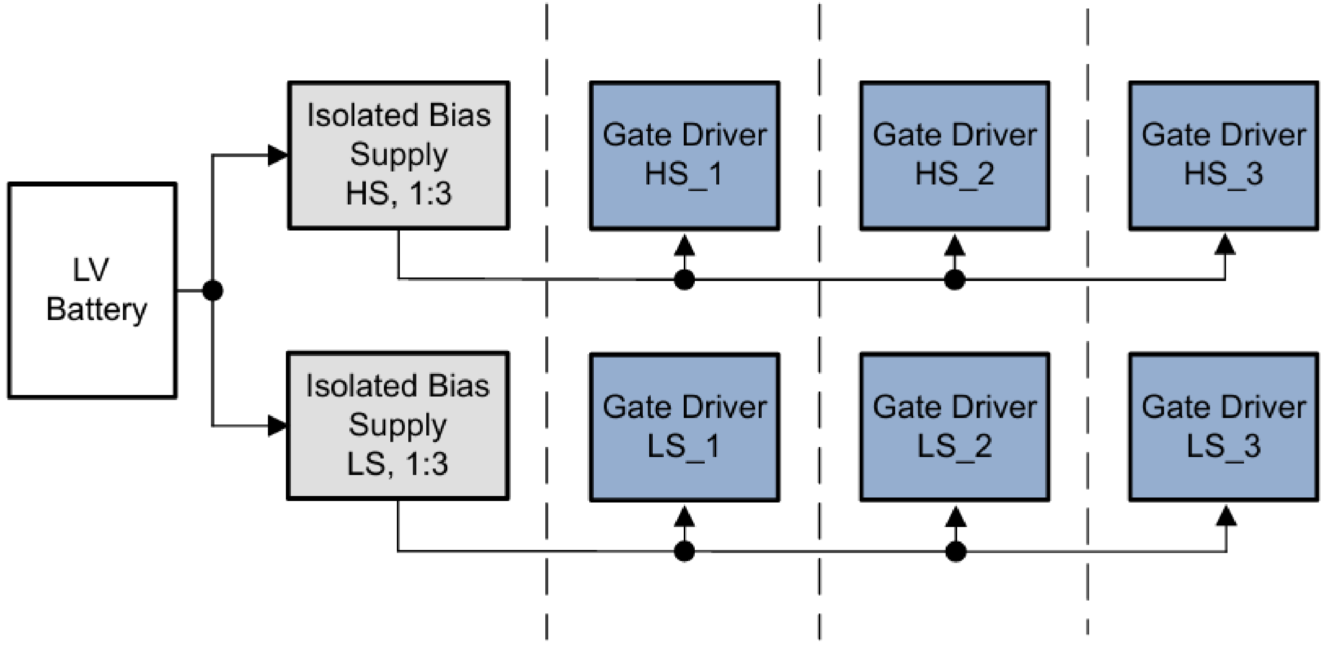

Figure 3-16. Semi-distributed Isolated Power Supply Architecture

3.5.3.4 HV Isolated Bias Supply

Beyond the previously discussed LV isolated bias supply architectures, HV isolated bias supply can also be implemented as a redundant power source for gate drivers in higher FuSa level designs. Figure 3-17 illustrates an example of this hybrid structure, where low-side gate drivers receive power from both the LV system and the HV battery, creating a redundant power path. This strategic configuration verifies that at least one set of drivers (in this case, the low-side drivers) maintains power availability even if the LV power system fails completely, which enables the system to achieve at least one of the possible safe states.

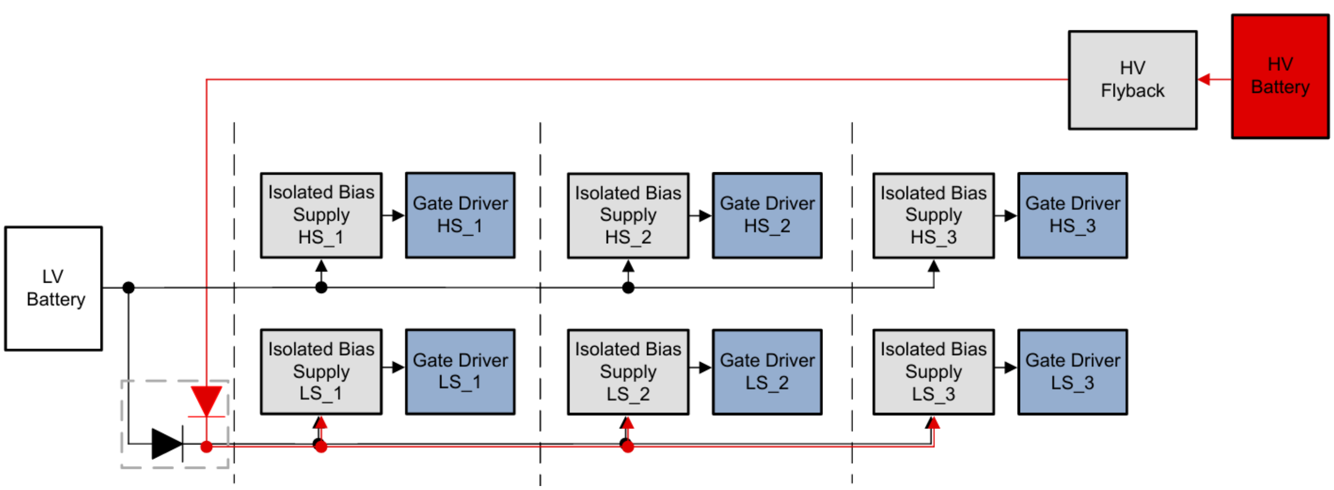

Figure 3-17. Implementing both HV and LV Isolated Bias Supply for FuSa design

3.5.3.5 TI's Design for Isolated Bias Supply in Traction Inverter

TI provides comprehensive solutions for all the isolated bias supply architectures previously discussed, offering designers flexibility to implement the most appropriate approach for their specific application requirements.

TI offers several variants of integrated DC/DC modules (UCC34xxx-Q1) for LV isolated power supply applications, as shown in Figure 3-18. These advanced modules feature an integrated transformer with H-bridge topology operating at frequencies exceeding 10MHz. This high level of integration eliminates the need for external transformers, resulting in significant reductions in system size and height. A key advantage of these integrated modules is the simplified output voltage configuration through straightforward feedback design. This feature substantially reduces the engineering effort required for isolated power supply design while delivering benefits in terms of compact size, low profile, and cost-effectiveness. Figure 3-19 provides a visual comparison between TI's integrated DC/DC modules and traditional bias supply approaches, highlighting the clear advantages in form factor and integration.

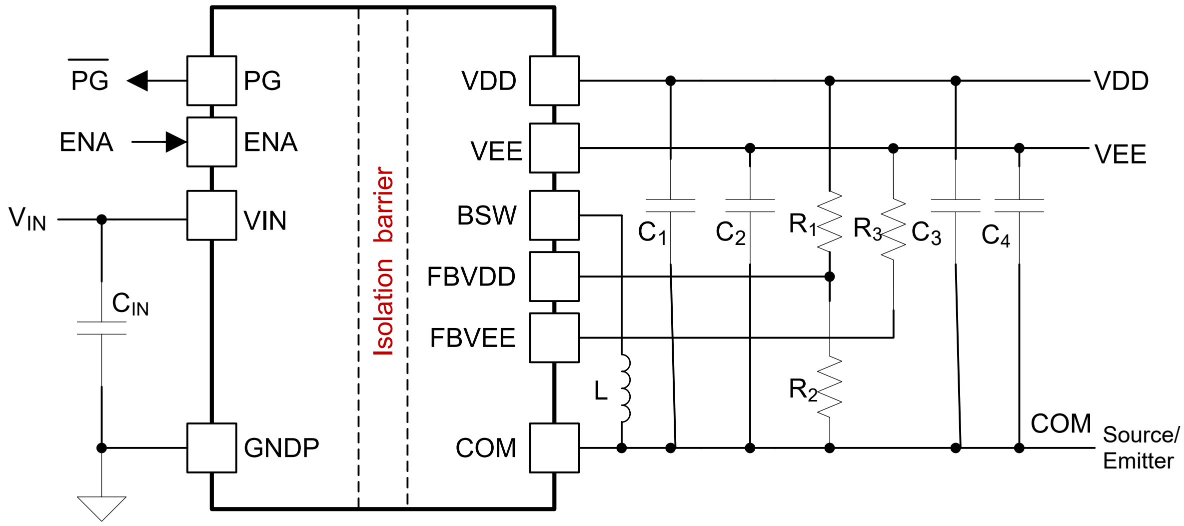

Figure 3-18. Application Block Diagram of UCC3414x-Q1 with Integrated Transformer and FETs

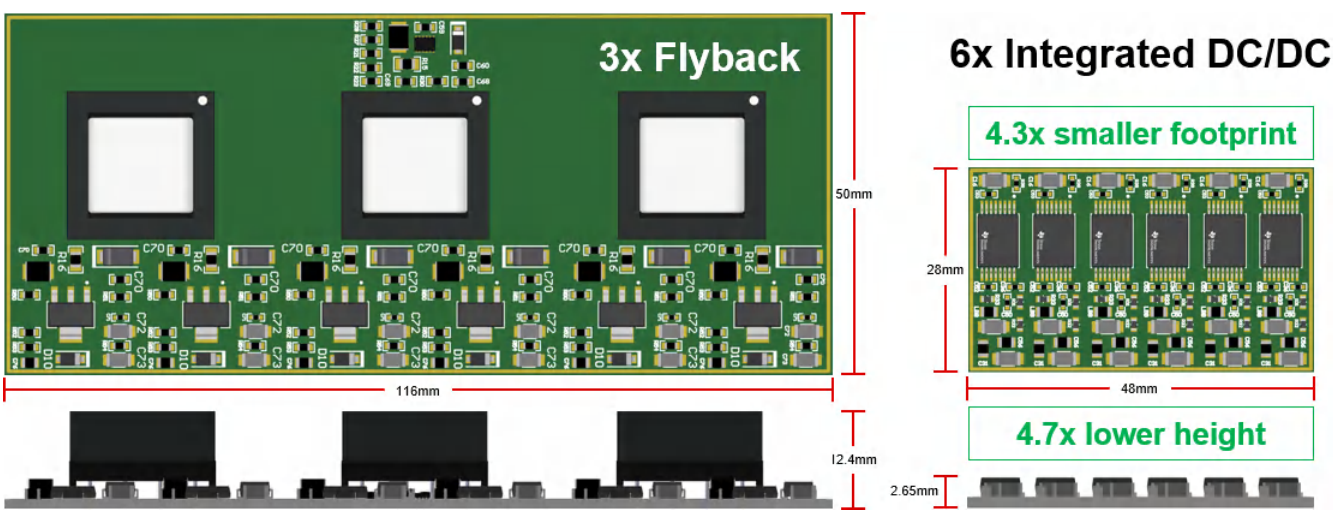

Figure 3-19. Size Comparison between Integrated DC/DC Module UCC3414x-Q1 and Flyback

Beyond these integrated modules, TI also offers solutions for alternative isolated power supply architectures and pre-regulator converters, including flyback (LM515x-Q1, LM(2)518x-Q1), LLC resonant converters (UCC25800-Q1, UCC259xx-Q1), push-pull (SN650x-Q1), HV flyback designs (UCC28C5x-Q1, UCC287xx-Q1, UCG288xx), and buck-boost converters (TPS55287x-Q1, UCC55289x-Q1). These options provide designers with additional implementation choices based on specific power requirements, isolation needs, and system constraints. For more comprehensive information about isolated bias power supply architectures and implementation options for HEV and EV traction inverters, please refer to TI's white paper: Isolated Bias Power Supply Architecture for HEV and EV Traction Inverters.

3.5.4 Power Management IC

Power management ICs serve a critical function in traction inverter systems by providing power to virtually all low-voltage components, including the MCU, sensors, CAN transceivers, gate drivers, logic circuits, and more. Without reliable and sufficient power supply to these elements, the traction inverter cannot execute the

FOC algorithms necessary to control the motor correctly. The TPS65386x-Q1 device, illustrated in Figure 3-20, represents TI's advanced solution for automotive power management. This highly integrated device incorporates a buck-boost converter with internal FETs that converts the input battery voltage to a configurable pre-regulated output voltage. This pre-regulated output then supplies power to other integrated linear regulators within the device and can also support external regulators if additional power rails are required.

The TPS65386x-Q1 also features a low-power mode capability, making it particularly well-suited for MCU power applications where power efficiency across different operating states is important. This device is classified as a TI FuSa-Compliant product, developed in accordance with ISO 26262:2018 standards and fully validated for automotive applications. Comprehensive documentation is available to support ISO 26262:2018 system design up to ASIL-D, with the device incorporating numerous safety mechanisms.

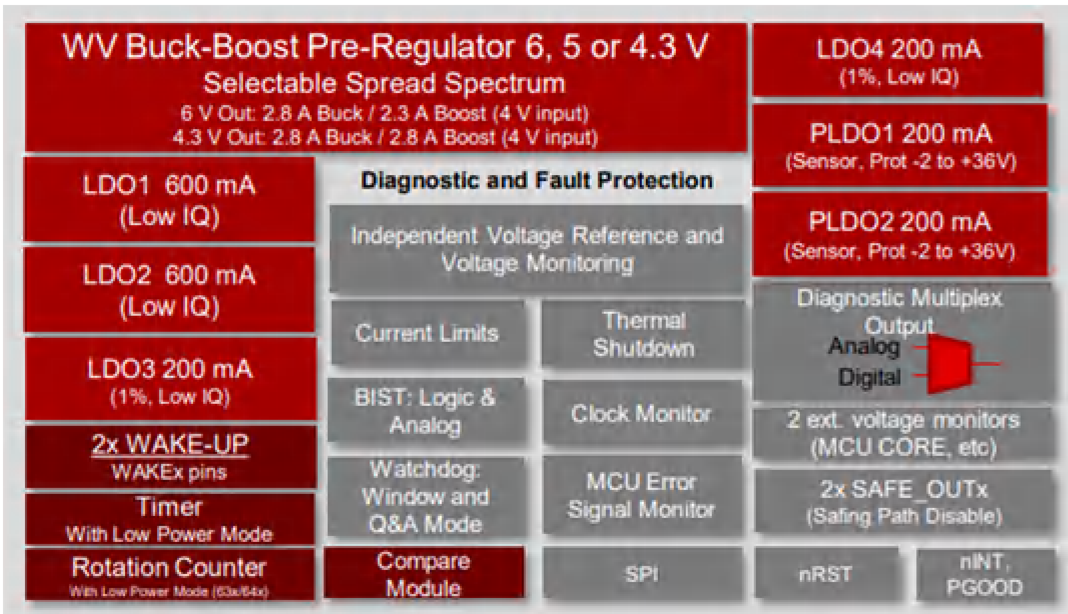

Figure 3-20. Resources of TPS65386x-Q1

3.5.4.1 Multiple Paths Power Rail with Protection and Independent Thermal Shut-Down

The TPS65386x-Q1 implements a sophisticated power architecture with multiple protected power paths and independent thermal management to ensure reliable operation even during partial failures.

The buck-boost regulator forms the core of this architecture, functioning as a synchronous DC-DC converter with integrated FETs. This highly efficient design minimizes power dissipation within the device, reducing thermal stress. The buck-boost converter transforms the input supply voltage to a lower voltage domain (VOUTBB), which serves as the supply for the LDO (Low-Dropout) and PLDO (Protected Low-Dropout) regulators. The converter is designed to supply all internal regulators at their maximum output currents while providing additional current capacity for external regulators if needed. A critical safety feature is the integrated junction-temperature monitoring system that prevents excessive power dissipation in the power MOSFETs. the buck-boost incorporates digital spread spectrum technology to reduce EMI across a wide frequency range, enhancing system electromagnetic compatibility.

The LDOx linear regulators offer flexible output voltage options ranging from 1.0V to 1.8V in 50mV increments, as well as fixed 2.5V, 3.0V, 3.3V, or 5V options. An unused LDOx regulator can be repurposed as a voltage monitor, adding monitoring capability to the system. Each LDOx includes its own independent junction-temperature monitor, ensuring that if an overtemperature event occurs in any single LDOx regulator, only that specific regulator is disabled while others continue to function. Depending on the device configuration, the resulting undervoltage event may trigger additional state transitions as needed. This selective shutdown capability means that even if the MCU core power or digital power is lost, external devices can still receive power. The TPLD1201-Q1 circuit shown in Figure 3-8 can leverage this capability to help the system enter a safe state even when the MCU is failed.

The PLDOx regulators offer even greater flexibility, supporting three operating modes: tracking mode, fixed output voltage LDO mode, or voltage monitor mode. These regulators incorporate robust protection against short circuits to both supply (+36V) and chassis ground (-2V), making them suitable for sensor applications where the supply may extend outside the ECU, as well as for standard internal applications such as position sensor power. The PLDO can also operate in tracking mode, referenced to the TRACK input pin. For enhanced reliability, the device incorporates two independent bandgap voltage reference sources for cross-checking and redundancy, addressing potential bandgap open circuit and drift failure modes.

This comprehensive power architecture with multiple independent power paths and protection mechanisms ensures that the traction inverter can maintain appropriate power to critical safety components even during partial power system failures.

3.5.4.2 Power Rail Voltage Monitoring

The TPS65386x-Q1 implements comprehensive voltage monitoring capabilities that are critical for FuSa in traction inverter applications. It continuously monitors multiple voltage rails, including the VBAT supply voltage, all internal regulator output voltages, external rails via dedicated EXT_VMONx pins, and internal bias voltages. When the VMON module detects an error event on any monitored voltage rail, it immediately sets the corresponding VMON error flag bit, alerting the system to the potential issue or turning off the failed power rail. To ensure the accuracy of the reference for the VMON, The main bandgap voltage reference is continuously cross-checked by a second independent bandgap reference. Additionally, an analog built-in self-test (ABIST) periodically runs diagnostic checks on the VMON module to verify its proper operation. Any failure occurs on each power rail will be reported, and the system can enter safe state based on the strategy.

The TPS65386x-Q1 also provides two channels of external voltage monitors that can be used to monitor critical external power rails, such as the MCU core input voltage or pre-regulator voltage. This extended monitoring capability enables higher system-level FuSa coverage. Figure 3-21 illustrates an example implementation where these external monitors are used to monitor an external DC-DC converter that powers the MCU core and other LDOs. It's worth noting that even quality-managed (QM) devices can be used as the DC-DC converter in this arrangement, as long as they are properly monitored by the TPS65386x-Q1. This monitoring relationship allows the overall power system to meet ASIL-D safety requirements despite using components with lower individual safety ratings, demonstrating the principle of safety composition through appropriate monitoring and fault detection.

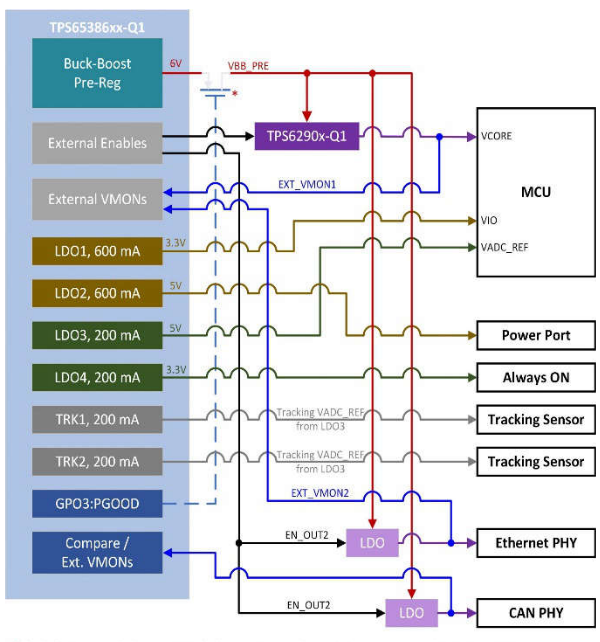

Figure 3-21. Example for TPS65386x-Q1 monitoring external power rails

3.5.4.3 MCU Fault Monitor and other Protection Mechanisms

The TPS65386x-Q1 monitors the module safety MCU. In case of the safety MCU hardware and/or software execution failure modes, PMIC will generate different post reactions depending on the severity rating, including interrupting to MCU, turn off external power stages and/or module communication interface(s) if the fault continues to exceed the threshold, re-boot the safety MCU. During these MCU non-operational periods, the TPLD1201-Q1 logic device can take over critical safety functions, helping the system enter an appropriate safe state even without MCU control.

Beyond these key safety mechanisms, the TPS65386x-Q1 incorporates numerous additional safety mechanisms that enhance the FuSa design:

- A watchdog with trigger and question-answer (Q&A) modes.
- MCU error-signal monitor to monitor (MCU ESM) a level or PWM signal provided to the ESM_IN input on this device from the MCU integrated error diagnostics function which outputs MCU faults on an output pin of the MCU.
- Clock monitoring of the internal oscillators (system clock and low-power clock)
- CRC on non-volatile memory (NVM).
- CRC on configuration registers.
- CRC on SPI communication.
- A diagnostic output pin which allows the MCU to access the internal analog and digital signals of the device.
- A reset output for the MCU and system (NRST)
- A power good output (PGOOD).
- An interrupt output (NINT).
- Safing outputs to stop power-stages or other system functions on detected faults. – Dedicated SAFE_OUT1 output– Multiplexed and configurable SAFE_OUT2, multiplexed on.
- Built-in self-test (BIST) that checks the device functionality at start-up and can be run under software command during run time.

- These extensive safety mechanisms ensure that the power management system can detect and respond to a wide range of potential failures, maintaining system safety even during complex fault scenarios. The combination of MCU monitoring, independent fault response capabilities, and comprehensive self-diagnostics makes the TPS65386x-Q1 a critical component in achieving high automotive safety integrity levels in traction inverter applications.

3.5.5 Position Sensor

Inductive sensor technology is gaining increasing popularity as the position sensing solution of choice for traction inverter motors, offering significant advantages in terms of cost, weight, and high-speed detection capabilities compared to traditional resolvers. The LDC5072/3-Q1 is an inductive resolver analog front-end for traction motor applications delivering these benefits while meeting stringent FuSa requirements. The device's features and safety mechanisms were previously detailed in Section 3.2.1.

Besides inductive sensor, TI also provide resolver excitation solution with 2nd order filter designed with power op-amp ALM2403/4-Q1. The block diagram of this implementation is illustrated in Figure 3-22. This innovative approach enables the conversion of SPWM signals generated by the MCU at fundamental frequencies of 10kHz to 20kHz into clean sine waves suitable for resolver excitation supporting adequate voltage and current. The detailed design information can be found in TI's application note: Applying the ALM2403-Q1 Single-Chip Resolver Solution to Reduce System Costs.

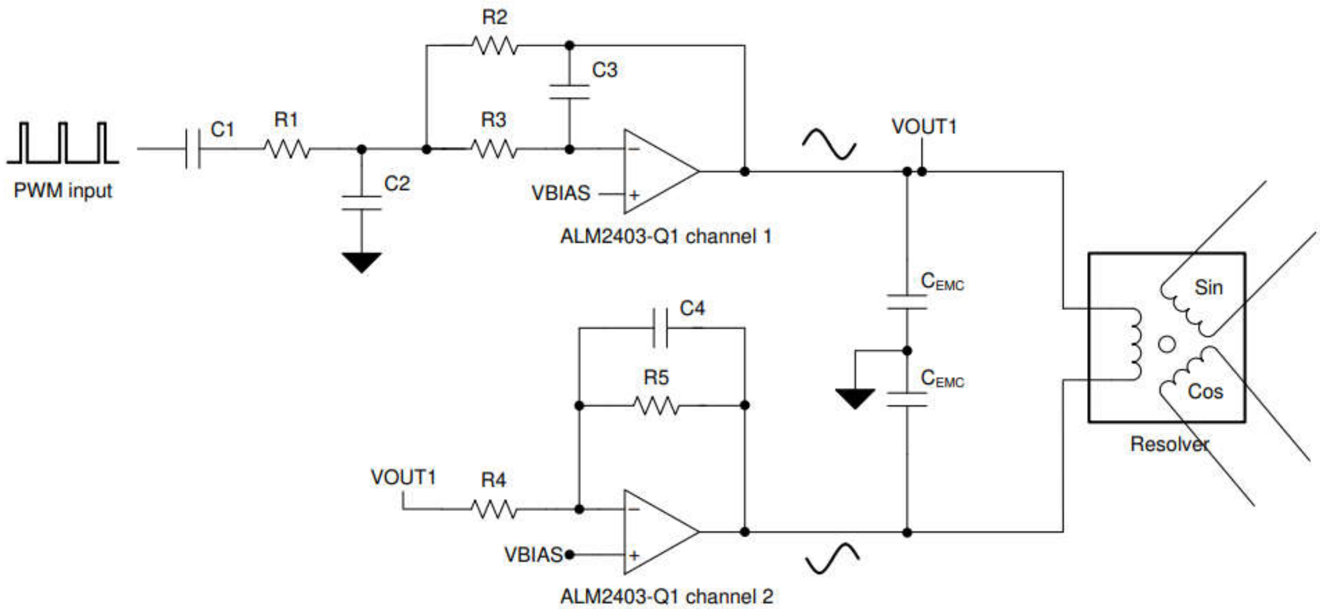

Figure 3-22. 2nd order filter design based on ALM2403-Q1 for resolver excitation

3.5.6 Current Sensor

In traction inverter systems, motor phase current sensing is critically important for both closed-loop motor speed and torque control, as well as for overcurrent protection. The TMCS2100-Q1 represents an approach as a contactless coreless Hall effect current sensor. Unlike traditional current sensors that require ferrite materials or inserting the devices into the busbar, the TMCS2100-Q1 can be simply mounted on the traction inverter control board positioned over the three-phase busbars to measure the magnetic field induced by the phase currents. This mounting flexibility eliminates the need for complex mechanical design considerations and reduces costs associated with fixtures and manufacturing processes.

With the internal algorithm and characterization process, the TMCS2100-Q1 can selectively detect the magnetic field induced by its target busbar while effectively ignoring effects caused by adjacent busbars. This capability allows the distance between adjacent busbars to be reduced to as little as 5mm, contributing to overall system size reduction. The operating block diagram illustrating this implementation is shown in Figure 3-23.

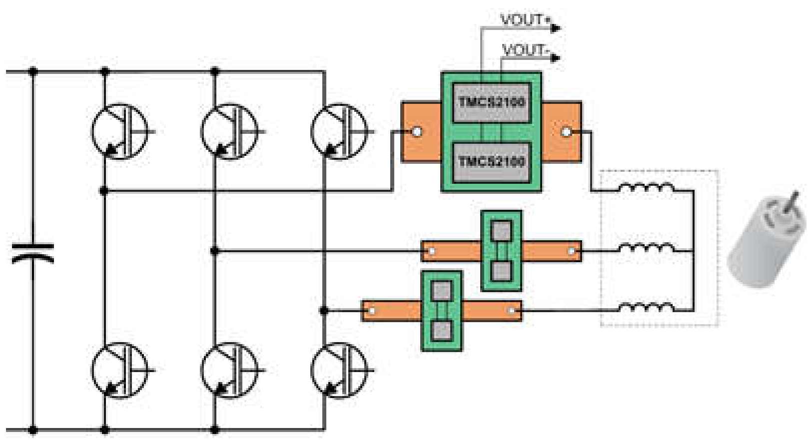

Figure 3-23. Block Diagram of TMCS2100-Q1 Measuring 3-phase AC Current

For FuSa design, several system-level safety mechanisms can be implemented to achieve FuSa targets:

- **Plausibility check**

In three-phase motor control systems, only two current sensing signals are theoretically required due to the principle that Ia+Ib+Ic = 0. Adding a third phase current sensor enables plausibility checking in software, serving as an effective safety mechanism. Through safety decomposition, each device can be assigned ASIL-B rating while achieving system-level ASIL-D compliance, or phase A and B are assigned QM rating and phase C is assigned ASIL-D rating.

- **Current sensing range detection**

If the TMCS2100-Q1 output exceeds its full-scale threshold, this can indicate either an actual overcurrent condition or a sensor output drift/error. Implementing current sensing range detection can address this failure mode and trigger appropriate safe state transitions. This will help to achieve around 60% coverage.

- **Torque calculation for checking current sensor outputs**

Two independent torque calculation methods can be implemented for cross-verification. The first method calculates torque using electrical power and motor speed, while the second uses three-phase currents and motor parameters for direct torque calculation. Comparing these two calculated values provides a means to validate current sensing accuracy.

- **Using another DC current sensing**

An additional DC current sensor measuring the DC input current of the inverter can be used to reconstruct the three-phase currents, providing another reference for validating AC current measurements.

Beyond coreless Hall-based current sensing, shunt-based current sensing remains popular in traction inverter applications. This approach places a precision shunt resistor in each busbar, connecting to external isolated operational amplifiers for current measurement. The AMC3302-Q1 is an isolated operational amplifier with integrated isolated power supply, eliminating the need for external isolated power sources. The block diagram of the AMC3302-Q1 is illustrated in Figure 3-24. TI also provides the normal isolated amplifier (AMC030x-Q1) for shunt based current sensing without the internal power supply with single/differential/modulation output modes. Besides inserting the shunt resistor into busbar, the resistor can also be integrated into the power module, which features better cost, thermal management and design size.

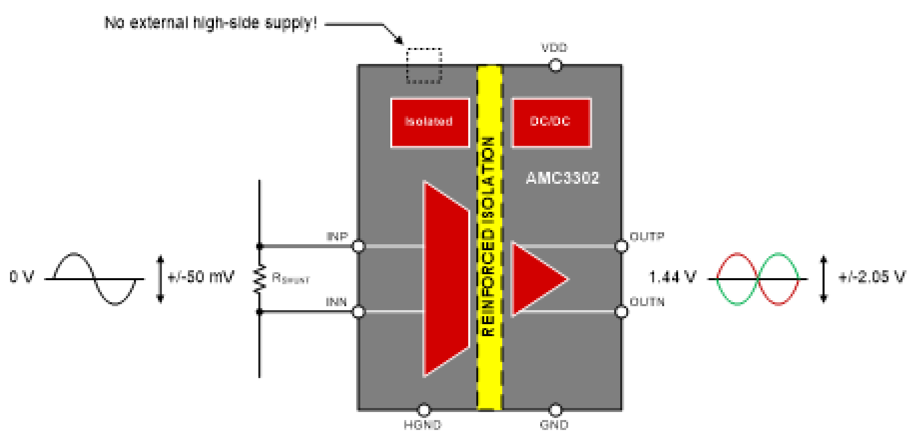

Figure 3-24. AMC3302-Q1 Block Diagram for Shunt-Based Current Sensing

3.5.7 Voltage Sensor

DC voltage sensing plays a critical role in traction inverter systems, serving multiple essential functions including control strategies such as field-weakening control and supporting OV/UV protection. Additionally, accurate voltage sensing is vital for closed-loop active discharge management and power/torque calculations. Isolated amplifier designs represent the most common approach for voltage sensing in traction inverter applications. These devices incorporate an isolation barrier that effectively separates system components operating at different common-mode voltage levels. This isolation is crucial for protecting the low-voltage control circuitry from the high-voltage DC bus, preventing electrical damage and verifying operator safety. Isolated amplifiers provide accurate voltage measurement while maintaining the galvanic isolation required in high-voltage automotive applications. The isolation barrier can alternatively be implemented using a high-resistance path, creating what is known as a non-isolated voltage sensing design.

3.5.7.1 Isolated DC Voltage Sensing

The AMC0311-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, featuring both single-end and differential-end output version. 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 3-25 shows the block diagram of the AMC0311-Q1 DC voltage sensing design.

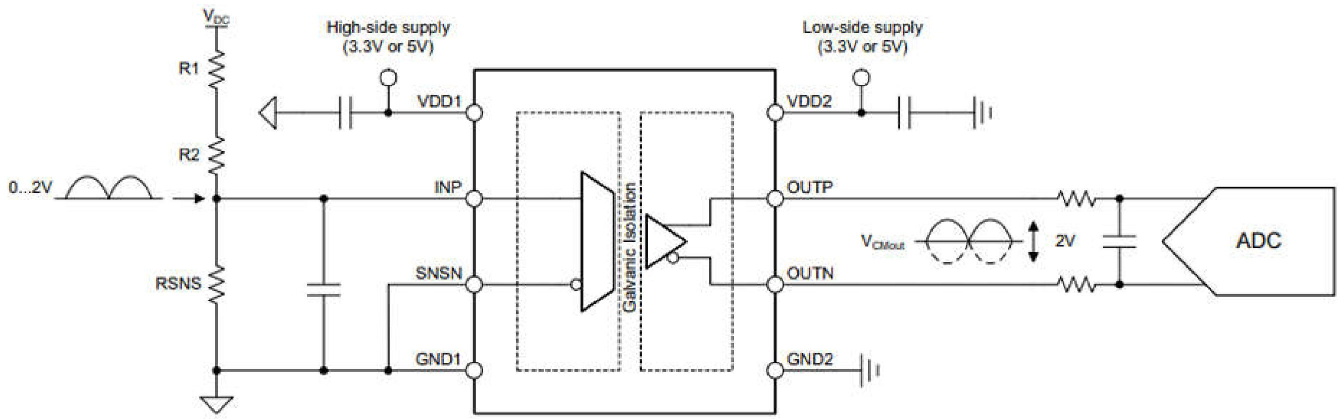

Figure 3-25. Block Diagram of AMC0311-Q1 for Isolated DC Voltage Sensing

To meet the FuSa requirement, traction inverter designs typically implement redundant DC voltage sensing paths using different technologies to avoid potential common cause failures. Figure 3-26 shows a typical dual-channel voltage sensing implementation:

- **Channel 1:** utilizing a conventional approach with a resistor ladder, AMC0311-Q1 isolated amplifier, and MCU ADC for signal conversion.
- **Channel 2:** employing a different technology stack with RES60A-Q1 (an integrated high-12.5MΩ resistor ladder device), ADC integrated in UCC5881-Q1, and MCU GPIO with eCAP or Sigma-Delta Filter Module (SDFM) or SPI for processing.

The two voltage sensing results are cross-checked against each other to provide redundant measurement verification, enhancing the overall FuSa of the system.

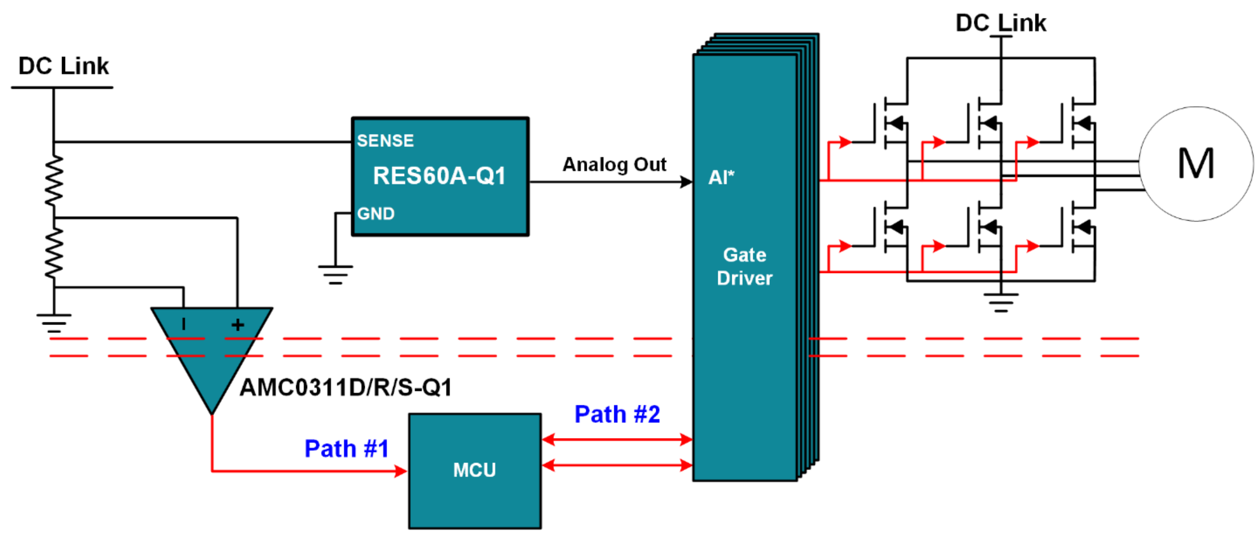

Figure 3-26. Two Channels DC Voltage Sensing with Different Technology for FuSa

Besides the traditional AMC0311-Q1 isolated amplifier, TI also provides several advanced integrated designs for voltage sensing:

- AMC038x-Q1 integrates the resistor ladder into the device, which significantly reduces the PCB area required for HV sensing while features much higher step-down accuracy than the traditional resistor ladder design.
- AMC3311-Q1 integrates the isolated DC-DC converter into the device, eliminating the need for an external isolated power supply to power the high-side circuitry. This higher level of integration reduces component count, simplifies design, and enhances reliability.
- AMC23C1x-Q1 functions as an isolated comparator that provides OV/UV signals directly to the MCU from the high-voltage side. This creates an independent monitoring path separate from the primary DC voltage sensing circuit, supporting designs with higher FuSa requirements.

3.5.7.2 Non-Isolated DC voltage sensing

Beyond isolated barrier approaches, high-impedance paths can also be effectively used to achieve isolation in DC voltage sensing applications. The differential operational amplifier with high-resistance input resistors represents a typical topology for this non-isolated sensing approach. INA160-Q1 and TPS371K-Q1 are the integrated differential op-amp with high input impedance for very high Common-Mode Rejection Ratio (CMRR) for high accuracy DC voltage sensing. This high input impedance allows the device to be connected directly to the high-voltage battery while maintaining safe operation. This is a cost-effective solution as it eliminates the need for isolation components such as capacitive or magnetic isolation barriers.

3.5.8 Temperature Sensor

In traction inverter systems, temperature sensing plays a critical role in overtemperature protection and adaptive driving strategy management regarding the degraded operating mode. TMP61-Q1 is TI silicon-based thermistor with a positive temperature coefficient (PTC). The TMP61-Q1 provides excellent linearity and consistent sensitivity across its 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 3-27 shows the typical resistance versus ambient temperature.

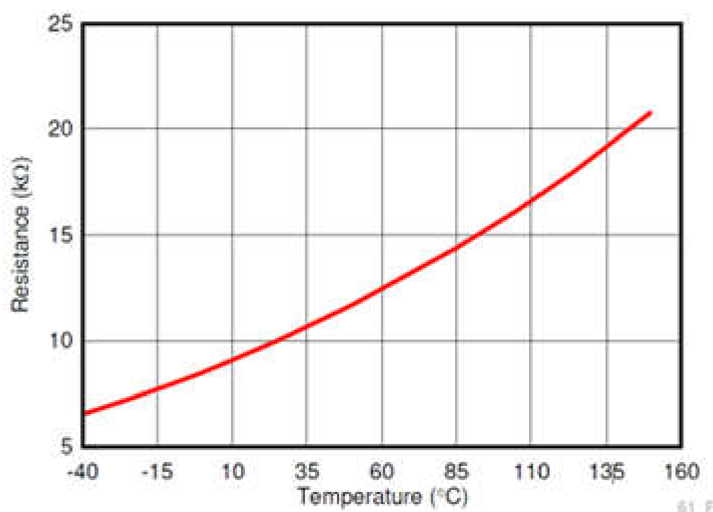

Figure 3-27. TMP61-Q1 PTC Resistance vs Temperature

The TMP61-Q1 can be directly connected to the gate driver ADC pins. Many gate drivers, including the UCC5881-Q1 discussed earlier, integrate constant current sources specifically designed for generating the measurement voltage across the TMP61-Q1. By utilizing multiple ADC channels available in the six gate drivers, the system can monitor the temperature of the power module at different locations. Also, it can be used as redundant measurements for FuSa requirement.

4 Summary

This paper has provided a comprehensive approach to implementing FuSa in traction inverter systems following ISO26262:2018 standard. Section 1 shows the fundamental importance of FuSa in traction inverters, explaining how failures could lead to hazardous conditions and introducing the V-model development process required for safety-critical automotive systems. Section 2 shows the systematic derivation of safety requirements through FTA and FMEA, establishing specific safety goals and safe states for traction inverters while demonstrating the progression from high-level safety goals to detailed technical safety requirements. Section 3 shows practical implementation strategies using TI's FuSa portfolio, detailing how components like MCU, smart gate drivers, position sensors, , power management ICs, etc. work together to create a robust safety architecture that can detect failures and transition to appropriate safe states. This document is intended to provide system designers with essential information and resources needed to develop FuSa compliant traction inverter systems designs that satisfy the required safety metrics.

5 References

1. TUV SUD, Understanding the ISO 26262 Standard: What you need to know | TÜV SÜD, webpage.
2. Texas Instruments, *Understanding FuSa FIT Base Failure Rate Estimates per IEC 623801 and SN 29500 (Rev. A)*, technical white paper.
3. Texas Instruments, *Streamlining FuSa Certification in Automotive and Industrial*, functional safety manual.
4. Texas Instruments, *FuSa Concept in On-Board Charger System*, application note.
5. Texas Instruments, *Automotive, High-Power, High-Performance SiC Traction Inverter Reference Design*, design guide.
6. Texas Instruments, *Isolated Bias Power Supply Architecture for HEV and EV Traction Inverters*, technical white paper.
7. Texas Instruments, *Auto FuSa and How TI is Helping Customers W/ High-Precision Sensors*, technical white paper.