Application Note

Functional Safety Manual for TLIN1431x-Q1

Table of Contents

List of Figures

List of Tables

1 Introduction

This document is a functional safety manual for the Texas Instruments TLIN1431-Q1 component. The specific orderable part numbers supported by this functional safety manual are as follows:

- TLIN14313RGYQ1
- TLIN14315RGYQ1

This functional safety manual provides information needed by system developers to help in the creation of a functional safety system using a TLIN1431x-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 TLIN1431-Q1 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 TLIN1431-Q1 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 TLIN1431x-Q1 component. For more information, refer to the TLIN1431-Q1 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 http://www.ti.com/technologies/functional-safety/overview.html.

Trademarks

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

2 TLIN1431x-Q1 Hardware Component Functional Safety Capability

This section summarizes the component functional safety capability.

This hardware component was developed according to the relevant requirements of ISO 26262:2018. FIT rates and failure mode distributions are provided as part of the Functional Safety Analysis Report for customers 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 elements" (ISO 26262-8:2016 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. Components being designed for functional safety applications 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.

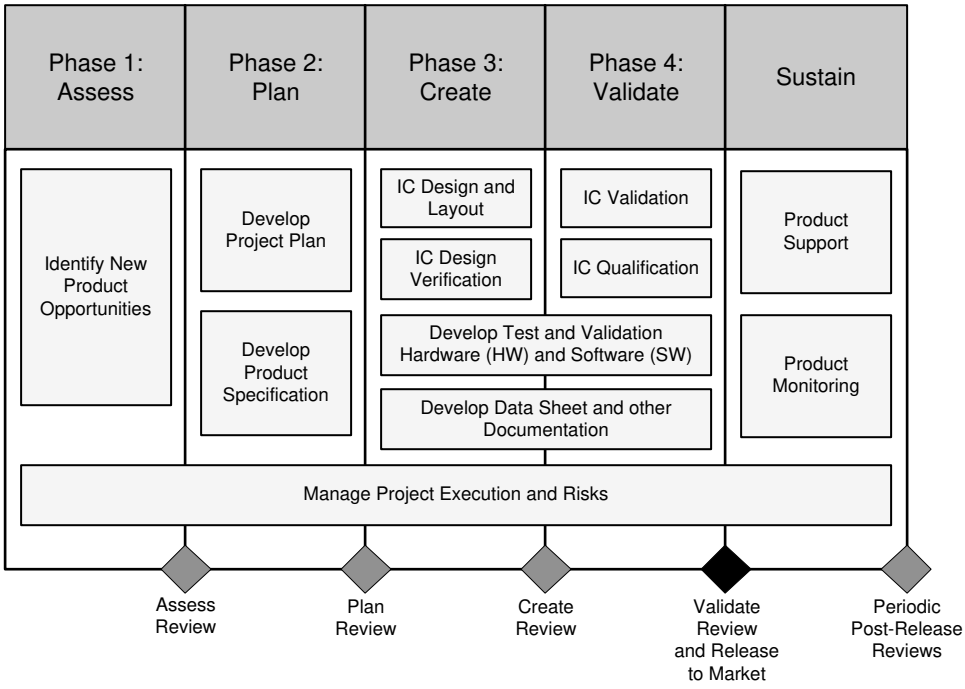


Figure 3-1. TI New-Product Development Process

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 B 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)
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		

4 TLIN1431x-Q1 Component Overview

The TLIN1431x-Q1 LIN transceiver is a Local Interconnect Network (LIN) physical layer transceiver, compliant to LIN 2.0, LIN 2.1, LIN 2.2, LIN 2.2A and ISO/DIS 17987–4 with integrated wake-up and protection features. The LIN bus is a single-wire, bi-directional bus that typically is used in low speed in-vehicle networks with data rates that range up to 20 kbps. The device LIN receiver works up to 100 kbps supporting in-line programming in normal mode. When the device is placed into fast mode both the transmitter and receiver supports up to 200 kbps. The device converts the LIN protocol data stream on the TXD input into a LIN bus signal using a current-limited wave-shaping driver which reduces electromagnetic emissions (EME). The receiver converts the data stream to logic level signals that are sent to the microprocessor through the RXD pin. The LIN bus has two states: dominant state (voltage near ground) and recessive state (voltage near battery). In the recessive state, the LIN bus is pulled high by the internal pull-up resistor (45 kΩ) and a series diode.

Ultra-low current consumption is possible using the sleep mode. The TLIN1431x-Q1 provides three methods to wake up from sleep mode: EN pin, WAKE pin and LIN bus in pin control mode and two in SPI control mode, WAKE pin and LIN bus. The device integrates a low dropout voltage regulator with a wide input from VSUP providing 5 V ±2.5% or 3.3 V ±2.5% with up to 125 mA of current depending upon system implementation.

The TLIN1431x-Q1 integrates a window based watchdog supervisor which has a programmable delay and window ratio determined by pin strapping or SPI communication. The device watchdog is controlled by pin configuration or SPI depending upon the state of pin 7 at power up. At power up, if pin 7 is externally pulled to ground, the device is configured for pin control of the device. If pin 7 is left floating or pulled up to VCC the pin becomes the nCS pin from the processors for SPI communication. If the pin is left floating at power up, the internal pull up configures the device for 3.3 V SPI control. If the processor uses 5 V IO a 500 kΩ pull up resistor to VCC is used for the 5 V version of the device. This allows the 5 V version of the device to work with both 3.3 V SPI or 5 V SPI. SPI communication is used for device configuration. In pin configuration nRST is asserted high when VCC increases above UVCC and stays high as long as VCC is above this threshold.

When the watchdog is controlled by the device pins, the state of the WDT pin determines the window time. WDI is used as the watchdog input trigger which is expected in the open window. If a watchdog error event takes place, the nWDR pin goes low to reset the processors. When using SPI, writing FFh to register 15h, WD_INPUT_TRIG, during the open window restarts the watchdog timer. The supervised processor must trigger the WDI pin or WD_INPUT_TRIG register within the defined window. When using SPI, the nRST pin can become the watchdog event output trigger for the processor if programmed this way but the nRST function are lost. The watchdog timer has a long initial window when entering standby, normal and fast modes that a watchdog input trigger is expected.

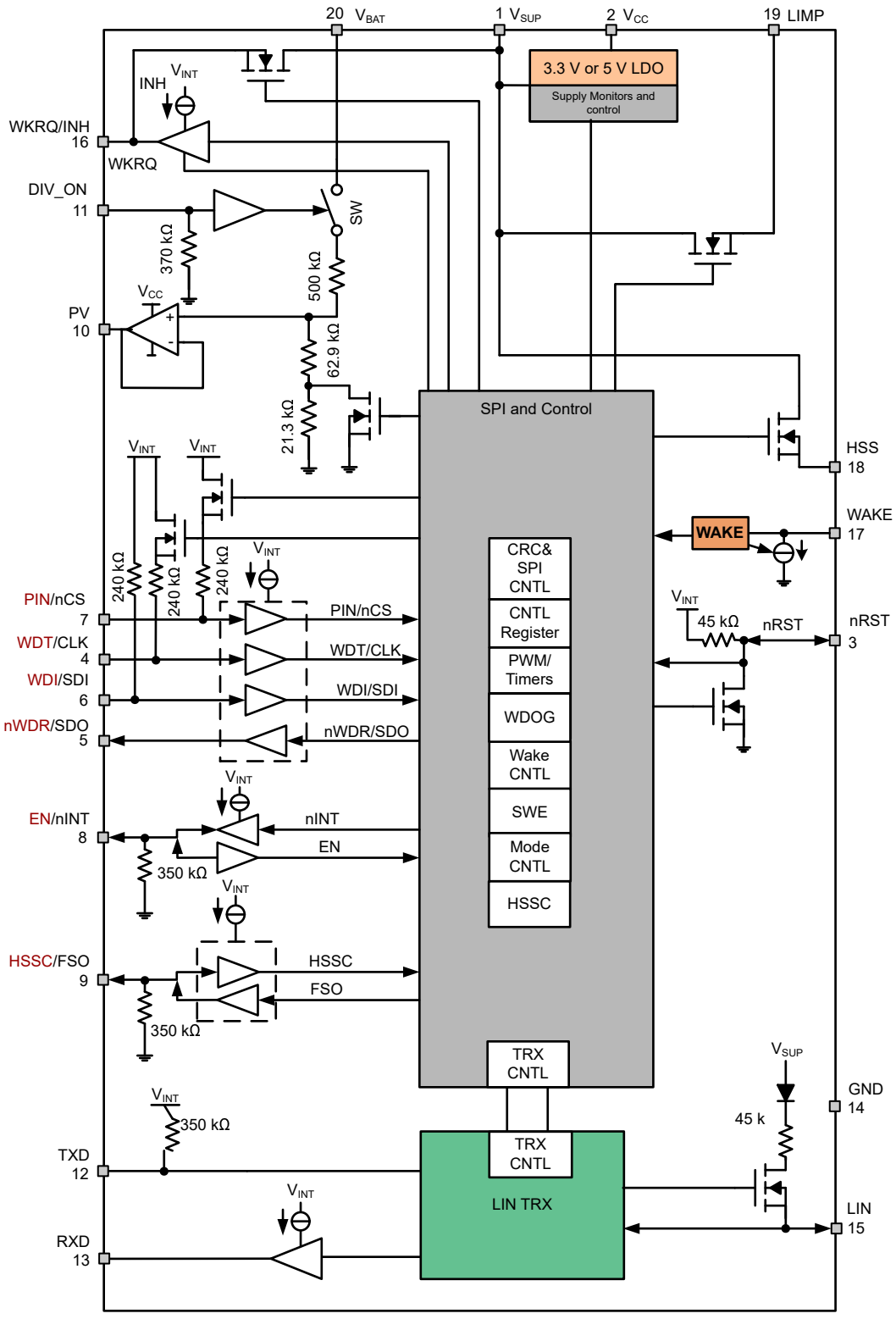


Figure 4-1. TLIN1431x-Q1 Block Diagram

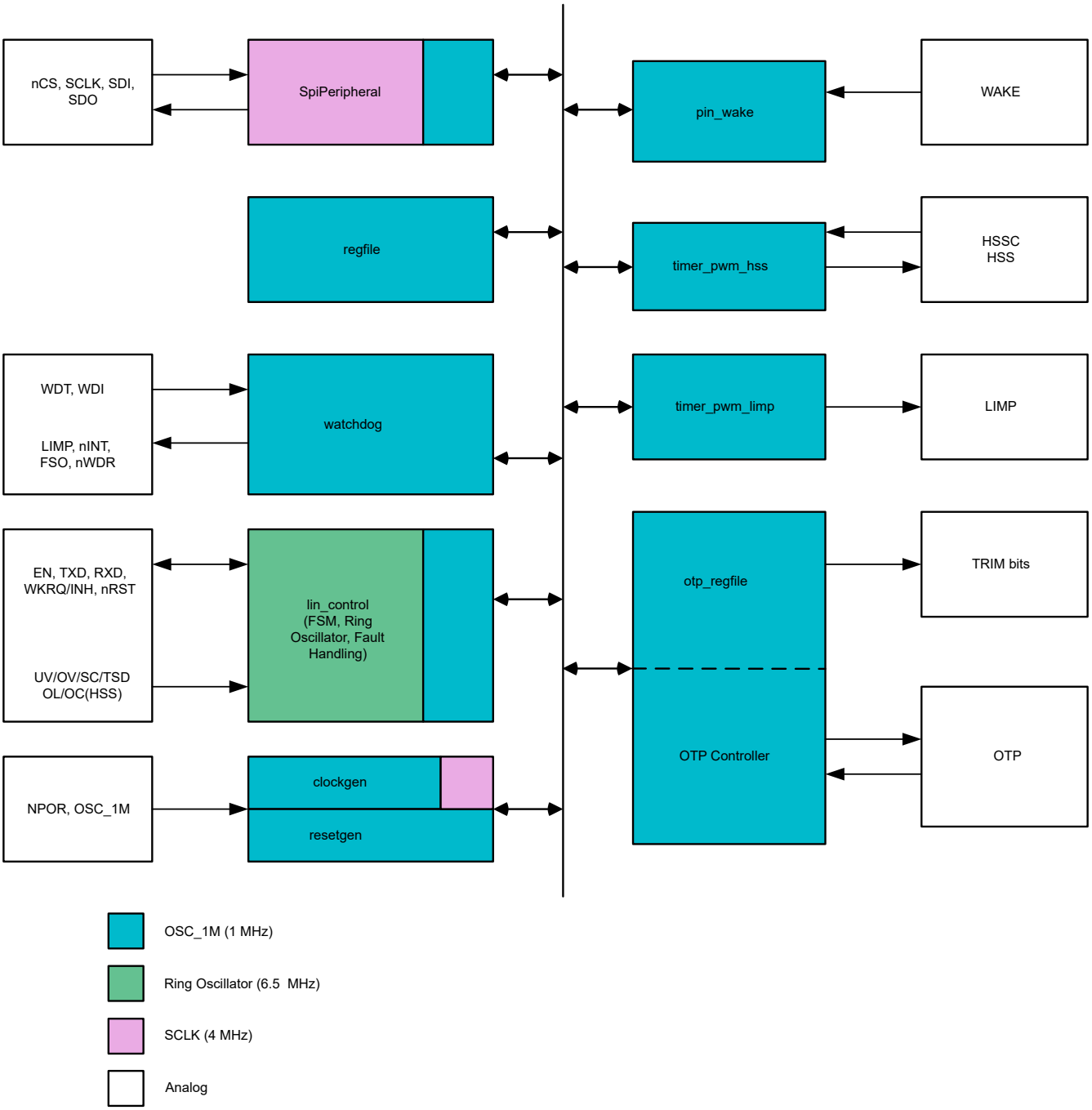


Figure 4-2. Digital Core Block Diagram

4.1 Targeted Applications

The TLIN1431x-Q1 component is targeted at general-purpose functional safety applications utilizing SPI control. 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 known 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 utilizing serial peripheral interface (SPI) to control the TLIN1431-Q1.

Figure 4-3 shows a generic block diagram for a general purpose system. This diagram is only an example and may not represent a complete system. Figure 4-4 provides potential failure points that have diagnostic or test ability mechanisms.

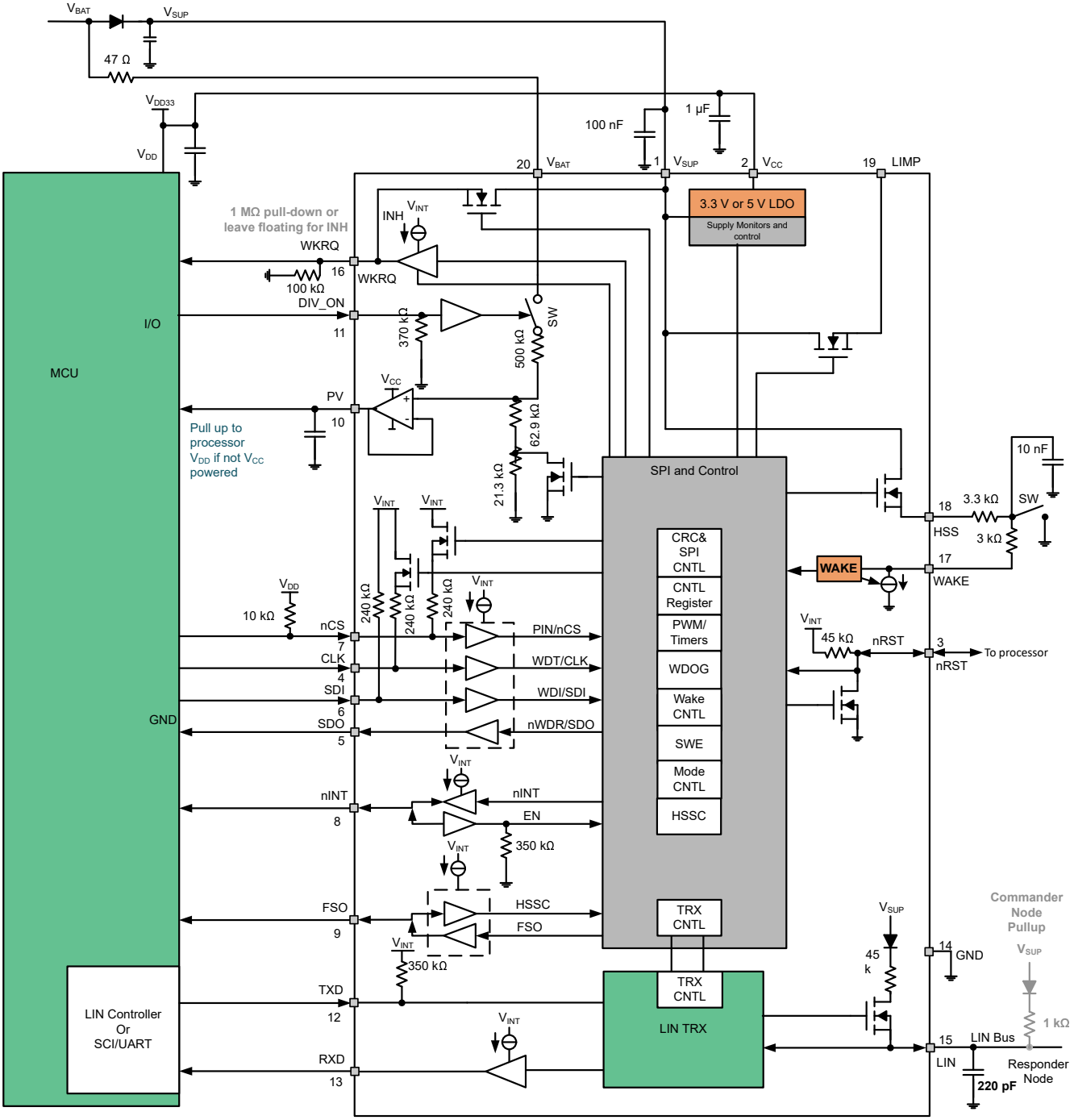


Figure 4-3. Typical Application - SPI Control

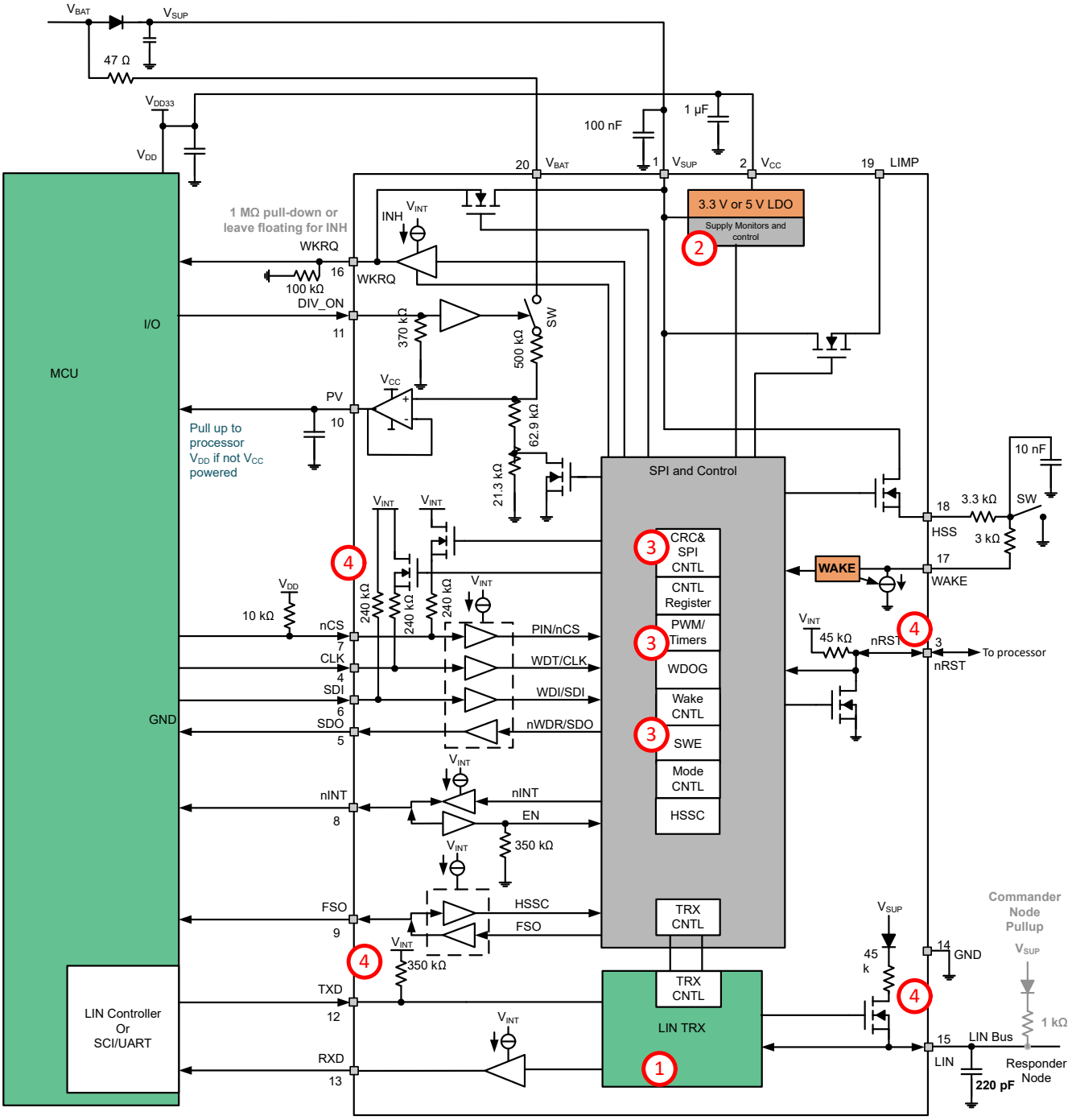


Figure 4-4. Typical Application - SPI Control Potential Failure Points

Table 4-1. SPI Control Potential Failure Points and Safety Mechanisms

Potential Failure Point from Figure 4-4	Potential Failure Point Description	Section
1	LIN communication	Section 6.3.1
2	Supply voltage rail monitoring	Section 6.3.2
3	SPI/Processor communication	Section 6.3.3
4	Floating pins	Section 6.3.4

4.2 Hardware Component Functional Safety Concept

The TLIN1431x-Q1 were 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).

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 6.3.

The 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 system integrator shall not exceed recommended operating conditions in the component data sheet
- **SA_3:** The system integrator uses SPI control, Pin 7 is either high-Z for 3.3 V I/O or pulled up to processor I/O voltage rail if 5 V for I/O is needed.
- **SA_4**: Typical applications as shown in Figure 4-3 .
- **SA_5**: The non-SPI communication control function is not used in the SEooC and is considered non-safety related.

Note

For functional safety applications, SPI communication control is to be used.

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.

5 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.

5.1 LIN Transceiver

The TLIN1431x-Q1 provides a Local Interconnect Network (LIN) transceiver physical layer used to communicate a node processor and the LIN bus. The LIN protocol layer has additional inherent mechanisms for data accuracy.

The following tests can be applied as functional safety mechanisms for this module (to provide diagnostic coverage on a specific function):

- SM-1: LIN TXD pin dominant state timeout; t_{TXD_DTO}
- SM-2: LIN bus stuck dominant
- SM-3: LIN bus short circuit limiter, I_{BUS_LIM}
- SM-20: LIN internal pull-up to VSUP
- SM-22: LIN protocol

5.2 Digital Core

The TLIN1431x-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, watchdog timer, and the sleep wake error timer. The digital core also interfaces with the internal OTP memory and has CRC checking capability to ensure good data retention.

The following tests can be applied as functional safety mechanisms for this module (to provide diagnostic coverage on a specific function):

- SM-9: Standby long timeout WD; t_{INITWD}
- SM-10: Timeout or Window watchdog error - Normal mode
- SM-11: SPI CRC Error
- SM-12: SPI communication error; SPIERR
- SM-13: Scratchpad write/read
- SM-14: Sleep Wake Error Timer; t_{INACT_FS}

5.3 Power Control IP

The TLIN1431x-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 3.6V supply, from the V_{SUP} 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.

The TLIN1431x-Q1 contains four internal voltage monitors to ensure the health of the supply voltages on the V_{SUP}, and V_{CC} pins respectively. These monitors are used to provide voltage lock out features for other internal circuits. The undervoltage V_{SUP} circuit monitors the V_{SUP} supply directly whereas the nPOR circuit monitors the internal digital supply voltage that is generated from V_{SUP}.

The TLIN1431x-Q1 has a voltage regulator output on the V_{CC} pin that is capable of sourcing up to 125 mA at either 3.3V or 5V. The voltage regulator has internal current limiting features and a short to ground detection flag to support diagnostic features. There is also another internal voltage regulator that is used to run the SPI pins at the appropriate voltage level. The V_{CC} supply voltage has both an undervoltage and overvoltage circuit monitoring the output.

The TLIN1431x-Q1 has a thermal shutdown feature that disables the LIN transmitter and voltage regulator and enter a thermal fail-safe mode should the silicon die overheat.

The following tests can be applied as functional safety mechanisms for this module (to provide diagnostic coverage on a specific function):

- SM-4: V_{CC} and Transceiver thermal shutdown; TSD
- SM-5: V_{CC} under voltage; UV_{CC}
- SM-6: V_{CC} over-voltage; OV_{CC}
- SM-7: V_{CC} short to ground; V_{CCSC}
- SM-8: V_{SUP} supply under voltage; UV_{SUP}

5.4 Digital Input/Output Pins and High-side Switch

The TLIN1431x-Q1 has 8 digital I/O pins, four of which are used to implement the SPI communications or watchdog functionality, two are utilized for the TXD and RXD signals for the LIN, and the last two are used for nRST and nINT interrupt functionality. Five of these input pins have integrated pull-up resistors that weakly bias them. The TLIN1431x-Q1 provides a reverse polarity protected resistor divider connected to VBAT with fast response times. The divider ratio is based upon the LDO output voltage value. The voltage divider is activated by a high on the DIV_ON pin.

The TLIN1431x-Q1 provides a high-side switch supporting up to a 100 mA load. The switch supports open load detection and over current detection. In SPI mode, it can be programmed to support a PWM. The HSS can be configured to use one of two timers that allows it to work with the WAKE pin. This supports cyclic sensing for sleep mode thus reducing sleep mode current.

The following tests can be applied as functional safety mechanisms for this module (to provide diagnostic coverage on a specific function):

- SM-15: CLK internal pull-up to V_{INT}
- SM-16: SDI internal pull-up to V_{INT}
- SM-17: nCS internal pull-up to V_{INT}
- SM-18: DIV_ON internal pull-down
- SM-19: TXD internal pull-up to V_{INT}
- SM-21: nRST internal pull-up to V_{CC}
- SM-23: HSS Over current detect
- SM-24: HSS Open load detection

6 TLIN1431x-Q1 Management of Random Faults

For a functional safety critical development it is necessary to manage both systematic and random faults. The TLIN1431x-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 the TLIN1431x-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.

6.1 Fault Reporting

The TLIN1431x-Q1 when configured for SPI control utilizes interrupt registers for fault reporting. The global interrupt register, 8'h50[7:0] provides information on where to find other interrupts that provide more detailed information on a fault, registers 8'h51 - 8'h53 and 8'h5A.

Table 6-1. INT_GLOBAL Register Field Descriptions (Address = 50h)

Bit	Field	Type	Reset	Description
7	GLOBALERR	RH	1b	Logical OR of all interrupts
6	INT_1	RH	0b	Logical OR of INT_1 register
5	INT_2	RH	1b	Logical OR of INT_2 register
4	INT_3	RH	0b	Logical OR of INT_3 register
3	RSVD	R	0b	Reserved
2	INT_4	RH	0b	Logical OR of INT_4 register
1-0	RSVD	R	0b	Reserved

Table 6-2. INT_1 Register Field Descriptions (Address = 51h)

Bit	Field	Type	Reset	Description
7	WD	R/W1C	0b	Watchdog event interrupt. NOTE: This interrupt bit is set for every watchdog error event and does not rely upon the Watchdog error counter
6	RSVD	R	0b	Reserved
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
3-0	RSVD	R	0b	Reserved

Table 6-3. INT_2 Register Field Descriptions (Address = 52h)

Bit	Field	Type	Reset	Description
7	SMS	R/W1C	0b	Sleep mode status flag. Only sets when sleep mode is entered by a fault
6	PWRON	R/W1C	1b	Power on
5	OVCC	R/W1C	0b	V_{CC} overvoltage
4	UVSUP	R/W1C	0b	V_{SUP} undervoltage
3	RSVD	R	0b	Reserved
2	UVCC	R/W1C	0b	V_{CC} undervoltage
1	TSD_VCC_LIN	R/W1C	0b	Thermal Shutdown due to VCC or LIN
0	TSD_HSS_LIMP	R/W1C	0b	Thermal Shutdown due to HSS or LIMP

Table 6-4. INT_3 Register Field Descriptions (Address = 53h)

Bit	Field	Type	Reset	Description0b
7	SPIERR	R/W1C	0b	Sets when SPI status bit sets
6	RSVD	R	0b	Reserved
5	FSM	R/W1C	0b	Entered fail-safe mode. Can be cleared while in failsafe mode.
4	CRCERR	R/W1C/U	0b	SPI CRC error detected
3	VCCSC	R/W1C/U	0b	V_{CC} short detected
2	RSRT_CNT	R/W1C/U	0b	Restart counter exceeded programmed count
1-0	RSVD	R	0b	Reserved

Table 6-5. INT_4 Register Field Descriptions (Address = 5Ah)

Bit	Field	Type	Reset	Description
7	LIN_WUP	R/W1C	0b	LIN bus wake
6	LIN_DTO	R/W1C	0b	LIN dominant state timeout
5-4	RSVD	R	00b	Reserved
3	HSSOC	R/W1C	0b	High side switch over current
2	HSSOL	R/W1C	0b	High side switch open load
1-0	RSVD	R	00b	Reserved

6.2 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 TLIN1431x-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.

6.3 Description of Functional Safety Mechanisms

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

6.3.1 LIN Bus and Communication

This high voltage input or output pin is a single wire LIN bus transmitter and receiver. The LIN pin can survive transient voltages up to 58 V. Reverse currents from the LIN to supply (V_{SUP}) are minimized with blocking diodes, even in the event of a ground shift or loss of supply (V_{SUP}). There is an internal pull-up resistor with a serial diode structure to V_{SUP}, so no external pull-up components are required for the LIN responder node applications. An external pull-up resistor (1 kΩ) and a series diode to V_{SUP} must be added when the device is used for commander node applications as per the LIN specification (ISO 17987-4).

The transmitter meets thresholds and AC parameters according to the LIN specification. The transmitter is a low side transistor with internal current limitation and thermal shutdown. During a thermal shutdown condition, the transmitter is disabled to protect the device. In fast mode the transmitter can support 200 kbps data rates.

The receiver's characteristic thresholds are ratiometric with the device supply pin according to the LIN specification. The receiver is capable of receiving higher data rates (>100 kbps) than supported by LIN or SAEJ2602 specifications. This allows the TLIN1431x-Q1 to be used for high speed downloads at the end-of-line production or other applications. The actual data rate achievable depends on system time constants (bus capacitance and pull-up resistance) and driver characteristics used in the system. In fast mode the transmitter and receiver can support 200 kbps.

6.3.1.1 SM-1: LIN TXD Pin Dominant State Timeout

During normal mode, if TXD is inadvertently driven permanently low by a hardware or software application failure, the LIN bus is protected by the dominant state timeout timer. This timer is triggered by a falling edge on the TXD pin. If the low signal remains on TXD for longer than t_{TXD_DTO}, the transmitter is disabled, thus allowing the LIN bus to return to recessive state and communication to resume on the bus. The protection is cleared and the t_{TXD_DTO} timer is reset by a rising edge on TXD. The TXD pin has an internal pull-up to ensure the device fails to a known recessive state if TXD is disconnected. During this fault, the transceiver remains in normal mode (assuming no change of stated request on EN), the RXD pin reflects the LIN bus and the LIN bus pull-up termination remains on. The TLIN1431x-Q1 can turn off TXD dominant state timeout when in SPI mode by using register 8'h1D[5] = 1b.

6.3.1.2 SM-2: LIN Bus Stuck Dominant System Fault: False Wake Up Lockout

The device contains logic to detect bus stuck dominant system faults and prevents the device from waking up falsely during the system fault. Upon entering sleep mode, the device detects the state of the LIN bus. If the bus is dominant, the wake-up logic is locked out until a valid recessive on the bus "clears" the bus stuck dominant, preventing excessive current use.

Figure 6-1 and Figure 6-2 show the behavior of this protection.

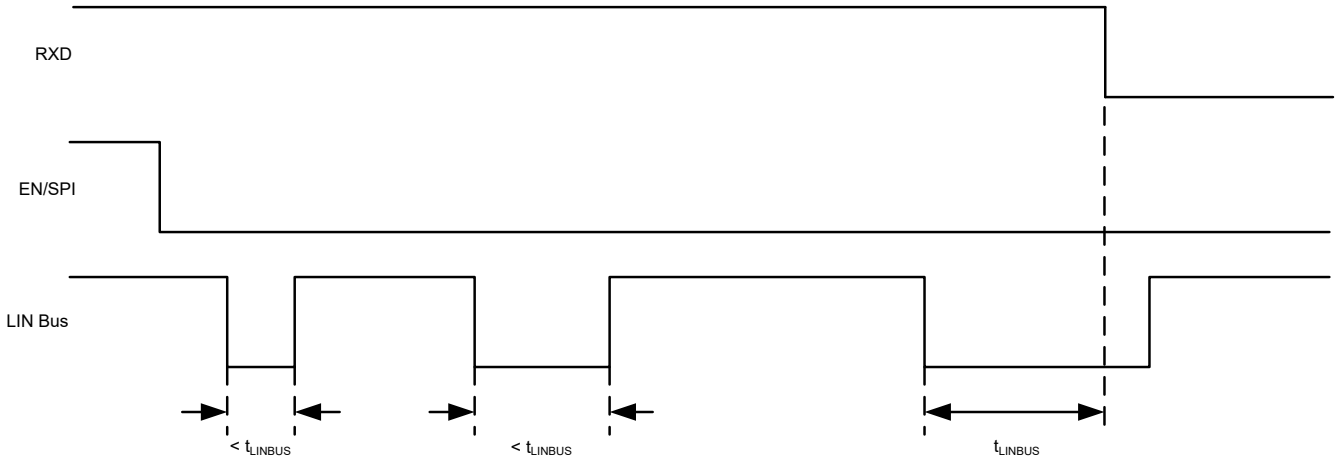


Figure 6-1. No Bus Fault: Entering Sleep Mode with Bus Recessive Condition and Wake Up

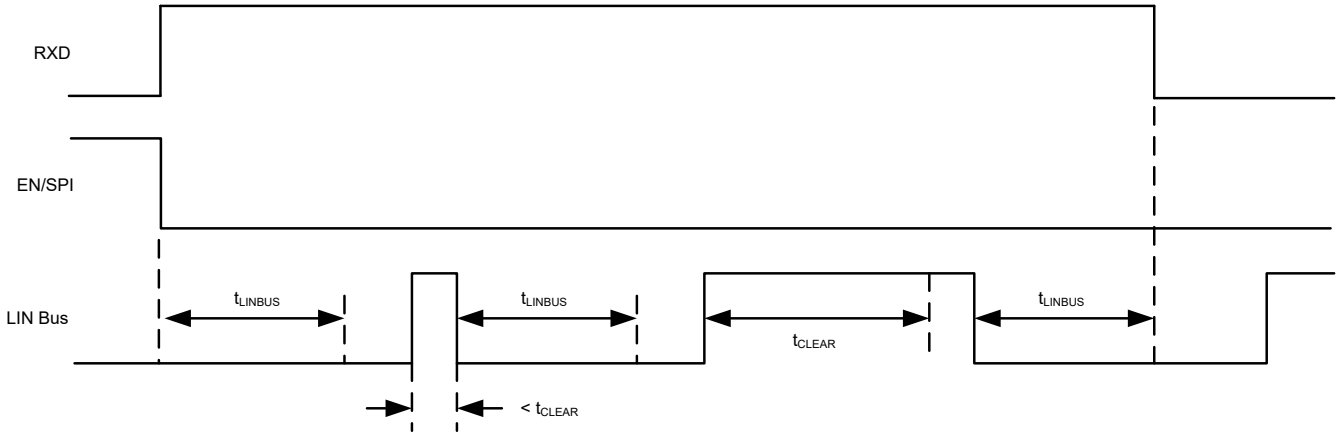


Figure 6-2. Bus Fault: Entering Sleep Mode with Bus Stuck Dominant Fault, Clearing, and Wake Up

6.3.1.3 SM-3: LIN Bus Short Circuit Limiter

The TLIN1431x-Q1 has mechanisms in place that limits the current through the LIN pin in case of a short to ground fault.

6.3.1.4 SM-20: LIN Internal pull-up to V_{SUP}

In case of open (floating pins) the default state of the LIN pin is provided by an integrated pull-up resistor that biases the pin recessive. This prevents inadvertent dominant signals from appearing on the LIN pin due to noise, which would result in inadvertent dominant signals on the RXD pin.

6.3.1.5 SM-22: LIN Protocol

LIN protocol has several mechanisms for detecting errors and the expected behavior of a responder device which can include disregarding data and going to the Dormant state. See the LIN standards for full explanation.

6.3.2 Voltage Rail Monitoring

The device has an integrated high-voltage input LDO that operates over a 5.5 V to 28 V input voltage range (V_{SUP}) for both 3.3 V and 5 V V_{CC}. The device has an output current capability of 125 mA and support fixed output voltages of 3.3 V (TLIN14313-Q1) or 5 V (TLIN14315-Q1). VCC is monitored for under-voltage, over-voltage and short circuit to GND. VSUP is monitored for under-voltage.

6.3.2.1 SM-4: V_{CC} and Transceiver Thermal Shutdown

The TLIN1431x-Q1 has multiple thermal sensors in the device to monitor the junction temperature of the die. The VCC LDO, LIN transmitter, and high side switch/LIMP cells are monitored. The action taken by the device is determined by which cell junction temperature is exceeded. Exceeding the maximum junction temperature for the LIN transmitter or LDO causes the LIN transmitter into the recessive state and turns off the VCC regulator. The nRST pin is pulled to ground during a LIN or VCC LDO TSD event. Once the over temperature fault condition has been removed and the junction temperature has cooled beyond the hysteresis temperature, the transmitter can be re-enabled. Exceeding the max junction temperature of the high side switch or LIMP cells cause the cells to be turned off.

In SPI mode, there are two interrupts that can be set due to a thermal event. If the LIN transceiver or VCC LDO junction temperature is exceeded the TSD_VCC_LIN interrupt is set and the devices taked the action previously described. If the high side switch or LIMP high side switch max junction temperature is exceeded the TSD_HSS_LIMP interrupt is set and the device takes the action previously described. In SPI mode, the device defaults to support fail-safe mode. The device enters fail-safe mode upon a TSD_VCC_LIN event and LIMP is turned on. Exiting fail-safe mode is the same as when the device is pin controlled. When fail-safe mode is disabled the device enters sleep mode upon a TSD_VCC_LIN event.

6.3.2.2 SM-5: V_{CC} Under-voltage

The V_{CC} pin is the current limited regulated output based supporting an accuracy of ±2.5%. In the event that the regulator drops out of regulation, the output tracks the input minus a drop based on the load current. When the input voltage drops below the UV_{SUP} threshold, the regulator turns off until the input voltage returns above the UV_{SUPR} level. The device uses the voltage regulator during Init mode to determine which function the WKRQ/INH, and what the IO voltage is when the 5V LDO is used. The device monitors V_{CC} for under-voltage. The device control method and whether fail-safe mode is enabled determine the behavior of the of the device for these events. Fail-safe mode is always active when the device is in pin control. In SPI control, the state diagram shows two paths: fail-safe mode enabled and fail-safe mode disabled. The path followed depends on whether fail-safe mode is enabled or disabled in 8'h17[0] FSM_DIS.

For an under-voltage event, V_{CC} is less than or equal to UV_{CCF}. After the t_{UVFLTR} time, the device pulls nRST low and transition to restart mode, if fail-safe disabled, or fail-safe mode. When entering either mode the SWE timer, t_{INACT_FS} starts and for SPI control the mode counter increments and the appropriate interrupt flags are set. To exit fail-safe mode the under-voltage has to clear and a wake event takes place prior to the SWE timer timing out. If the under-voltage event has not cleared when the wake event takes place or if the SWE timer times out the device enters sleep mode. Figure 6-3 shows how a UV_{CC} event is handled.

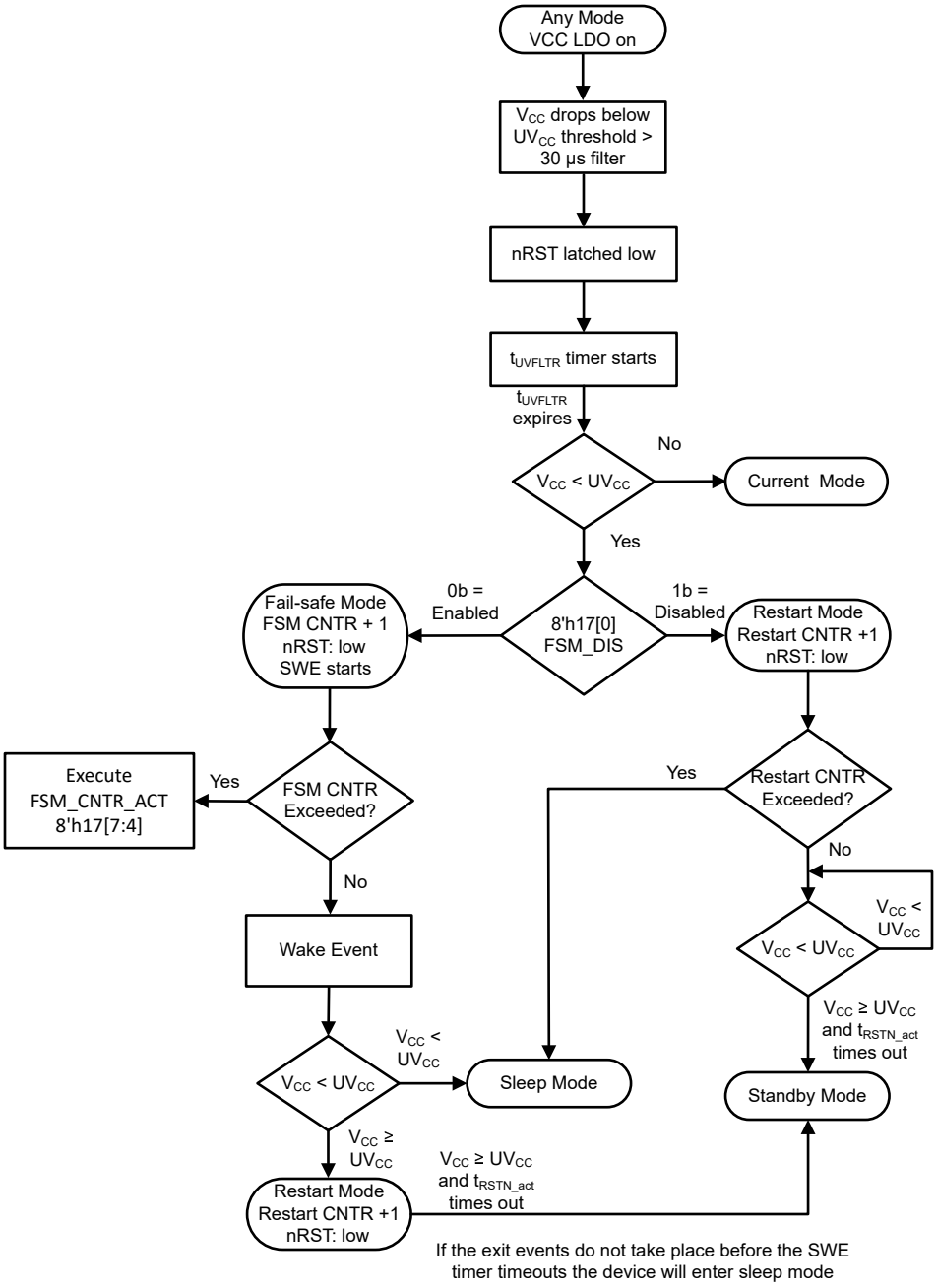
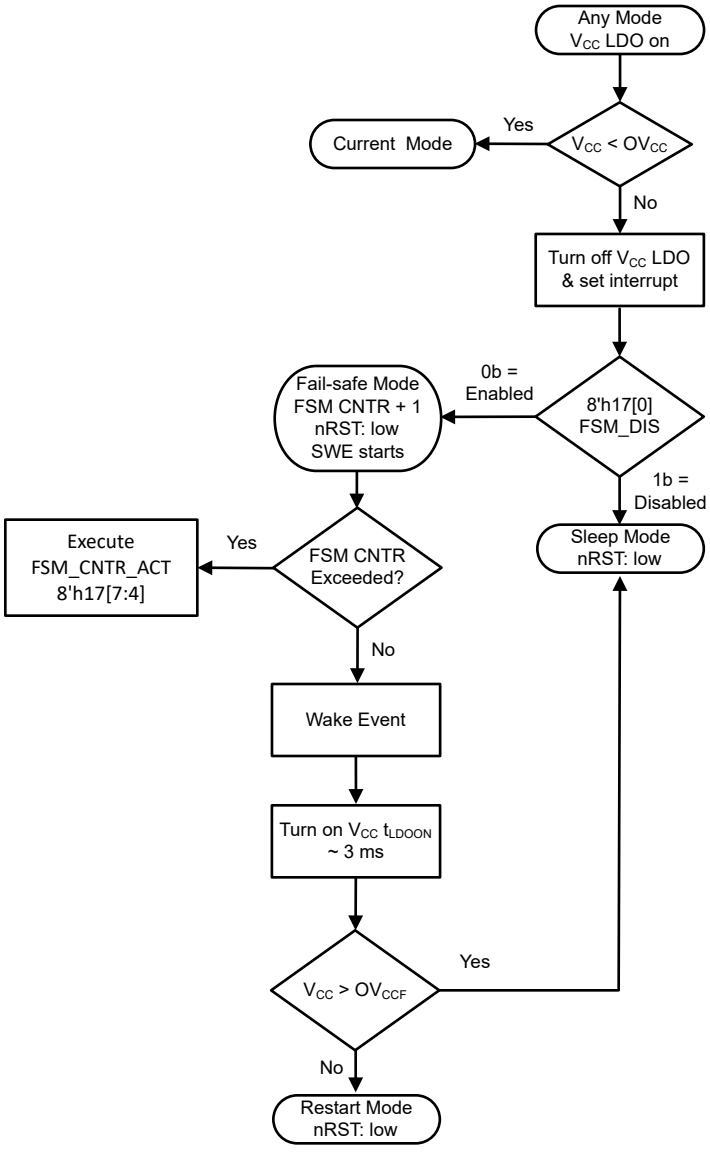


Figure 6-3. UV_{CC} flow chart

6.3.2.3 SM-6: V_{CC} Over-voltage

The device monitors V_{CC} for over-voltage events. For an over-voltage event, OV_{CC}, the device turns off the V_{CC} LDO and transitions to either sleep mode, fail-safe mode disabled, or fail-safe mode. When a wake event takes place the V_{CC} LDO is turned on for t_{LDOON} to determine if the over-voltage is still present. If cleared, the device enters restart mode from either sleep or fail-safe modes. When in fail-safe mode, if the over-voltage has not cleared when the wake event takes place the device transitions to sleep mode. Figure 6-4 shows how an OV_{CC} event is handled.

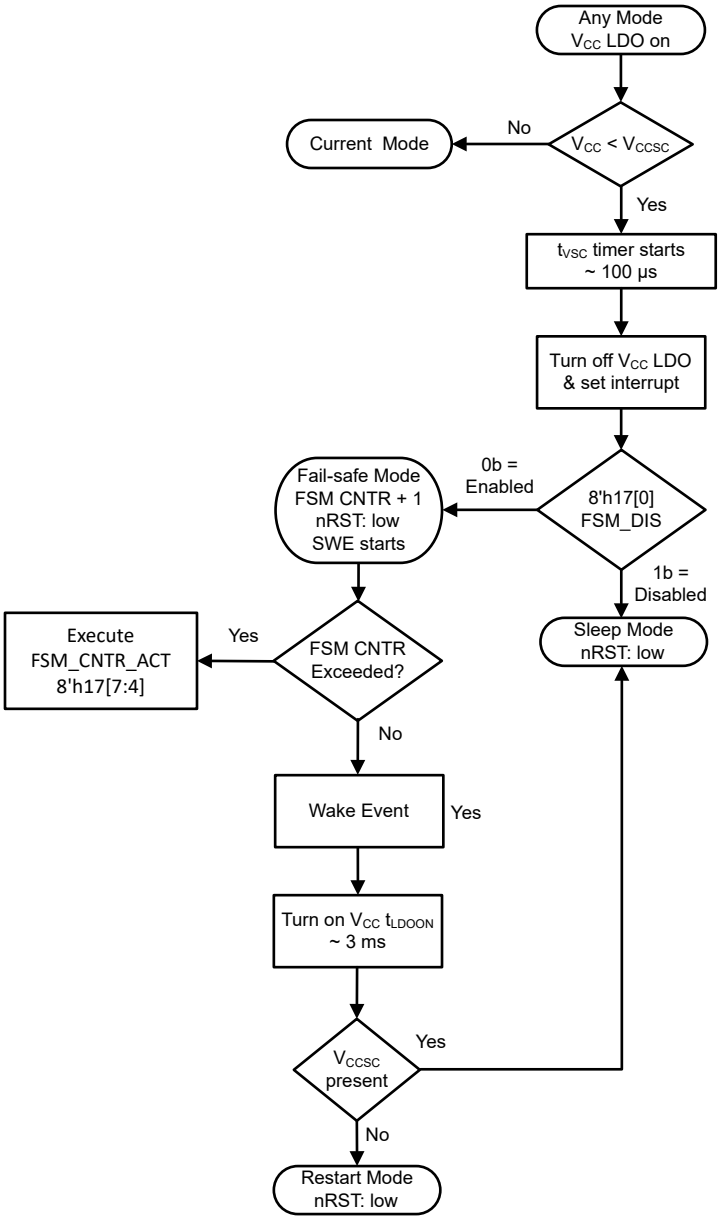


If the exit events do not take place before the SWE timer timeouts the device will enter sleep mode

Figure 6-4. OV_{CC} flow chart

6.3.2.4 SM-7: V_{CC} Short to Ground

The device monitors V_{CC} for short to ground events. For a short to ground event, V_{CCSC}, the device turns off the V_{CC} LDO and transitions to either sleep mode, fail-safe mode disabled, or fail-safe mode. When a wake event takes place, the V_{CC} LDO is turned on for t_{LDOON} to determine if the short to ground is still present. If cleared, the device enters restart mode from either sleep or fail-safe modes. When in fail-safe mode, if the short to ground has not cleared when the wake event takes place the device transitions to sleep mode. Figure 6-5 shows how a short to ground event on V_{CC} is handled.



If the exit events do not take place before the SWE timer timeouts the device will enter sleep mode

Figure 6-5. V_{CCSC}, short to ground

6.3.2.5 SM-8: V_{SUP} Under-voltage

The device monitors V_{SUP} for two low voltage thresholds, UV_{SUP} and V_{nPOR}. When V_{SUP} drops below UV_{SUPF} and is above V_{nPORF}, the device is in an under-voltage power state. Once V_{SUP} ramps above UV_{SUPR} the device enters restart mode and turns on the V_{CC} LDO. When V_{SUP} drops below V_{nPORF} the device goes into a power off state. Once V_{SUP} ramps above V_{nPORR}, the device prepares the digital core to wake up. The device waits for

V_{SUP} to rise above UV_{SUPR} and then turns on the V_{CC} LDO. Once V_{SUP} and V_{CC} are above their under-voltage levels, the device enters Init mode. The described under-voltage events are also considered brown out events and more information can be found at Device Brownout information in the data sheet.

6.3.3 Processor Communication

The TLIN1431x-Q1 has several ways to determine if the communication between the processor and device is functioning correctly. SM-9 through SM-14 provide information on these methodologies.

6.3.3.1 SM-9 and SM-10: Watchdog

The TLIN1431x-Q1 has an integrated watchdog function and provides two watchdog types that can be set up when using SPI control: window watchdog or timeout watchdog. If more frequent (i.e. <16 ms) input trigger events are desired it is suggested to us the timeout watchdog. When using timeout watchdog, the input trigger can occur anywhere before the timeout and is not tied to an open window. The device defaults to window watchdog at power up but can be programmed to support timeout watchdog. The watchdog registers for input trigger and configuration are located at 8'h13 through 8'h16. WD_CONFIG_1 register 8'h13[7:4] and WD_CONFIG_2 register 8'h14[7:5] are used to set up timing. See Table 6-6 for available watchdog timing.

When using the window watchdog, it is important to understand the closed and open window aspects. The device is set up with a 50%/50% open and closed window and is based on an internal oscillator with a ± 10% accuracy range. To determine when to provide the input trigger, this variance needs to be considered. For example, using the 64 ms nominal total window provides a closed and open window that are each 32 ms. Taking the ±10% internal oscillator into account means the total window could range from 57.6 ms to 70.4 ms. The closed and open window could then range from 22.4 ms to 35.2 ms. From the 57.6 ms total window and 35.2 ms closed window, the total open window is 22.4 ms. The trigger event needs to happen at 46.4 ms ± 11.2 ms. See Figure 6-6 for when the initial window is needed and when the device would expect a watchdog input trigger for a window watchdog configuration. See Figure 6-7 and Figure 6-8 for state diagrams on how the WD behaves.

The TLIN1431x-Q1 has a watchdog error counter used in SPI control mode. This counter is an up down counter that increments for every missed window or incorrect input watchdog trigger event. In SPI control, the error counter is set at one by default. The counter decrements for every correct input trigger and increments on every incorrect input trigger, but it never drops below zero. When the programmed counter is reached, the device transitions to restart mode and pulls nRST pin low for t_{NRST_TOG}. At the end of this time, the device transitions back to standby mode releasing the nRST pin to high. This counter can be changed to 1 (every error), 9, or 15 using 8'h16[7:6]. The error counter can be read at register 8'h14[4:1]. In pin control, nWDR is pulled low for every watchdog error.

If the watchdog error count is set at one, the first input failure causes the device to transition to restart. This allows the system to check the counter after the first input trigger to see if a valid input was sent. Every incorrect watchdog input causes the interrupt to be set and nINT is pulled low.

The LIMP pin provides a limp home capability when connected to external circuitry. When in sleep mode, the LIMP pin is off. When the error counter reaches the watchdog trigger event level, the LIMP pin turns on connecting VSUP to the pin as described in the LIMP pin section.

Table 6-6. Watchdog Window and Timeout Timer Configuration (ms)

WD_TIMER (ms)	Register 8'h13[5:4] WD_PRE			
Register 8'14[7:5]	00	01	10	11
000	4	8	12	16
001	32	64	96	128
010	128	256	384	512
011	256	384	512	768
100	512	1024	1536	2048
101	2048	4096	6144	8192
110	10240	20240	RSVD	RSVD
1111	RSVD	RSVD	RSVD	RSVD

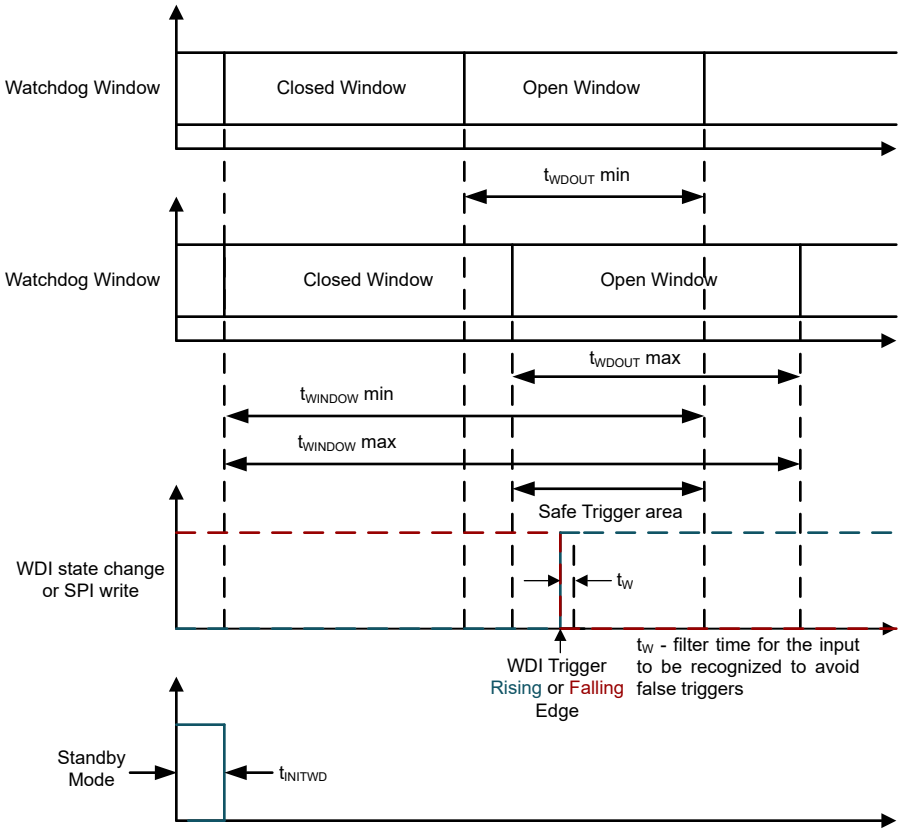


Figure 6-6. Watchdog Timing Diagram

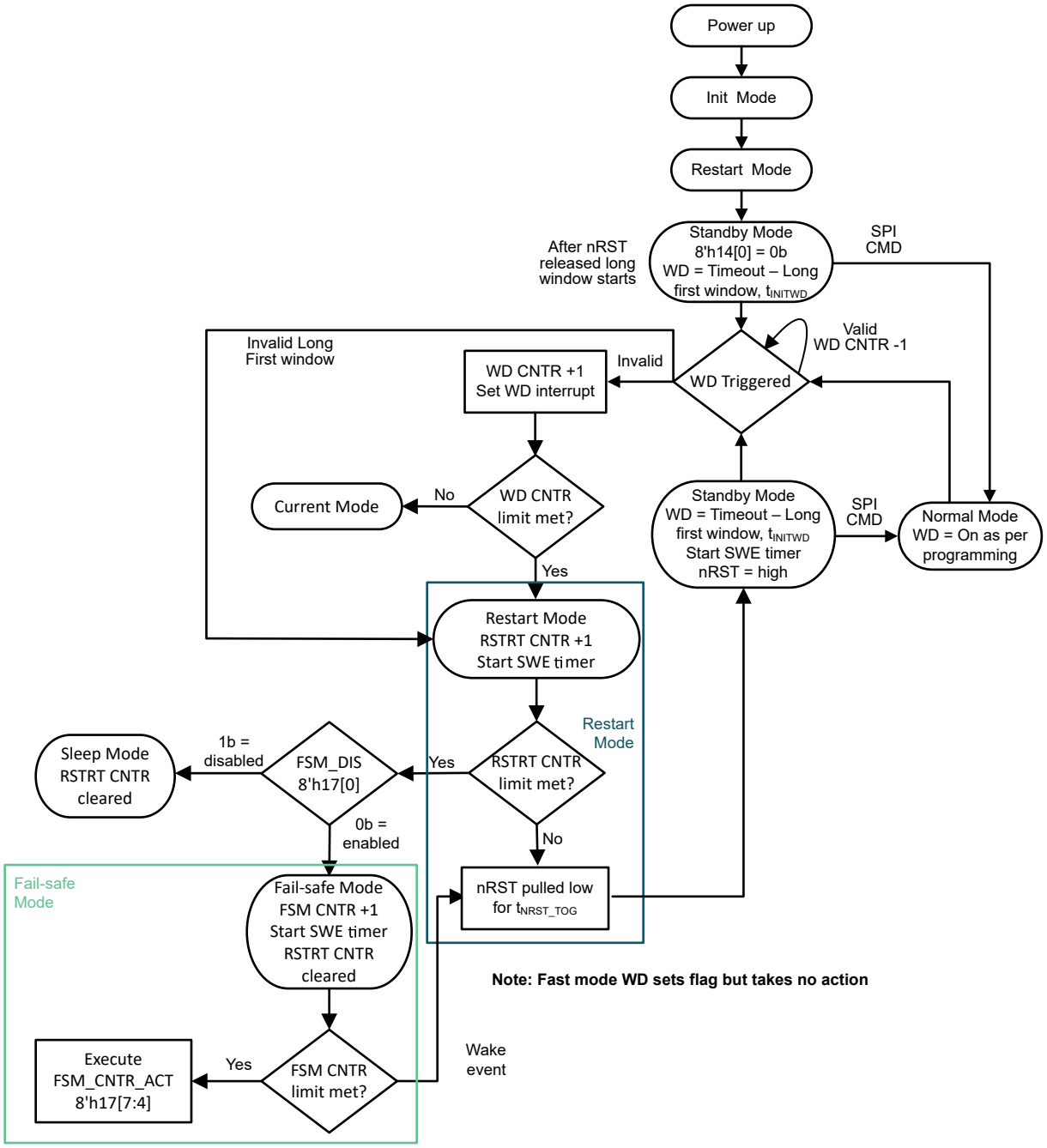


Figure 6-7. Watchdog state diagram in SPI mode; Standby Mode Enabled

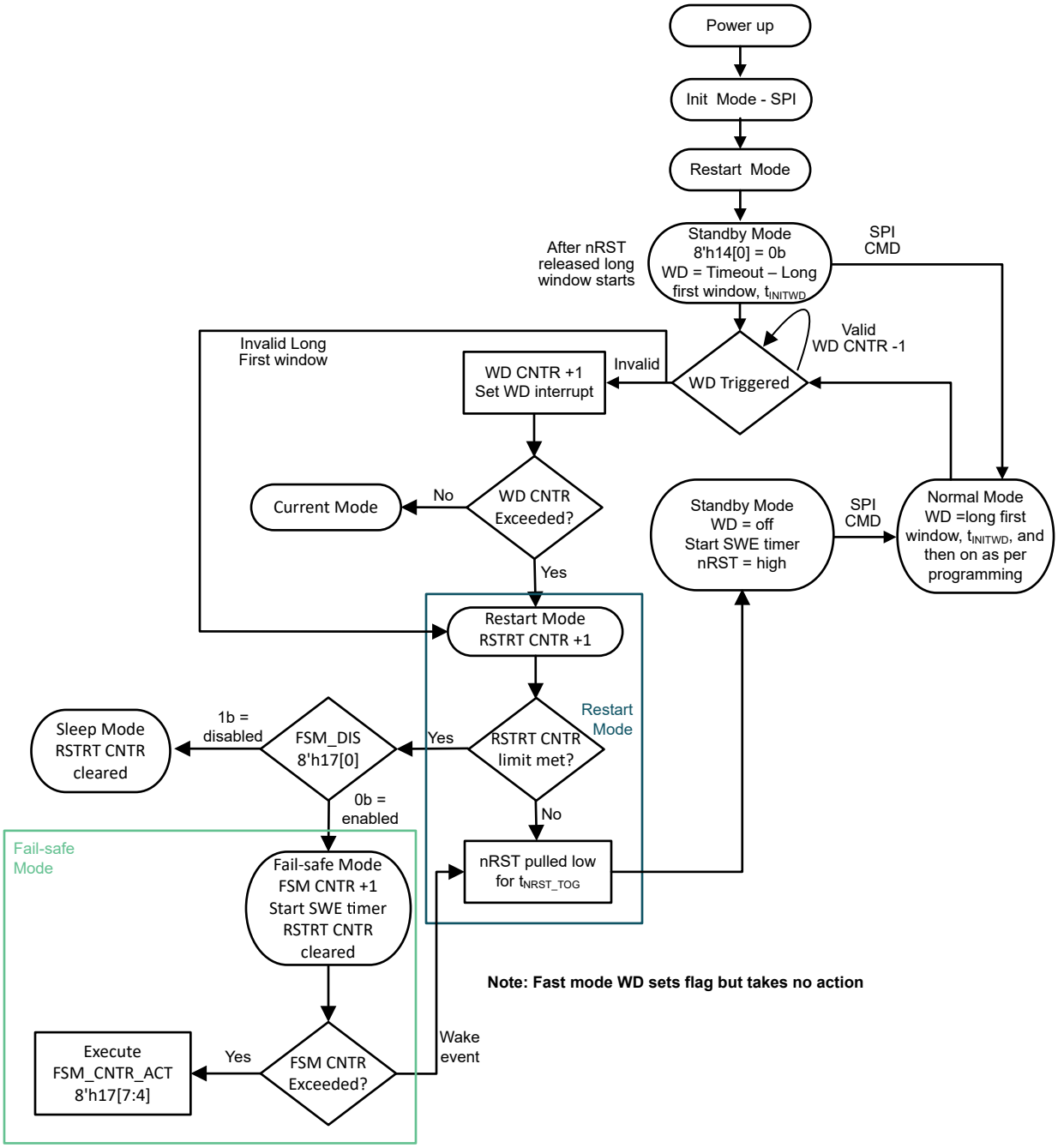


Figure 6-8. Watchdog state diagram in SPI mode; Standby Mode Disabled

Note

- When the mode is changed while the timeout or window watchdog is running, it restarts once entering the new mode, fast, normal and standby.
- If the watchdog configuration is changed on-the-fly while the watchdog is running, it resets the error counter to 1 and resets the watchdog timers.

6.3.3.1.1 SM-9: Standby Mode Long Window Timeout Watchdog

When the device enters standby mode, a watchdog trigger is expected within the first long window, t_{INITWD}, which is typically 150 ms. When entering standby mode from restart mode, there is a nRST transition from low to high. This transition starts the t_{INITWD} timer. After this initial long window, the watchdog expects the trigger event to take place as programmed which could be window or timeout. See Figure 6-7 for state diagrams on how the WD behaves when watchdog is enabled in standby mode.

6.3.3.1.2 SM-10: Normal Mode Watchdog

When entering normal mode, the programmed watchdog timer starts based upon the WD_CONFIG_1 register 8'h13[7:4] and WD_CONFIG_2 register 8'h14[7:5]. If WD is disabled in standby mode the same long window is implemented in normal mode. See Figure 6-8 for state diagrams on how the WD behaves with standby mode disabled.

6.3.3.2 SM-11: SPI CRC

The TLIN1431x-Q1 supports cyclic redundancy check (CRC) for SPI transactions and is default disabled. Register 8'h0A[0] can be used to enable this feature. The default polynomial supports AutoSAR CRC8H2F, $X^8 + X^5 + X^3 + X^2 + X + 1$, see Table 6-7. CRC8 according to SAE J1850 is also supported and can be selected at register 8'h0B[0], see Table 6-8.

When CRC is enabled, a filler byte of 00h is used to calculate the CRC value during a read/write operation, see Figure 6-9 and Figure 6-10.

When a CRC error takes place, registers 8'h50[7], 8'h50[4], and 8'h53[4] will be indicated.

Table 6-7. CRC8H27

SPI Transactions	
CRC result width	8 bits
Polynomial	2Fh
Initial value	FFh
Input data reflected	No
Result data reflected	No
XOR value	FFh
Check	DFh
Magic Check	42h

Table 6-8. CRC8 SAE J1850

SPI Transactions	
CRC result width	8 bits
Polynomial	1Dh
Initial value	FFh
Input data reflected	No
Result data reflected	No
XOR value	FFh
Check	4Bh
Magic Check	C4h

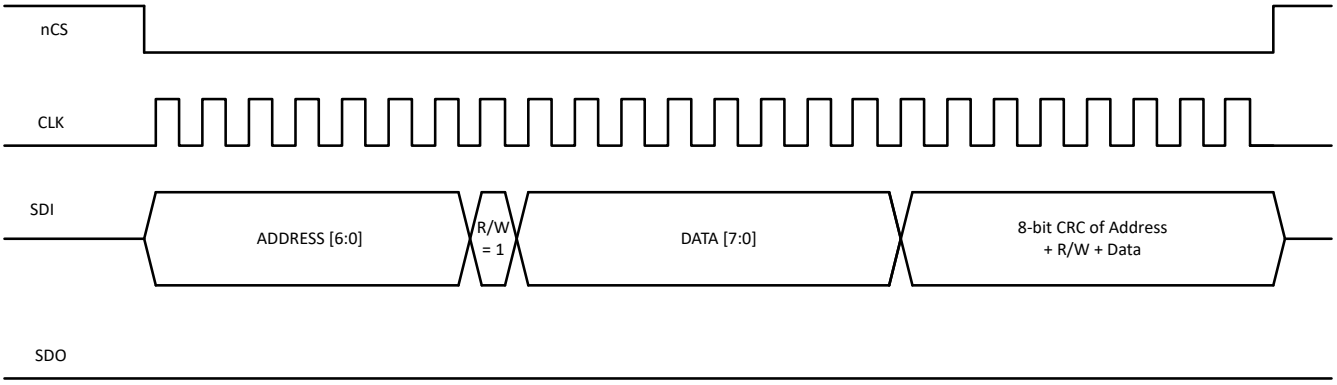


Figure 6-9. SPI Write with CRC

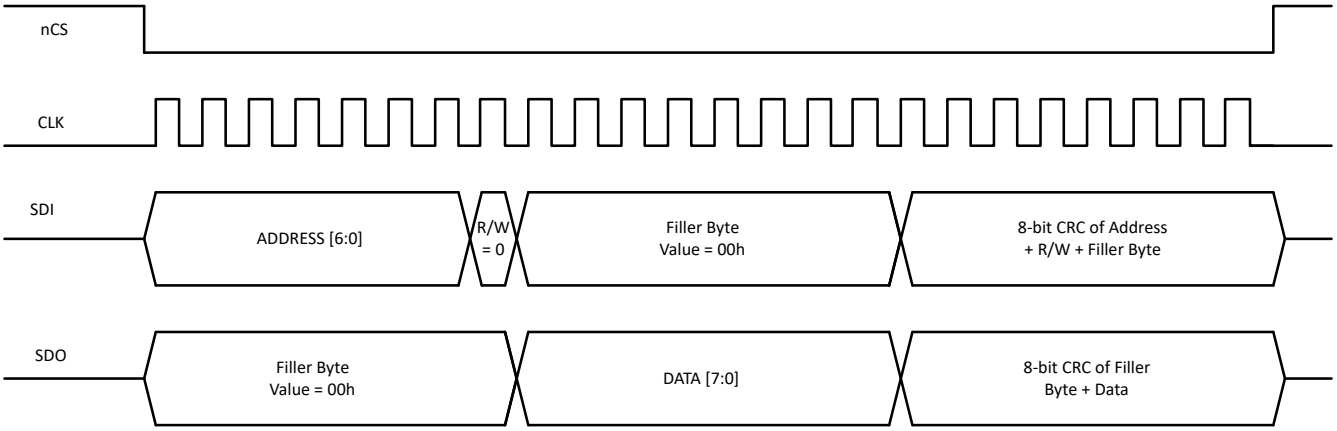


Figure 6-10. SPI Read with CRC

6.3.3.3 SM-12: SPI Communication Error; SPIERR

The Serial Peripheral 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 CLK (Serial Clock). Each SPI transaction is 16 bits containing an address and read/write command byte followed by one data byte. If SPI CRC is enabled each transaction is 24 bits containing an address and read/write command byte followed by one data byte and one CRC 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 (CLK). The data is shifted into an appropriately 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 CLK and the nCS has a rising edge to deselect the device. 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, is set.

6.3.3.4 SM-13: Scratchpad Write/Read Register

The TLIN1431x-Q1 provides a memory scratchpad, register 8'h0F[7:0], that makes it possible to write and read back data for verification of accuracy. This verifies SPI interface to register space.

6.3.3.5 SM-14: Sleep Wake Error Timer; t_{INACT_FS}

The TLIN1431x-Q1 implements a sleep wake error timer, t_{INACT_FS}. The purpose of the SWE timer is to keep the device and the node from being stuck in a high-power state. This timer is used to place the device into fail-safe or sleep mode due to fault conditions. In Pin mode, the SWE timer starts automatically when entering fail-safe and restart modes. A wake event causes the device to move from sleep mode to restart mode and if V_{CC} does not exceed UV_{CC} before the SWE timer times out the device re-enters sleep mode. This happens in either SPI or pin control modes.

In SPI mode, the SWE timer, when enabled, automatically starts when the device enters fail-safe, restart and standby modes. When the device leaves restart mode and enters standby mode, the processor must initiate a SPI transaction before the SWE timer times out or the device enters fail-safe mode. This timer can be disabled at register 8'h1C[7] = 1. If the SWE timer duration is changed, this is accomplished register 8'h1C[6:3]. It can be changed from default of 5 min to between 30 seconds and 10 min.

6.3.4 Digital Input/Output Pins and High-side Switch

There are internal pull-ups or pull-downs on critical terminals to place the device into known states if the terminal floats. Several of these are only active when the TLIN1431x-Q1 is in SPI control.

Table 6-9. Internal Pull-up or Pull-down table

Safety Mechanism	Pin	Pull-up or Pull-down	Typical Value	Comment
SM-15	CLK	Pull-up	240 kΩ	Keeps CLK pin from floating
SM-16	SDI	Pull-up	240 kΩ	Keeps SDI pin from floating
SM-17	nCS	Pull-up	240 kΩ	Keeps nCS from floating and enabling SPI when not intended
SM-18	DIV_ON	Pull-down	370 kΩ	Keeps DIV_ON pin from floating and turning on the VBAT monitor when not intended
SM-19	TXD	Pull-up	350 kΩ	Keeps TXD pin from floating dominant which could cause LIN but to be forced dominant
SM-20	LIN	Pull-up	45 kΩ	Keeps LIN bus from being forced dominant which would cause RXD pin to be forced dominant
SM-21	nRST	Pull-up	45 kΩ	Keeps nRST from floating and as active low pin indicates when VCC is in under-voltage, watchdog error or device is in reset mode.

6.3.4.1 SM-15: CLK internal pull-up to V_{INT}

For open (floating pins), the default state of CLK pin is provided by an integrated pull-up resistor that weakly biases the pin.

6.3.4.2 SM-16: SDI internal pull-up to V_{INT}

For open (floating pins), the default state of SDI pin is provided by an integrated pull-up resistor that weakly biases the pin.

6.3.4.3 SM-17: nCS Internal pull-up to V_{INT}

For open (floating pins), the default state of nCS pin is provided by an integrated pull-up resistor that weakly biases the pin. This keeps the device SPI from being constantly enabled or intermittently enabled due to noise.

6.3.4.4 SM-18: DIV_ON Internal pull-down to GND

For open (floating pins), the default state of the DIV_ON pin is provided by an integrated pull-down resistor that weakly biases the pin. This keeps the pin from inadvertently turning on the VBAT monitor due to noise.

6.3.4.5 SM-19: TXD Internal pull-up to V_{INT}

For open (floating pins), the default state of the TXD pin is provided by an integrated pull-up resistor that weakly biases the pin. This keeps the TXD pin from inadvertently having a dominant on TXD due to noise.

6.3.4.6 SM-21: nRST Internal pull-up to V_{INT}

For open (floating pins), the default state of the nRST pin is provided by an integrated pull-up resistor that biases the pin to V_{INT}. The nRST pin is an active low output that indicates when VCC is in under-voltage, when a watchdog error occurs, and when the device is in restart mode.

6.3.4.7 SM-23: HSS Over Current Detect

When the high-side switch is on and over current is detected the device turns off the HSS to avoid damage and indicates to processor, 8'h5A[3].

6.3.4.8 SM-24: HSS Open Load Detect

The device monitors the high-side switch for open load condition. When detected, it indicates to processor that there is an open load, 8'h5A[2].

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 5. 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 6.2 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	LIN TXD pin dominant state timeout; t_{TXD_DTO}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - In normal and fast mode	80 ms	The device monitors the TXD pin for a stuck dominant for t_{TXD_DTO} then the device turns off the LIN transceiver and indicate the fault at register h'5A[6].	3 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-2	LIN bus stuck dominant	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - In normal and fast mode	3 µs	Upon entering sleep mode, the device detects the state of the LIN bus. If the bus is dominant, the wake-up logic is locked out until a valid recessive on the bus “clears” the bus stuck dominant, preventing excessive current use.	3 µs
SM-3	LIN bus short circuit limiter, I_{BUS_LIM}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Periodic	NA	Limits the current through the LIN pin.	NA
SM-4	V_{CC} and Transceiver thermal shutdown; TSD	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - All modes except for sleep mode	10 µs	Turn off the CAN transceiver and set the interrupt bit registers h'50[7], h'50[5] and h'52[1] indicating junction temperature exceeded and indicate an interrupt back to the MCU using the nINT pin and enter fail-safe mode or TSD protected mode.	3 µs
SM-5	V_{CC} under voltage; UV_{CC}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - All modes except for sleep mode	4 ms	Device enters programmed mode, restart or fail-safe, sets interrupt bits and indicates UV_{CC} condition back to MCU with nINT pin, 8'h52[2] UVCC interrupt.	3 µs
SM-6	V_{CC} over-voltage; OV_{CC}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - All modes except for sleep mode	150 µs	Device enters programmed mode, fail-safe or sleep mode, sets interrupt bits and indicates OV_{CC} condition back to MCU with nINT pin, 8'h52[5] OVCC interrupt.	3 µs
SM-7	V_{CC} short to ground; V_{CCSC}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - All modes except for sleep mode	125 µs	Device enters programmed mode, fail-safe or sleep mode, sets interrupt bits and indicates V_{CCSC} condition back to MCU with nINT pin, 8'h53[3] VCCSC interrupt.	3 µs
SM-8	V_{SUP} supply under voltage; UV_{SUP}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - All modes except for sleep mode	125 µs	Device enters UVSUP state and sets interrupt, 8'h52[4] UVSUP letting processor know that this event took place.	3 µs
SM-9	Standby long timeout WD; t_{INITWD}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Periodic - Upon entering standby mode.	200 ms	Missing window cause an interrupt flag to be set and indication back to MCU with nINT pin and setting interrupt 8'h51[7] WD.	5 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-10	Timeout or window watchdog error - Normal mode	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	Programmable 4 ms to 20 s	Increments WD error counter and if exceeded programmed value enters programmed mode, restart or fail-safe mode, set WD interrupt and indicate back to MCU with nINT pin and setting interrupt 8'h51[7] WD.	5 µs
SM-11	SPI CRC Error	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	8 µs	The device shall monitor MCU SPI communication utilizing 8-bit CRC and if the CRC is invalid the MCU write to the device is blocked. Interrupt 8'h53[4] CRCERR is set.	2 µs
SM-12	SPI communication error; SPIERR	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	8 µs	The device shall monitor MCU SPI communication utilizing clock count check and if too many or not enough clock signals the MCU write to the device is blocked and interrupt bit set and indicated fault back to MCU with the nINT pin and interrupt 8'h53[7] SPIERR is set.	2 µs
SM-13	Scratchpad write/ read	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	16 µs	Using the scratchpad, h'F[7:0], by the processor makes it possible to write and read back data for the purpose of verifying SPI communication.	16 µs
SM-14	Sleep Wake Error Timer; t_{INACT_FS}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	Programmable 30 seconds to 10 min Default 5 min	The Sleep Wake Error timer is used to determine if inactivity indicated loss of communication with MCU and causes the device to transition to either fail-safe mode or sleep mode. Interrupt 8'h51[4] WKERR is set along with 8'h52[7] SMS and/or 8'h53[5] FSM as applicable.	5 µs
SM-15	CLK internal pull-up to V_{INT}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	NA	Avoids floating pin.	NA
SM-16	SDI internal pull-up to V_{INT}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	NA	Avoids floating pin.	NA
SM-17	nCS internal pull-up to V_{INT}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	NA	Avoids floating pin.	NA

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-18	DIV_ON internal pull-down	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	NA	Avoids floating pin.	NA
SM-19	TXD internal pull-up to V_{INT}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	NA	Avoids floating pin causing LIN bus being stuck dominant.	NA
SM-20	LIN internal pull-up to V_{SUP}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	NA	Avoids floating pin causing LIN bus being stuck dominant.	NA
SM-21	nRST internal pull-up to V_{INT}	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous	NA	Avoids floating pin, indicates to processor a UV_{CC} event, watchdog failure event and device in restart mode. Also utilized as a device power on reset input.	NA
SM-22	LIN protocol	Safety Mechanism	System Functional Safety Mechanism	Periodic	NA	LIN protocol has several mechanisms that makes sure the data provided is correct, like checksum. If incorrect the processor disregards the LIN data.	NA
SM-23	HSS Current Limit	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - when on	20 µs	Turns off the HSS to avoid damage and interrupt 8'h5A[3] HSSOC is set.	3 µs
SM-24	HSS Open Load Detect	Safety Mechanism	Component Hardware Functional Safety Mechanisms	Continuous - when on	80 µs	Indicates to processor that there is an open load on HSS and interrupt 8'h5A[2] HSSOL is set.	3 µs

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 Product Preview	Overview of functional safety considerations in product development and product architecture. Delivered ahead of public product announcement.
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 [1]	Summary of arguments and evidence of compliance to functional safety standards. References a specific component, component family, or TI process that was analyzed.
Assessment Certificate [1]	Evidence of compliance to functional safety standards. References a specific component, component family, or TI process that was analyzed. Provided by a 3rd party functional safety assessor.

(1) When an Assessment Certificate is available for a TI functional safety product, the Functional Safety Report may not be provided. When a Functional Safety Report is provided, an Assessment Certificate may not be available. These two documents fulfill the same functional safety requirements, and are used interchangeably depending on the TI functional safety product.

C Revision History

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

DATE	REVISION	NOTES
December 2022	*	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