Functional Safety Information

Functional Safety Manual for TCAN1167-Q1

Table of Contents

List of Figures

List of Tables

1 Introduction

This document is a functional safety manual for the Texas Instruments TCAN1167-Q1 component. The specific orderable part numbers supported by this functional safety manual are as follows:

- [TCAN1167-Q1] (Orderable Part #: TCAN1167DMTRQ1)

This functional safety manual provides information needed by system developers to help in the creation of a functional safety system using a TCAN1167-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 (for example IEC 61508, ISO 26262, and so forth)
- 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 should have a general familiarity with the TCAN1167-Q1 component. For more information, refer to the data sheet. 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 .

Trademarks

TI E2E™ is a trademark of Texas Instruments.
All trademarks are the property of their respective owners.

2 TCAN1167-Q1 Hardware Component Functional Safety Capability

This section summarizes the component functional safety capability.

This hardware component:

- Was not developed according to the requirements of any functional safety standard.
- FIT rates and failure mode distributions are provided as part of the Functional Safety Analysis Report for custromers to calculate random fault integrity metrics.
- Recommendations are provided in this Functional Safety Manual for external safety mechanisms that may provide coverage for component failure modes.
- TI recommends that this component is integrated into the system through the strategy of "evaluation of hardware element" (ISO 26262-8:2018 clause 13).

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.

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.

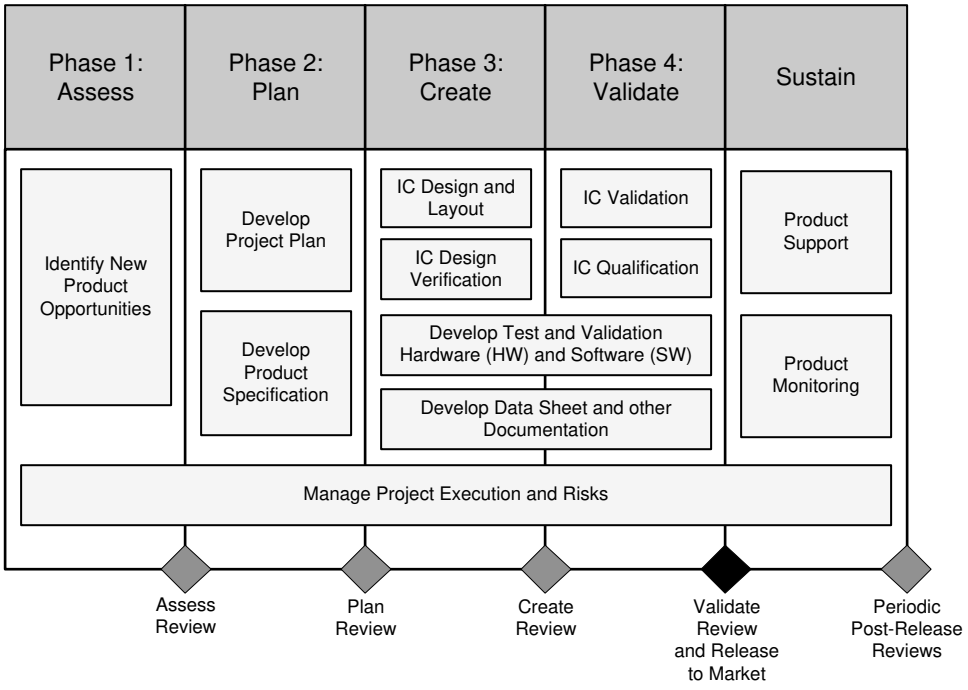

Figure 3-1. TI New-Product Development Process

4 Description of Hardware Component Parts

A semiconductor component can be divided into parts to enable a more granular functional safety analysis. This can be useful to help assign specific functional safety mechanisms to portions of the design where they provide coverage ending up with a more complete and customizable functional safety analysis. This section includes a brief description of each hardware part of this component and lists the functional safety mechanisms that can be applied to each. This section is intended to provide additional details about the assignment of functional safety mechanisms that can be found in the Safety Analysis Report. The content in this section is also summarized in Appendix A.

4.1 CAN Transceiver

The TCAN1167-Q1 provides a flexible data rate controller area network (CAN FD) transceiver used to communicate a node processor and the CAN bus. CAN protocol has inherent mechanisms for data accuracy and is outside the scope of the device.

The following sections provide the functional safety mechanisms that cover the CAN transceiver:

- Section 5.3.1.1
- Section 5.3.1.2
- Section 5.3.1.3
- Section 5.3.2.1

4.2 Digital Core

The TCAN1167-Q1 contains an internal digital core that operates the device and contains several diagnostic features such as: TXD dominant time out timer, SPI communication processor and addressable registers, time out, windowed, or Q&A watchdog timer, and the sleep wake error timer. The digital core also interfaces with the internal EEPROM memory and has CRC checking capability to ensure good data retention.

The following sections provide the functional safety mechanisms that cover the digital core:

- Section 5.3.1.4
- Section 5.3.3.1
- Section 5.3.3.2
- Section 5.3.3.3
- Section 5.3.3.4
- Section 5.3.4.1

4.3 EEPROM

The TCAN1167-Q1 has an internal EEPROM memory for storing device trim selections. This EEPROM is programmed in a test only mode utilizing an internal charge pump and is monitored with a CRC check by the digital core of the device.

The following sections provide the functional safety mechanisms that cover the EEPROM:

- Section 5.3.4.1

4.4 Power Control IP

The TCAN1167-Q1 contains several circuit blocks that are responsible for internal power management of the device. The power control unit encompasses two internal regulators to generate a 5V and 1.5V supply, from the VSUP supply, for the analog and digital circuitry needed for the device to operate. The power control unit contains a bandgap voltage and current reference to provide biasing to the internal analog circuits. There is an oscillator inside the device that generates clock signals that operate the digital core in a synchronous fashion.

4.5 Voltage Monitors

The TCAN1167-Q1 contains two internal voltage monitors to ensure the health of the supply voltages on the VSUP, and VCCOUT pins respectively. These monitors are used to provide voltage lock out features for othe internal circuits.

The following sections provide the functional safety mechanisms that cover the voltage monitors:

- Section 5.3.2.1

- Section 5.3.2.2
- Section 5.3.2.3
- Section 5.3.2.4

4.6 Thermal Shutdown

The TCAN1167-Q1 has a thermal shutdown feature that will disable the CAN transmitter and enter a thermal fail-safe mode should the silicon die overheat.

The following sections provide the functional safety mechanisms that cover the thermal shutdown:

- Section 5.3.1.2

4.7 Digital Input/Outputs

The TCAN1167-Q1 has 6 digital I/O pins, four of which are used to implement the SPI communications and the other two are utilized for the TXD and RXD signals for the CAN. These digital I/Os operate on the VCCOUT pin. Four of these input pins have integrated pull-up resistors that weakly bias them.

The following sections provide the functional safety mechanisms that cover the digital inputs and outputs:

- Section 5.3.5.1
- Section 5.3.5.2
- Section 5.3.5.3
- Section 5.3.5.4

5 TCAN1167-Q1 Management of Random Faults

For a functional safety critical development it is necessary to manage both systematic and random faults. The TCAN1167-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 theTCAN1167-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

The TCAN1167-Q1 utilizes interrupt registers for fault reporting. The global register is provided from the device whenever nCS is pulled low and a valid clock is provided on the SCLK pin. This register provides information on where to find other interrupts.

Table 5-1. INT_GLOBAL Register Field Descriptions (Address = 50h)

Bit	Field	Type	Reset	Description
7	GLOBALERR	RH	0b	Logical OR of all interrupts
6	INT_1	RH	0b	Logical OR of INT_1 register
5	INT_2	RH	0b	Logical OR of INT_2 register
4	INT_3	RH	0b	Logical OR of INT_3 register
3	INT_CANBUS	RH	0b	Logical OR of INT_CANBUS register
2-0	RSVD	R	0b	Reserved

Table 5-2. INT_1 Register Field Descriptions (Address = 51h)

Bit	Field	Type	Reset	Description
7	WD	R/W1C	0b	Watchdog event interrupt. NOTE: This interrupt bit will be set for every watchdog error event and does not reliy upon the Watchdog error counter
6	CANINT	R/W1C	0b	CAN bus wake up interrupt
5	LWU	R/W1C	0b	Local wake up
4	WKERR	R/W1C	0b	Wake error bit is set when the SWE timer has expired and the state machine has returned to Sleep mode
3	RSVD	R	0b	Reserved
2	CANSLNT	R/W1C	0b	CAN silent
1	RSVD	R	0b	Reserved
0	CANDOM	R/W1C	0b	CAN bus stuck dominant

Table 5-3. INT_2 Register Field Descriptions (Address = 52h)

Bit	Field	Type	Reset	Description
7	RSVD	R	0b	Reserved
6	PWRON	R/W1C	1b	Power on
5	OVCCOUT	R/W1C	0b	V_{CCOUT} overvoltage
4	UVSUP	R/W1C	0b	V_{SUP} undervoltage
3	RSVD	R	0b	Reserved
2	UVCCOUT	R/W1C	0b	V_{CCOUT} undervoltage
1	TSD	R/W1C	0b	Thermal Shutdown
0	TSDW	R/W1C	0b	Thermal Shutdown Warning

Table 5-4. INT_3 Register Field Descriptions (Address = 53h)

Bit	Field	Type	Reset	Description
7	SPIERR	R/W1C	0b	Sets when SPI status bit sets
6-0	RSVD	R	00h	Reserved

Table 5-5. INT_CANBUS Register Field Descriptions (Address = 54h)

Bit	Field	Type	Reset	Description
7:6	RESERVED	R	0b	Reserved. Reads return 0.
5	CANHCANL	R/W1C	0b	CANH and CANL shorted together
4	CANHBAT	R/W1C	0b	CANH shorted to Vbat
3	CANLGND	R/W1C	0b	CANL shorted to GND
2	CANBUSOPEN	R/W1C	0b	CAN bus open
1	CANBUSGND	R/W1C	0b	CAN bus shorted to GND or CANH shorted to GND
0	CANBUSBAT	R/W1C	0b	CAN bus shorted to Vbat or CANL shorted to Vbat

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 TCAN1167-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 CAN Communication

The TCAN1167-Q1 are enhanced high-speed CAN FD transceivers. These devices are configured using serial peripheral interface (SPI) in order to use all the features available. The TCAN1167-Q1 provides CAN FD transceiver function: differential transmit capability to the bus and differential receive capability from the bus. The device includes many protection features providing device and CAN network robustness. The CAN bus has two logical states during operation: recessive and dominant.

Recessive bus state is when the bus is biased to a common mode of about 2.5 V via the high resistance internal input resistors of the receiver of each node on the bus across the termination resistors. Recessive is equivalent to logic high and is typically a differential voltage 0.5 V or less between CANH and CANL. Recessive state is also the idle state.

Dominant bus state is when the bus is driven differentially by one or more drivers. Current is induced to flow through the termination resistors and generate a differential voltage on the bus. Dominant is equivalent to logic low and is a differential voltage on the bus greater than the minimum threshold of 0.9 V for a CAN dominant. A dominant state overwrites the recessive state.

The following sections provide the functional safety mechanisms that cover the CAN communication:

- Section 5.3.1.1
- Section 5.3.1.2
- Section 5.3.1.3
- Section 5.3.1.4
- Section 5.3.1.5

5.3.1.1 SM-1: CAN bus fault diagnostics

The TCAN1167-Q1 provides advanced bus fault detection. The device can determine certain fault conditions and set a status/interrupt flag so that the MCU can understand what the fault is. Detection takes place and is recorded if the fault is present during four dominant to recessive transitions with each dominant bit being > 1.5 us. As with any bus architecture where terminantion resistors are at each end not every fault can be specified to the lowest level, meaning exact location. The fault detection circuitry is monitoring the CANH and CANL pins (currents) to determine if there is a short to battery, short to ground, short to each other or opens. From a system perspective, the location of the device also determines what can be detected. See device datasheet for detailed description of the CAN bus fault diagnostic.

5.3.1.2 SM-2: Thermal Shutdown

The TCAN1167-Q1 has two trigger points for thermal events. The first is a thermal shutdown warning. Once the temperature exceeds this limit, an interrupt is issued. The second is the actual thermal shutdown (TSD) event.

This is a device preservation event. If the junction temperature of the device exceeds the thermal shut down threshold the device turns off the CAN transceiver and CAN transceiver circuitry thus blocking the signal to bus transmission path. A thermal shut down interrupt flag is set, and an interrupt is inserted so that the microprocessor is informed. If this event happens, other interrupt flags may be set as well. An example is a bus fault where the CAN bus is shorted to Vbat. When this happens, the digital core and SPI interface is still active. After a time of ≈ 300 ms the device checks the temperature of the junction. Thermal shutdown timer, t_{TSD}, starts when TSD fault event starts and checks to see if the TSD fault has been cleared every 300 ms. While in thermal shut down protected mode, a SPI write to change the device to either Normal or Standby mode is ignored while writes to change to sleep mode are accepted.

If the TSD event takes place and fail-safe mode is enabled, the same process takes place with and instead off thermal shut down protected stated the device enters fail-safe mode.

5.3.1.3 SM-3: CAN bus short circuit limiter, I_{OS}

These devices limit the short-circuit current when a CAN bus line is shorted. The CAN driver is current limited (dominant and recessive) with values of ± 115 mA for I_{OS_DOM} and ± 5 mA for I_{OS_REC}. During CAN communication the bus switches between dominant and recessive states; thus, the short-circuit current may be viewed either as the current during each bus state or as a DC average current. For system current and power considerations in the termination resistors and common mode choke ratings, the average short-circuit current should be used. The percentage dominant is limited by the TXD dominant time out and CAN protocol which has forced state changes and recessive bits such as bit stuffing, control fields, and inter frame space. These ensure there is a minimum recessive amount of time on the bus even if the data field contains a high percentage of dominant bits. See data sheet for more information.

5.3.1.4 SM-4: CAN TXD pin dominant state timeout; (t_{TXD_DTO})

The device supports dominant state time out (DTO). This is an internal function based upon the TXD path. The TXD DTO circuit prevents the local node from blocking network communication in event of a hardware or software failure where TXD is held dominant (LOW) longer than the time out period t_{TXD_DTO}. The TXD DTO circuit is triggered by a falling edge on TXD. If no rising edge is seen before the time out constant of the circuit, t_{TXD_DTO}, the CAN driver is disabled. This frees the bus for communication between other nodes on the network. The CAN driver is re-activated when a recessive signal (HIGH) is seen on TXD terminal; thus, clearing the

dominant time out. The receiver remains active and the RXD terminal reflects the activity on the CAN bus and the bus terminals is biased to recessive level during a TXD DTO fault.

5.3.1.5 SM-18: CAN protocol

CAN protocol has several mechanisms that will make sure the data provided is correct, such as CRC. If incorrect, the processor will disregard the CAN packet and often times has a mechanism to signal that the CRC that was received did not match the data.

5.3.2 Supply Voltage Rail Monitoring

There are two under voltage events monitored in the TCAN1167-Q1: VSUP and VCCOUT. VSUP is an input source for the TCAN1167-Q1, and VCCOUT is the LDO output that is used for the CAN transceiver as well as external power sourcing. These pins have have under voltage detection circuitry which places the device into a protected state if an under voltage fault occurs, UV_{SUP} and UV_{CCOUT}. This protects the bus during an under voltage event on these terminals. If VSUP is under voltage, the device loses the source needed to keep the internal regulators active. This causes the device to go into a state where communication between the microprocessor and the TCAN1167-Q1 is disabled. The TCAN1167-Q1 is not able to receive information from the bus; and thus, does not passs any signals from the bus, including any Bus Wake via BWRR signals to the microprocessor.

The following sections provide the functional safety mechanisms that cover the supply voltage rail monitoring:

- Section 5.3.2.1
- Section 5.3.2.2
- Section 5.3.2.3
- Section 5.3.2.4

5.3.2.1 SM-5: VCCOUT LDO short circuit current limit

The device has short circuit current limit (I_{L_VCCOUT}), which limits the maximum amount of current that can be sourced by the LDO. Depending on bus state/fault and ambient temperature, that prolonged time at I_{L_VCCOUT} could eventually trigger a thermal shutdown (TSD) event if the additional current load heats the die up enough.

5.3.2.2 SM-6: VSUP supply undervoltage; UV_{SUP}

The TCAN1167-Q1 monitors the VSUP supply rail for under voltage events (UV_{SUPF}). If this threshold is crossed, the filter time (t_{UVFLTR}) starts and must expire to be considered an under voltage event. A UV_{SUP} event will cause the INH pin to turn off. When VSUP is greater than UV_{SUPR}, the SWE timer will start as the device enters standby mode.

5.3.2.3 SM-7: VCCOUT undervoltage; UV_{CCOUT}

The TCAN1167-Q1 monitors the VCCOUT supply rail that powers the CAN transceiver. For undervoltage events, there is a filter time that the event must last longer than (t_{UVFLT}) for the t_{UVSLP} timer to start. Once the t_{UVSLP} timer expires and the under voltage condition is still present, the device enters sleep mode.

5.3.2.4 SM-8: VCC overvoltage; OV_{CCOUT}

Similarly to the VCCOUT undervoltage, there is a VCCOUT overvoltage flag. This is an interrupt/status flag that puts the device into a fail-safe state. While in fail-safe, the CAN transceiver is disabled to prevent affecting the bus.

5.3.3 SPI/Processor Communication

The TCAN1167-Q1 has several ways to determine if the communication between the processor and the device is functioning correctly.

The following sections provide the functional safety mechanisms that cover the SPI and processor communication:

- Section 5.3.3.1
- Section 5.3.3.2
- Section 5.3.3.3
- Section 5.3.3.4

5.3.3.1 SM-9: Timeout, Window or Q&A watchdog error

The TCAN1167-Q1 supports an integrated watchdog function. The devices provide a default window-based watchdog as well as a selectable time-out and question and answer (Q&A) watchdog using the SPI interface. The watchdog timer does not start until the first input trigger event when in normal and standby (when enabled) operational modes. The watchdog timer is off in sleep mode. The nINT pin will refelect a watchdog failure. See the datasheet for detailed description on watchdog capability.

5.3.3.2 SM-10: SPI communication error; SPIERR

The Serial Peripherial Interface (SPI) uses a standard configuration. Physically the digital interface pins are nCS (Chip Select Not), SDI (Serial Data In), SDO (Serial Data Out) and SCLK (Serial Clock). Each SPI transaction is a 16, 24 or 32 bits containing an address and read/write command byte followed by one to three data bytes.

Supporting two and three data bytes is accomplished utilizing burst read and write where the address is automatically incremented for the data along with the same number of clock cycles per bit. The data shifted out on the SDO pin for the transaction always starts with the Global Status Register (byte).

Once the SPI is enabled by a low on nCS, the device samples the input data on each rising edge of the SPI clock (SCLK). The data is shifted into an appropriate sized shift register and after the correct number of clock cycles the shift register is full and the SPI transaction is complete. For a write command code, the new data is written into the addressed register only after the exact number of clock cycles have been shifted in by SCLK and the nCS has a rising edge to deselect the device. For a burst write if there are 31 clock cycles of SCLK (1 clock cycle less than the full 3 byte write), the third byte write won't happen while the first two bytes write will be executed. If the correct number of clock cycles and data are not shifted in during one SPI transaction (nCS low), interrupts at 8'h50[7], 8'h50[4] and 8'h53[7], SPIERR, will be set.

5.3.3.3 SM-11: Scratchpad write/read

The TCAN1167-Q1 provide a memory scratchpad, 8'h0F[7:0] that makes it possible to write and read back data for verification of accuracy. This verifies the SPI interface to register space.

5.3.3.4 SM-12: Sleep Wake Error Timer; $t_{INACTIVE}$

The sleep wake error (SWE) timer is a timer used to determine if specific external and internal functions are working. Upon power up, POR or UV_{SUP} event, the SWE timer starts, $t_{INACTIVE}$, and the processor has typically 4.5 minutes to configure the device, clear the PWRON flag or change the device to normal or listen mode. This feature cannot be disabled for power up. If the device has not had the PWRON flag cleared or been placed into normal or listen mode, it enters sleep mode and sets the WKERR flag.

5.3.4 Device Internal EEPROM

The TCAN1167-Q1 uses an internal EEPROM for certain performance trimming. Upon power up, the device loads an internal register from the EEPROM and performs a CRC check. This is repeated when the device leaves sleep mode or fail-safe mode due to a wake event.

The following sections provide the functional safety mechanisms that cover the EEPROM:

- Section 5.3.4.1

5.3.4.1 SM-13: Internal memory CRC; CRC_EEPROM

The CRC_EEPROM interrupt is set when the internal EEPROM used for trimming has a CRC error. Upon power up the device loads an internal register from the EEPROM and performs a CRC check. If an error is present after eight attempts of loading valid data the CRC_EEPROM interrupt will be set. This will indicate an error that may impact device performance. This is repeated when the device leaves sleep mode or fail-safe mode due to a wake event. The device will perform a CRC check on the internal registers loaded from the EEPROM. If there is an error the device will reload the registers from the EEPROM. If there is a CRC error the device will attempt to load the internal registers up to eight times. After the eighth attempt the CRC_EEPROM interrupt flag will be set. This will indicate an error that may impact the device performance.

5.3.5 Floating Pins

There are internal pull ups on critical terminals to place the device into known states if the terminal floats.

Table 5-6. Terminal Fail-Safe Biasing

TERMINAL	PULL-UP or PULL-DOWN	COMMENT
TXD	Pull-up	Weakly biases TXD toward recessive to prevent bus blockage or TXD DTO triggering
nCS	Pull-up	Weakly biases nCS high to prevent un-intended SPI communication
SCLK	Pull-down	Weakly biased to ground
INH	Pull-down	Weakly biased to ground

The following sections provide the functional safety mechanisms that cover floating pins:

- Section 5.3.5.1
- Section 5.3.5.2
- Section 5.3.5.3
- Section 5.3.5.4

5.3.5.1 SM-14: SCLK internal pull-down to GND

In case of open (floating pins), the default state of the SCLK pin is provided by an integrated pull-down resistor that weakly biases the pin to GND.

5.3.5.2 SM-15: nRST and SDI internal pull-up to VCCOUT

In case of open (floating pins), the default state of the nRST and SDI pins is provided by integrated pull-up resistors that weakly biases the pin to VCCOUT.

5.3.5.3 SM-16: nCS internal pull-up to VCCOUT

In case of open (floating pins), the default state of the nCS pin is provided by an integrated pull-up resistor that weakly biases the pin to VCCOUT.

5.3.5.4 SM-17: TXD internal pull-up to VCCOUT

In case of open (floating pins), the default state of the TXD pin is provided by an integrated pull-up resistor that weakly biases the pin to VCCOUT.

5.4 TCAN1167-Q1 Component Overview

The TCAN1167-Q1 is a high speed Controller Area Network (CAN) system basis chip (SBC) that meets the physical layer requirements of the ISO 11898-2:2016 high speed CAN specification. The transceiver supports both classical CAN and CAN FD networks up to 8 megabits per second (Mbps).

The TCAN1167-Q1 supports a wide input supply range and integrates a 5-V LDO output. The 5-V LDO output (V_{CCOUT}) supplies the CAN transceiver voltage internally as well as additional current externally.

The TCAN1167-Q1 allows for system-level reductions in battery current consumption by selectively enabling the various power supplies that may be present on a system via the INH output pin. This allows an ultra-low-current sleep state where power is gated to all system components except for the TCAN1167-Q1, while monitoring the CAN bus. When a wake-up event is detected, the TCAN1167-Q1 initiates system start-up by driving INH high.

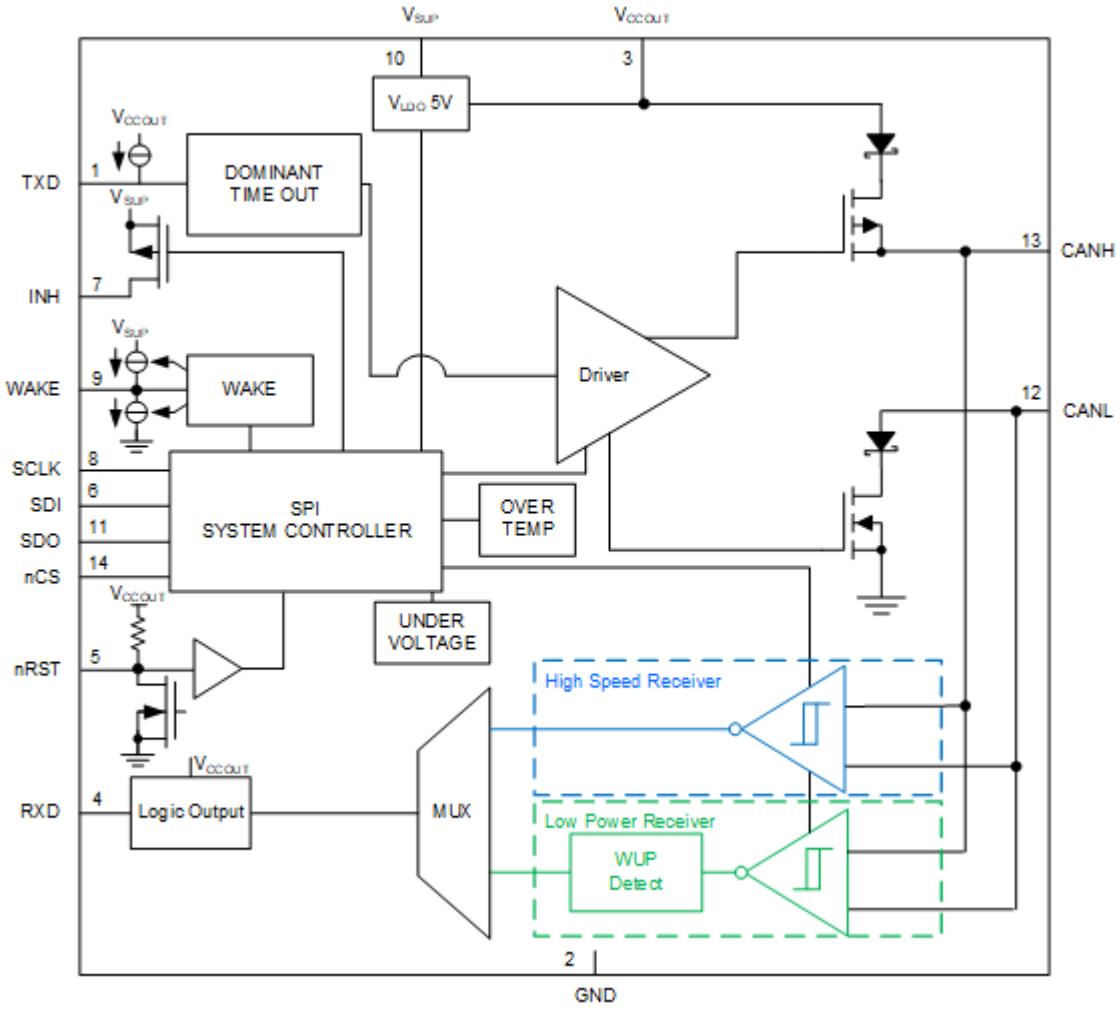

Figure 5-1. TCAN1167-Q1 Block Diagram

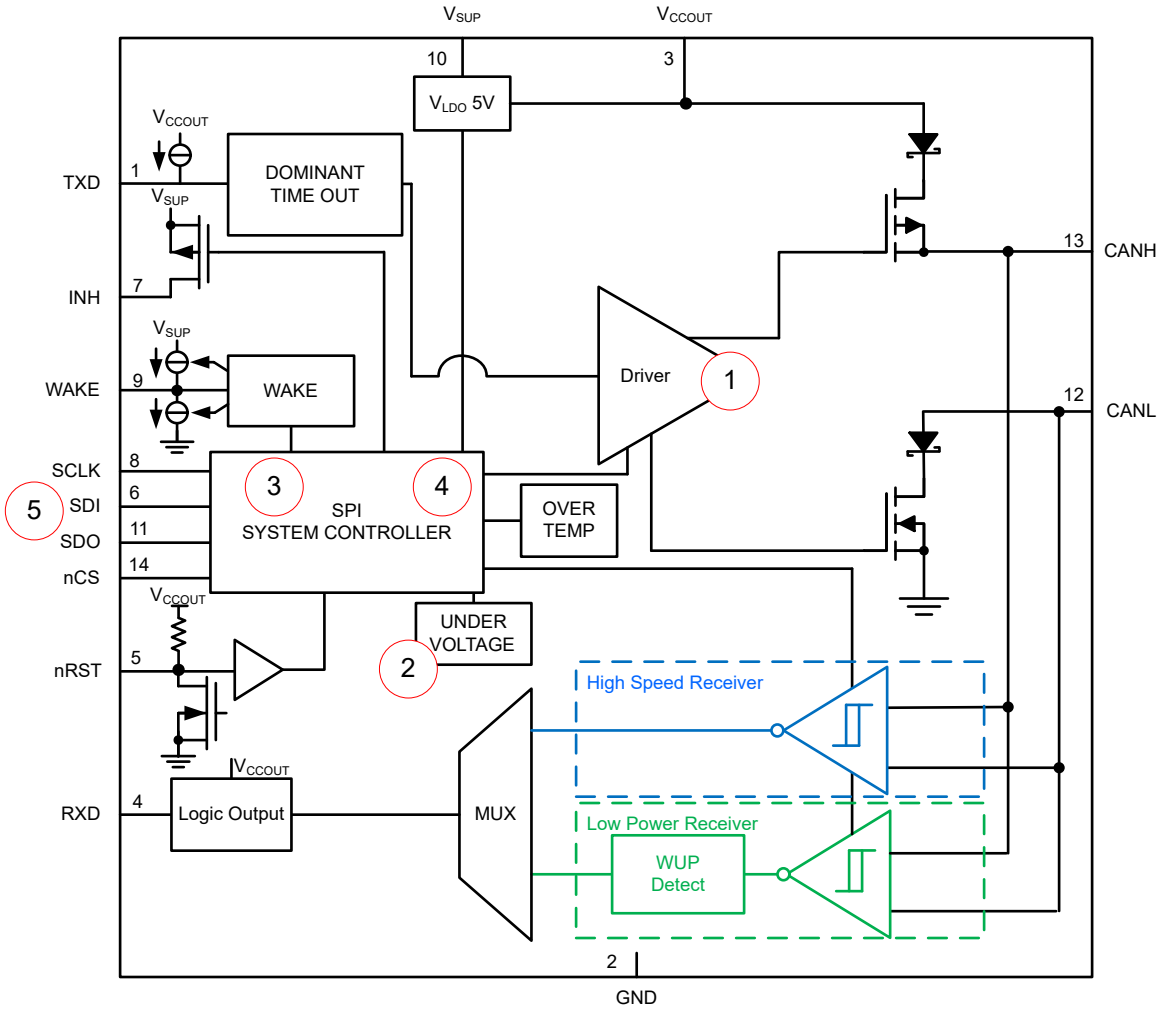

Figure 5-2. Potential Failure Points

Table 5-7. Potential Failure Points and Safety Mechanisms

Potential Failure Point	Potential Failure Point Description	Section
1	CAN communication	See Section 5.3.1.1, Section 5.3.1.2, Section 5.3.1.3, Section 5.3.2.1
2	Supply voltage rail monitoring	See Section 5.3.2.1, Section 5.3.2.2, Section 5.3.2.3, Section 5.3.2.4
3	SPI/Processor communication	See Section 5.3.1.4, Section 5.3.3.1, Section 5.3.3.2, Section 5.3.3.3, Section 5.3.3.4, Section 5.3.4.1
4	EEPROM	See Section 5.3.4.1
5	Floating pins	See Section 5.3.5.1, Section 5.3.5.2, Section 5.3.5.3, Section 5.3.5.4

5.4.1 Targeted Applications

The TCAN1167-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:

- General purpose applications containing a processor and external power.

Figure 5-3 shows a generic block diagram for a general purpose system. This diagram is only an example and may not represent a complete system.

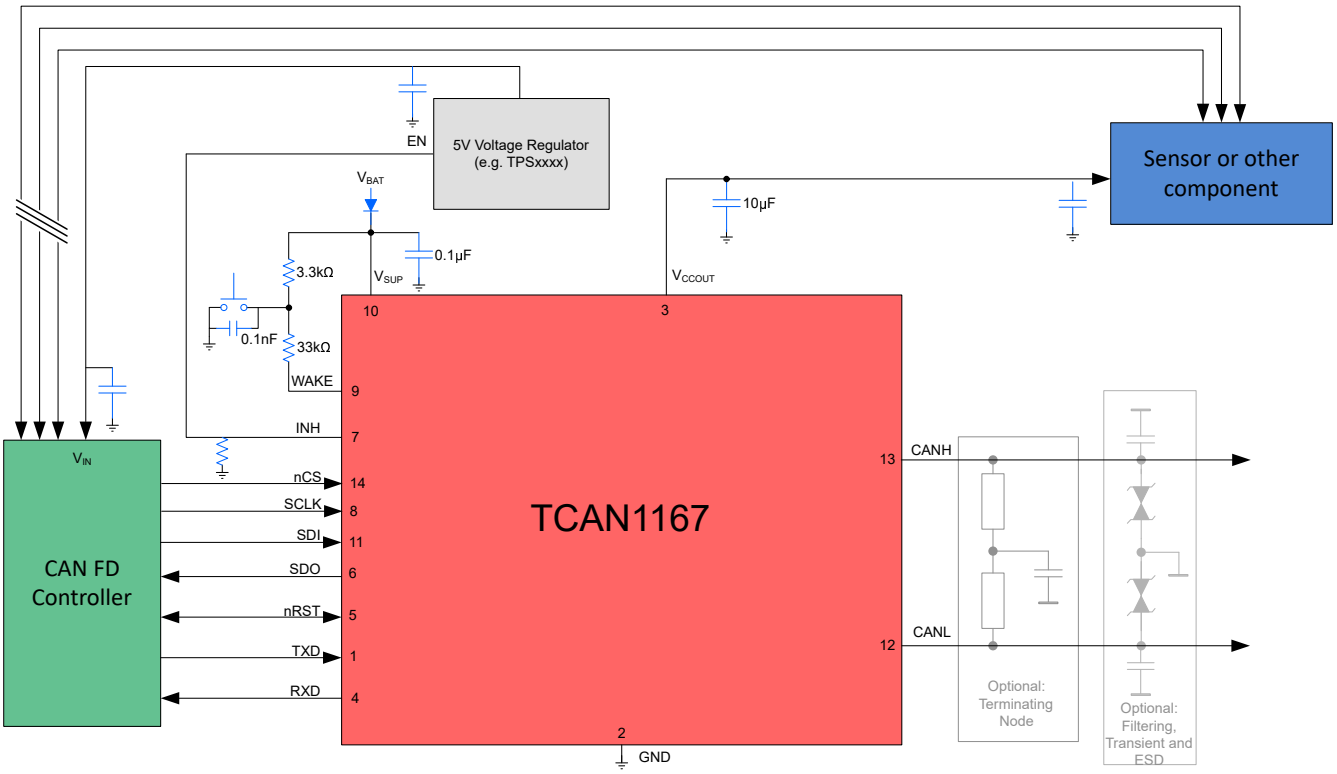

Figure 5-3. TCAN1167-Q1 Typical Application

5.4.2 Hardware Component Functional Safety Concept

The TCAN1167-Q1 was developed using Texas Instruments Incorporated Quality Managed product development process and qualified according to AEC Q100 Grade 1. The process falls under TI's Functional Safety Quality-Managed, per ISO 26262:2018 as a Safety Element out of Context (SEooC).

5.4.3 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 TCAN1167-Q1 Functional Safety Analysis was done under the following system assumptions:

- **[SA_1]** The system integrator shall not exceed the recommended operating conditions in the component data sheet.
- **[SA_2]** A typical application is as shown in Figure 5-3

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.

A Summary of Recommended Functional Safety Mechanism Usage

Table A-2 summarizes the functional safety mechanisms present in hardware or recommend for implementation in software or at the system level as described in Section 4. Table A-1 describes each column in Table A-2 and gives examples of what content could appear in each cell.

Table A-1. Legend of Functional Safety Mechanisms

Functional Safety Mechanism	Description
TI Safety Mechanism Unique Identifier	A unique identifier assigned to this safety mechanism for easier tracking.
Safety Mechanism Name	The full name of this safety mechanism.
Safety Mechanism Category	**Safety Mechanism** - This test provides coverage for faults on the primary function. It may also provide coverage on another safety mechanism. **Test for Safety Mechanism** - This test provides coverage for faults of a safety mechanism only. It does not provide coverage on the primary function. **Fault Avoidance** - This is typically a feature used to improve the effectiveness of a related safety mechanism.
Safety Mechanism Type	Can be either hardware, software, a combination of both hardware and software, or system. See Section 5.2 for more details.
Safety Mechanism Operation Interval	The timing behavior of the safety mechanism with respect to the test interval defined for a functional safety requirement / functional safety goal. Can be either continuous, or on-demand. **Continuous** - the safety mechanism constantly monitors the hardware-under-test for a failure condition. **Periodic or On-Demand** - the safety mechanism is executed periodically, when demanded by the application. This includes Built-In Self-Tests that are executed one time per drive cycle or once every few hours.
Test Execution Time	Time period required for the safety mechanism to complete, not including error reporting time. Note: Certain parameters are not set until there is a concrete implementation in a specific component. When component specific information is required, the component data sheet should be referenced. Note: For software-driven tests, the majority contribution of the Test Execution Time is often software implementation-dependent.
Action on Detected Fault	The response that this safety mechanism takes when an error is detected. Note: For software-driven tests, the Action on Detected Fault may depend on software implementation.
Time to Report	Typical time required for safety mechanism to indicate a detected fault to the system. Note: For software-driven tests, the majority contribution of the Time to Report is often software implementation-dependent.

Table A-2. Summary of Functional Safety Mechanisms

TI Safety Mechanism Unique Identifier	Safety Mechanism Name	Safety Mechanism Category	Safety Mechanism Type	Safety Mechanism Operation Interval	Test Execution Time	Action on Detected Fault	Time to Report
SM-1	CAN bus fault	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - In normal mode	150 ns	Interrupt bits in 8'h50[7], 8'h50[3], and register 8'h54[6:0] indicates a CAN bus fault.	50 ns
SM-2	Thermal shutdown; TSD	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	4.4 µs	Turn off the CAN transceiver and set the interrupt bit registers 8'h50[7], 8'50[5], and 8'h52[1] indicating junction temperature exceeded and enters TSD protected mode.	1.1 µs

Table A-2. Summary of Functional Safety Mechanisms (continued)

TI Safety Mechanism Unique Identifier	Safety Mechanism Name	Safety Mechanism Category	Safety Mechanism Type	Safety Mechanism Operation Interval	Test Execution Time	Action on Detected Fault	Time to Report
SM-3	CAN bus short circuit limiter, I_{OS}	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	N/A	Limits the current through the CANH and CANL pins.	N/A
SM-4	CAN TXD pin dominant state timeout; t_{TXD_DTO}	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - in normal mode	3.5 ms	The device will turn off the CAN transceiver and indicate the fault at 8'h50[7], 8'h50[6], 8'h51[0].	1.1 µs
SM-5	VCCOUT LDO short circuit current limit	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	N/A	Limits the current through the VCCOUT pin.	N/A
SM-6	VSUP supply undervoltage; UV_{SUP}	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	2.2 µs	Device enters programmed mode, sleep or fail-safe mode, sets interrupt registers 8'h50[7], 8'h50[5] and 8'h52[4] and indicates UVSUP condition.	1.1 µs
SM-7	VCCOUT undervoltage; UV_{CCOUT}	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	330 ms	Device enters reset mode, sets interrupt registers 8'h50[7], 8'h50[5] and 8'h52[2] and indicates UVCCOUT condition.	1.1 µs
SM-8	VCCOUT overvoltage; OV_{CCOUT}	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	2.2 µs	Device enters fail-safe mode, sets interrupt registers 8'h50[7], 8'h50[5] and 8'h52[5] and indicates OVCCOUT condition.	1.1 µs
SM-9	Timeout, Window or Q&A watchdog error	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous	Programmable	Increments WD error counter and if exceeded programmed value will set WD interrupt, and hold nRST low for $t_{nRST(warm)}$ and indicate back to MCU with nINT pin.	1.1 µs
SM-10	SPI communication error; SPIERR	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous	50 ns after rising edge of nCS	The device shall monitor MCU SPI communication utilizing clock count check and if there are too many or not enough clock signals the MCU write to the device will be blocked and 8'h50[7], 8'h50[4] and 8'h53[7].	1.1 µs
SM-11	Scratchpad write/ read	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous when MCU is initialized	SPI clock rate dependent as a write plus data followed by a read and data required	Using the scratchpad, 8'h0F[7:0], by the processor makes it possible to write and read back data to determine SPI communication is valid.	N/A

Table A-2. Summary of Functional Safety Mechanisms (continued)

TI Safety Mechanism Unique Identifier	Safety Mechanism Name	Safety Mechanism Category	Safety Mechanism Type	Safety Mechanism Operation Interval	Test Execution Time	Action on Detected Fault	Time to Report
SM-12	Sleep Wake Error Timer; $t_{INACTIVE}$	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous	5 min	If $t_{INACTIVE}$ times out, device will enter sleep mode and will indicate the fault at 8'h50[7], 8'h50[4] and 8'h53[5].	1.1 µs
SM-13	Internal memory CRC; CRC_EEPROM	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Periodic - Exiting fail-safe and sleep modes	425 µs	The device will attempt to load and CRC check the EEPROM up to eight times and if fail it will indicate the the fault at 8'h50[7], 8'h50[4] and 8'h53[0].	1.1 µs
SM-14	SCLK internal pull-down to GND	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous	N/A	Avoids floating pin	N/A
SM-15	nRST and SDI internal pull-up to VCCOUT	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	N/A	Avoids floating pin	N/A
SM-16	nCS internal pull-up to VCCOUT	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	N/A	Avoids floating pin	N/A
SM-17	TXD internal pull-up to VCCOUT	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Continuous - all modes except for sleep	N/A	Avoids floating pin	N/A
SM-18	CAN protocol	Safety Mechanism	Component Hardare Functional Safety Mechanisms	Periodic	N/A	CAN protocol has several mechanism that will make sure the data provided is correct, like CRC. If incorrect the processor will disregard the CAN packets	N/A

B 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.

B.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.

B.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 B-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
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

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

Functional Safety Lifecycle Activity(1)	TI Execution	Customer Execution
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, ask our TI E2E™ support experts.

B.3 Information Provided

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

Table B-2. Product Functional Safety Documentation

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

C Revision History

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

DATE	REVISION	NOTES
December 2021	*	Initial Release

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), 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 will 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 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.

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

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265