Functional Safety Information

Safety Manual for TPS65381-Q1 and TPS65381A-Q1 Multirail Power Supply

ABSTRACT

This document is a safety manual for the Texas Instruments TPS65381x-Q1 (TPS65381-Q1 and TPS65381A-Q1) multirail power supply. This manual provides information to help developers integrate the TPS65381x-Q1 device into safety related systems.

Table of Contents

List of Figures

List of Tables

Trademarks

C2000™ and Hercules™, are trademarks of Texas Instruments.
All trademarks are the property of their respective owners.

1 Introduction

The system and equipment manufacturer or designer (as user of this document) is responsible to ensure that their systems (and any TI hardware or software components incorporated in their systems) meet all applicable safety, regulatory, and system-level performance requirements. All application and safety-related information in this document (including application descriptions, suggested safety measures, suggested TI products, and other materials) is provided for reference only. Users understand and agree that their use of TI components in safety-critical applications is entirely at their risk, and that user (as buyer) agrees to defend, indemnify, and hold harmless TI from any and all damages, claims, suits, or expense resulting from such use.

This safety manual provides information to help system developers create safety-related systems using the supported TPS65381x-Q1 multirail power supply. This document contains:

- An overview of the product architecture
- An overview of the development process used to reduce systematic failures
- An overview of the safety architecture for management of random failures
- Assumptions of Use (AoU) that the system integrator may consider to use this part in an ISO26262-compliant system.
- The details of architecture partitions, and implemented safety mechanisms

Separate documents provide the following information, not covered in this document:

- Failure rates estimation
- Qualitative failure analysis (design FMEA)
- Quantitative failure analysis (quantitative FMEDA)
- Safety metrics calculated per targeted standards per system example implementation

TI expects that the user of this document has a general familiarity with the TPS65381x-Q1 device. This document is intended to be used in conjunction with the pertinent data sheets and other documentation for the products under development. This partition of technical content is intended to simplify development, reduce duplication of content, and avoid confusion as compared to the definition of safety manual in IEC 61508:2010.

2 Product Overview

The TPS65381x-Q1 device is a multirail power supply designed to supply microcontrollers (MCUs) in safety-relevant applications, such as those found in automotive and industrial markets. The device supports Texas Instruments' Hercules™ TMS570 MCU and C2000™ families, and various other MCUs with dual-core lockstep (LS) or loosely-coupled architectures (LC).

The TPS65381x-Q1 integrates multiple supply rails to power the MCU, transceiver (CAN or other), and an external sensor. An asynchronous buck switch-mode power-supply converter with internal FET converts the input supply (battery) to a 6-V preregulator output. This 6 V supplies the other regulators.

The integrated 5-V linear regulator with internal FET is typically used to supply a transceiver or other peripheral. A second integrated linear regulator, also with internal FET, regulates to a selectable 5-V or 3.3-V MCU I/O voltage.

The TPS65381x-Q1 includes the VDD1 voltage-regulator controller, typically used to supply the MCU core rail. This linear regulator controller uses an external FET and resistor divider (for adjustment). It regulates the 6 V to an adjustable voltage of between 0.8 V and 3.3 V for the core.

The device includes a sensor supply, VSOUT1.

The device has an integrated charge pump to provide an overdrive voltage for the internal regulators. One option for reverse-battery protection uses the charge-pump output to control an external NMOS transistor. This solution allows for a lower minimum battery voltage operation compared to a traditional reverse-battery blocking diode because there is less voltage drop across the transistor.

The device monitors undervoltage and overvoltage on all regulator outputs, battery voltage, and internal supply rails. A second band-gap reference, independent from the main band-gap reference, monitors for undervoltage and overvoltage, to avoid any drifts in the main band-gap reference being undetected. In addition, the device implements regulator current limits and temperature protections.

The TPS65381x-Q1 functional safety architecture features a watchdog configurable for question and answer (Q&A) mode or trigger mode, MCU error-signal monitor (ESM), diagnostic check for the MCU ESM, clock monitoring on internal oscillators, self-check on clock monitor, CRC on internal nonvolatile memory (EEPROM), CRC for configuration registers, diagnostic multiplex output to route internal analog (AMUX) and digital (DMUX) signals out through the DIAG_OUT pin, and a reset circuit for the MCU. A built-in self-test (BIST) allows for monitoring the device functionality at power up.

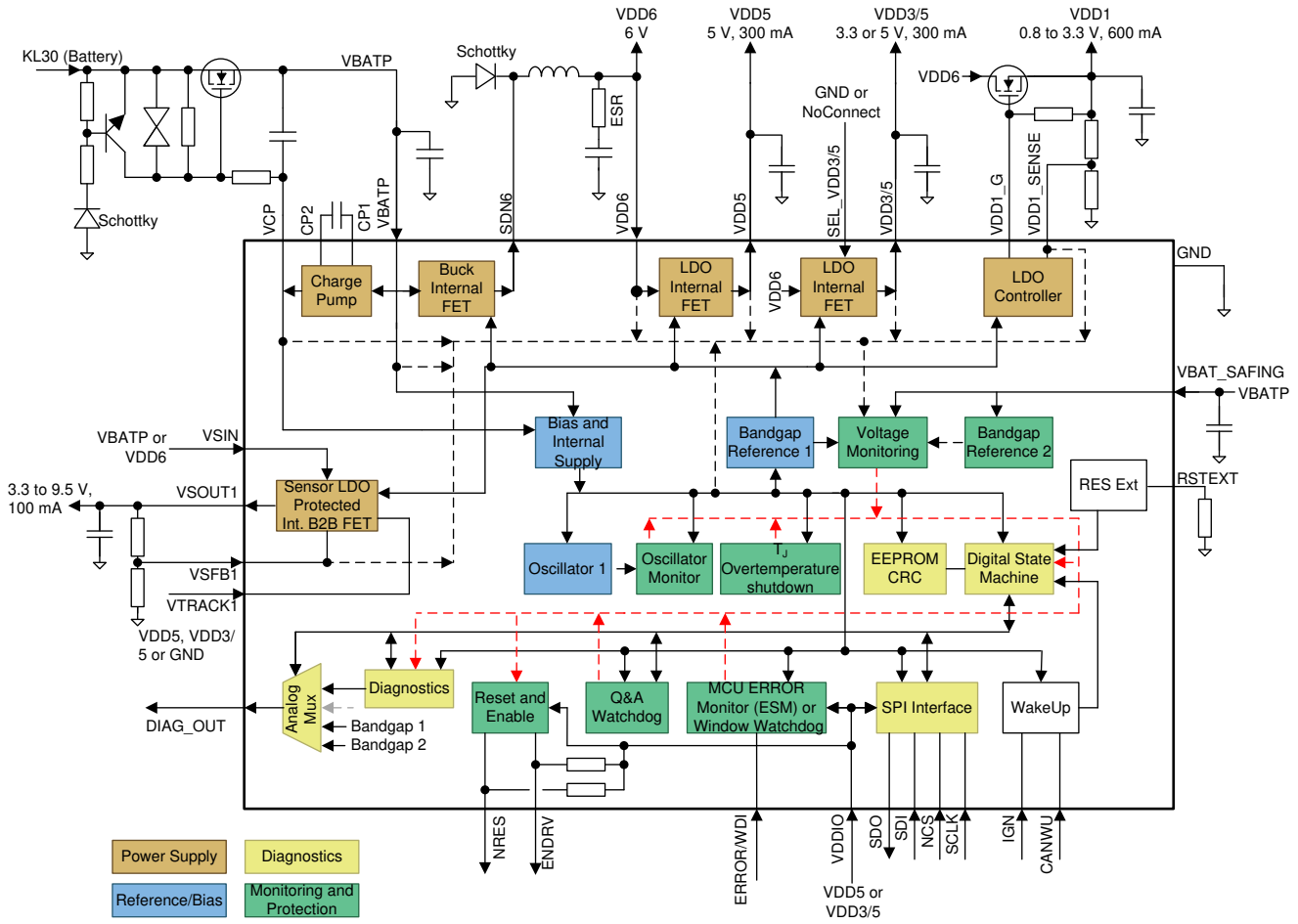


Figure 2-1. TPS65381x-Q1 Architecture Overview

2.1 Safety Functions and Diagnostics Overview

The TPS65381x-Q1 device is intended for use in automotive and industrial safety-relevant applications. The following list of monitoring and protection blocks are those that improve the diagnostic coverage and decrease the undetected fault rate:

- Voltage monitor (VMON)
- Analog built-in self-test (ABIST) diagnostics for safety analog blocks
- Logic built-in self-test (LBIST) for safety controller functions
- Loss-of-clock monitor (LCMON)
- Junction temperature monitoring (overtemperature)
- Current-limit for all power supplies with integrated FETs
- Analog MUX (AMUX) for externally monitored diagnostics and debug
- Digital MUX (DMUX) for externally monitored diagnostics and debug
- Watchdog configurable for trigger mode (open and close window) or question and answer mode
- MCU error signal monitor (ESM) for monitoring the error output from functional safety architecture MCUs
- Controlled and protected enable output (ENDRV) for external power stages or peripheral wakeup
- Device configuration register CRC protection
- EEPROM analog trim content CRC protection
- SPI command decoder with parity check
- SPI data output feedback check
- Reset circuit for initializing external MCU
- Device state controller with SAFE state in case of detected error event

2.2 Target Applications

The TPS65381x-Q1 device is designed for use as the microcontroller power supply in general-purpose safety applications such as:

- Motor-control systems, electronic power steering (EPS) systems, and electrical vehicle (EV) power train
- Automotive braking systems, including anti-lock braking (ABS), anti-lock braking with traction control (ABS+ TC), and electronic stability control (ESC)
- Automotive airbag applications
- Battery Monitoring applications
- Industrial safety applications, including motor-driver, factory automation, building control, and other applications

In designing this component, TI made various assumptions about how it could be used to address expected requirements for motor-control systems, braking applications, and airbag applications.

In the case of overlapping requirements between target systems, TI designed the device respecting the most stringent requirement. For example, the fault-tolerant response-time intervals in an ESC application are typically on the order of 100 ms. In an EPS application, the fault-tolerant response-time interval is typically on the order of 10 ms. In such case, TI has performed timer subsystem analysis respecting a fault-tolerant time interval less than 10 ms.

Although TI has considered certain applications while developing this device, this should not restrict a customer who wishes to implement other systems. With all safety-critical components, the system integrator must rationalize the component safety concept to confirm that it meets the system safety requirements.

2.3 Product Safety Constraints

The TPS65381x-Q1 device is a complex design not developed targeting a single, specific application. Therefore a single set of product safety constraints cannot govern all viable uses of the product. The additional documentation provides an example implementation of the TPS65381x-Q1 product in a common system, with relevant product-safety constraints.

The TPS65381x-Q1 Safety Analysis was performed under the following system assumptions:

- This device receives appropriate power on VBATP, VBAT_SAFING and VSIN input rails.
- The device is appropriately connected to the system's MCU or processor and other peripherals.
- This device is connected to a MCU or other processor capable of reading and reacting to reported faults as necessary.
- The TPS65381x-Q1 is configured correctly for the MCU and system requirements.
- The regulation and voltage monitoring accuracy of the device are not considered to violate the safety goal.
- Key device pins such as NRES, ENDRV, DIAG_OUT, SPI are connected to a MCU or processor and used as outlined in the device datasheet and functional safety documentation.
- All requirements in the TPS65381x-Q1 data sheet are followed.

3 Development Process for Management of Systematic Faults

For functional safety development, it is necessary to manage both systematic and random faults. Texas Instruments follows a new-product development process for all of its components which helps to decrease the probability of systematic failures. This new-product development process is described in Section 3.1.

3.1 TI New-Product Development Process

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

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

The standard development process breaks development into phases:

- Assess
- Plan
- Create
- Validate

Figure 3-1 shows the standard process.

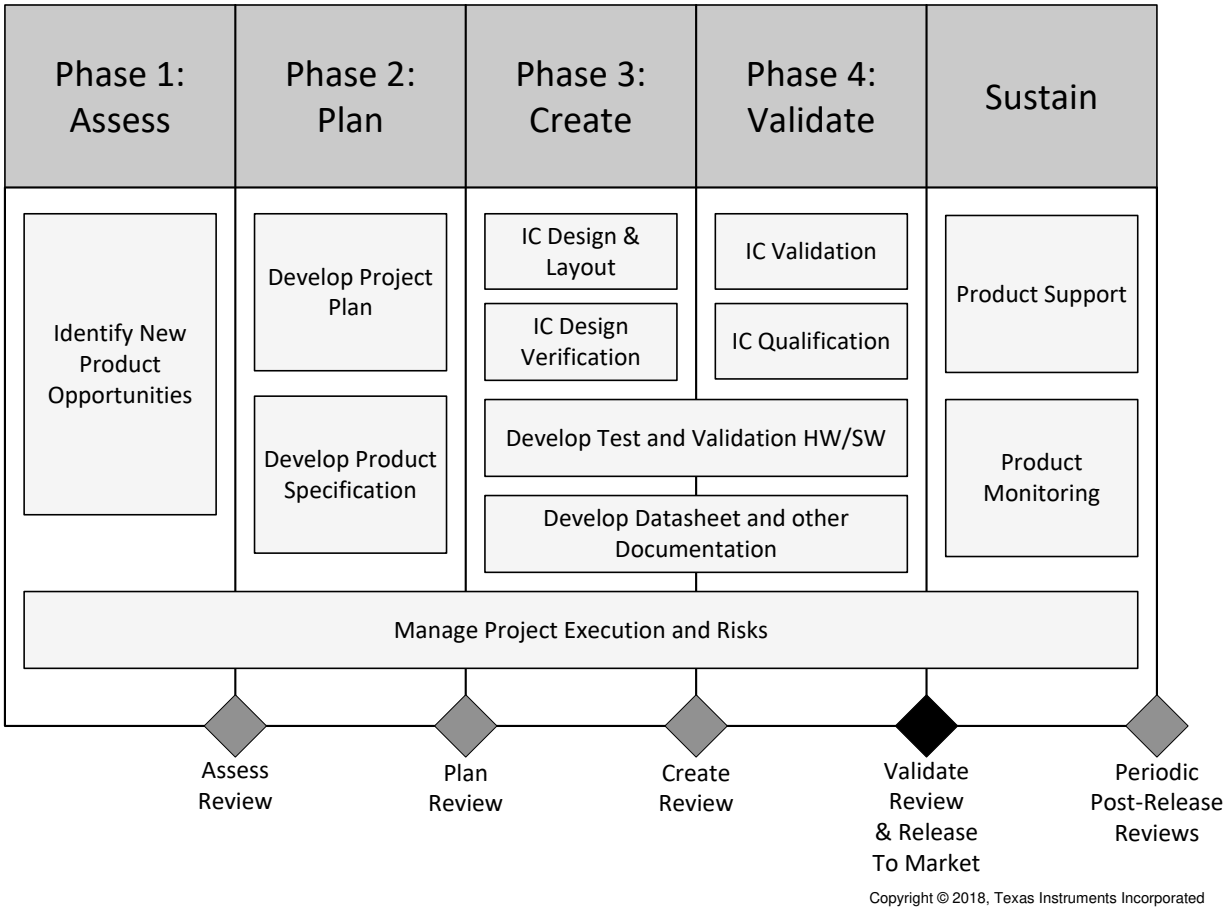


Figure 3-1. TI New-Product Development Process

4 TPS65381x-Q1 Product Architecture for Management of Random Faults

For safety-critical development, managing both systematic and random faults is required. The TPS65381x-Q1 product architecture has several modules that can detect and respond to random faults returning the device to a safe state. The effectiveness of fault management also depends on other elements of the safety system and how they are interconnected as described in part as follows.

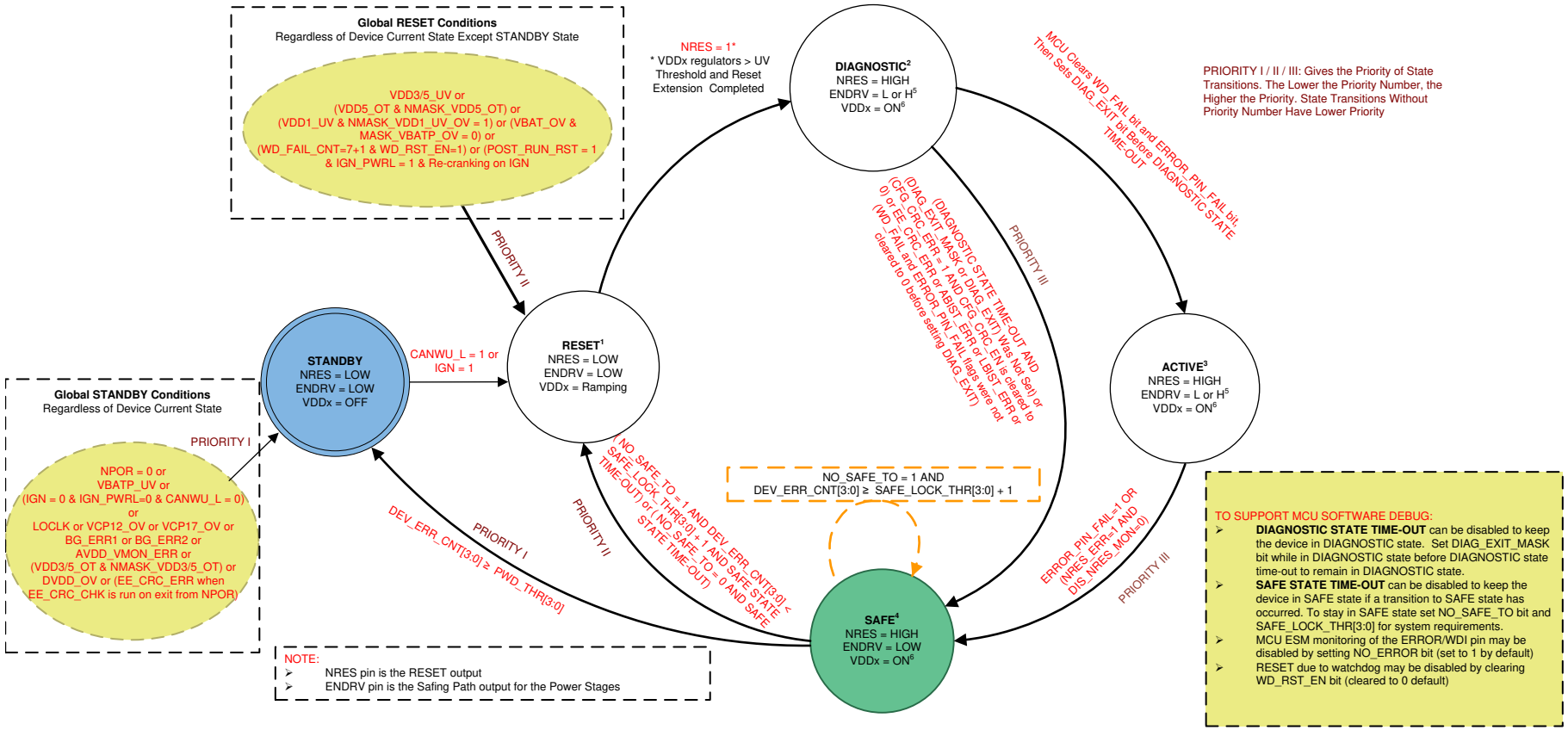
The TPS65381x-Q1 device has a core set of modules allocated for continuously operating hardware safety mechanisms. It also provides programmable mechanisms to transition the device to the default (safe) operating mode in the event of systematic or random faults. This section introduces these operation modes and safety mechanisms of the TPS65381x-Q1 device:

- PRCM (power, reset, clock management) controller
- Device state controller
- Independent band-gap reference voltages
- Independent internal analog voltage supplies for monitoring, diagnostics, and regulator circuits
- Wake-up, power down, and standby detection circuit

4.1 Device Operating States

The TPS65381x-Q1 device has multiple operating states. These operating states should be monitored by the system developer in their software and system-level design concepts. Refer to the product data sheet for details on the operation of the operating-states state machine. Figure 4-1 an overview of the operating-states state machine.

Device Operating States (continued)



(1) RESET State: SPI, Watchdog and MCU ESM are in reset; see the data sheet for conditions that prevent the wake up from the STANDBY state to the RESET state.

(2) DIAGNOSTIC State: BIST (LBIST with ABIST) is initiated on the transition into the DIAGNOSTIC state. See the data sheet for options to disable automatic BIST run, the DIAGNOSTIC state time-out and diagnostics the MCU may perform on safety functions. WD_FAIL_CNT reinitializes to 5 on transition into the DIAGNOSTIC state.

(3) ACTIVE State: WD_FAIL_CNT reinitializes to 5 during transition into the ACTIVE state. During the ACTIVE state the MCU may perform diagnostics of some safety functions, see the data sheet for more details.

(4) SAFE State: DEV_ERR_CNT[3:0] increments on any transition to the SAFE state. See the data sheet for details on SAFE state time-out.

(5) The ENDRV pin level is dependent on the ENABLE_DRV bit, WD_FAIL_CNT[2:0] counter value, and VDDx_OV as shown in Figure 4-2 in the DIAGNOSTIC and ACTIVE states.

(6) The VDD5 and VSOUT1 regulators may be enabled or disabled in the DIAGNOSTIC, ACTIVE, and SAFE states.

Figure 4-1. Device Controller State Diagram

4.2 NRES (MCU Reset) Driver and ENDRV (SAFING Path Enable) Driver

The ENDRV pin features a read-back circuit to compare the external ENDRV level with the internally applied ENDRV level. This feature is to detect a possible failure in the ENDRV pullup or pulldown components. The MCU can detect a failure by applying an appropriate diagnostic routine while the TPS65381x-Q1 device is in the DIAGNOSTIC state. This can be done by decrementing the WD_FAIL_CNT[2:0] counter to less than five and setting the ENABLE_DRV bit to ensure the ENDRV pin goes high, then the MCU causes the WD_FAIL_CNT[2:0] counter to increment greater than four and makes sure the ENDRV pin goes low. The MCU then clears the ENABLE_DRV bit until the full DIAGNOSTIC routine is complete and the system is ready to transition to normal operation. For normal operation the MCU commands the TPS65381x-Q1 device to transition to the ACTIVE state and then resets the ENABLE_DRV bit to 1. The NRES output is normally used to reset the MCU when the TPS65381x-Q1 device detects faults that cause the device to transition to the RESET or STANDBY state.

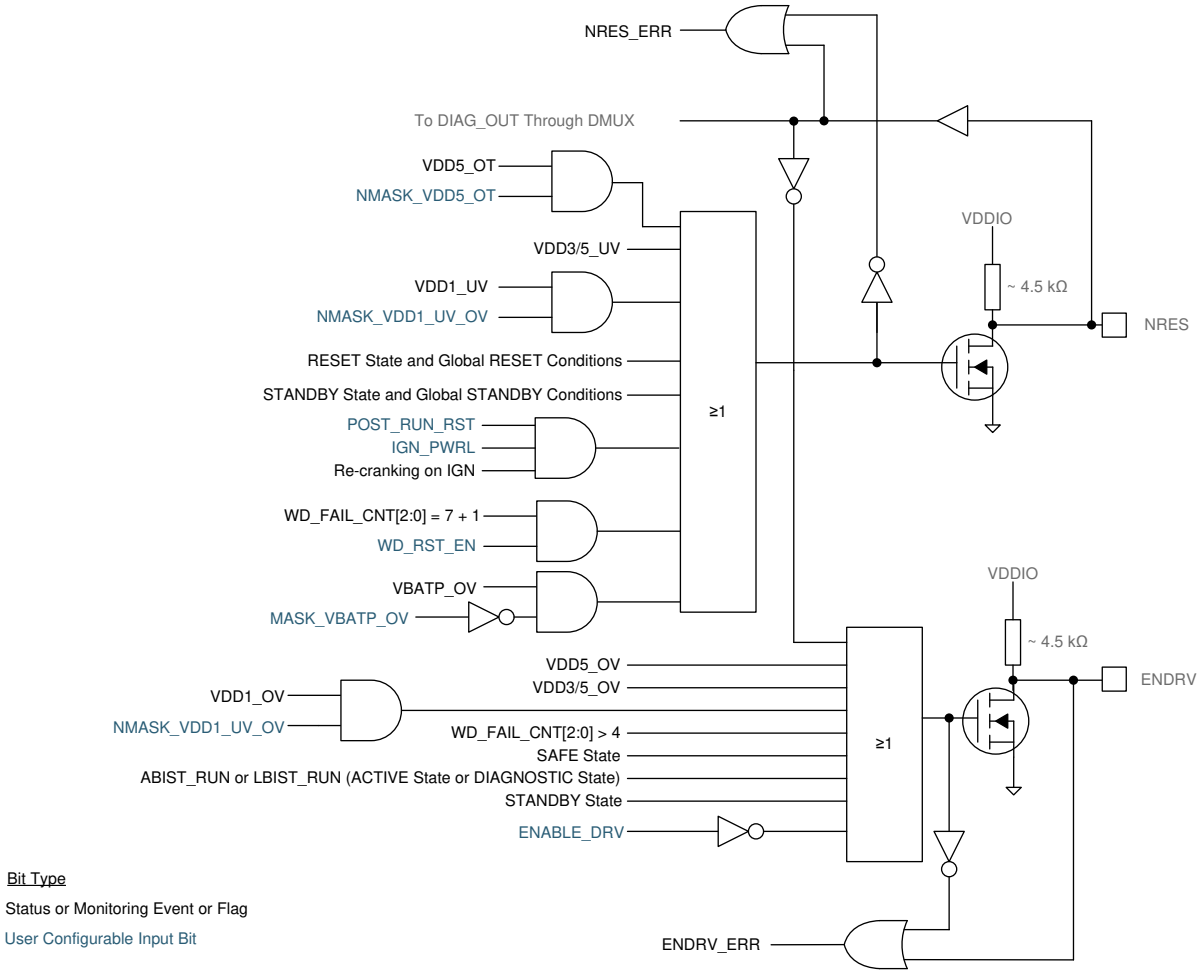


Figure 4-2. Reset (NRES) and Enable (ENDRV) Circuit

5 TPS65381x-Q1 Architecture Safety Mechanisms and Assumptions of Use

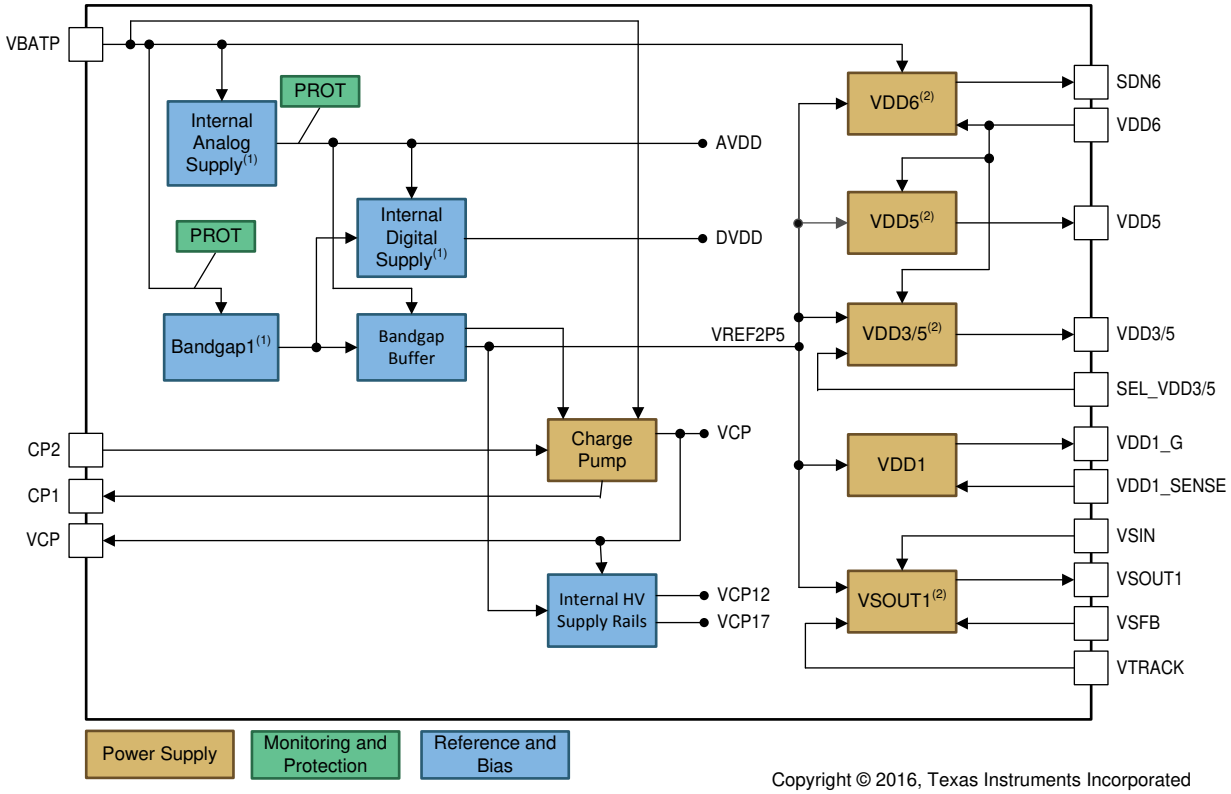
This section summarizes the safety mechanisms for each major functional block of TPS65381x-Q1 architecture and provides general assumptions of use. Use this information to determine the strategy for using safety mechanisms. The product data sheet contains the details of each safety mechanism. The FMEDA notes the effectiveness of these safety mechanisms. The system integrator must comprehensively assess effectiveness in the context of the specific end use.

5.1 Power Supply

The TPS65381x-Q1 device requires an external battery or other power supply. The supply voltage is monitored for undervoltage (UV) and overvoltage (OV) conditions. Analog built-in-self-test (ABIST) covers UV and OV comparator diagnostics.

Depending on the regulator and possible mask bit settings, when an UV or OV event is detected the device may indicate the OV or UV event or transition to the STANDBY or RESET state.

5.2 Regulated Supplies



(1) Blocks are turned on during standby.

(2) Integrated current limit. Current limit is combined for the VDD6 and VDD3/5 regulator.

Figure 5-1. Regulated Supplies

5.2.1 VDD6 Buck Switch-Mode Supply

The current limit and overtemperature protection circuit (shared with VDD3/5 overtemperature) protect the internal MOSFET against excess power dissipation.

5.2.2 VDD5 Linear Supply

Current limit protects this output against shorts to ground and limits output voltage overshoot during power up or during line or load transients. Current-limit and overtemperature protection circuits protect the internal MOSFET against excess power dissipation.

5.2.3 VDD3/5 Linear Supply

The SEL_VDD3/5 pin selects the output voltage level (not connected or open selects 3.3 V, pin to ground selects 5 V). The state of this pin is sampled and latched at power up from the STANDBY state. After latching at power up, any later change in the state of this pin does not change the output voltage level of the VDD3/5 regulator.

A current limit protects this output against shorts to ground and limits output voltage overshoot during power up or during line or load transients. Current limit and overtemperature protection circuits protect the internal MOSFET against excess power dissipation.

5.2.4 VDD1 Linear Supply

Use of an external power NMOS reduces the on-chip power consumption. Limiting the VDD1 gate output prevents gate-source overvoltage stress during power up or during line or load transients.

The VDD1 LDO controller does not have a current limit or overtemperature protection for the external NMOS FET. Therefore, TI recommends supplying the VDD1 LDO controller from VDD6 the regulator. VDD6 current limit acts as a current limit for the VDD1 LDO controller and also limits the power dissipation.

If the VDD1 regulator is not being used, leave the VDD1_G and VDD1_SENSE pins open. An internal pullup device on the VDD1_SENSE pin detects the open connection and pulls up the VDD1_SENSE pin. This forces the regulation loop to bring the VDD1_G output down. This mechanism also masks the VDD1_OV flag in the VMON_STAT_2 register and therefore ENDRV pin action from a VDD1 OV condition is also masked. These actions are equivalent to clearing the NMASK_VDD1_UV_OV bit in the DEV_CFG1 register to 0. This internal pullup device on the VDD1_SENSE pin also prevents a real VDD1 overvoltage on the MCU core supply in case of an open connection to the VDD1_SENSE pin, as it brings the VDD1_G pin down. Therefore, in this situation, the VDD1 output voltage is 0 V.

The internal pullup for the VDD1_SENSE pin also prevents a VDD1 overvoltage on the MCU core supply in case of an open connection in the feedback network, because it brings the VDD1_G pin low. So in this situation, the VDD1 output voltage is 0 V.

Note

The following cases must be considered with respect to the VDD1 linear supply, assuming a typical application where the VDD1 regulator is supplied from the VDD6 preregulator.

In a fault case, if the VDD1_G pin (pin 26) is shorted to the VDD6 pin (pin 27), the VDD1_G pin is pulled up to VDD6. The VDD1 regulator output voltage will increase to VDD6. The resulting overvoltage on VDD1 will not be detected because the overvoltage on VDD1 pulls the VDD1_SENSE pin higher than the threshold for the floating pin detection on the VDD1_SENSE pin. No impact occurs to the ENDRV pin level, device state, or NRES pin level.

In a fault case, if the VDD1_SENSE (pin 24) is shorted to ground or the GND (pin 23) or the PGND (pin 25), the VDD1_G output voltage increases to its maximum output voltage. The VDD1 regulator output increases to VDD6. If the NMASK_VDD1_UV_OV bit is cleared to 0 (default), the resulting overvoltage on VDD1 and undervoltage on VDD1_SENSE is masked so no impact occurs to the device operation. If the NMASK_VDD1_UV_OV bit is set to 1, the device will detect an undervoltage on the VDD1_SENSE pin causing a transition to RESET state which drives the NRES pin low and the ENDRV pin low.

5.2.5 VSOUT1 Linear Supply

The intent of this supply is to provide a supply for a sensor or other peripheral. Current limit protects this output against shorts to ground and limits output voltage overshoot during power up or during line or load transients. Current-limit and overtemperature protection circuits protect the internal MOSFET against excess power dissipation. If the supply is used to supply a sensor outside the ECU additional protections may be required.

5.2.6 Charge Pump

The charge-pump overdrive voltage can be used to drive the gate of an external NMOS power FET acting as reverse-battery protection. Such reverse-battery protection allows for a lower minimum battery voltage operation compared to a traditional reverse-battery blocking diode.

5.3 Diagnostic, Monitoring, and Protection Functions

5.3.1 External MCU Fault Detection and Management

When the integrated diagnostics detect an external MCU fault, indication of the error is necessary. The TPS65381x-Q1 device uses the watchdog function, or MCU error signal monitor (ESM) to monitor the external MCU for hardware and software faults. On detection of an external MCU fault in the ACTIVE state, the TPS65381-Q1 device transitions to the SAFE or RESET state and can increment the device error counter depending on the specific fault and state transition. Refer to the data sheet for all state transitions caused by MCU faults.

In the SAFE state, the MCU can perform additional diagnostics to confirm the root cause of the fault.

If the detected fault condition or event has caused the MCU to be nonresponsive, the TPS65381x-Q1 watchdog detects a timeout event, when the watchdog failure counter (WD_FAIL_CNT[2:0]) has a next timeout after it reaches 7, the device transitions through the RESET state, pulling the NRES pin low and asserts a reset to the external MCU attempting to recover the MCU from the non-responsive state.

In case the MCU does not provide the correct signal to the MCU ESM in the TPS65381x-Q1 device, the TPS65381x-Q1 transitions to the SAFE state. Depending on how the NO_SAFE_TO, SAFE_LOCK_THR[3:0], and PWD_THR[3:0] bits are configured, the device either stays locked in the SAFE state or stays in the SAFE state for a configurable SAFE state time-out time before transitioning to either the RESET or STANDBY state. Refer to the *SAFE State* section of the data sheet for details on configuring these registers for the desired response of the specific application. When the TPS65381x-Q1 device transitions to the SAFE state it increments the device-error counter, DEV_ERR_CNT[3:0]. When the device-error counter reaches values matching the programmable thresholds, the TPS65381x-Q1 device transitions states accordingly.

The MCU can test the TPS65381x-Q1 device in the DIAGNOSTIC state by forcing watchdog failures while the WD_RST_EN bit is set to 0 and the MCU ESM failures. Detected watchdog failures while the WD_RST_EN bit is 0 do not cause a transition to the RESET state. Detected MCU ESM failures in the DIAGNOSTIC state do not cause a transition to the SAFE state. The error flags from forced failures during the DIAGNOSTIC state must be cleared before transition to the ACTIVE state for normal operation.

5.3.1.1 External MCU Error Signal Monitor (MCU ESM)

This block monitors the external MCU error conditions signaled to the TPS65381x-Q1 device on the ERROR/WDI input pin. The monitor has two configuration options for use with microcontrollers with dual-core lockstep (LS) or loosely coupled (LC) architectures:

- TMS570 mode: Detecting a low pulse signal with programmable expected low pulse duration.
- PWM mode: Detecting a PWM signal with programmable frequency and duty cycle.

The ERROR_CFG bit in the SAFETY_FUNC_CFG register controls the operating mode. The SAFETY_ERR_PWM_L register sets the expected low signaling duration for TMS570 mode and low pulse duration for PWM mode. The SAFETY_ERR_PWM_H register sets the expected PWM high pulse duration in PWM mode.

Logic BIST (LBIST) adds diagnostic coverage to the module. The MCU ESM can only be used when the watchdog is operated in Q & A mode.

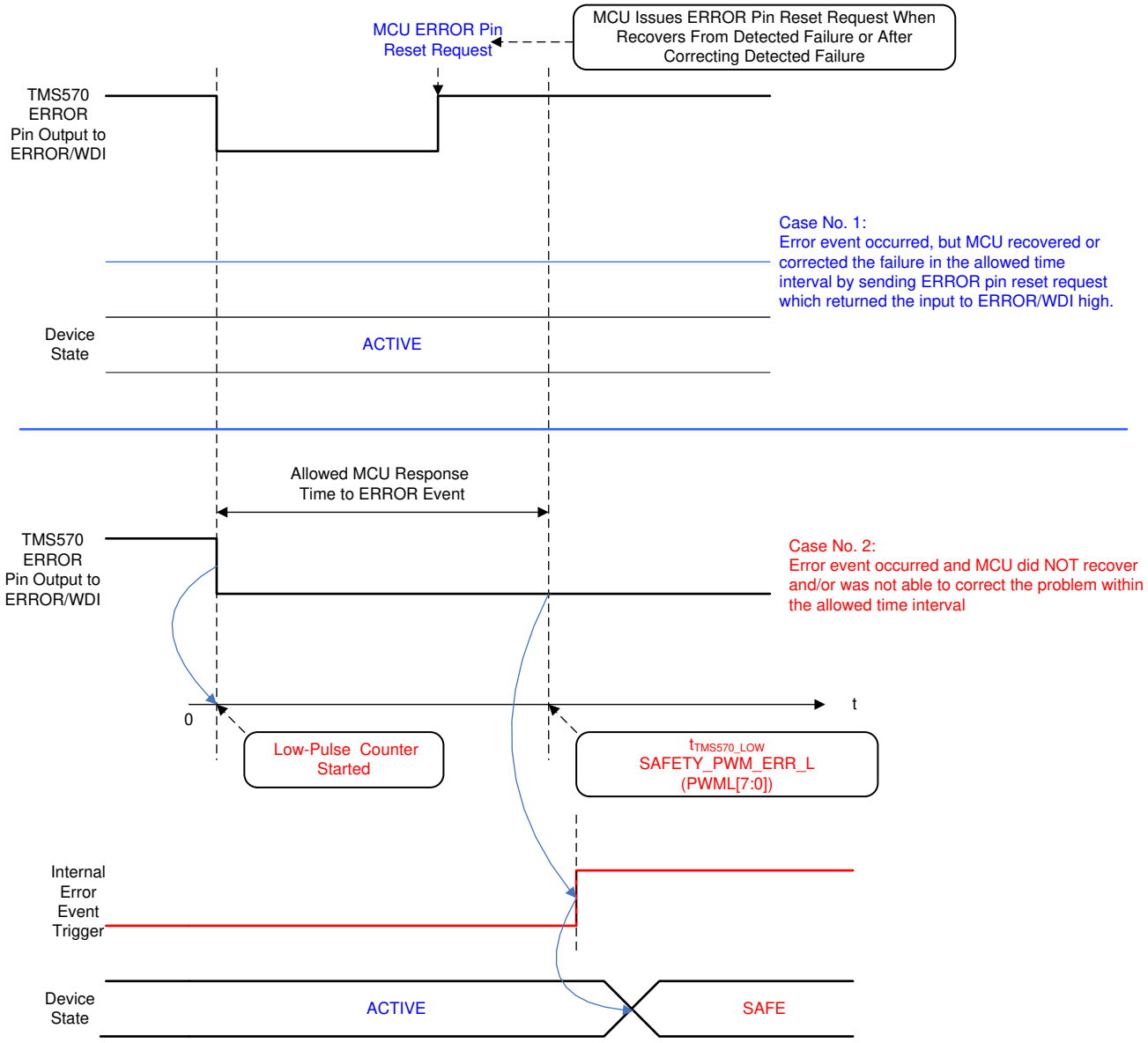


Figure 5-2. Error Detection Case Scenarios in TMS570 Mode

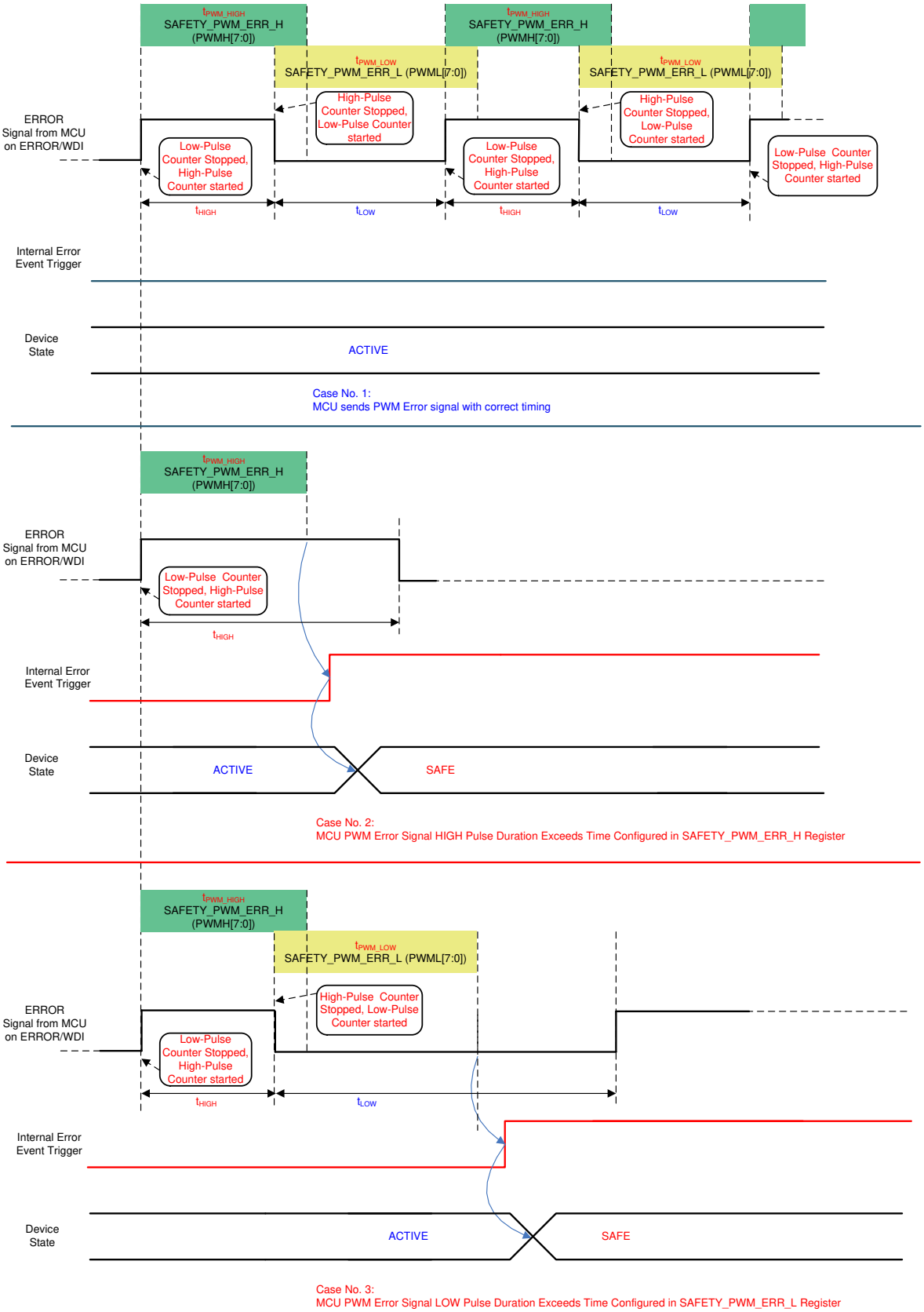


Figure 5-3. Error Detection Case Scenarios in PWM Mode

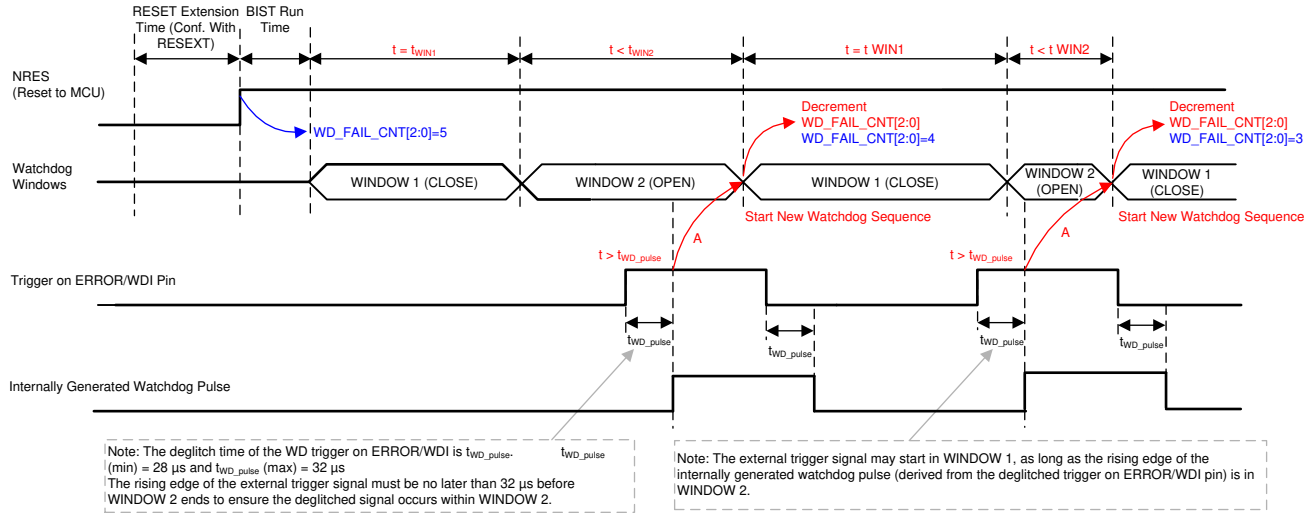
5.3.1.2 Watchdog Timer

The watchdog timer monitors proper function of the external MCU. The watchdog has two modes of operation: trigger mode or question and answer (Q&A) mode.

Trigger mode	The MCU indicates normal operation by periodically sending a watchdog trigger (pulse) on the ERROR/WDI pin, which a window watchdog must receive within a defined time windows.
Q&A mode	The MCU sends the watchdog information through SPI. The MCU reads or calculates the next question and provides four answer bytes for each question. The fourth answer byte must be in the Window 2 and all answer bytes must be correct and provided in the correct order.

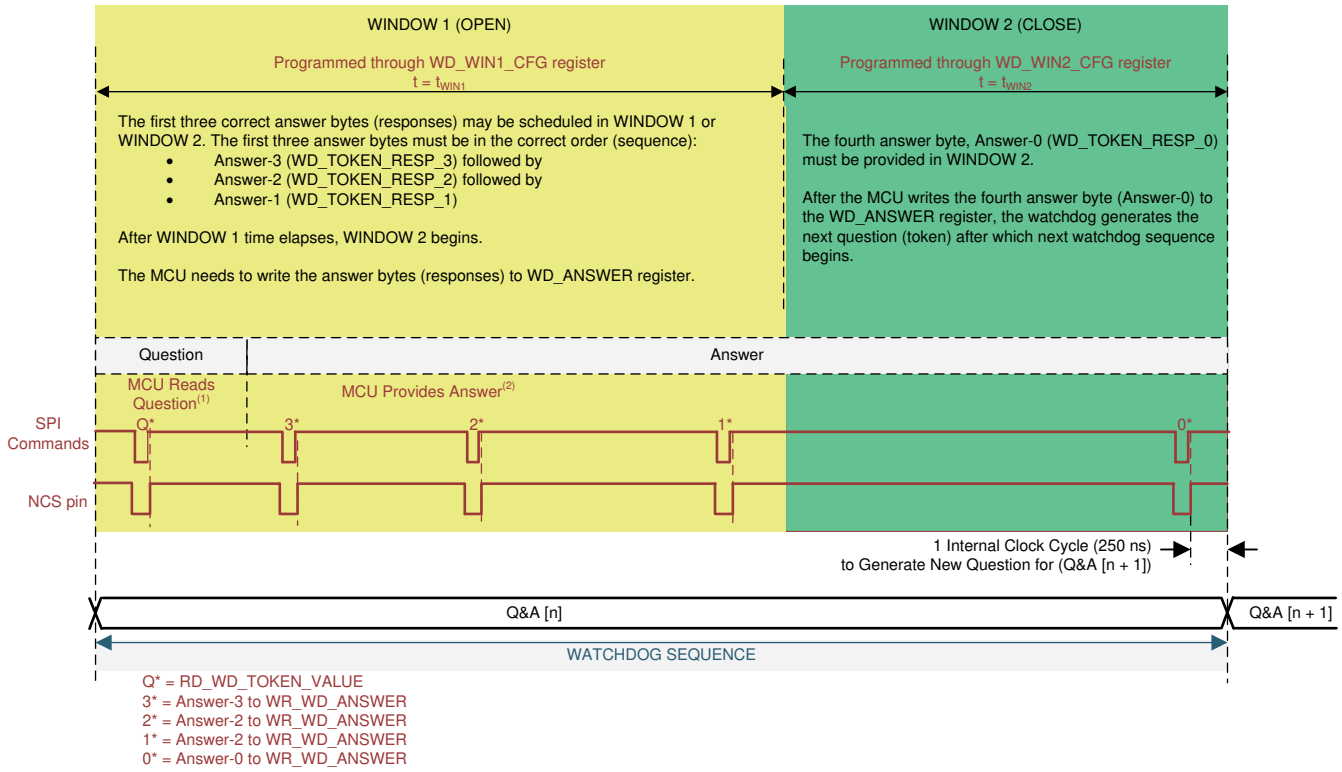
The watchdog configuration is controlled by the WD_CFG bit the SAFETY_FUNC_CFG register. The default configuration is trigger mode.

Actions are taken based on a watchdog failure counter, WD_FAIL_CNT[2:0]. *Good events* in both modes decrement the WD_FAIL_CNT[2:0] counter and *bad events* increment the counter. When the WD_FAIL_CNT[2:0] counter is less than five, the ENDRV pin can be asserted high by setting the ENABLE_DRV bit. If the MCU responds incorrectly or not at all, *bad events*, or *time-out*, are detected and the WD_FAIL_CNT[2:0] counter increment. When the WD_FAIL_CNT[2:0] counter is five or greater, the ENDRV pin is not able to be asserted high, even if the ENABLE_DRV bit is set high. If the MCU does not recover and the WD_FAIL_CNT[2:0] counter reaches 7 + 1 (the next *bad* or *time-out* event after the fail counter reaches 7) while the WD_RST_EN bit is 1 the device transitions to the RESET state and the NRES pin is pulled low. If the NRES pin is connected to the reset input circuits of the MCU, the MCU is also reset.



A. When a *good event* is received in Window 2 (OPEN), 1 system clock-cycle (250 ns, typical) later the next watchdog sequence begins. Therefore the actual length of Window 2 (OPEN) depends on when the MCU sends the good event.

Figure 5-4. Example Cases for Good Events in Trigger Mode



(1) The MCU is not required to read the question (token). The MCU can begin giving the correct answer bytes Answer-3, Answer-2, Answer-1, anywhere in Window 1 or Window 2. The new question (token) is generated and a new watchdog sequence started within 1 system clock cycle after the final Answer-0 as long as the answer was a *good event*. A *bad event* or *time-out event* causes a new watchdog sequence to start, however a new question (token) isl not generated.
(2) The MCU can put other SPI commands in-between the WR_WD_ANSWER commands (even rerequesting the question). These SPI commands have no influence on the detection of a *good event*, as long as the four correct answer bytes are in the correct order, and the fourth correct answer byte is provided in Window 2.

Figure 5-5. Watchdog Sequence in Q&A Mode

5.3.2 Voltage Monitor (VMON)

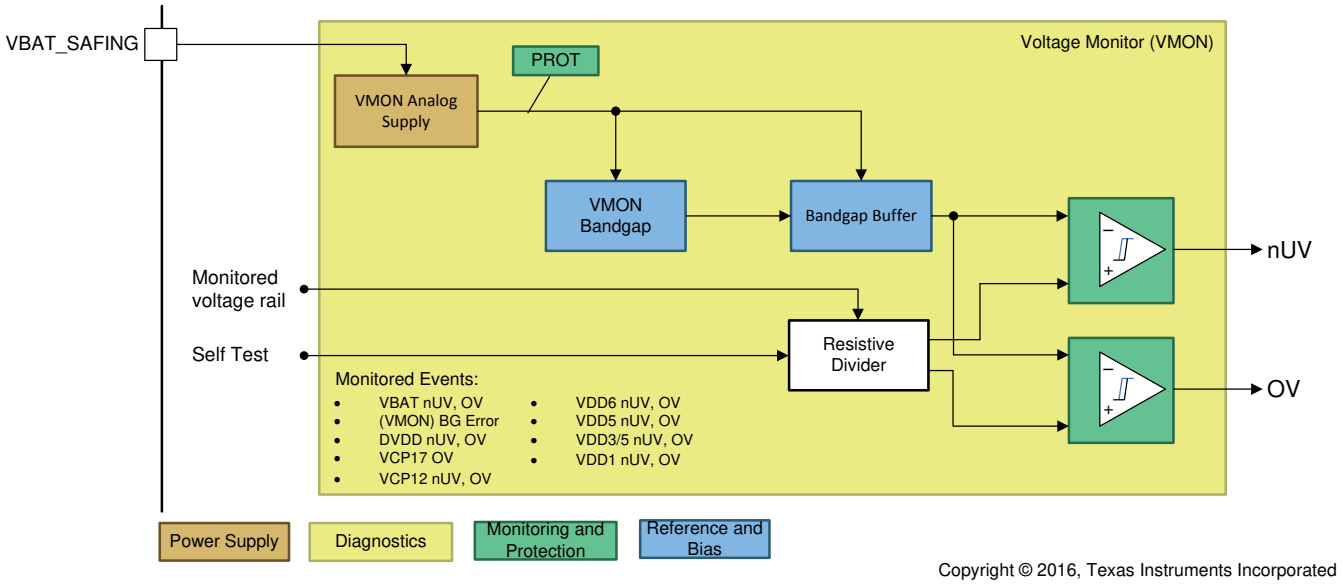
A voltage-monitor module (VMON) supervises the VBATP supply voltage, and all regulator outputs and internally generated voltages. The corresponding VMON register status flag bits indicate an undervoltage (UV) or overvoltage (OV) condition:

- VMON flag bit set to 0 when the regulator (voltage rail) is within specification
- VMON flag bit set to 1 when the regulator (voltage rail) is outside tolerance band

Undervoltage and overvoltage comparators perform the monitoring. The reference voltage (BANDGAP_REF2) for the VMON module is independent of the system reference voltage (BANDGAP_REF1) used by regulators.

A glitch-filtering function (deglitch) ensures reliable monitoring without false setting of the VMON status flag bits. A separate supply pin, VBAT_SAFING, supplies the complete VMON block.

Analog built-in self-test (ABIST) covers VMON comparator diagnostics, executed during device power up from STANDBY state. It may also be activated by the MCU though a SPI request when the device is in the DIAGNOSTIC or ACTIVE state. Emulation of each monitored voltage rail for an undervoltage and overvoltage condition on the corresponding comparator inputs forces the corresponding comparator to toggle multiple times (in a toggling pattern observed and checked by ABIST controller).



A. Monitoring of the sensor-supply output voltage occurs within the sensor supply itself using BG1 as a reference.
B. The BG1 error is caught by VMON using VMON BG as a reference.

Figure 5-6. Voltage Monitoring

5.3.3 Loss-of-Clock Monitor (LCMON)

The loss-of-clock monitor (LCMON) detects internal oscillator failures:

- Oscillator clock stuck high or stuck low
- Reduced clock frequency

The LCMON is enabled during a power-up event after a power-on reset is released. The clock monitor remains active during device normal operation (STANDBY, RESET, DIAGNOSTIC, ACTIVE, and SAFE states). In case of a clock failure:

- The device transitions to the STANDBY state.
- All regulators are disabled.
- The digital core is reinitialized
- The reset to the external MCU is asserted low (NRES).
- The failure condition is indicated by the LOCLK bit in the SAFETY_STAT_4 register.

The LCMON has a self-test structure that is activated and monitored by an analog BIST (ABIST). The external MCU can recheck the clock monitor any time when the device is in the DIAGNOSTIC state or the ACTIVE state. The enabled diagnostics emulate a clock failure that causes the LCMON output to toggle. The LCMON toggling pattern is checked by the ABIST, while the external MCU can check that the loss-of-clock status bit is being set during active test. During this self-test, the actual oscillator frequency (4 MHz) is not changed because of this self-test.

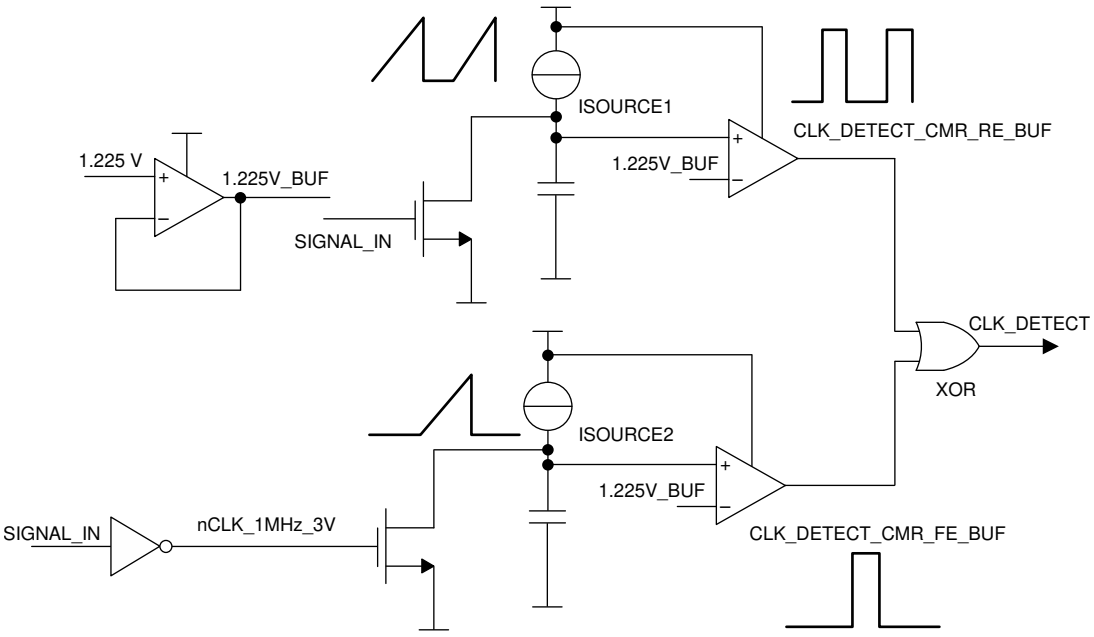


Figure 5-7. Loss-of-Clock Monitor

5.3.4 Junction Temperature Monitoring and Current Limiting

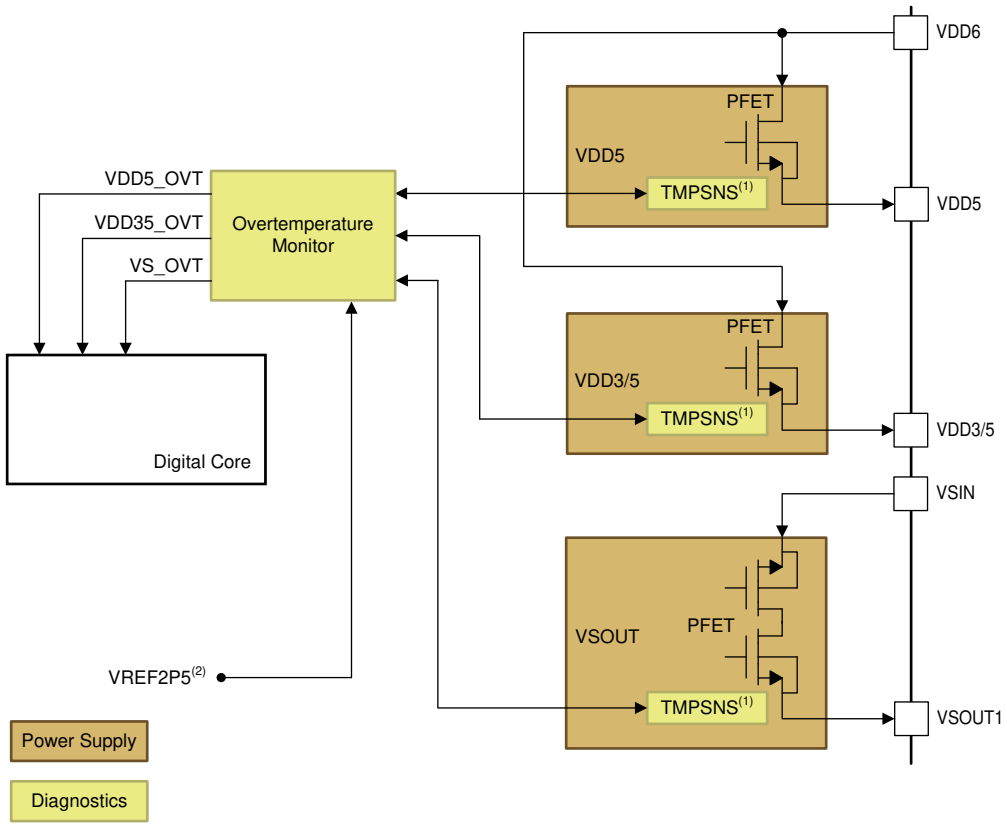
Each regulated supply with an internal power FET has junction-temperature monitoring with thermal shutdown protection. Refer to the data sheet for details on the impact of an overtemperature event on the device state and status bits for each regulator.

The VDD6, VDD3/5, VDD5, and VSOUT1 regulators include a current-limit circuit for additional protection against excessive power consumption and thermal overstress. The detection of a current limit sets a status bit for the VDD3/5 (VDD3/5_ILIM bit) and VDD5 (VDD5_ILIM bit) regulators. The current limit for the VDD3/5, VDD5, and VSOUT1 regulators may also be monitored with the diagnostic MUX output using the digital MUX (DMUX) and DIAG_OUT pin. The DMUX signal names are VDD3/5_CL, VDD5_CL and VSOUT1_CL.

Note

The VDD6 and VDD3/5 regulators share a junction-temperature monitor, but have independent current-limiting circuits.

In a typical application, the VDD1 linear regulator controller with external FET uses VDD6 as a preregulator and receives indirect current limit from the VDD6 current limit.



(1) Temperature sense elements are placed close to the power-FETs (PFETs) of the corresponding power supplies.
(2) VREF2P5 is monitored by VMON.

Figure 5-8. Temperature Monitoring

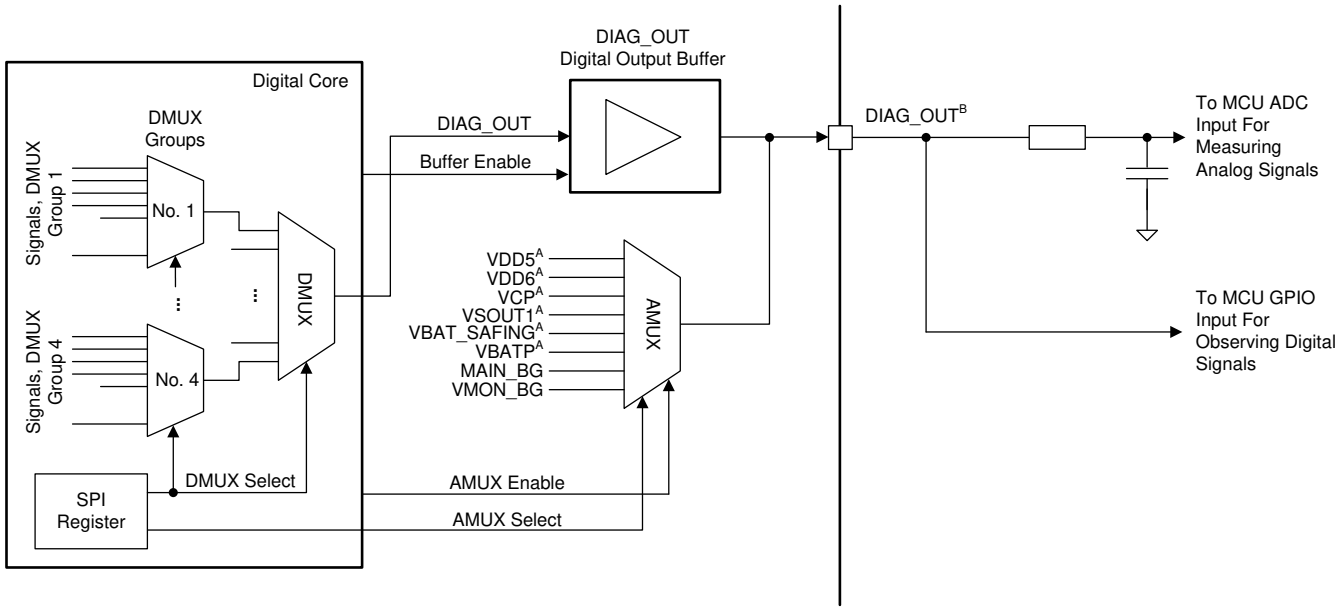
5.3.5 Analog and Digital MUX (AMUX and DMUX) and Diagnostic Output Pin (DIAG_OUT)

A multiplexer switches critical analog and digital signals to the DIAG_OUT pin for monitoring by the MCU. The DIAG_CFG_CTRL and DIAG_MUX_SEL registers program the multiplexer.

Connecting the DIAG_OUT output pin to the MCU ADC input provides redundant monitoring of safety-critical supply voltages.

The analog MUX (AMUX) and digital MUX (DMUX) facilitates external pin interconnect tests by feeding back the input pin state, internal module self-test status, or safety-critical comparator output.

Refer to the data sheet for details on using the DIAG_OUT pin for AMUX and DMUX.



A. Marked analog signals put out with divider ratio.

B. If the application must measure analog signals with an MCU ADC and monitor digital signals with an MCU GPIO, the application design must assure the GPIO input stage does not affect the ADC measurements. If isolating the MCU GPIO is not possible within the MCU, the application design must achieve the necessary isolation externally

Figure 5-9. Diagnostic Output Pin, DIAG_OUT

Note

When enabling the DIAG_OUT MUX while using SPI communication: the SDO is not in the high-impedance state while the NCS pin is HIGH and the DIAG_OUT MUX is enabled. Software or hardware modification may be required. For hardware modifications, check the SDO threshold level and drive capability if resistors are used to adjust the voltage level of the SDO pin on the SPI bus.

5.3.6 Analog Built-In Self-Test (ABIST)

The ABIST is the controller and monitor circuit for performing self-checking diagnostics on critical analog functions:

- VMON undervoltage and overvoltage comparators
- Clock monitor (LCMON)
- EEPROM analog trim content check (CRC protection)

During the self-test on the VMON undervoltage and overvoltage comparators, the monitored voltage rails themselves do not change, so no real undervoltage or overvoltage occurs on any of these rails. Furthermore, also during the self-check on the clock monitor, the actual oscillator frequency (4 MHz) is not changed.

In case of an ABIST failure while in the DIAGNOSTIC state, including a power-up event, the device enters the SAFE state without asserting a reset to the external MCU and the ABIST_ERR status flag remain latched in the digital core until a successful ABIST run. This allows the external MCU to detect the ABIST failure by reading the ABIST_ERR bits in the SAFETY_STAT_3 register. In case of an ABIST failure while in the ACTIVE state, the device sets the ABIST_ERR status flag, but no state transition occurs.

In the DIAGNOSTIC or ACTIVE state, the external MCU can activate ABIST. During an active ABIST run, the device cannot monitor the state of regulated supplies.

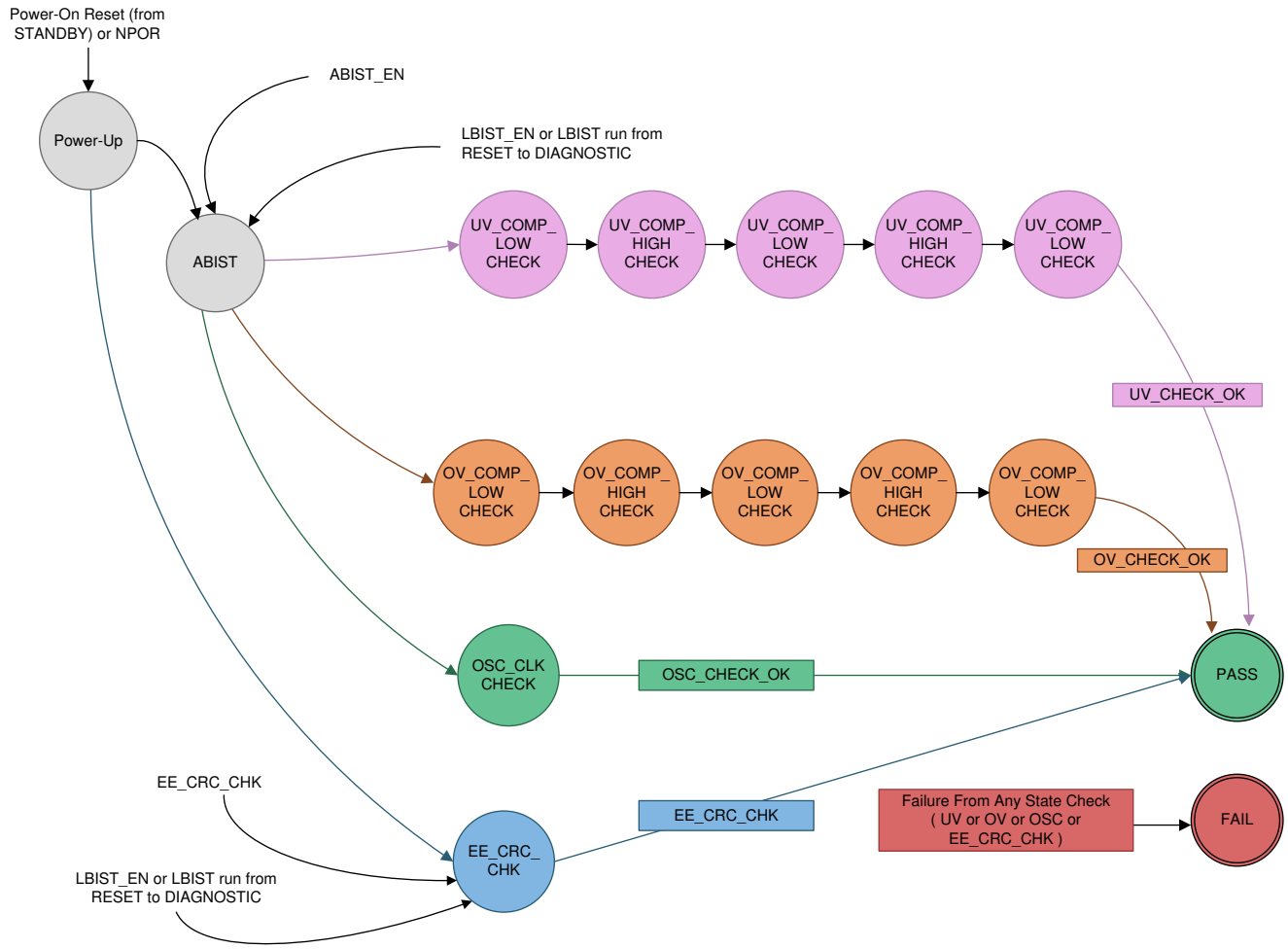


Figure 5-10. ABIST Run States

5.3.7 Logic Built-In Self-Test (LBIST)

The LBIST tests the digital-core safety-critical functions and has the follow characteristics:

- The LBIST includes an application-controllable LBIST engine which applies test vectors to the digital core.
- The LBIST engine provides stuck-at-fault grade test coverage to logic blocks under test.
- The LBIST engine has a time-out counter as a fail-safe feature.

The BIST (LBIST with ABIST) is activated with any transition out of the RESET state during power-up events. The BIST is also activated with any other transition out of the RESET state unless the AUTO_BIST_DIS bit in the SAFETY_BIST_CTRL register is set.

For complete details on the LBIST operation, refer to the device data sheet.

5.3.8 Device Configuration Register Protection

This function offers a mechanism to help protect safety SPI-mapped registers by means of SPI write-access protection and CRC check.

The register access protection includes two distinctive features:

- A register cannot be written after write-access lock protection is set. The lock is cleared by software or by a power-on reset.
- CRC protection for configuration registers.

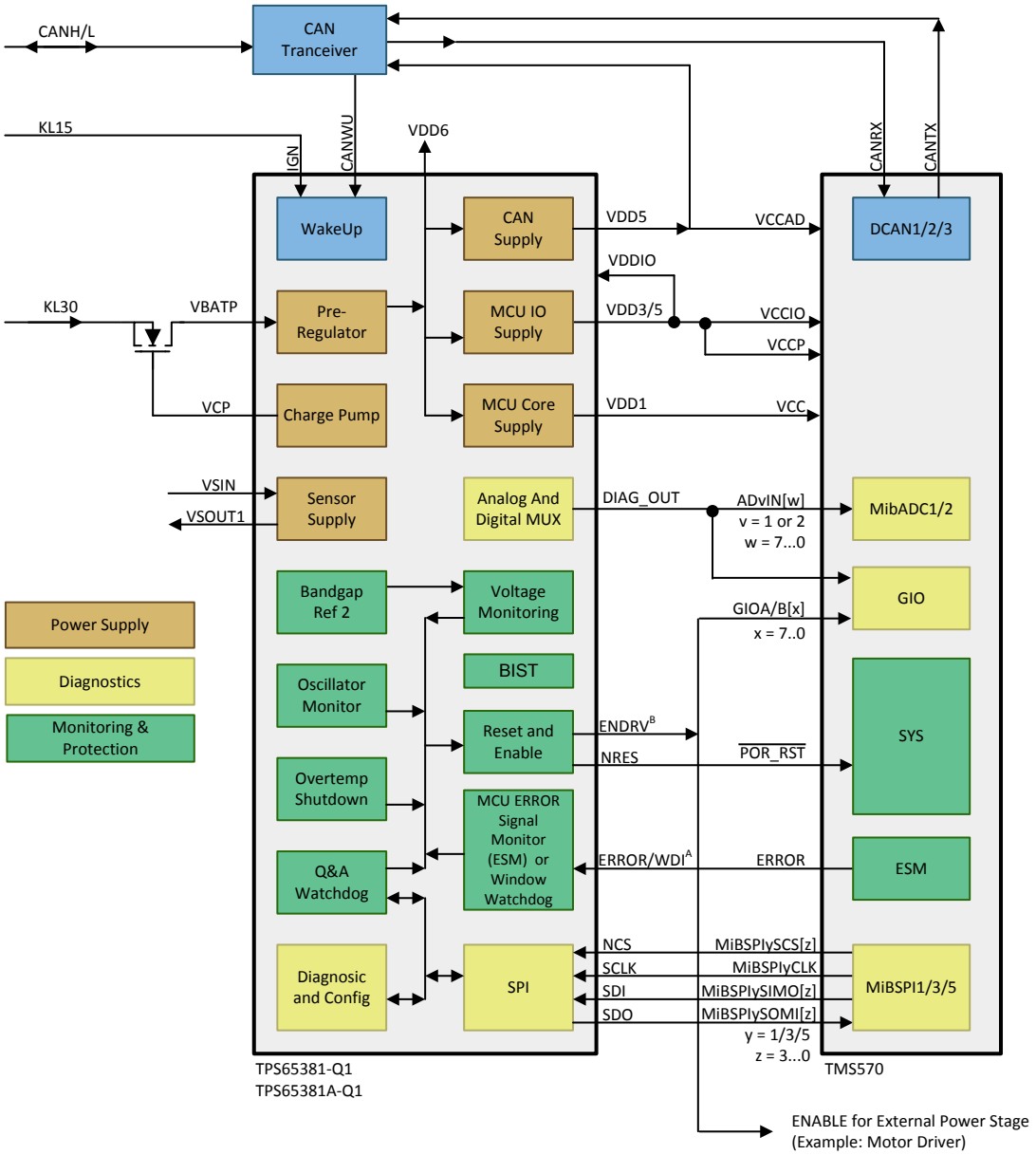
The CRC controller is a diagnostic module, which performs the CRC to verify the integrity of the SPI-mapped register space. A signature representing the content of the safety registers is obtained when the content is read into the CRC controller. The responsibility of the CRC controller is to calculate the signature for a set of data and then compare the calculated signature value against a predetermined good-signature value stored in the SAFETY_CFG_CRC register by the MCU.

For complete details on the Device Configuration Register Protection operation, refer to the device data sheet.

6 Application Diagrams

The following sections show the TPS65381x-Q1 application diagrams.

6.1 TPS65381x-Q1 With TMS570

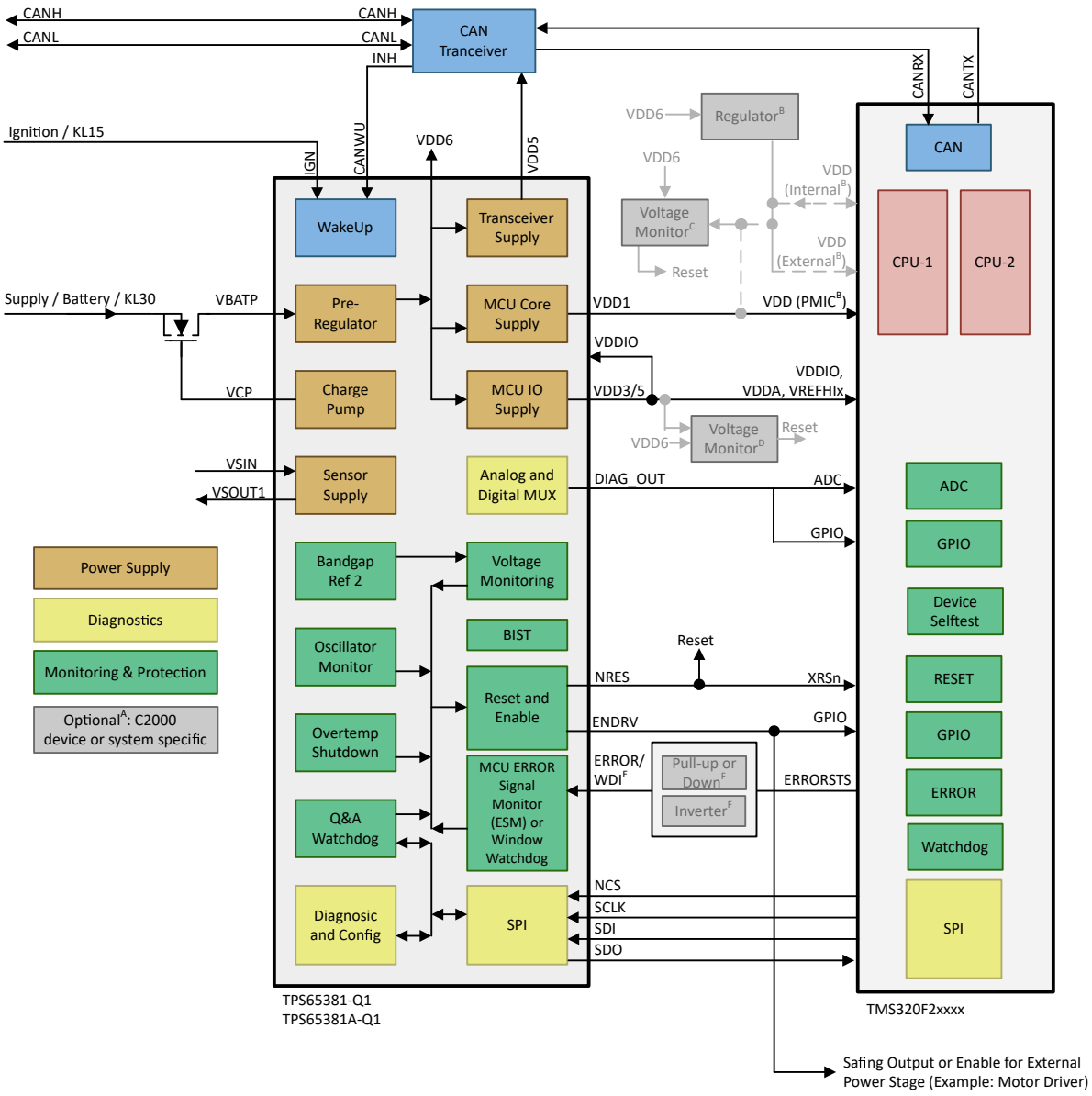


A. The ERROR/WDI pin can be configured as an input for the MCU ESM in the case of TMS570, C2000™ or other dual-core MCU or as a window watchdog input (TMS470 or other single core MCU).

B. The ENDRV output can be configured as either as ENABLE for the external power stage (typical use), or optionally as warm-RESET for the TMS570.

Figure 6-1. TPS65381x-Q1 With TMS570

6.2 TPS65381x-Q1 With C2000™



A. Optional implementations that may be necessary depending on the specific C2000™ device used and specific system requirements. Please see detailed information on the specific C2000™ device.

B. Different C2000™ MCU devices have specific power supply requirements for the core supply, VDD. Different devices may generate their own core supply internally, use the core supply from the TPS65381x-Q1 PMIC, or use an external regulator.

C. Depending on the specific C2000™ MCU and the core rail generation, voltage monitoring may be provided within the PMIC or an external voltage monitor may be needed.

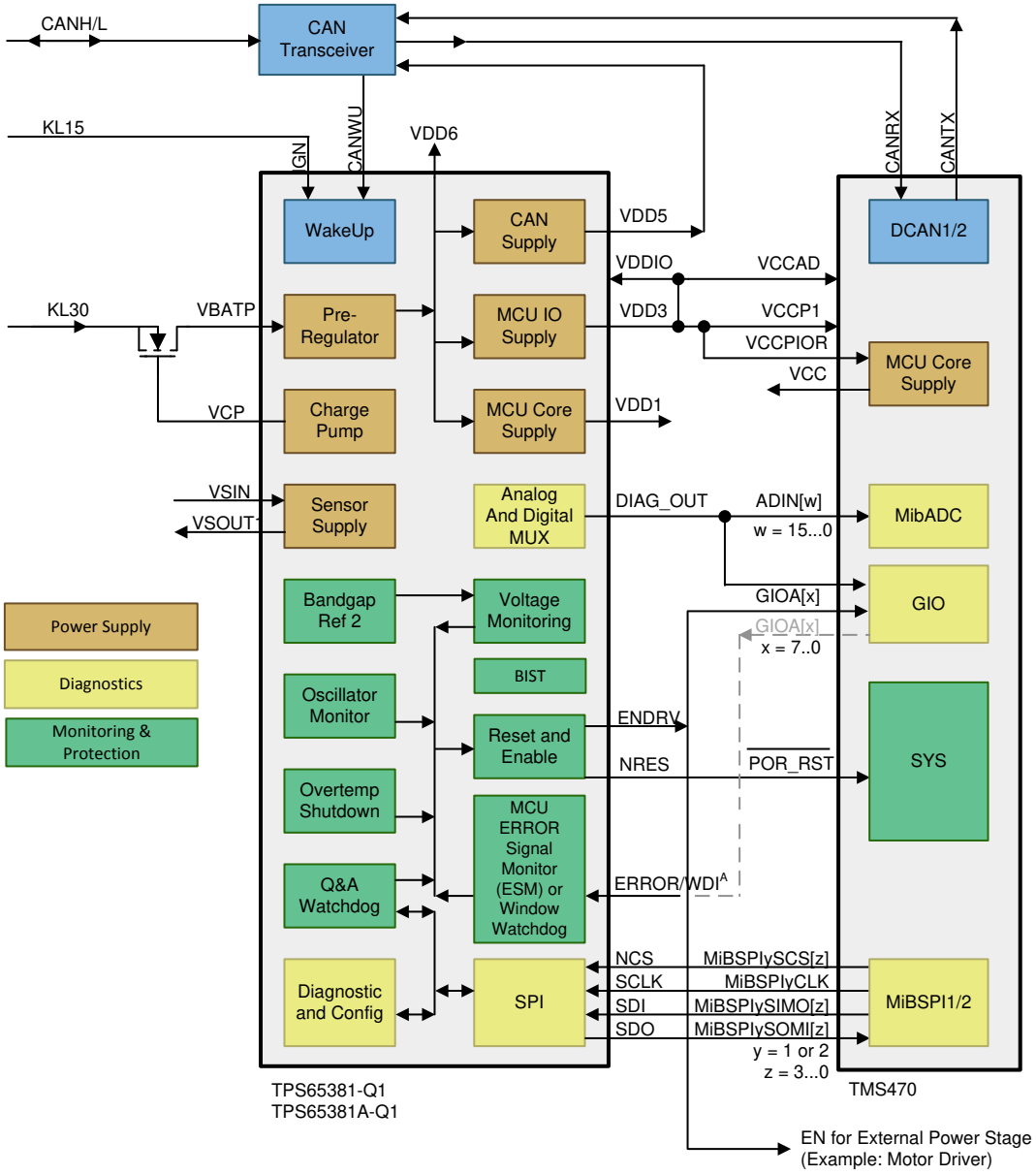
D. Depending on the specific C2000™ MCU and the IO supply requirements, voltage monitoring may be provided within the PMIC or an external voltage monitor may be needed.

E. The ERROR/WDI pin can be configured as an input for the MCU ESM or the watchdog in trigger mode. The assumed use case with the C2000™ is this pin is used as the ERROR input to the MCU ESM monitoring the C2000™ ERRORSTS pin output and the watchdog is in Question and Answer mode.

F. An external resistor must be added to pull the ERRORSTS pin to its ERROR level by default. The polarity of the ERRORSTS pin varies depending on the C2000 device being used, consult the device data manual for more information. An inverter must be used in cases where the polarity of the ERRORSTS pin differs from that of the ERROR/WDI pin while in the MCU ESM function. The polarity of either pin is not programmable.

Figure 6-2. TPS65381x-Q1 with C2000™

6.3 TPS65381x-Q1 With TMS470



A. The ERROR/WDI pin can be configured as an input for the MCU ESM in the case of TMS570 or other dual-core MCU or as a window watchdog input (TMS470 or other single core MCU).

Figure 6-3. TPS65381x-Q1 With TMS470 (Using an Internal MCU Core Supply)

7 TPS65381x-Q1 as Safety Element out of Context (SEooC)

This section contains a Safety Element out of Context (SEooC) analysis of the TPS65381x-Q1 device. Texas Instruments has made assumptions on the typical safety-system configurations using this device. System-level safety analysis is the responsibility of the developer of these systems and not Texas Instruments. As such, this section is intended to be informative only to help explain how to use the features of TPS65381x-Q1 device to assist the system designer in achieving a given ASIL or SIL level. Customers are responsible for putting this device into the context of their system and analyzing the ASIL or SIL coverage achieved therein. The TPS65381x-Q1 device has been designed to perform and function in the ways described in this safety manual presuming that they are in a system that uses and interconnects them with other components and elements as described.

Note

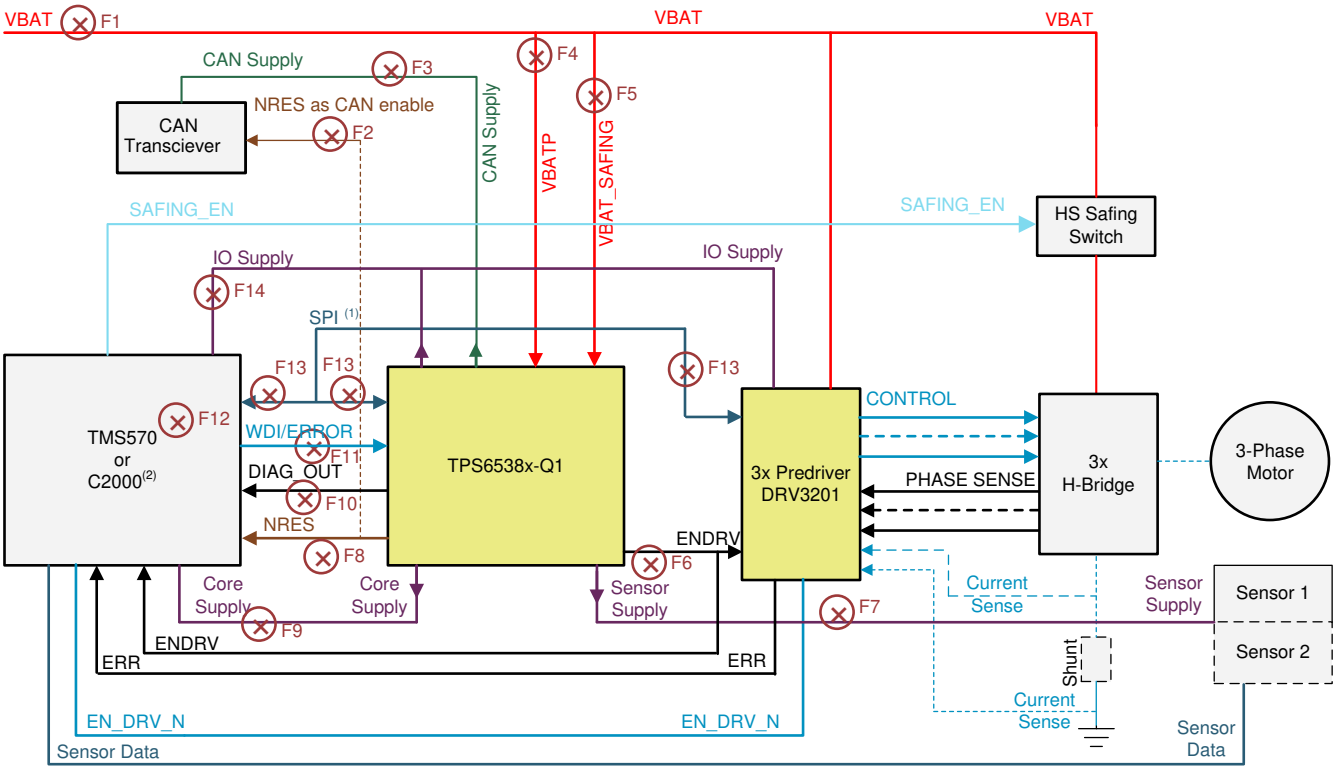
The system designer can choose to use this TPS65381x-Q1 device in other safety-relevant systems.

7.1 TPS65381x-Q1 Used in an EV/HEV Inverter System

Several system configurations can be considered when using the TPS653381x-Q1 device. This SEooC analysis focuses on using the TPS65381x-Q1 in an electric vehicle (EV) or hybrid-electric vehicle (HEV) inverter system. Most motor-control systems tend to have similar electrical structure including a main microcontroller (MCU) for decision making, motor-drive circuitry, a motor, a position-feedback sensor with associated signal conditioning, and some type of power supply. Because of this, most of the analysis in this section can be applied to other motor-control systems as well. Figure 7-1 shows one implementation of this electric vehicle (EV) or hybrid-electric vehicle (HEV) inverter system where the TPS65381x-Q1 device interfaces with the main microcontroller (MCU) and supplies the motor-position sensor.

This safety analysis of the assumed inverter system focuses only on the TPS65381x-Q1 device and surrounding supply voltages, signals, and communications. For the complete system functional-safety analysis, faults of the other blocks such as the MCU, motor-position sensor, torque sensor, CAN Interface, and motor predriver must be analyzed as well.

In this configuration, when the TPS65381x-Q1 detects a fault in the system, it will set fault bits and may transition to the RESET state (ENDRV and NRES pins low), SAFE state (ENDRV pin low) or STANDBY state (ENDRV and NRES pins low). When a fault is detected by TPS65381x-Q1 causing ENDRV to go low, it is assumed the system is designed to place itself in a safe state by shutting off the inverter system and notifying the user that service is required. When the TPS65381x-Q1 transitions to its SAFE state, the MCU can read the status registers and determine which fault occurred. When the TPS65381x-Q1 transitions to RESET state the MCU is assumed to be in a reset because the NRES pin is low. When the TPS65381x-Q1 transitions to STANDBY state it is assume the MCU is unpowered (reset) because the voltage regulators are off and the NRES and ENDRV pins are low.



(1) When enabling the DIAG_OUT MUX while using SPI communication: the SDO pin is not in the high-impedance state while the NCS pin is HIGH and the DIAG_OUT MUX is enabled. Software or hardware modification may be required. For hardware modifications, check the SDO threshold level and drive capability if resistors are used to adjust the voltage level of the SDO pin on the SPI bus.
(2) Depending on the specific C2000™ MCU and the core rail generation, voltage monitoring may be provided within the PMIC or an external voltage monitor may be needed.

Figure 7-1. EV/HEV Inverter System

Table 7-1. Example Fault Detection for the Assumed EV/HEV Inverter System

Fault	Impact	Detection and Protection
Fault 1		
VBAT supply short or open	• A common-cause failure affects the complete Inverter ECU.	• VBAT undervoltage detected by the TPS65381x-Q1 device by the VBATP UV monitor, TPS65381x-Q1 transitions to STANDBY state and system brought to a safe state (ENDRV pin is low).
Fault 2		
CAN enable short or open	• Disabled CAN PHY with no communication to other ECUs	• MCU safing function detects failure with a dedicated GPIO to sense CAN PHY enable signal(1)
Fault 3		
CAN supply (VDD5) short or open	• CAN PHY is not functional and no communication is performed with other ECUs	• In case of a CAN supply short-to-GND fault, theTPS65381x-Q1 device detects UV condition and sets the VDD5_UV bit • In case of a CAN supply open fault, the MCU detects no communication

Table 7-1. Example Fault Detection for the Assumed EV/HEV Inverter System (continued)

Fault	Impact	Detection and Protection
Fault 4.1		
TPS65381x-Q1 main supply (VBATP) supply short	• No regulated power supplies • The MCU is in unpowered (reset) • The bridge driver is in the RESET state	• The TPS65381x-Q1 VBATP UV monitor detects an UV condition, and transitions the device to the STANDBY state. • The system powers down and is brought to a safe state (ENDRV and NRES pins are low).
Fault 4.2		
TPS65381x-Q1 main supply (VBATP) supply open	• No regulated power supplies • The MCU is unpowered (reset) • The bridge driver is in the RESET state	• The TPS65381x-Q1 VBATP UV monitor detects an UV condition, and transitions the device to the STANDBY state. • The system is powers down is brought to a safe state (ENDRV and NRES pins are low).
Fault 5.1		
TPS65381x-Q1 VMON (VBAT_SAFING) supply short	• No system supply monitoring functions are available. • The MCU is unpowered (reset) • The bridge driver remains in the RESET state.	• The internal voltage monitor indicates an undervoltage event, transitions the TPS65381x-Q1 device to the STANDBY state which keeps the MCU supply off. • The system is brought to a safe state (ENDRV and NRES pins are low).
Fault 5.2		
TPS65381x-Q1 VMON (VBAT_SAFING) supply open	• No system supply-monitoring functions are available. • The MCU is unpowered (reset). • The bridge driver remains in the RESET state.	• The internal voltage monitor indicates an undervoltage event, transitions the TPS65381x-Q1 device to the STANDBY state which keeps the MCU supply off. • The system is brought to a safe state (ENDRV and NRES pins are low).
Fault 6		
TPS65381x-Q1 ENDRV short or open	• The external power-stage enable (or safing path enable) is not controllable.	• The TPS65381x-Q1 ENDRV read-back diagnostics can help the MCU detect the failure by reading the ENDRV_ERR bit to determine a mis-match of the state of the ENDRV pin and the expected driver output on the ENDRV pin. • The second system safing path enable should provide the required redundancy in case of an ENDRV short high
Fault 7		
TPS65381x-Q1 sensor-supply short or open	• No functioning sensor in the system • Potential sensor damage if short to supply (VBAT) occurs	• The TPS65381x-Q1 VSOUT1 sensor supply voltage monitor detects both UV or OV events. The MCU monitors the VSOUT1_OV bit and VSOUT1_UV bit and disables the sensor supply. The MCU can also disable the external power states and place the system in a safe state if necessary due to loss of the sensor data because of the shorted or open supply sensor supply. • Sensor supply monitor covered by internal diagnostics and its status (UV or OV) read by the MCU through SPI.

Table 7-1. Example Fault Detection for the Assumed EV/HEV Inverter System (continued)

Fault	Impact	Detection and Protection
Fault 8		
TPS65381x-Q1 NRES pin short or open	• The MCU reset function is not correct: – In case of a short to GND, the MCU remains in permanent reset and the system is disabled – In case of a short to high or VBAT, the MCU is never reinitialized and potentially damaged – In case of an open, MCU remains in permanent reset because of an internal pulldown on the MCU reset input pin, and the system is disabled	• Diagnostics and monitoring detects NRES external faults because of an NRES short or open: – Watchdog function – MCU ESM function – Interconnect diagnostics – The NRES_ERR monitor in the TPS65381x-Q1 device, when enabled by DIS_NRES_MON set to 1, detects a mismatch and places the device in the SAFE state (ENDRV pin goes low) and the system transitions to a safe state.
Fault 9.1		
TPS65381x-Q1 VDD3/5 or VDD1 short or open (MCU core supply fault)	• In case of a short to GND: – The MCU is in reset or powered-down and the system is disabled – The VDD3/5 regulator is disabled	• Diagnostics and monitoring detects a VDD3/5 or VDD1 short to GND: – VDD3/5 current limit is applied – VDD3/5 UV detected and power-stages are disabled (ENDRV pin is low), the device transitions to the RESET state (NRES pin is low) – With VDD3/5 current limit, eventually overtemperature condition can occur and disable the VDD3/5 regulator or the TPS65381x-Q1 device transitions to the STANDBY state – VDD1 UV detected, the TPS65381x-Q1 device transitions to the RESET state when the NMASK_VDD1_UV_OV bit is 1 (NRES pin is low)
Fault 9.2		
TPS65381x-Q1 VDD3/5 or VDD1 short or open (MCU core supply fault)	• In case of open: – The MCU is powered-down and the system is disabled.	• Diagnostics and monitoring detects a VDD3/5 or VDD1 open fault – The MCU is not responsive and a watchdog or MCU ESM failure is detected
Fault 10		
TPS65381x-Q1 DIAG_OUT (AMUX/ DMUX) short or open	• The MCU disables the system because of failed TPS65381x-Q1 diagnostics	• All MCU-to-TPS65381x-Q1 interconnect diagnostics fail and the MCU software can decide to disable the system
Fault 11		
TPS65381x-Q1 ERROR/WDI pin short or open	• An MCU error is detected • An MCU reset is asserted and the system is disabled	• The MCU runs diagnostics on the ERROR/WDI pin after a power-up event in either watchdog trigger mode or MCU ESM. The MCU detects a short or open and the MCU software can decide to disable the system. • The TPS65381x-Q1 device in either watchdog trigger mode or MCU ESM detects an error in the ACTIVE state and transitions the device to the RESET or SAFE state which drives the ENDRV pin low to brining the system to a safe state.

Table 7-1. Example Fault Detection for the Assumed EV/HEV Inverter System (continued)

Fault	Impact	Detection and Protection
Fault 12		
MCU locks	• The MCU is powered-down and the system is disabled	• TPS65381x-Q1 detects a watchdog and or MCU ESM failure • For a watchdog failure when WD_RST_EN is set to 1, the device will transition to RESET state (NRES and ENDRV pins low) • For a MCU ESM failure the device transitions to SAFE state (ENDRV pin is low), depending on configuration of TPS65381x-Q1 and the DEV_ERR_CNT the device may transition to RESET state (NRES and ENDRV pins are low), remain locked in SAFE state (ENDRV pin is low) or transition to STANDBY state (power off, NRES and ENDRV pins are low).
Fault 13		
TPS65381x-Q1 SPI short or open	• The MCU is powered-down and the system is disabled	• The MCU detects a lack of communication or incorrect communication with the TPS65381x-Q1 device • The TPS65381x-Q1 SPI error flags are read by the MCU, the MCU software takes appropriate action • Q&A mode watchdog failure would be detected. For a watchdog failure when WD_RST_EN is set to 1, the device will transition to RESET state (NRES and ENDRV pins low) • If these faults cause a device transition to SAFE state (ENDRV pin is low), depending on configuration of TPS65381x-Q1 and the DEV_ERR_CNT the device may transition to RESET state (NRES and ENDRV pins are low), remain locked in SAFE state (ENDRV pin is low) or transition to STANDBY state (power off, NRES and ENDRV pins are low).

Table 7-1. Example Fault Detection for the Assumed EV/HEV Inverter System (continued)

Fault	Impact	Detection and Protection
Fault 14		
I/O supply short or open	• In case of a short to GND: – The MCU is in reset or powered-down and the system is disabled – The VDD3/5 regulator is disabled • In case of an open: – The MCU is powered-down and the system is disabled	• Diagnostics and monitoring detects the VDD3/5 or VDD1 short to GND: – VDD3/5 current limit is applied – VDD3/5 UV detected and power-stages are disabled (the ENDRV pin is driven low), the device transitions to the RESET state (NRES and ENDRV pins low) – With VDD3/5 current limit, eventually overtemperature condition may occur and disables VDD3/5 or transitions TPS65381x-Q1 to the STANDBY state (unpowered, NRES and ENDRV pins low) – VDD1 UV detected, the TPS65381x-Q1 device transitions to the RESET when the NMASK_VDD1_UV_OV bit is 1 (NRES and ENDRV pins low) • Diagnostics and monitoring detects a VDD3/5 or VDD1 open fault: – The MCU is not responsive and a watchdog or MCU ESM failure is detected.For a MCU ESM failure the device transitions to SAFE state (ENDRV pin is low), depending on configuration of TPS65381x-Q1 and the DEV_ERR_CNT the device may transition to RESET state (NRES and ENDRV pins are low), remain locked in SAFE state (ENDRV pin is low) or transition to STANDBY state (power off, NRES and ENDRV pins are low).

(1) CAN PHY enable signal can be the same as MCU power-on reset driven by the TPS65381x-Q1 device.

7.2 SPI Note

Note

When enabling the DIAG_OUT MUX while using SPI communication the SDO pin is not in the high-impedance state while the NCS pin is HIGH and the DIAG_OUT MUX is enabled. Software or hardware modification may be required. For hardware modifications, check the SDO threshold level and drive capability if resistors are used to adjust the voltage level of the SDO pin on the SPI bus.

8 Revision History

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

Changes from Revision C (January 2018) to Revision D (August 2021)	Page
• Updated the numbering format for tables, figures, and cross-references throughout the document	1
• Updated the Development Process for Management of Systematic Faults section	8
• Updated the Figure TPS65381x-Q1 with C2000™ to include updated C2000™ MCU devices	26
• Updated footnote for Figure EV/HEV Inverter System with C2000™ to include updated C2000™ MCU devices	28

Changes from Revision B (May 2017) to Revision C (January 2018)	Page
• Added clarification in the *VDD1 Linear Supply* section about the VDD1_G pin and VDD1_SENSE pin short circuit to pin considerations	13
• Added clarification in the *Junction Temperature Monitoring and Current Limiting* section about status bits and DMUX signal outputs.	20
• Added clarification in the *Junction Temperature Monitoring and Current Limiting* section about indirect current limit from VDD6 for VDD1 linear regulator controller with external FET.	20

Changes from Revision A (October 2014) to Revision B (March 2017)	Page
• Added the TPS65381A-Q1 device to the document	3
• Changed all sections with the addition of TPS65381A-Q1 and updated product data sheets for both TPS65381-Q1 and TPS65381A-Q1	3

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