Functional Safety Manual for DRV3263-Q1

Functional Safety Information

Literature Number: SFFSBB3
APRIL 2026

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

Chapter 1
Introduction

This document is a functional safety manual for the Texas Instruments DRV3263-Q1 component (48-pin package). The specific orderable part numbers supported by this functional safety manual are as follows:

Device	Orderable Part Number
DRV3263-Q1	DRV3263QRGZRQ1

This functional safety manual provides information needed by system developers to help in the creation of a functional safety system using a DRV3263-Q1 component. This document includes:

- An overview of the component architecture
- An overview of the development process used to decrease the probability of systematic failures
- An overview of the functional safety architecture for management of random failures
- The details of architecture partitions and implemented functional safety mechanisms

The following information is documented in the *Functional Safety Analysis Report* and is not repeated in this document:

- Summary of failure rates (FIT) of the component
- Summary of functional safety metrics of the hardware component for targeted standards (ISO 26262)
- Quantitative functional safety analysis (also known as FMEDA, Failure Modes, Effects, and Diagnostics Analysis) with detail of the different parts of the component, allowing for customized application of functional safety mechanisms
- Assumptions used in the calculation of functional safety metrics

The following information is documented in the *Functional Safety Report* and is not repeated in this document:

- Results of assessments of compliance to targeted standards

The user of this document needs general familiarity with the DRV3263-Q1 component. For more information, refer to the DRV3263-Q1 datasheet. This document is intended to be used in conjunction with the pertinent data sheets, technical reference manuals, and other component documentation.

For information that is beyond the scope of the listed deliverables, contact your TI sales representative or go to TI Functional Safety.

ADVANCE INFORMATION for preproduction products; subject to change without notice.

Trademarks

All trademarks are the property of their respective owners.

Chapter 2

DRV3263-Q1 Hardware Component Functional Safety Capability

This section summarizes the component functional safety capability.

This hardware component:

- Is being developed as a functional Safety Element out of Context (SEooC)
- Is being developed according to the relevant requirements of ISO 26262:2018
- Targets systematic integrity of ASIL D
- Targets to include sufficient functional safety mechanisms for random fault integrity requirements of ASIL D

Chapter 3

Development Process for Management of Systematic Faults

For functional safety development, it is necessary to manage both systematic and random faults. Texas Instruments follows a new-product development process for all of its components which helps to decrease the probability of systematic failures. This new-product development process is described in Section 3.1. Components being designed for functional safety applications will additionally follow the requirements of TI's functional safety development process, which is described in Section 3.2.

3.1 TI New-Product Development Process

Texas Instruments has been developing components for automotive and industrial markets since 1996. Automotive markets have strong requirements regarding quality management and product reliability. The TI new-product development process features many elements necessary to manage systematic faults. Additionally, the documentation and reports for these components can be used to assist with compliance to a wide range of standards for customer's end applications including automotive and industrial systems (e.g., ISO 26262-4, IEC 61508-2).

This component was developed using TI's new product development process which has been certified as compliant to ISO 9001 / IATF 16949 as assessed by Bureau Veritas (BV).

The standard development process breaks development into phases:

- Assess
- Plan
- Create
- Validate

Figure 3-1 shows the standard process.

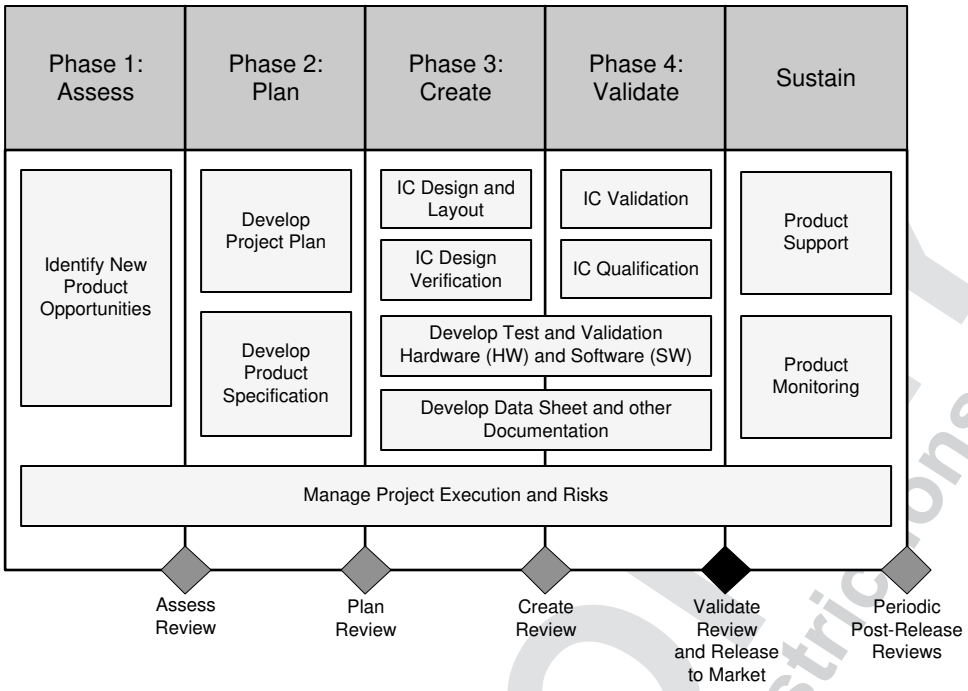

Figure 3-1. TI New-Product Development Process

3.2 TI Functional Safety Development Process

The TI functional safety development flow derives from ISO 26262 and IEC 61508 a set of requirements and methodologies to be applied to semiconductor development. This flow is combined with TI's standard new product development process to develop TI functional safety components. The details of this functional safety development flow are described in the TI internal specification - SafeTI Functional Safety Hardware.

Key elements of the TI functional safety-development flow are as follows:

- Assumptions on system level design, functional safety concept, and requirements based on TI's experience with components in functional safety applications
- Qualitative and quantitative functional safety analysis techniques including analysis of silicon failure modes and application of functional safety mechanisms
- Base FIT rate estimation based on multiple industry standards and TI manufacturing data
- Documentation of functional safety work products during the component development
- Integration of lessons learned through multiple functional safety component developments, functional safety standard working groups, and the expertise of TI customers

Table 3-1 lists these functional safety development activities which are overlaid atop the standard development flow in Figure 3-1.

Refer to Appendix A for more information about which functional safety lifecycle activities TI performs.

The customer facing work products derived from this TI functional safety process are applicable to many other functional safety standards beyond ISO 26262 and IEC 61508.

Table 3-1. Functional Safety Activities Overlaid on top of TI's Standard Development Process

Assess	Plan	Create	Validate	Sustain and End-of-Life
Determine if functional safety process execution is required	Define component target SIL/ASIL capability	Develop component level functional safety requirements	Validate functional safety design in silicon	Document any reported issues (as needed)
Nominate a functional safety manager	Generate functional safety plan	Include functional safety requirements in design specification	Characterize the functional safety design	Perform incident reporting of sustaining operations (as needed)

Table 3-1. Functional Safety Activities Overlaid on top of TI's Standard Development Process (continued)

Assess	Plan	Create	Validate	Sustain and End-of-Life
End of Phase Audit	Verify the functional safety plan	Verify the design specification	Qualify the functional safety design (per AEC-Q100)	Update work products (as needed)
	Initiate functional safety case	Start functional safety design	Finalize functional safety case	
	Analyze target applications to generate system level functional safety assumptions	Perform qualitative analysis of design (i.e. failure mode analysis)	Perform assessment of project	
	End of Phase Audit	Verify the qualitative analysis	Release functional safety manual	
		Verify the functional safety design	Release functional safety analysis report	
		Perform quantitative analysis of design (i.e. FMEDA)	Release functional safety report	
		Verify the quantitative analysis	End of Phase Audit	
		Iterate functional safety design as necessary		
		End of Phase Audit		

Chapter 4

DRV3263-Q1 Component Overview

The DRV3263-Q1 is an integrated smart gate driver for 24V and 48V automotive three-phase BLDC applications. The device provides three half-bridge gate drivers, each capable of driving high-side and low-side N-channel power MOSFETs. The Smart Gate Drive architecture supports configurable peak gate drive current from 16-mA up to 1A source and 2A sink. The DRV3263-Q1 operates across a wide input range from 8 to 85V. A trickle charge pump allows for the gate drivers to support 100% PWM duty cycle control, and provides overdrive gate drive voltage of external switches.

The DRV3263-Q1 provides low-side current sense amplifiers to support resistor based low-side current sensing. The low offset of the amplifiers enables the system to obtain precise motor current measurement.

A wide range of diagnostics and protection features integrated in the DRV3263-Q1 enable a robust motor drive system design and help eliminate the needs of external components. The highly configurable device response allows the device to be integrated seamlessly into a variety of system designs.

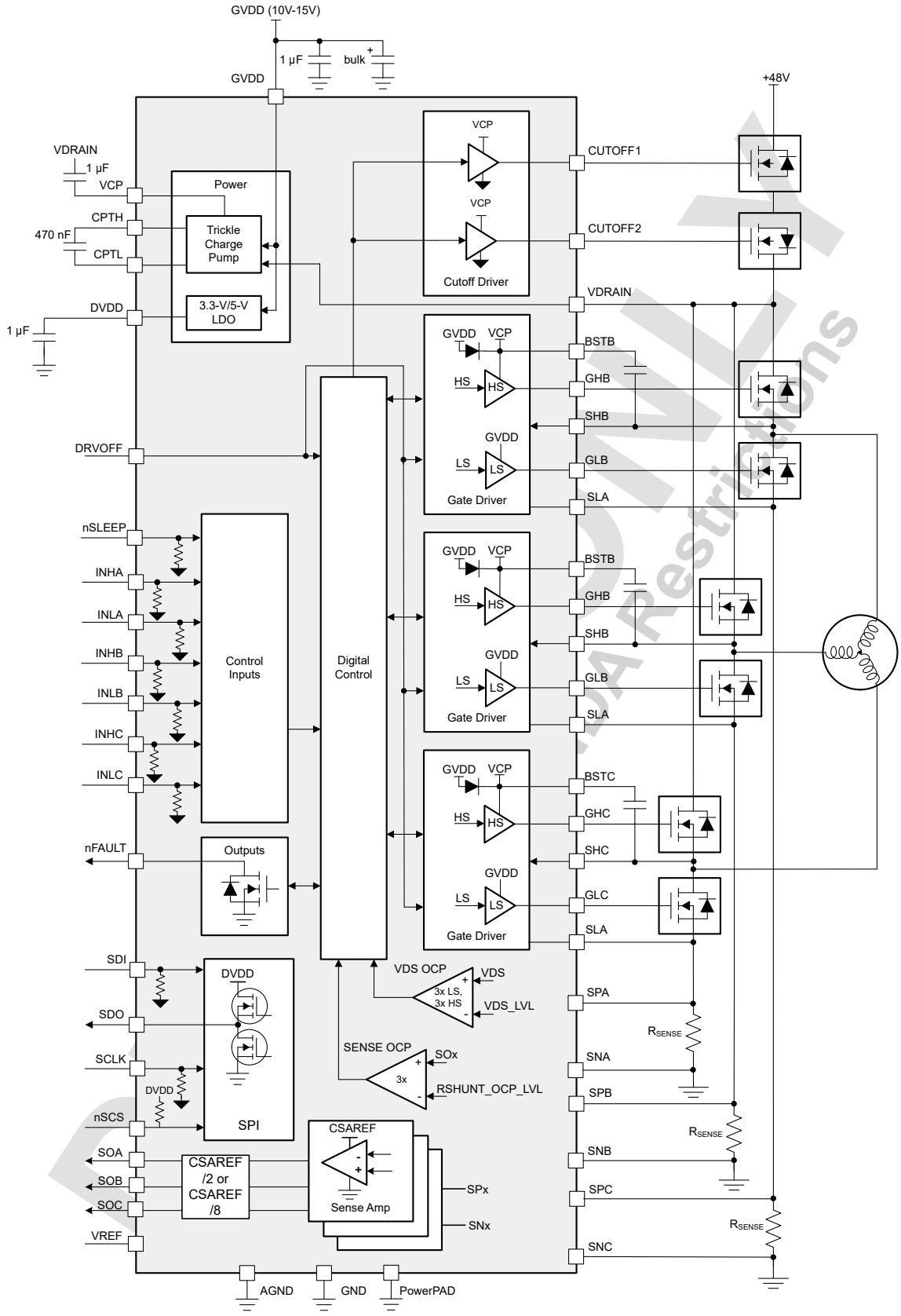

Figure 4-1. DRV3263-Q1 Block Diagram

4.1 Targeted Applications

The DRV3263-Q1 component is targeted at general-purpose functional safety applications. This is called Safety Element out of Context (SEooC) development according to ISO 26262-10. In this case, the development is done based on assumptions on the conditions of the semiconductor component usage, and then the assumptions are verified at the system level. This method is also used to meet the related requirements of IEC 61508 at the semiconductor level. This section describes some of the target applications for this component, the component safety concept, and then describes the assumptions about the systems (also know as Assumptions of Use or AoU) that were made in performing the safety analysis.

Example target applications include, but are not limited to, the following:

- 24-V / 48-V Automotive Motor-Control Applications
  - Fuel and Coolant Pumps
  - Cooling and HVAC Fans
  - Door/Lift Gate Modules

Figure 4-2 shows a generic block diagram for a 48V automotive motor drive system. This diagram is only an example and may not represent a complete system.

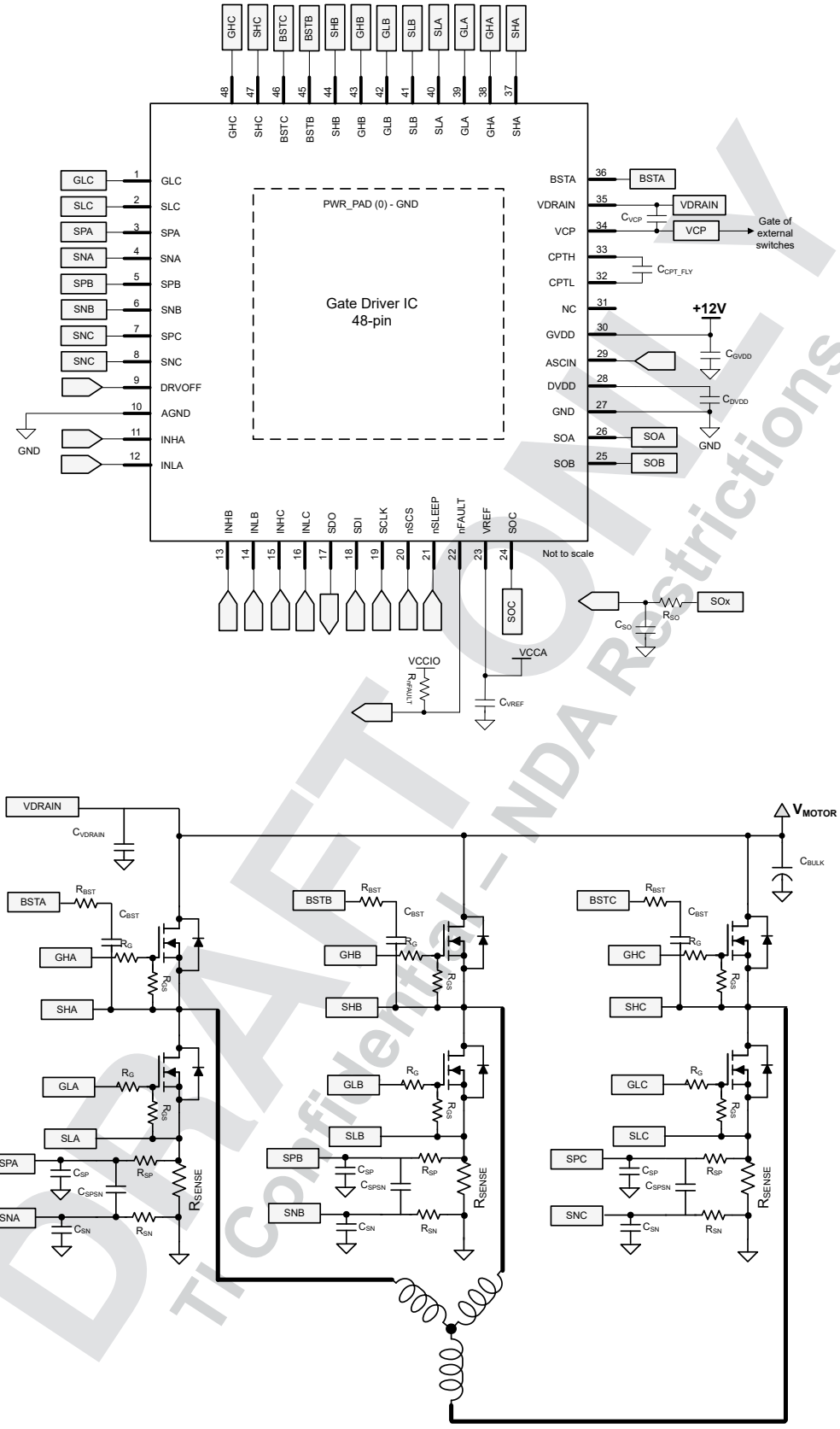

Figure 4-2. DRV3263-Q1 Typical Application

4.2 Hardware Component Functional Safety Concept

The primary Safety Goal of the DRV3263-Q1 is to prevent unintended motor assist. The assumed Functional Safety Requirements are that the system shall remove motor assist power when unintended assist is detected. The Fault Tolerant Time Interval (FTTI) is defined as 10ms. The safe state is defined as all six MOSFETs OFF.

The Safety Goals of the DRV3263-Q1 are:

Table 4-1. DRV3263-Q1 Safety Goals

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI	Safe State
SG-1	Preventing unintended motor assist	ASIL D	10ms	Shutdown of motor assist (all FETs OFF)
SG-2	Preventing loss of motor assist	QM	10ms	Perceived by system
SG-3	Prevent overvoltage of the 48V rail	TBD	TBD	Active Short Circuit (HS or LS FETs ON)

The assumed Functional Safety Requirements are:

Table 4-2. DRV3263-Q1 Functional Safety Requirements

Functional Safety Requirement ID	Assumed System Safety Requirements	ASIL	FTTI
FSR-1	System shall remove motor assist power when unintended assist is detected	ASIL D	10ms
FSR-2	System shall detect sudden loss of motor assist	QM	10ms

4.3 Hardware Component Configuration

The DRV3263-Q1 has two levels of hardware component configuration:

1. The first level of configuration (referred to as pre-configuration) is performed at TI during manufacturing of the device. This pre-configuration occurs before production of the system incorporating the DRV3263-Q1. The pre-configured settings in this first level include information like trim settings and orderable configuration options, and cannot be modified during operation of the system.
2. The second level of configuration is performed by the MCU during operation of the system.

4.4 Functional Safety Constraints and Assumptions

In creating a functional Safety Element out of Context (SEooC) concept and doing the functional safety analysis, TI generates a series of assumptions on system level design, functional safety concept, and requirements. These assumptions (sometimes called Assumptions of Use) are listed below. Additional assumptions about the detailed implementation of safety mechanisms are separately located in Section 5.3.

The DRV3263-Q1 Functional Safety Analysis was done under the following system assumptions:

- **[SA_1]**The system integrator shall follow all requirements in the component data sheet.
- **[SA_2]**The DRV3263-Q1 is powered by an externally generated rail between 8V and 15V (typically 12V), and is also connected to the 48V power supply in the system. The device provides power for most of the internal functions like gate driver, charge pumps, monitors, and I/O unless otherwise specified. DRV3263-Q1 drives external power MOSFETs to provide motor current.
- **[SA_3]**External power supply IC provides power to the system MCU including core, I/O, and ADC. It also provides a current sense reference (VREF) to DRV3263-Q1.

- **[SA_4]**System MCU provides the commutation control signals (PWM inputs) to the DRV3263-Q1 based on position sensor information. System MCU interfaces with the position sensor, and MCU ADC is used to measure motor current through current sense amplifier output. System MCU is also used for diagnostic purposes of the system including the driver IC.
- **[SA_5]** SPI is used to communicate between the DRV3263-Q1 and System MCU for status monitoring and configuration.
- **[SA_6]**It is assumed that the system doesn't significantly affect the controllability of the vehicle if the system loses assist by the motor, such as in the case of all power FETs turned OFF. If all power FETs are turned OFF and the fault is reported to the MCU to take action, it is assumed to be in the safe state.
- **[SA_7]**It is assumed that MCU-controlled system diagnostics are implemented for output plausibility (current sense amplifier/phase voltage) checks, monitoring diagnostics, and SPI + I/O diagnostics.
- **[SA_8]** It is assumed that the DRV3263-Q1 is using the 6xPWM interface mode with input-referred (open-loop) deadtime and the 32-bit CRC-enabled SPI mode.

During integration activities these assumptions of use and integration guidelines described for this component shall be considered. Use caution if one of the above functional safety assumptions on this component cannot be met, as some identified gaps may be unresolvable at the system level.

Chapter 5

DRV3263-Q1 Management of Random Faults

For a functional safety critical development it is necessary to manage both systematic and random faults. The DRV3263-Q1 component architecture includes many functional safety mechanisms, which can detect and respond to random faults when used correctly. This section of the document describes the architectural functional safety concept for each sub-block of theDRV3263-Q1 component. The system integrator shall review the recommended functional safety mechanisms in the functional safety analysis report (FMEDA) in addition to this safety manual to determine the appropriate functional safety mechanisms to include in their system. The component data sheet or technical reference manual (if available) are useful tools for finding more specific information about the implementation of these features.

5.1 Fault Reporting

5.2 Functional Safety Mechanism Categories

This section includes a description of the different types of functional safety mechanisms that are applied to the design blocks of the DRV3263-Q1 component.

The functional safety mechanism categories are defined as follows:

Component Hardware Functional Safety Mechanisms	A safety mechanism that is implemented by TI in silicon which can communicate error status upon the detection of failures. The safety mechanism may require software to enable its functionality, to take action when a failure is detected, or both.
Component Hardware and Software Functional Safety Mechanisms	A test recommended by TI which requires both, safety mechanism hardware which has been implemented in silicon by TI, and which requires software. The failure modes of the hardware used in this safety mechanisms are analyzed or described as part of the functional safety analysis or FMEDA. The system implementer is responsible for analyzing the software aspects for this safety mechanism.
Component Software Functional Safety Mechanisms	A software test recommended by TI. The failure modes of the software used in this safety mechanism are not analyzed or described in the functional safety analysis or FMEDA. For some components, TI may provide example code or supporting code for the software functional safety mechanisms. This code is intended to aid in the development, but the customer shall do integration testing and verification as needed for their system functional safety concept.
System Functional Safety Mechanisms	A safety mechanism implemented externally of this component. For example an external monitoring IC would be considered to be a system functional safety mechanism.
Test for Safety Mechanisms	This test provides coverage for faults on a safety mechanism only. It does not provide coverage for the primary function.
Alternative Safety Mechanisms	An alternative safety mechanism is not capable of detecting a fault of safety mechanism hardware, but instead is capable of recognizing the primary function fault (that another safety mechanism may have failed to detect). Alternate safety mechanisms are typically used when there is no direct test for a safety mechanism.

5.3 Description of Functional Safety Mechanisms

This section provides a brief summary of the functional safety mechanisms available on this component.

5.3.1 SM101 DVDD Over voltage Monitor (DVDD_OV)

Description

The monitoring function is used to detect the over voltage condition of DVDD digital power supply. This function is initiated by the device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. MCU can check the fault flag via SPI.

Impact if not used

The over voltage condition of DVDD regulator is not covered by the device. System MCU shall have an external measure to monitor the digital power supply pin DVDD and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets SPI register bits DVDD_OV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If DVDD_OV register bit is 1, DVDD Over voltage condition has been detected.

Diagnostic Coverage Rationale

DVDD over voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.2 SM102 DVDD Under voltage Monitor (DVDD_UV)

Description

The monitoring function is used to detect the under voltage condition of DVDD digital power supply. This function is initiated by the device and runs all the time during operation. MCU doesn't need to enable the function. If the condition is detected, the device pulls down gate driver. Bootstrap and charge pump are disabled. No flag is available because digital core is in reset state

Impact if not used

N/A. The monitoring function cannot be disabled.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU detects a fault signal on nFAULT pin (active low).
Step3. MCU will detect a SPI access failure because device is in reset state. To detect the failure, MCU needs to run plausibility check of the SPI response periodically.

Diagnostic Coverage Rationale

DVDD under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.3 SM103/104 Internal Regulator voltage Monitors (V5MON_UV / V5SLP_UV)

Description

The monitoring function is used to detect the under voltage condition of the V5MON and V5SLP rails. These power supplies are used for internal biasing, and are not available on device pins. The function is initiated by the device and runs all the time during operation. There is no MCU configurability of this function. The MCU can check the fault flag via SPI.

Impact if not used

N/A. The monitoring function cannot be disabled.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU detects a fault signal on nFAULT pin (active low).
Step3. MCU reads the SPI status registers (optional to identify the cause). If INT_REG_FLT register bit is 1, an internal regulator over voltage or under voltage condition has been detected.

Diagnostic Coverage Rationale

Internal regulator voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.4 SM201 VDRAIN Over voltage voltage Monitor (VDRAIN_OV)

Description

The monitoring functions are used to detect the over voltage of high-side FET drain input (VDRAIN). The functions are initiated by the device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. MCU can check the fault flag via SPI.

Impact if not used

The over voltage condition of high-side FET drain input (VDRAIN) is not covered by the device. System MCU shall have an external measure to monitor the digital power supply signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets SPI register bits VDRAIN_MON_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If VDRAIN_OV register bit is 1, VDRAIN Over voltage condition has been detected.

Diagnostic Coverage Rationale

VDRAIN over voltage and under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.5 SM202 VDRAIN Under Voltage Warning Monitor (VDRAIN_UVH)

Description

The monitoring functions are used to detect the under voltage of high-side FET drain input (VDRAIN). This is the "high" threshold for VDRAIN under voltage, which marks the expected minimum of the VDRAIN operating range. The functions are initiated by the device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. MCU can check the fault flag via SPI.

Impact if not used

The over voltage condition of high-side FET drain input (VDRAIN) is not covered by the device. System MCU shall have an external measure to monitor the digital power supply signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets SPI register bits VDRAIN_UVH_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If VDRAIN_UVH register bit is 1, VDRAIN under voltage condition has been detected.

Diagnostic Coverage Rationale

VDRAIN over voltage and under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.6 SM203 VDRAIN Under Voltage Fault Monitor (VDRAIN_UVL)

Description

The monitoring functions are used to detect the under voltage of high-side FET drain input (VDRAIN). This is the "low" threshold for VDRAIN under voltage, and indicates the threshold at which core device functionality will start to be compromised. The functions are initiated by the device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. MCU can check the fault flag via SPI.

Impact if not used

The under voltage condition of high-side FET drain input (VDRAIN) is not covered by the device. System MCU shall have an external measure to monitor the digital power supply signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets SPI register bits VDRAIN_UVL_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If VDRAIN_UVL register bit is 1, VDRAIN under voltage condition has been detected.

Diagnostic Coverage Rationale

VDRAIN over voltage and under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.7 SM204 VCP Under Voltage Monitor (VCP_UV)

Description

The monitoring function is used to detect the under voltage condition of trickle charge pump (VCP device pin). This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The under voltage condition of the trickle charge pump (VCP) is not covered by the device. System MCU shall have an external measure to monitor the charge pump signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits VCP_UV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If VCP_UV register bit is 1, VCP under voltage condition has been detected.

Diagnostic Coverage Rationale

VCP under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.8 SM205 GVDD Over voltage Monitor (GVDD_OV)

Description

The monitoring function is used to detect the over voltage condition of 12V external supply (GVDD device pin). This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The over voltage condition of the 12V external supply (GVDD) is not covered by the device. System MCU shall have an external measure to monitor the charge pump signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits GVDD_OV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI register IC_STAT4 (optional to identify the cause). If GVDD_OV register bit is 1, GVDD Over voltage condition has been detected.

Diagnostic Coverage Rationale

GVDD over voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.9 SM206 GVDD Under Voltage Warning Monitor (GVDD_UV_BST)

Description

The monitoring function is used to detect the under voltage condition of 12V external supply (GVDD device pin). This is the "high" threshold of GVDD under voltage monitoring, and indicates the point at which GVDD is exiting the expected ~12V range and will start to cause VGS <10V on the external MOSFETs. This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The under voltage condition of the 12V charge pump (GVDD) is not covered by the device. System MCU shall have an external measure to monitor the charge pump signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits GVDD_UV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI register IC_STAT4 (optional to identify the cause). If GVDD_UV register bit is 1, GVDD under voltage condition has been detected.

Diagnostic Coverage Rationale

GVDD under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.10 SM207 GVDD Under Voltage Monitor (GVDD_UVH)

Description

The monitoring function is used to detect the under voltage condition of 12V external supply (GVDD device pin). This is the "middle" threshold for GVDD under voltage monitoring, and represents the point at which the gate driver can no longer sufficiently turn on the gates of the external MOSFETs. This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The under voltage condition of the 12V charge pump (GVDD) is not covered by the device. System MCU shall have an external measure to monitor the charge pump signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits GVDD_UV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI register IC_STAT4 (optional to identify the cause). If GVDD_UV register bit is 1, GVDD under voltage condition has been detected.

Diagnostic Coverage Rationale

GVDD under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.11 SM208 GVDD Under Voltage Lockout Monitor (GVDD_UVL)

Description

The monitoring function is used to detect the under voltage condition of the external 12V supply (GVDD device pin). This fault is the "low" threshold of GVDD under voltage monitoring, and represents the point at which the GVDD supply is no longer sufficient to maintain the internal supplies of the device. This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function, and fault response cannot be selected because the device will power down if the GVDD supply drops below this level. If the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. SPI communication is unavailable, but nFAULT will be pulled low.

Impact if not used

N/A

Limitation

None.

Assumption of use - Proposed method outside device

Step 1. The device enters operation mode (nFAULT= High).
Step 2. MCU detects a fault signal on nFAULT pin (active low).
Step 3. MCU reads the SPI registers. If the SPI query does not return any values, then the part is in the unpowered state.

Diagnostic Coverage Rationale

GVDD under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.12 SM209 CSA REF Over voltage Monitor (CSA REF_OV)

Description

The monitoring function is used to detect the over voltage condition of the CSA reference supply (CSA REF device pin). This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The over voltage condition of the CSA reference supply (CSA REF) is not covered by the device. System MCU shall have an external measure to monitor the charge pump signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits CSA REF_OV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT1 pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If CSA REF_OV register bit is 1, CSA REF Over voltage condition has been detected.

Diagnostic Coverage Rationale

CSA REF over voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor. The threshold voltage for the comparator is generated from the BG_SAFE bandgap reference, which is monitored with an independent monitor to avoid common-cause failures due to supply or reference voltage failure.

5.3.13 SM209 VREF Under Voltage Monitor (VREF_UV)

Description

The monitoring function is used to detect the under voltage condition of CSA reference supply (VREF device pin). This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The under voltage condition of the CSA reference supply (VREF) is not covered by the device. System MCU shall have an external measure to monitor the CSA reference supply and take an action to avoid unintended system operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits CSA REF_UV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If CSA REF_UV register bit is 1, CSA REF under voltage condition has been detected.

Diagnostic Coverage Rationale

VREF under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.14 SM211 Bootstrap Over voltage Monitor (BST_OV)

Description

The monitoring function is used to detect the over voltage condition of the bootstrap supply (BST device pin). This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The over voltage condition of the bootstrap supply (BST) is not covered by the device. System MCU shall have an external measure to monitor the charge pump signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits BST_OV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT1 pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If BST_OV register bit is 1, BST Over voltage condition has been detected.

Diagnostic Coverage Rationale

BST over voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor. The threshold voltage for the comparator is generated from the BG_SAFE bandgap reference, which is monitored with an independent monitor to avoid common-cause failures due to supply or reference voltage failure.

5.3.15 SM210 Bootstrap Under Voltage Monitor (BST_UV)

Description

The monitoring function is used to detect the under voltage condition of bootstrap supply (BST device pin). This function is initiated by device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device pulls down gate driver. Charge pump and bootstraps are disabled. MCU can check the fault flag via SPI.

Impact if not used

The under voltage condition of the bootstrap supply (BST) is not covered by the device. System MCU shall have an external measure to monitor the charge pump signal and take an action to avoid unintended gate driver operation.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT= High).
Step2. MCU sets SPI register bits BST_UV_MODE = 1b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If BST_UV register bit is 1, BST under voltage condition has been detected.

Diagnostic Coverage Rationale

BST under voltage monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.16 SM301 VDS Monitoring

Description

The monitoring function is used to detect the failure mode of the external Power FETs, e.g. short of external Power FETs between Source and Drain. This function is initiated by the device and runs all the time during the operation after the gate driver is enabled. It is enabled by default, and MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the fault is detected, the device pulls down all the gate drivers and asserts nFAULT pin low. MCU can check the fault flag via SPI.

Impact if not used

The failure modes of the external power stage have reduced coverage. System may need external measure to monitor the power stage.

Limitation

The VDS is monitored when gate driver is pulled high (external power FET is ON state). The VDS is not monitored when gate driver is pulled low (external power FET is OFF state).

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets the parameters of VDS monitor; SPI register bits VDS_MODE, VDS_BLK and VDS_DEG.
Step3. MCU drives INH/INL pins. DRVOFF = Low.
Step4. MCU detects a fault signal on nFAULT pin (active low).
Step5. MCU reads the SPI status registers (optional to identify the cause). If VDS_Hx or VDS_Lx register bit is 1, VDS fault condition has been detected.

Diagnostic Coverage Rationale

VDS monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.17 SM302 VGS Monitoring

Description

The monitoring function is used to detect the failure mode of Gate Driver, e.g. Gate Driver output stuck at low. This function is initiated by the device and runs all the time during the operation after the gate driver is enabled. It is enabled by default, and MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the fault is detected, the device pulls down all the gate drivers and asserts nFAULT pin low. MCU can check the fault flag via SPI.

Impact if not used

The single point fault of gate driver is not covered by the device.

Limitation

If 12-V power supply is lower than the recommended operation condition (lower than 9-V), the gate driver output voltage can be lower than the VGS monitor threshold. If the gate driver outputs switch in this condition, the device will detect VGS fault.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High). ENABLE_DRV = 1b.
Step2. MCU drives INH/INL pins. DRVOFF = Low.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If VGS_Hx or VGS_Lx register bit is 1, VGS fault condition has been detected.

Diagnostic Coverage Rationale

VGS monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.18 SM303 VSENSE Monitoring

Description

The monitoring function is used to detect overcurrent failures in the power stage by monitoring the current sense amplifier output. This function is initiated by the device and runs all the time during the operation after the gate driver is enabled. It is enabled by default, and MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the fault is detected, the device pulls down all the gate drivers and asserts nFAULT pin low. MCU can check the fault flag via SPI.

Impact if not used

The failure modes of the external power stage have reduced coverage. System may need external measure to monitor the power stage.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets the parameters of VSENSE OCP monitor; SPI register bits SNS_OCP_MODE and SNS_OCP_LVL.
Step3. MCU drives INH/INL pins. DRVOFF = Low.
Step4. MCU detects a fault signal on nFAULT pin (active low).
Step5. MCU reads the SPI status registers (optional to identify the cause). If SNS_OCP_X register bit is 1, VSENSE fault condition has been detected.

Diagnostic Coverage Rationale

VSENSE Monitoring is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.19 SM304 Phase Diagnostic

Description

The monitoring function is used to detect MOSFET failures in the power stage at startup by applying a weak pullup/pulldown current to the SHx node. This function is initiated by the MCU and runs during startup before starting motor operation.

Impact if not used

The failure modes of the external power stage may have reduced coverage. Typically VDS Monitoring and VSENSE monitoring can detect short-to-battery and short-to-GND overcurrent failures, but the Phase Diagnostic allows detection without a high-current event. This diagnostic is not used in the TI-provided FMEDA for the device, but this SM is still defined to enable easier system-level utilization.

Limitation

Diagnostic must be performed before starting motor operation.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets the PHDEN_Hx (pull-up) or PHDEN_Lx (pull-down) bits in DIAG_CTRL1
Step3. MCU reads the VDS_Hx/VDS_Lx bits to determine if the phase is being pulled up or pulled down. If VDS_Hx/VDS_Lx bits do not match expectation (indicating a short to battery or short to GND), system takes the appropriate reaction.

Diagnostic Coverage Rationale

VSENSE Monitoring is considered to have medium diagnostic coverage (90%) due to the limited current of the diagnostic pullup/pulldown. Some high-resistance MOSFET failures may not be detected.

5.3.20 SM401 SPI CRC

Description

The safety mechanism is used to detect a fault of SPI Transfer data protocol. MCU initiates the safety mechanism and calculates the CRC data. The device compares the CRC value calculated by MCU and the CRC value calculated by device. If the fault is detected, the device reports a fault flag in a SPI register. MCU can check the fault flag.

Impact if not used

The latent fault coverage of SPI transfer is decreased.

Limitation

MCU needs to calculate CRC on the SPI data for each SPI transaction.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU calculates the SDI CRC value for the address, command bit, and data bits (24 bits), and sends SPI frame data to device including 8-bit CRC value (32 bits total).
Step3. Inside device, SDI CRC is calculated and compared to the transmitted value. If values do not match, this indicates corruption in the SDI transmission, so the SPI command is rejected, nFAULT is set low, and SPI_CRC_FLT is set to 1b.
Step4. MCU calculates SDO CRC based on the first 24 bits of the SPI frame, and compares to the 8 bit CRC value. If the values do not match, this indicates corruption in the SDO transmission.

Diagnostic Coverage Rationale

SPI CRC Check is considered to have high (99%) coverage based on the mathematical detection probability for any number of bit corruptions for the 32-bit SPI frame with 8-bit CRC.

5.3.21 SM402 SPI Clock Monitor

Description

The safety mechanism is used to detect the latent fault of the SPI Interface. This function is initiated by the device and monitors all the SPI transfers. MCU doesn't have to enable the function. If the fault is detected, the device set the fault flag and asserts nFAULT pin low. MCU can check the fault flag via SPI.

Impact if not used

N/A. This safety mechanism cannot be disabled.

Limitation

None

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU detects a fault signal on nFAULT pin (active low).
Step3. MCU reads the SPI status registers. If SPI_OK is 0b, SPI clock fault,SPI address fault, or SPI CRC fault is detected by the device. MCU reads the SPI status registers (optional to identify the cause). If SPI_CLK_FLT register bit is 1, SPI clock fault condition has been detected.

5.3.22 SM403 SPI Address Fault Monitor

Description

The safety mechanism is used to detect the latent fault of the SPI Interface. This function is initiated by the device and monitors all the SPI transfers. MCU doesn't have to enable the function. If the fault is detected, the device set the fault flag and asserts nFAULT pin low. MCU can check the fault flag via SPI.

Impact if not used

N/A. This safety mechanism cannot be disabled.

Limitation

None

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU detects a fault signal on nFAULT pin (active low).
Step3. MCU reads the SPI status registers. If SPI_OK is 0b, SPI clock fault, SPI address fault, or SPI CRC fault is detected by the device. MCU reads the SPI status registers (optional to identify the cause). If SPI_ADDR_FLT register bit is 1, SPI address fault condition has been detected.

5.3.23 SM404 One Time Program memory CRC test (OTP CRC)

Description

The safety mechanism is used to detect a fault of OTP Data Content. TI production test information including trim data of device internal analog functions is stored in OTP memory. The OTP memory is programmed during the TI production test. At every power up, the data is automatically loaded from OTP memory, and the memory CRC test runs. This function is initiated by the device and runs once at device power up. MCU doesn't have to enable the function. If the fault is detected, the device report the fault on SPI flag (OTP_CRC_FLT). Additionally, the presence of this fault implies that analog parameters may not meet the accuracy defined in the datasheet due to the potential loss of trim settings. MCU can check the device status and the fault flag.

Impact if not used

N/A. This safety mechanism cannot be disabled.

Limitation

No limitation, but the device doesn't report the fault on nFAULT pin. MCU needs to check status register bit.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU must read the SPI status registers. If OTP_CRC_FLT register bit is 1, OTP memory fault has been detected.

Diagnostic Coverage Rationale

OTP CRC is considered to have a medium coverage (90%) because it utilizes a CRC polynomial with a hamming distance of 4.

5.3.24 SM405 Shoot-Through Protection (STP)

Description

The safety mechanism is used to detect the single point fault of INHx and INLx input control signals, e.g. the input signal stuck high. This function is initiated by the device and runs all the time during the operation after the gate driver is enabled. It is enabled by default, and MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the fault is detected, the device enforces gate driver to low during the shoot through condition. If the fault is detected nFAULT is driven low. MCU can check the fault flag.

Impact if not used

N/A. The monitoring function cannot be disabled.

Limitation

None

Assumption of use - Proposed method outside device

Step1. Dead time control and shoot through protection are enabled by default.
Step2. MCU drives INH/INL pins.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If STP_FLT register bit is 1, a shoot-through violation condition has been detected.

Diagnostic Coverage Rationale

Dead time control and shoot through protection are considered to have a high diagnostic coverage (99%) as they are digital logic filters that directly compare the incoming INHx/INLx input buffers before allowing the gate drive signals to progress further in the gate drive control path.

5.3.25 SM406 Dead Time Protection

Description

The safety mechanism is used to detect the single point fault of INHx and INLx input control signals, e.g. the input signal stuck high. This function is initiated by the device and runs all the time during the operation after the gate driver is enabled. It is enabled by default, and MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the fault is detected, the device enforce gate driver to low while the dead time is violated. If the fault is detected nFAULT is driven low. MCU can check the fault flag.

Impact if not used

N/A. The monitoring function cannot be disabled.

Limitation

None

Assumption of use - Proposed method outside device

Step1. Dead time control and shoot through protection are enabled by default.
Step2. MCU drives INH/INL pins.
Step3. MCU detects a fault signal on nFAULT pin (active low).
Step4. MCU reads the SPI status registers (optional to identify the cause). If DEADT_FLT register bit is 1, a dead time violation condition has been detected.

Diagnostic Coverage Rationale

Dead time control and shoot through protection are considered to have a high diagnostic coverage (99%) as they are digital logic filters that directly compare the incoming INHx/INLx input buffers before allowing the gate drive signals to progress further in the gate drive control path.

5.3.26 SM407 Device Mode Monitor

Description

The safety mechanism is used to detect the latent fault of TI test mode detection. This function is initiated by the device and is monitoring the fault all the time. MCU doesn't have to enable the function. If the fault is detected, the device sets the fault flag in a SPI status register.

Impact if not used

The latent fault of TI test mode detection is not covered.

Limitation

No limitation,

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU detects a fault signal on nFAULT pin.
Step3. MCU reads the SPI status registers. If DEV_MODE_FLT register bit is 1, a device mode fault condition has been detected.

Diagnostic Coverage Rationale

Device error mode detection is considered to have a medium diagnostic coverage (90%) as it is a fixed-function digital monitor observing the operating mode of the device's digital logic.

5.3.27 SM408 Configuration Data CRC

Description

The safety mechanism is used to detect a single point fault of the device configuration registers, e.g. bit flip. MCU shall initiate this function. After it is enabled, the device runs a CRC calculation every 1ms and compares the calculation result with the expected value. If the fault is detected, the device sets the fault flag and asserts the nFAULT pin low. MCU can check the device status and the fault flag via SPI.

Impact if not used

The diagnostic coverage of register map is decreased.

Limitation

The target configuration registers cannot be changed while the CRC runs, otherwise the device reports fault to MCU.

Assumption of use - Proposed method outside device

Step1. MCU writes SPI registers of device configurations.
Step2. After configuration is done, MCU writes 1 to the CFG_CRC_EN register to start a periodic CRC calculation running on device.
Step3. MCU detects a fault signal on nFAULT pin.
Step4. MCU reads the SPI status registers (optional to identify the cause). If CFG_CRC_FLT register bit is 1, Configuration register fault condition has been detected.

Diagnostic Coverage Rationale

Configuration Data CRC is considered to have a medium coverage (90%) because it utilizes a CRC polynomial with a hamming distance of 4.

5.3.28 SM501 Overtemperature Warning/Shutdown (OTSD)

Description

The monitoring function is used to detect the over temperature condition of the device. This function is initiated by the device and runs all the time during operation. MCU doesn't need to enable the function but can select fault (shutdown) mode or warning mode. If shutdown mode is selected and the condition is detected, the device disables the gate drivers, bootstraps, and charge pump. The device sets the fault flag and asserts the nFAULT pin low. The MCU can check the fault flag.

Impact if not used

The continuous over heating of the device can cause reliability issue or potential permanent damage. The system must take an action if over temperature condition is reported by the device.

Limitation

No limitation

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sets SPI register bits OTSD_MODE = 01b to enable fault (shutdown) mode.
Step3. MCU detects a fault signal on nFAULT pin.
Step4. MCU reads the SPI status registers. If OTSD register bit is 1, over temperature condition has been detected.

Diagnostic Coverage Rationale

Over-temperature shut-down is considered to have high diagnostic coverage (99%) due to the comparator-based monitor.

5.3.29 SM502 Independent Shutdown Path (DRVOFF)

Description

The function supports MCU action to put the gate driver in shutdown mode. If MCU drives DRVOFF high, the gate driver outputs are pulled low to turn OFF the external power FETs.

Impact if not used

The shutdown path needs to be implemented by the system.

Limitation

None

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High). ENABLE_DRV = 1b.
Step2. MCU drives DRVOFF high.

Diagnostic Coverage Rationale

Independent Shutdown Path (DRVOFF) is considered to have high diagnostic coverage (99%) due to using an independent supply from the INHx/INLx control, and including a digital core bypass to directly shut down the output stage in event of a digital core failure.

5.3.30 SM503 Independent Shutdown Path (nSLEEP)

Description

The function supports MCU action to put the gate driver in shutdown mode. If MCU drives nSLEEP low, the gate driver outputs are pulled low to turn OFF the external power FETs, and the internal regulators are powered down.

Impact if not used

The shutdown path needs to be implemented by the system.

Limitation

None

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High). ENABLE_DRV = 1b.
Step2. MCU drives DRVOFF low.

Diagnostic Coverage Rationale

Independent Shutdown Path (nSLEEP) is considered to have medium diagnostic coverage (99%) due to the use of a separate power domain (V5SLP) vs the normal operation control path INHx/INLx (VDD_GPIO).

5.3.31 SM504 VDS Monitoring Diagnostic

Description

The safety mechanism is used to detect the latent point faults of VDS comparator. The MCU initiates the function and monitors the fault flag.

Impact if not used

The latent fault of the VDS comparator are not covered by the device.

Limitation

This safety mechanism is available when the gate driver is enabled (SPI register bit ENABLE_DRV = 1b).

Assumption of use – Proposed method outside the device

Step 1. VDS monitoring is enabled when ENABLE_DRV = 1b. The INHx and INLx pins are driven low, (x=1,2,3).
Step 2. The MCU sets VDS_DIAG to 1.
Step 3. The MCU drives INL1 high.
Step 4. The MCU reads the SPI status registers.
Step 5. If the fault register bit is 1, the MCU knows that the VDS comparator worked correctly.
Step 6. Repeat steps 2-4 for the channel 2 and 3.
Step 7. Repeat steps 2-5 for INHx.

Diagnostic Coverage Rationale

The VDS monitor diagnostic is considered to have medium coverage (90%). Normally, the VDS monitoring signal is low, so this diagnostic uses dynamic principles by intentionally forcing the VDS comparator high, so that the comparator output is not stuck low. Dynamic-principles type diagnostics are typically considered capable of achieving medium coverage by ISO26262.

See Chapter 5 for more information regarding the description of hardware components.

5.3.32 SM505 VGS Monitoring Diagnostic

Description

The safety mechanism is used to detect a latent fault of VGS monitoring, for example, the VGS comparator output is stuck low. The MCU needs to initiate the diagnosis.

Impact if not used

The latent fault of the VGS monitor is not covered.

Limitation

Since both the high-side and low-side power FETs of all channels are turned off due to the shutdown test, the diagnosis must be performed during the system diagnosis phase. The VGS monitor diagnostic is designed to verify IC_STAT3 (VGS_xx), where the VGS comparator is monitoring for VGS > 8.5V (or > 6.3V if VGS_LVL = 1), when INHx and INLx are high.

Assumption of use – Proposed method outside the device

Step 1. The device enters operation mode (nFAULT = High).
Step 2. The MCU sets VGS_DIAG = 1b.
Step 3. The MCU disables the VDS monitor to avoid an unintended shutdown of the gate driver.
Step 4. The MCU drives the INHx or INLx pins high
Step 5. The MCU reads the SPI status registers. If the read result of VGS_xx is set 1, the VGS monitor is not stuck low.

Diagnostic Coverage Rationale

The VGS monitor diagnostic is considered to have medium coverage (90%). Normally, the VGS monitoring signal is low, so this diagnostic uses dynamic principles by intentionally forcing the VGS comparator high, so that the comparator output is not stuck low. Dynamic-principles type diagnostics are typically considered capable of achieving medium coverage by ISO26262.

See Chapter 5 for more information regarding the description of hardware components.

5.3.33 SM506 Sense OCP Diagnostic (SNS_OCP_DIAG)

Description

The diagnostic function is used to detect latent faults of the SNS OCP comparator. The MCU initiates the function, and monitors the fault flag. If shutdown mode is selected and the condition is detected, the device pulls down the gate driver. The charge pump and bootstraps are disabled. The MCU can check the fault flag through an SPI.

Impact if not used

The latent fault of the SNS OCP comparator is not covered.

Limitation

None.

Assumption of use – Proposed method outside the device

Step 1. The device enters operation mode (nFAULT= High).
Step 2. The MCU sets the SPI register bits SNS_OCP_DIAG = 1b to enable the diagnostic.
Step 3. The MCU detects a fault signal on the nFAULT pin (active low).
Step 4. The MCU reads the SPI status registers. If the SNS_OCP_x register bits are 1, the MCU knows that the SNS OCP comparator is not stuck low.

Diagnostic Coverage Rationale

The sense OCP diagnostic is considered to have medium diagnostic coverage (90%). Normally, the SNS_OCP monitoring signal is low, so this diagnostic uses dynamic principles by intentionally forcing the SNS_OCP comparator high, so that the comparator output is not stuck low. Dynamic-principles type diagnostics are typically considered capable of achieving medium coverage by ISO26262.

See Chapter 5 for more information regarding the description of hardware components.

5.3.34 SM507: Analog Built-In Self-Test (Analog BIST)

Description

The safety mechanism is used to detect a latent fault of the voltage monitor OV and UV comparators, for example, the output is stuck high and low. This function is initiated by the device and runs once at device power up. The MCU does not have to enable the function. If the fault is detected, the device reports the fault in the SPI register. The MCU can check the fault flag through an SPI.

Impact if not used

N/A. The monitoring function cannot be disabled.

Limitation

No limitation, but the device does not report the fault on the nFAULT pin. The MCU needs to check the status register bit.

Assumption of use – Proposed method outside the device

Step 1. The device enters operation mode (nFAULT = High).
Step 2. The MCU reads the SPI status registers. If the ABIST_FLT = 1, an analog BIST was failing at power up.

Diagnostic Coverage Rationale

Analog BIST is considered to have medium coverage (90%). Normally, the voltage monitoring comparator outputs are low, so this diagnostic uses dynamic principles by intentionally forcing the comparators high, so that the comparator outputs are not stuck low. Dynamic-principles type diagnostics are typically considered capable of achieving medium coverage by ISO26262.

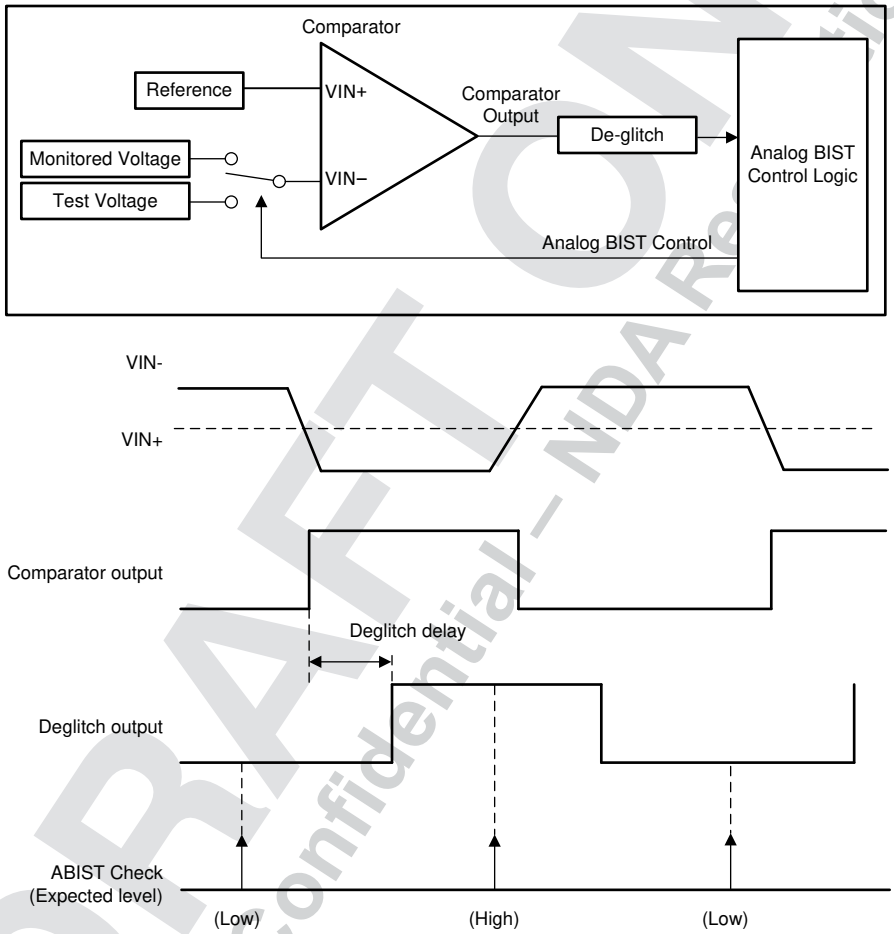

Figure 5-1. Analog BIST Control

See Chapter 5 for more information regarding the description of hardware components.

5.3.35 SM901 CSA Plausibility Check

Description

The system assumes the failure mode of current sense is monitored by external measures.

Impact if not used

The failure mode of current sense is not covered.

Limitation

In case of DVDD under voltage or device sleep mode, Current Sense Amplifier is disabled.

Assumption of use - Proposed method outside device

MCU monitors the output of current sense SOx (x=1,2,3) by using ADC, and performs the plausibility check at start-up and during operation.

Diagnostic Coverage Rationale

CSA Plausibility check is considered to typically have high diagnostic coverage (99%), but diagnostic coverage will depend on the system's implementation method for the diagnostic.

5.3.36 SM902 Independent Shutdown Path (DRVOFF) Diagnostic

Description

This safety mechanism is used to detect the latent failure of the DRVOFF independent shut-down path.

Impact if not used

The shutdown path cannot be used in case of multiple point faults of DRVOFF shut-down path and gate driver.

Limitation

Since the both high-side and low-side power FETs of all channels will be turned off due to the shutdown test, the diagnosis must be performed during system diagnosis phase

Assumption of use - Proposed method outside device

Step 1. The device enters operation mode (nFAULT = High).
Step 2. MCU sets DRVOFF_DIAG = 1b to force digital core to ignore DRVOFF signal.
Step 3. MCU sets VDS and VGS monitors to "Warn" mode avoid fault-induced shutdown of gate driver.
Step 4. MCU sets DRVOFF signal high.
Step 5. MCU drives INHx or INLx pins high
Step6. MCU reads the SPI status registers (for VDS or VGS faults). If the read result of VDS_xx or VGS_xx is set 1, then MCU knows that DRVOFF has successfully prevented gate turn-on, confirming the pin connection and internal shutdown path.

Diagnostic Coverage Rationale

Independent Shutdown Path (DRVOFF) Diagnostic is considered to have medium coverage (90%). Normally DRVOFF is low, so this diagnostic uses dynamic principles by intentionally forcing DRVOFF high, ensuring that the input is not stuck low. This type of diagnostic is typically considered capable of achieving medium coverage per ISO26262.
In the context of pin level tailoring within the FMEDA, the Independent Shutdown Path Diagnostic is considered to have high (99%) coverage due to the limited number of failure modes (pin short or pin open).

5.3.37 SM903 Independent Shutdown Path (nSLEEP) Diagnostic

Description

This safety mechanism is used to detect the latent failure of the nSLEEP independent shut-down path.

Impact if not used

The shutdown path cannot be used in case of multiple point faults of nSLEEP shut-down path and gate driver.

Limitation

Since the device will be turned off due to the shutdown test, the diagnosis must be performed during system diagnosis phase

Assumption of use - Proposed method outside device

Step 1. The device enters operation mode (nFAULT = High).
Step 2. MCU sets nSLEEP low for greater than the deglitch time
Step 3. MCU monitors nFAULT and SPI to confirm that the device has powered down.

Diagnostic Coverage Rationale

Independent Shutdown Path (nSLEEP) Diagnostic is considered to have medium coverage (90%). Normally nSLEEP is high, so this diagnostic uses dynamic principles by intentionally forcing nSLEEP low, ensuring that the input is not stuck high. This type of diagnostic is typically considered capable of achieving medium coverage per ISO26262.
In the context of pin level tailoring within the FMEDA, the Independent Shutdown Path Diagnostic is considered to have high (99%) coverage due to the limited number of failure modes (pin short or pin open).

5.3.38 SM904 nFAULT Diagnostic

Description

MCU intentionally causes fault condition of device and monitors nFAULT pin. Sending SPI command with undefined address can be used as an example.

Impact if not used

The latent fault of nFAULT reporting is not covered.

Limitation

No limitation,

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU sends a SPI command with undefined address in the datasheet register map.
Step3. MCU monitors nFAULT. nFAULT is expected be asserted (active low) because of SPI address fault.
Step4. MCU sets CLR_FLT bit to 1. nFAULT must go high.

Diagnostic Coverage Rationale

nFAULT Diagnostic is considered to have medium coverage (90%). Normally nFAULT is high, so this diagnostic uses dynamic principles by intentionally forcing nFAULT low, ensuring that the input is not stuck high. This type of diagnostic is typically considered capable of achieving medium coverage per ISO26262.
In the context of pin level tailoring within the FMEDA, the nFAULT Diagnostic is considered to have high (99%) coverage due to the limited number of failure modes (pin short or pin open).

5.3.39 SM905 Power Up Time Measurement

Description

MCU monitors nFAULT pin at power up (PVDD power up or nSLEEP driven high). MCU checks the nFAULT level after tWAKE time.

Impact if not used

Device internal fault at power up is not covered.

Limitation

No limitation,

Assumption of use - Proposed method outside device

Step1. MCU starts a timer when MCU drives nSLEEP high.
Step2. After tWAKE time (=5ms) passes, MCU checks nFAULT logic level. If the nFAULT is low, the device is failing at power up.

Diagnostic Coverage Rationale

Power up time measurement is considered to have low (60%) coverage for V5SLP due to common-cause failure (V5SLP is the supply for nFAULT output). For other power rails, power up time measurement is considered to have high (99% coverage) because these power supplies are independent from nFAULT, and have independent UV/OV monitors to avoid common-cause failures due to supply or reference voltage failure.

5.3.40 SM906 Phase Voltage Plausibility Check

Description

The SHx voltage can be reduced through a voltage divider and a low pass filter to remove the PWM carrier frequency, and then sampled by the MCU ADC to infer the effective duty cycle achieved by the power MOSFETs.

Impact if not used

The metric of single-point/latent fault of digital I/O and gate driver may be affected.

Limitation

None.

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU samples the SHx voltage using ADC.
Step3. MCU compares measurement against the commanded duty cycle.

Diagnostic Coverage Rationale

Phase voltage plausibility check is considered to typically have medium (90%) coverage because the monitor requires a periodic check to be performed by the MCU. Final diagnostic coverage will depend on system implementation.

5.3.41 SM907 SPI Test Register

Description

The special SPI test register is used to detect the latent fault of SPI Interface. MCU initiates the safety mechanism and compares the read data with the expected value.

Impact if not used

The metric of latent fault of SPI interface is impacted.

Limitation

None

Assumption of use - Proposed method outside device

Step1. The device enters operation mode (nFAULT = High).
Step2. MCU writes 0x55 to SPI_TEST register.
Step3. MCU reads SPI_TEST register and compares it with 0x55.
Step4. MCU writes 0xAA to SPI_TEST register.
Step5. MCU reads SPI_TEST register and compares it with 0xAA.

Diagnostic Coverage Rationale

SPI Test Storage Register is considered to have medium (90%) coverage because it is not possible to ascertain if the communication issue with the device is occurring on the input or output of the SPI interface.

5.3.42 SM910 SPI Register Map Readback

Description

The external measure is used to detect a fault of SPI write register access. MCU reads the control registers after the write register request, and verifies the read data.

Impact if not used

The diagnostic coverage of SPI transfer is decreased.

Limitation

No limitation.

Assumption of use - Proposed method outside device

Step1. MCU sends SPI write register request
Step2. MCU reads the register data
Step3. MCU compares the data of Step2 and the data of Step1.
Step4. If the data mismatch is found, MCU takes an action for the fault.

Diagnostic Coverage Rationale

SPI register map readback is considered to have medium (90%) coverage because it is not possible to ascertain if the communication issue with the device is occurring on the input or output of the SPI interface.

5.3.43 SM911 Default Register Contents Plausibility Check

Description

The external measure is used to detect a reset of the device.

Impact if not used

Alternative method of detecting device reset will need to be implemented.

Limitation

No limitation.

Assumption of use - Proposed method outside device

Step1. MCU modifies a SPI register (like SPI_TEST) to a non-reset value
Step2. MCU reads the register data
Step3. If register data has returned to power-up default, then a device reset has occurred.

Diagnostic Coverage Rationale

Default register contents plausibility check is considered to have medium (90%) coverage because it is not possible to ascertain if the communication issue with the device is occurring on the input or output of the SPI interface.

Appendix A
Distributed Developments

A Development Interface Agreement (DIA) is intended to capture the agreement between two parties towards the management of each party's responsibilities related to the development of a functional safety system. TI functional safety components are typically designed for many different systems and are considered to be Safety Elements out of Context (SEooC) hardware components. The system integrator is then responsible for taking the information provided in the hardware component safety manual, safety analysis report and safety report to perform system integration activities. Because there is no distribution of development activities, TI does not accept DIAs with system integrators.

TI functional safety components are products that TI represents, promotes or markets as helping customers mitigate functional safety related risks in an end application and/or as compliant with an industry functional safety standard or FS-QM. For more information about TI functional safety components, go to TI.com/functionalsafety.

A.1 How the Functional Safety Lifecycle Applies to TI Functional Safety Products

TI has tailored the functional safety lifecycles of ISO 26262 and IEC 61508 to best match the needs of a functional Safety Element out of Context (SEooC) development. The functional safety standards are written in the context of the functional safety systems, which means that some requirements only apply at the system level. Since TI functional safety components are hardware or software components, TI has tailored the functional safety activities to create new product development processes for hardware and for software that makes sure state-of-the-art techniques and measures are applied as appropriate. These new product development processes have been certified by third-party functional safety experts. To find these certifications, go to TI.com/functionalsafety.

A.2 Activities Performed by Texas Instruments

The TI functional safety products are hardware components developed as functional Safety Elements out of Context. As such, TI's functional safety activities focus on those related to management of functional safety around hardware component development. System level architecture, design, and functional safety analysis are not within the scope of TI activities and are the responsibility of the customer. Some techniques for integrating the SEooC safety analysis of this hardware component into the system level can be found in ISO 26262-11.

Table A-1. Activities Performed by Texas Instruments versus Performed by the customer

Functional Safety Lifecycle Activity[1]	TI Execution	Customer Execution
Management of functional safety	Yes	Yes
Definition of end equipment and item	No	Yes
Hazard analysis and risk assessment (of end equipment/ item)	No	Yes
Creation of end equipment functional safety concept	No. Assumptions made for internal development.	Yes
Allocation of end equipment requirements to sub-systems, hardware components, and software components	No. Assumptions made for internal development.	Yes

Table A-1. Activities Performed by Texas Instruments versus Performed by the customer (continued)

Functional Safety Lifecycle Activity[1]	TI Execution	Customer Execution
Definition of hardware component safety requirements	Yes	No
Hardware component architecture and design execution	Yes	No
Hardware component functional safety analysis	Yes	No
Hardware component verification and validation (V&V)	V&V executed to support internal development.	Yes
Integration of hardware component into end equipment	No	Yes
Verification of IC performance in end equipment	No	Yes
Selection of safety mechanisms to be applied to IC	No	Yes
End equipment level verification and validation	No	Yes
End equipment level functional safety analysis	No	Yes
End equipment level functional safety assessment	No	Yes
End equipment release to production	No	Yes
Management of functional safety issues in production	Support provided as needed	Yes

(1) For component technical questions, contact TI local support.

A.3 Information Provided

Texas instruments has summarized what it considers the most critical functional safety work products that are available to the customer under a nondisclosure agreement (NDA). NDAs are required to protect proprietary and sensitive information disclosed in certain functional safety documents.

Table A-2. Product Functional Safety Documentation

Deliverable Name	Contents
Functional Safety Manual (preliminary draft available)	User guide for the functional safety features of the product, including system level assumptions of use.
Functional Safety Analysis Report (preliminary draft available)	Results of all available functional safety analysis documented in a format that allows computation of custom metrics.
Functional Safety Report (to be released after TI internal assessment is completed)	Summary of arguments and evidence of compliance to functional safety standards. References a specific component, component family, or TI process that was analyzed.

Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

DATE	REVISION	NOTES
March 2026	0p2	Customer preview draft
April 2026	0p1	Initial preliminary draft

This page intentionally left blank.

IMPORTANT NOTICE AND DISCLAIMER

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

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

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

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

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

Last updated 10/2025