Functional Safety Manual for TPS3704x-Q1

Functional Safety Information

Literature Number: SFFS169A
APRIL 2022 – REVISED MAY 2022

Table of Contents

1 Introduction......5
2 TPS3704x-Q1 Hardware Component Functional Safety Capability......7
3 Development Process for Management of Systematic Faults......9
3.1 TI New-Product Development Process......9
3.2 TI Functional Safety Development Process......10
4 TPS3704x-Q1 Component Overview......13
4.1 Targeted Applications......16
4.2 Hardware Component Functional Safety Concept......18
4.3 Functional Safety Constraints and Assumptions......19
5 Description of Hardware Component Parts......21
6 TPS3704x-Q1 Management of Random Faults......25
6.1 Fault Reporting......25
6.2 Functional Safety Mechanism Categories......25
6.3 Description of Functional Safety Mechanisms......27
A Summary of Recommended Functional Safety Mechanism Usage......29
B Distributed Developments......31
B.1 How the Functional Safety Lifecycle Applies to TI Functional Safety Products......31
B.2 Activities Performed by Texas Instruments......31
B.3 Information Provided......32
C Revision History......33

List of Figures

Figure 1-1. Device Naming Convention......5
Figure 3-1. TI New-Product Development Process......10
Figure 4-1. TPS37041-Q1 Single-Channel Functional Block Diagram......13
Figure 4-2. TPS37042-Q1 Dual-Channel Functional Block Diagram......14
Figure 4-3. TPS37043-Q1 Triple-Channel Functional Block Diagram......14
Figure 4-4. TPS37044-Q1 Quadruple-Channel Functional Block Diagram......15
Figure 4-5. TPS3704x-Q1 Typical Automotive Application......16
Figure 4-6. TPS3704x-Q1Typical Industrial Application Circuit......17
Figure 4-7. TPS3704x-Q1Typical Application Circuit......18
Figure 5-1. TPS3704x-Q1 Quad-channel Internal Block Diagram......22
Figure 5-2. TPS3704x-Q1 Dual-channel Internal Block Diagram......23

List of Tables

Table 3-1. Functional Safety Activities Overlaid on top of TI's Standard Development Process......10
Table A-1. Legend of Functional Safety Mechanisms......29
Table A-2. Assumed Safety Diagnostic Requirements......30
Table B-1. Activities Performed by Texas Instruments versus Performed by the customer......31
Table B-2. Product Functional Safety Documentation......32

This page intentionally left blank.

This document is a functional safety manual for the Texas Instruments TPS3704x-Q1 component. The specific orderable part numbers supported by this functional safety manual are as shown in the device naming convention. For non automotive grade parts remove the -Q1 from the device name.

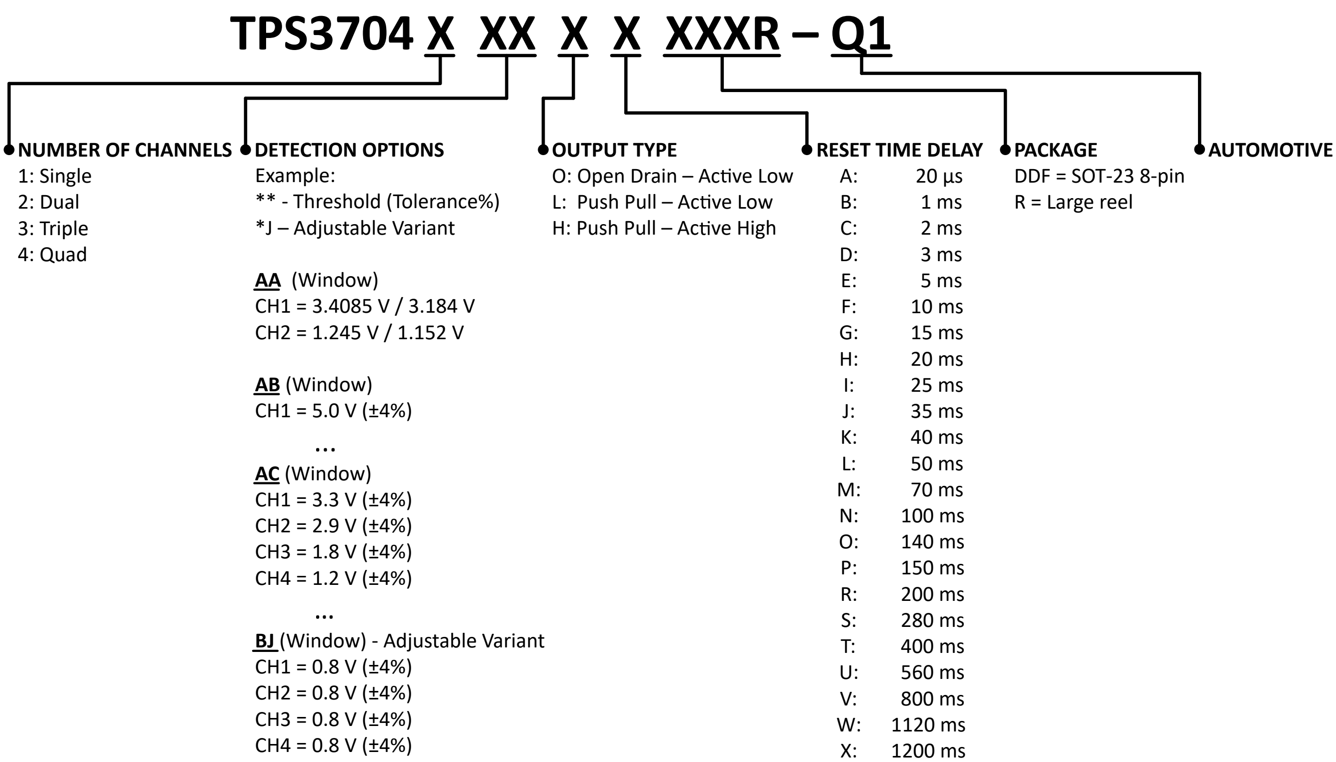

Figure 1-1. Device Naming Convention

This functional safety manual provides information needed by system developers to help in the creation of a functional safety system using a TPS3704x-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 TPS3704x-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 TPS3704x-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 TPS3704x-Q1 component. For more information, refer to the TPS3704x-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 https://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.

Chapter 2

TPS3704x-Q1 Hardware Component Functional Safety Capability

This section summarizes the component functional safety capability.

This hardware component:

- Was developed as a functional Safety Element out of Context (SEooC)
- Was developed according to the relevant requirements of IEC 61508:2010
- Was developed according to the relevant requirements of ISO 26262:2018
- Includes sufficient functional safety mechanisms for random fault integrity requirements of SIL-1
- Includes sufficient functional safety mechanisms for random fault integrity requirements of ASIL-A
- Achieves systematic integrity of SIL-3
- Achieves systematic integrity of ASIL-D
- Has passed a functional safety assessment by Texas Instruments

This page intentionally left blank.

Chapter 3

Development Process for Management of Systematic Faults

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

3.1 TI New-Product Development Process

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

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

The standard development process breaks development into phases:

- Assess
- Plan
- Create
- Validate

Figure 3-1 shows the standard process.

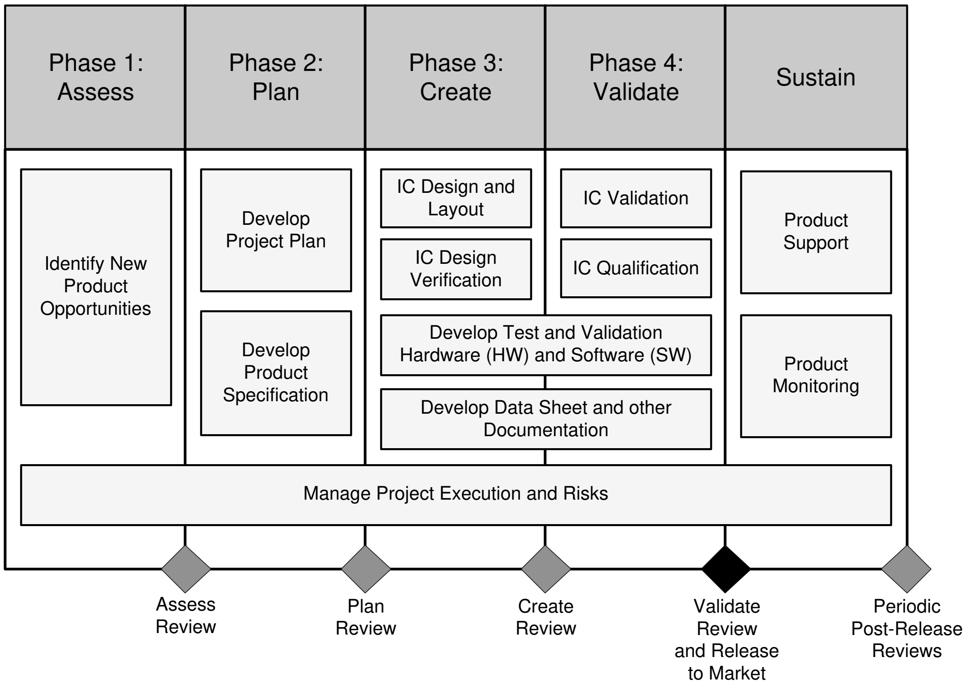

Figure 3-1. TI New-Product Development Process

3.2 TI Functional Safety Development Process

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

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

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

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

Refer to Appendix 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)

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

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

This page intentionally left blank.

TPS3704x-Q1 Component Overview

The following figures are Block Diagrams showing the components for single-channel, dual-channel, triple-channel, and quadruple-channel devices.

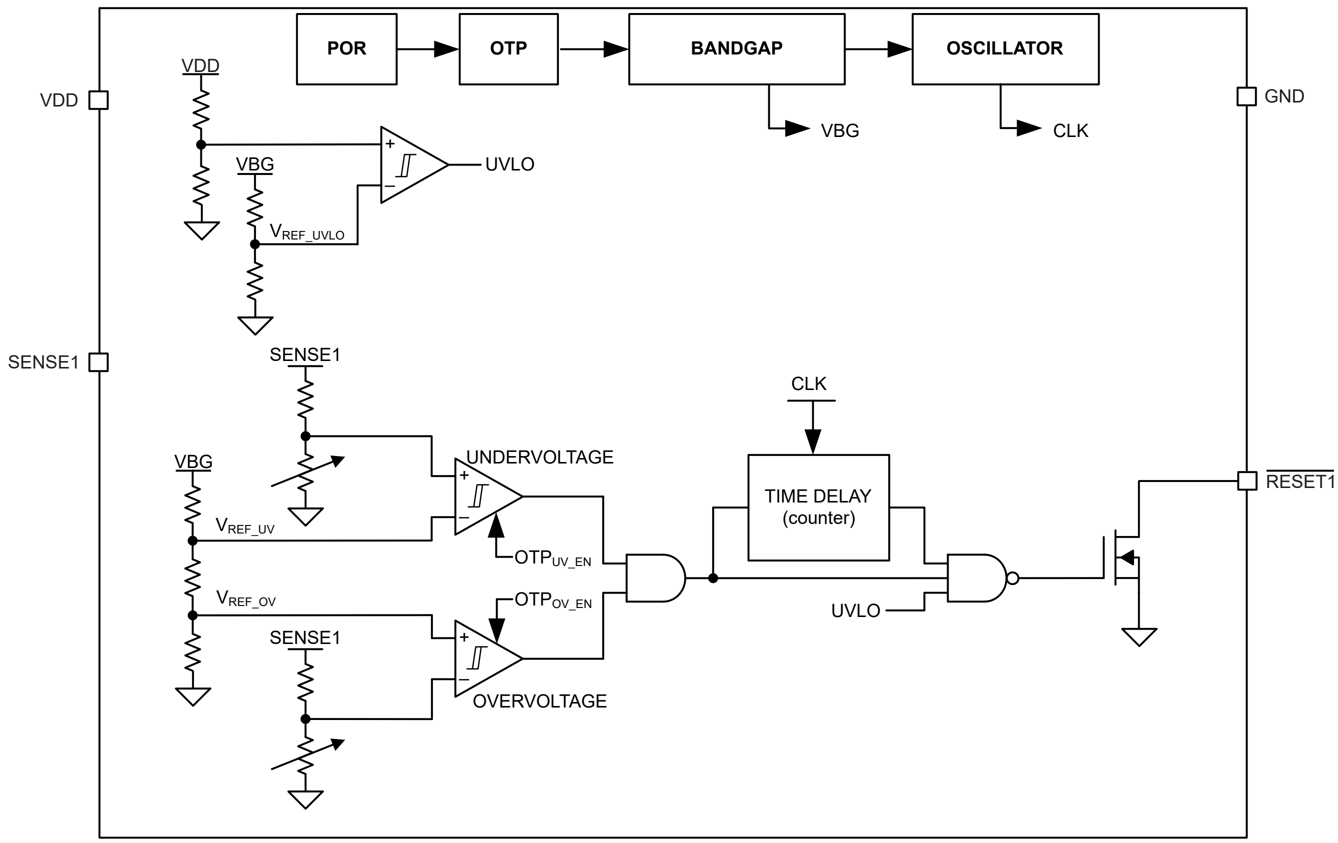

Figure 4-1. TPS37041-Q1 Single-Channel Functional Block Diagram

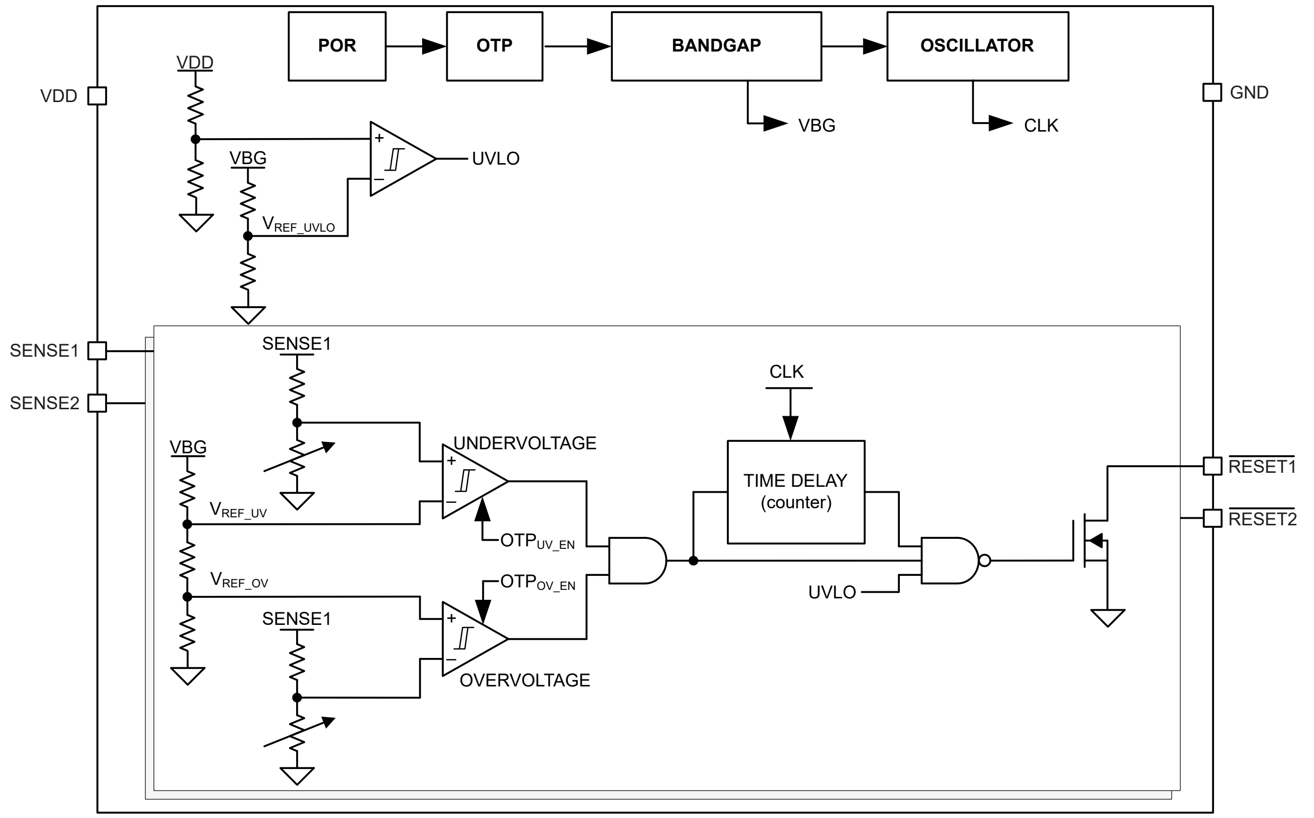

Figure 4-2. TPS37042-Q1 Dual-Channel Functional Block Diagram

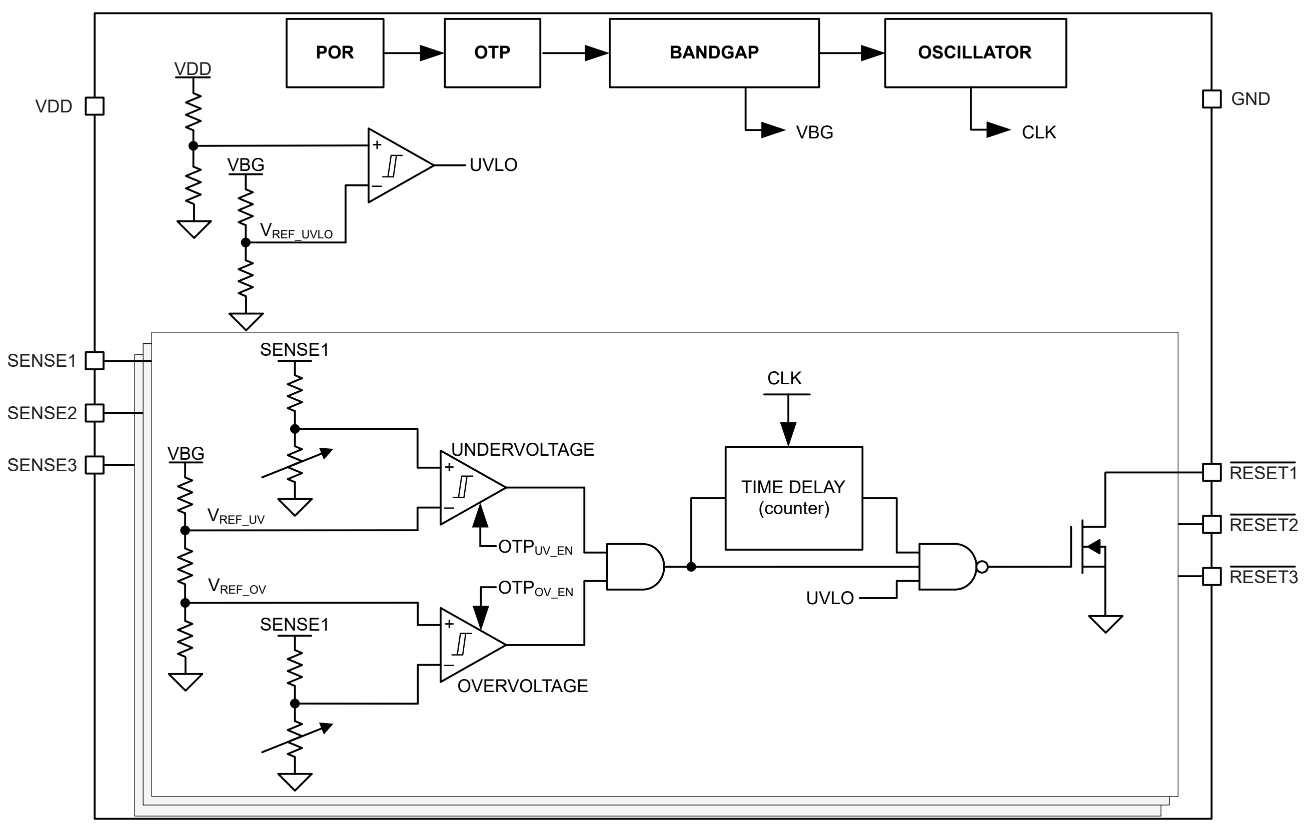

Figure 4-3. TPS37043-Q1 Triple-Channel Functional Block Diagram

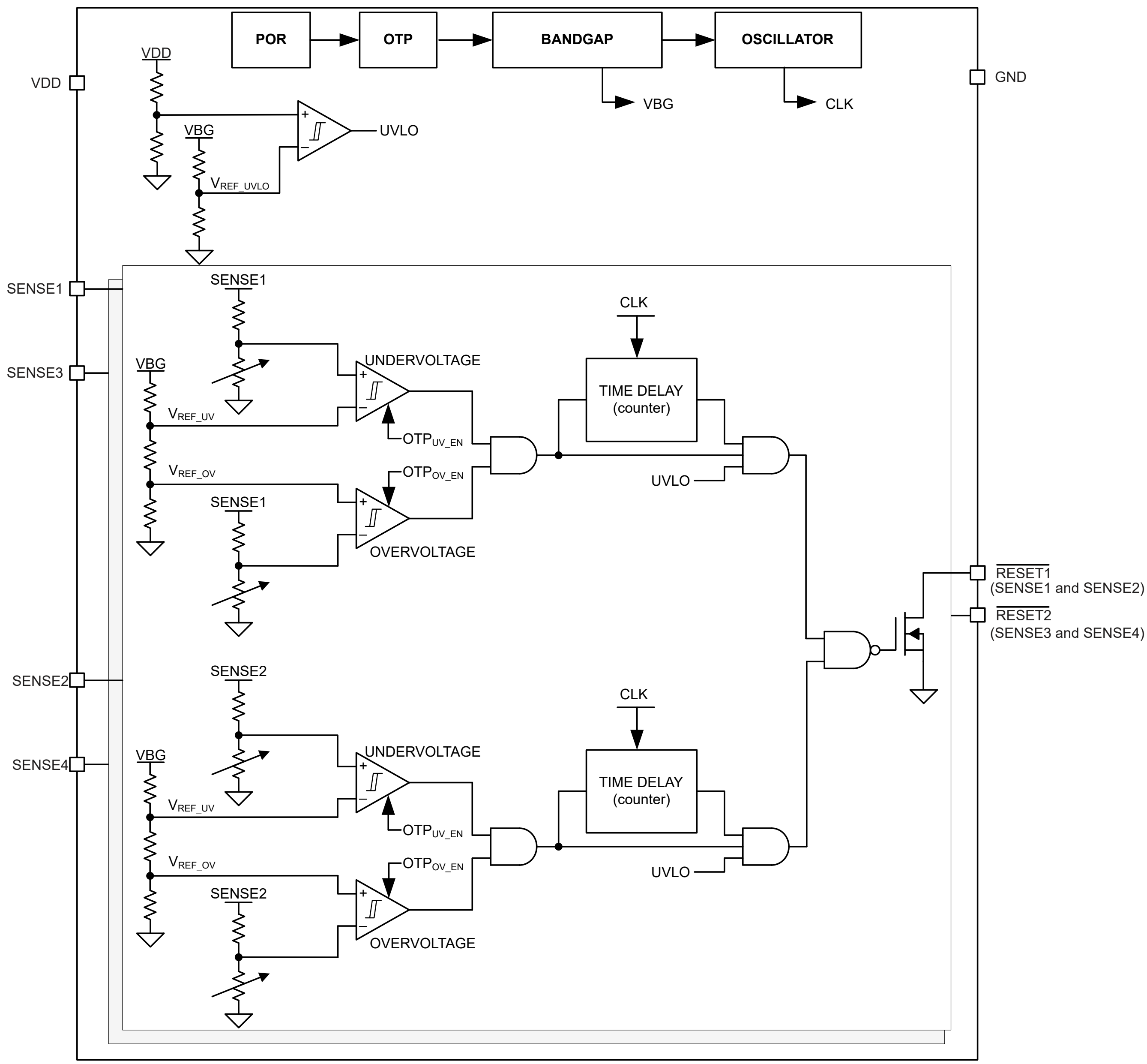

Figure 4-4. TPS37044-Q1 Quadruple-Channel Functional Block Diagram

4.1 Targeted Applications

The TPS3704x-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 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:

- Advanced Driver Assistance System (ADAS)
- Automotive infotainment & cluster
- HEV/EV
- Body electronics and lighting
- Factory automation
- Building automoation
- Medical
- Motor Drives
- Grid infrastructure
- Wireless infrastructure
- Data center & enterprise computing

Figure 4-5 shows a generic block diagram for an automotive system. This diagram is only an example and may not represent a complete system.

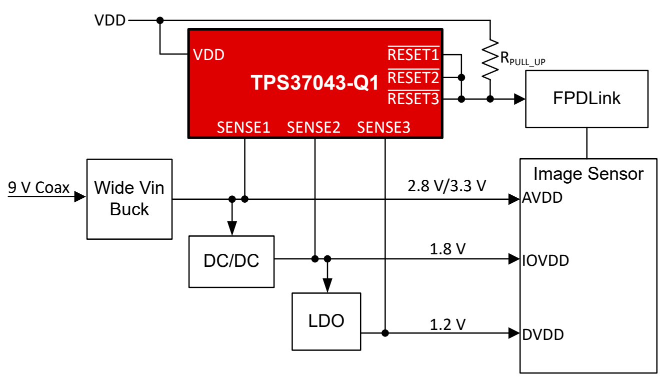

Figure 4-5. TPS3704x-Q1 Typical Automotive Application

Figure 4-6 shows a generic block diagram for an industrial system. This diagram is only an example and may not represent a complete system.

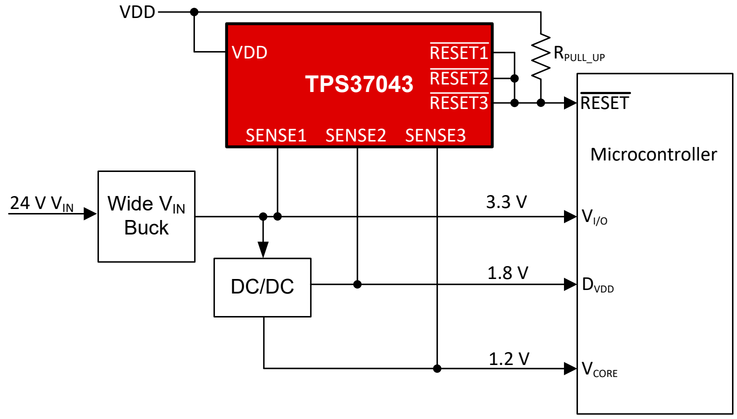

Figure 4-6. TPS3704x-Q1Typical Industrial Application Circuit

4.2 Hardware Component Functional Safety Concept

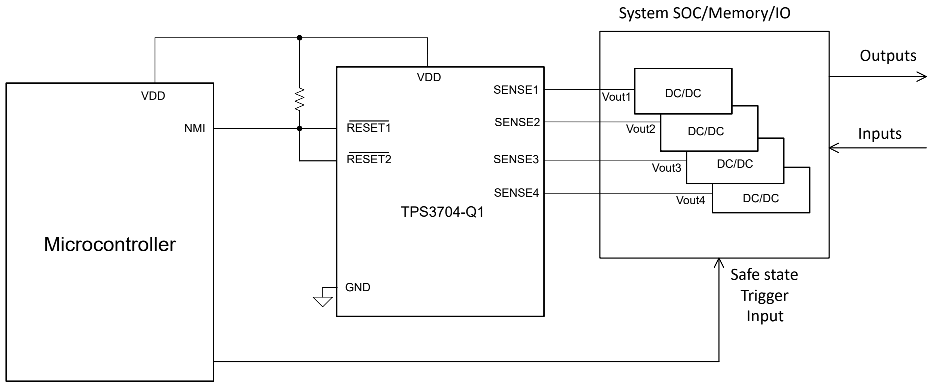

Figure 4-7. TPS3704x-Q1Typical Application Circuit

TPS3704x is used to monitor rails for systems such as camera systems, rain sensors, display systems etc.

It monitors each rail for over voltage and under voltage faults. The thresholds for fault setting are defined by the rail voltage level being monitored and the SOC, interface, memory abs max and min levels that should not be exceeded. The basic functional safety assumption is that if an abs max or min limit is violated the system can operate in an undefined state which could violate safety goals and lead to hazards.

If an over voltage or under voltage fault happens the RESETx pin associated with that SENSEx pin is asserted low. In normal operation on power up the RESETx pin goes high after the startup delay (tSTRT) plus Reset delay (TD). The functional safety concept is that when a fault is detected the RESETx pin goes low within the propagation delay (Tpd). This RESETx pin is connected to an NMI (Non maskable interrupt) of the Microcontroller or SOC. In Figure 4-7 it is shown that once the microcontroller gets a NMI it then takes action to trigger the safe state for the system.

In summary the basic premise of the functional safety concept is detect overvoltage and/or under voltage faults and perform a system reset to put the system in a safe state. The RESETx output can be connected to any input that is responsible for taking the system to a safe state. In Figure 4-7 it goes to an NMI of a microcontroller. In some system implementations it may trigger the system safe state directly.

Once the system is in a safe state there should be also defined what is the sequence of events that need to happen to take it out of the safe state.

Depending on the type of system it may sometimes be required to do a power reboot to clear the safe state or it can automatically be cleared if the fault that caused the RESET is gone (i.e. the output voltage comes back within spec). Once the voltage comes back within spec the RESETx pin is deasserted after the Reset time delay.

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 TPS3704x-Q1 Functional Safety Analysis was done under the following system assumptions:

- **[SA_1]** The external System shall determine on TPS3704x-Q1 reset signal whether transistion to safe state is needed and execute that transition.
- **[SA_2]** Voltage thresholds and timing requirements for TPS3704x-Q1 shall be set to match system requirements.
- **[SA-3]** The system shall include a voltage clamp to prevent overvoltage on the sense inputs of TPS3704x-Q1
- **[SA-4]** All inputs to the TPS3704x-Q1 SVS shall meet the recommended operating conditions defined in the device specification and does not exceed absolute operating conditions defined therein
- **[SA-5]** The operating temperature of the TPS3704x-Q1 SVS shall meet the ambient and junction temperature limits defined in the device specification
- **[SA-6]** All external components to the TPS3704x-Q1 SVS shall meet the electrical characteristics defined in the device specification
- **[SA-7]** The layout of the system board shall follow the layout guidelines as defined in the TPS3704x-Q1SVS device specification

TPS3704x-Q1 shall be considered in the safe state when no power is applied, or when operating in a fully functional and fault-free integrated system.

TPS3704x-Q1 shall be considered in a safe state when Over-Voltage (OV), Under-Voltage(UV), is detected on one or more sense inputs and signaled to an external host element of the system/item. The host is responsible for fault reaction and transitioning of the system to a system safe state.

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.

This page intentionally left blank.

Chapter 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.

Figure 5-1 and Figure 5-2 show the internal block diagrams of the TPS3704x-Q1 quad-channel and dual-channel devices respectively.

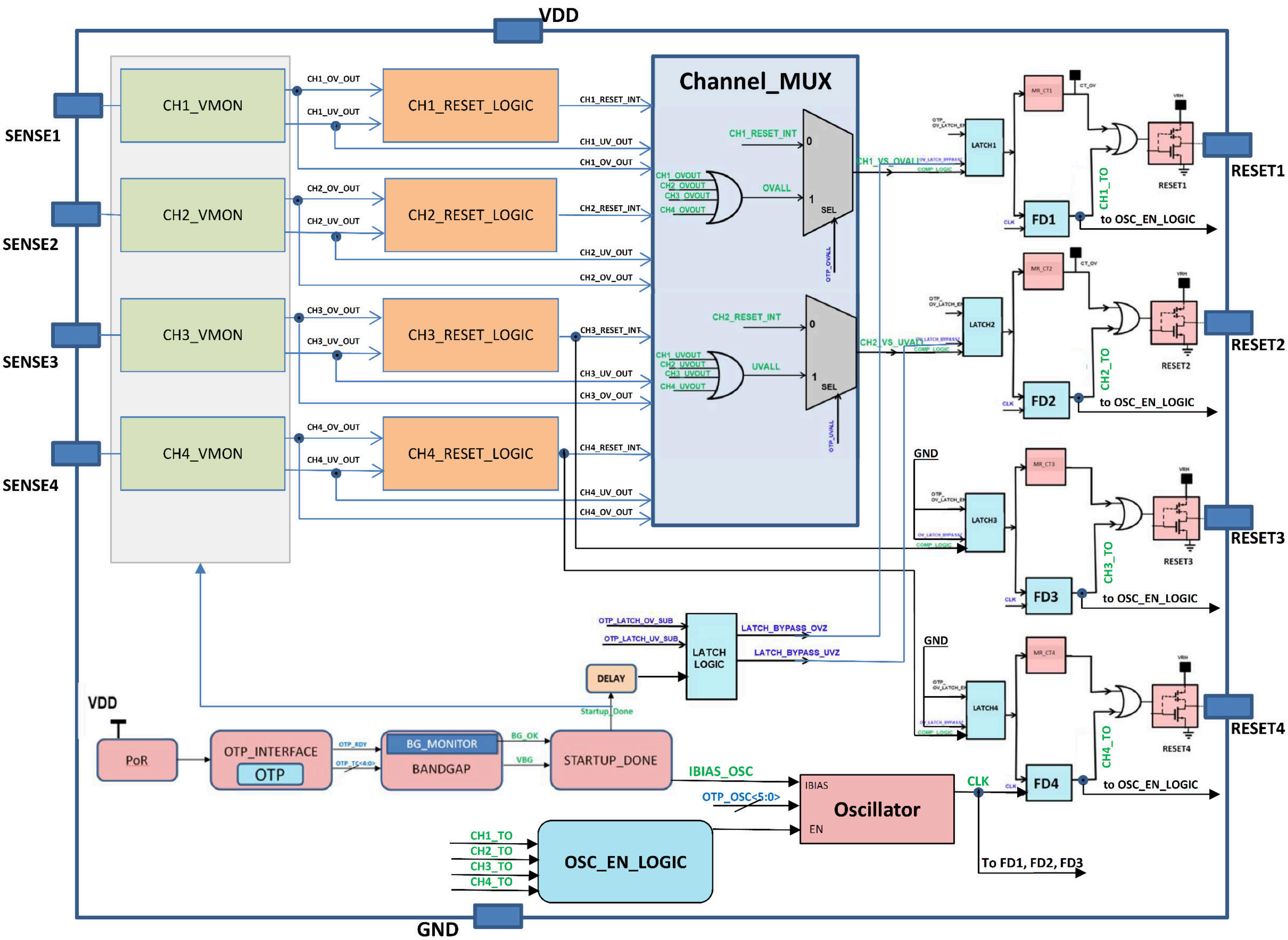

Figure 5-1. TPS3704x-Q1 Quad-channel Internal Block Diagram

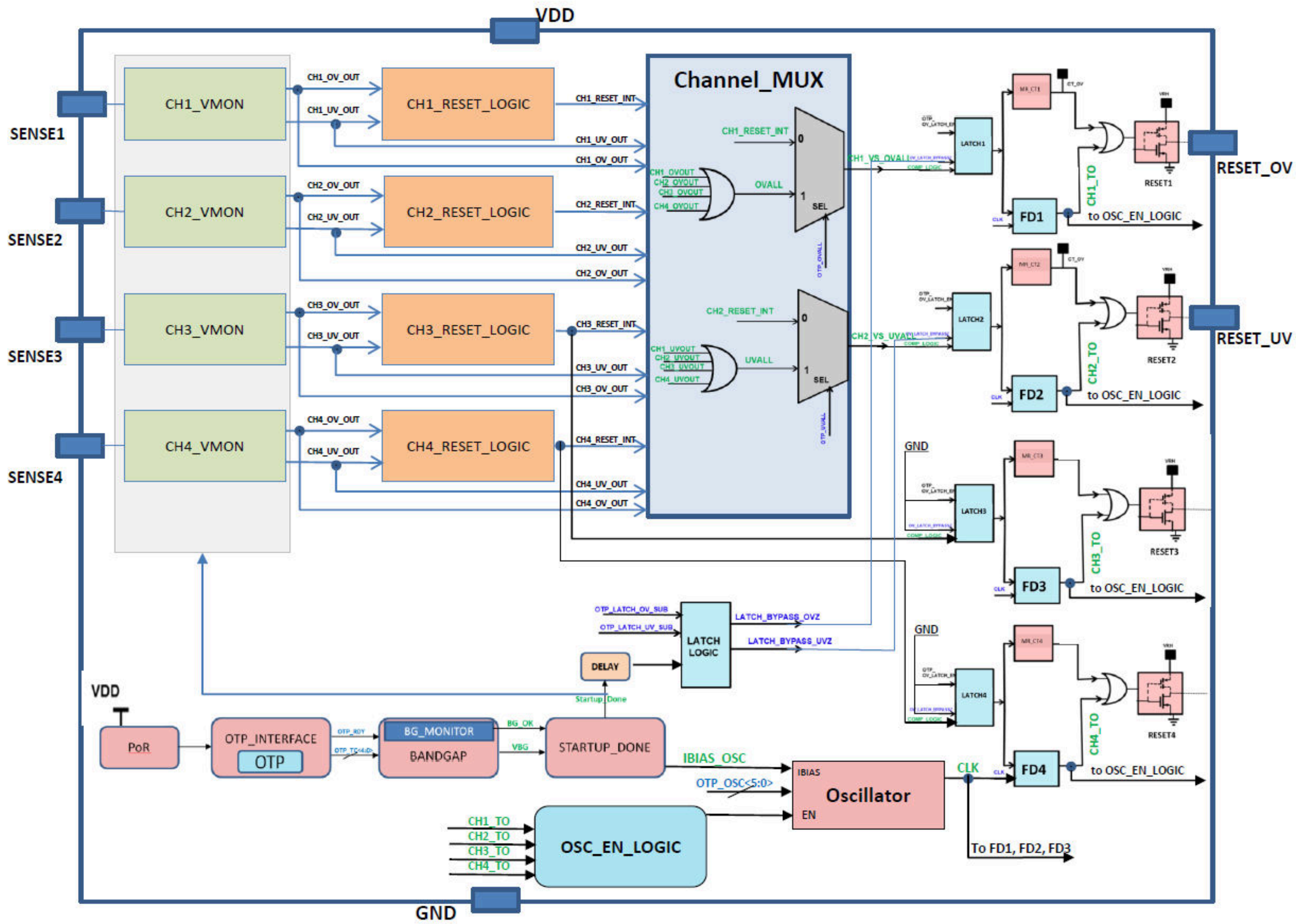

Figure 5-2. TPS3704x-Q1 Dual-channel Internal Block Diagram

TPS3704x-Q1 is a family of quad, triple, dual, and single precision voltage supervisor(s) where each channel has overvoltage and undervoltage detection capability. The TPS3704x-Q1 features a highly accurate window threshold voltage where the upper and lower thresholds can be customized for symmetric or asymmetric tolerances. The reset signal for the TPS3704x-Q1 is asserted, with a fault detection time delay (t_{PD} = 10 µs max), when the sense voltage is outside of the overvoltage and undervoltage thresholds.

TPS3704x-Q1 includes the resistors used to set the overvoltage and undervoltage thresholds internal to the device. These internal resistors allow for lower component counts and greatly simplifies the design because no additional margins are needed to account for the accuracy of external resistors. The level of integration in the TPS3704x-Q1 enables a total small solution size for any application.

The TPS3704x-Q1 is capable to monitor any voltage rail with high resolution (V_{IT} ≤ 0.8 V: 20 mV steps / V_{IT} > 0.8 V: 0.5% or 20 mV steps whichever is lower). The device includes fixed reset time delay (t_D) options ranging from 20 µs to 1200 ms and can monitor up to four channels while maintaining an ultra-low I_Q current of 20 µA (max).

This page intentionally left blank.

Chapter 6

TPS3704x-Q1 Management of Random Faults

For a functional safety critical development it is necessary to manage both systematic and random faults. The TPS3704x-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 theTPS3704x-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

$\overline{\text{RESETx}}$/RESETx asserts when SENSEx falls outside of the over-voltage or under-voltage threshold window. $\overline{\text{RESETx}}$/RESETx stays asserted for the reset timeout period after SENSEx fall back within the window threshold. Active-low, open-drain reset output, requires an external pullup resistor. For TPS37044, $\overline{\text{RESETx}}$/RESETx asserts when either SENSEx or SENSEx fall outside of the window threshold. The pin can be left floating if it is unused.

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 TPS3704x-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.

SM01 - OTP Write Protection

The OTP Write Protection ensures that the OTP cells are only written to when necessary. 2 Key Security- Fast slew rate input pulses, Secure sequence along with Clock, Fast Clocking required to enable OTP write. OTP Lock bits set after programming with Checksum bit for data verification. This method prevents rewrite of OTP in production. Checksum Bit verifies data integrity.

SM02 - SENSEx UV

For each Sense channel n(1..4), the TPS3704x-Q1 shall assert RESET_UV when the voltage on the SENSEn pin is less than the programmed OTP_UV_VALn threshold for a time-interval longer than the sense propagation delay tPD.

SM03 - SENSEx OV

For each Sense channel n(1..4), the TPS3704x-Q1 shall assert RESET_OV when the voltage on the SENSEn pin is greater than the programmed OTP_OV_VALn threshold for a time-interval longer than the sense propagation delay tPD.

SM04 - Configuration Checksum

OTP Checksum bit shall be checked at system startup before latch load to confirm OTP integrity. RESET will not be released at startup if there is a checksum mismatch

SME03 - RESET verifcation at startup

The TPS3704x-Q1 Shall assert all available RESET outputs during startup and release once Device has reached Safe active state. Host to Monitor RESET outputs at startup and confirm assertion, followed by de-assertion on expected timeline. This method can be used to detect issues with RESET pins, unexpected delays in RESET reponse, Issues with Latch logic, etc.

This page intentionally left blank.

Appendix 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 Chapter 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. Assumed Safety Diagnostic Requirements

Hardware Safety Requirement ID	Technical Safety Requirement ID	Assumed Diagnostic Requirement (Safety Features in IC that meet corresponding system requirements)	ASIL	FTTI	Status
HSR1-1.1	TSR1-1	For each SENSEx (x=1..4) channel, the TPS3704x-Q1 shall assert CHx_UV_OUT when the voltage on the SENSEx pin is less than the programmed OTP_UV_VALx threshold for a time-interval longer than the propagation detect delay tPD.	ASIL A	100ms	Assumed
HSR1-1.2	TSR1-1	For each SENSEx (x=1..4) channel, the TPS3704x-Q1 shall assert CHx_OV_OUT when the voltage on the SENSEx pin is greater than the programmed OTP_OV_VALx threshold for a time-interval longer than the propagation detect delay tPD.	ASIL A	100ms	Assumed
HSR1-1.3	TSR1-1	The TPS3704x-Q1 shall assert each RESETn (n=1..3) output based on CHANx_OV_OUT and CHx_UV_OUT (x=1..4) dependant on device configuration. These options include: RESETn (n=from 1 to 3) matched to same SENSEx (OV only, UV only, or Window), and two RESET (RESET_OV and RESET_UV) calculated as OR(x=1..4) of all available CHx_OV_OUT and CHx_UV_OUT respectively.	ASIL A	100ms	Assumed
HSR1-1.4	TSR1-1	In the case of RESET asserted on one or more of the RESET ouptut pins due to voltage fault, the TPS3704x-Q1 shall remain in active state to monitor for additional voltage faults.	ASIL A	100ms	Assumed
HSR1-1.5	TSR1-1	In the case of RESET asserted on one or more of the RESET ouptut pins due to voltage fault, the RESET shall remain asserted for the configured reset delay tD.	ASIL A	100ms	Assumed
HSR2-1.1	TSR2-1	The TPS3704x-Q1 shall assert all RESETn (n=1..4 depending on configuration) at startup for tSTRT and then release reset once VDD > VDD(MIN).	ASIL A	100ms	Assumed

Appendix 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

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

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

(1) For component technical questions, 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 will be used interchangeably depending on the TI functional safety product.

Revision History

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

Changes from Revision * (April 2022) to Revision A (May 2022) **Page**

- Initial Public Release... 5

This page intentionally left blank.