Application Report
SLVA622–October 2013

# Safety Manual for the TPS65311-Q1 High-Voltage Power-Management IC

Samir Camdzic

**ABSTRACT**

This document is a safety manual for the Texas Instruments TPS65311-Q1 device which is a high-voltage power-management IC for safety-critical applications. The device uses a common safety architecture, implemented in multiple application focused products.

**Contents**



**List of Figures**

**List of Tables**

# 1 Introduction

A system and equipment manufacturer or designer (as user of this document) is responsible for ensuring 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 as a reference only. Users must understand and agree that their use of TI components in safety-critical applications is entirely at their risk, and that the user (as the 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 required by system developers to assist in the creation of a safety-critical system using a supported TPS65311-Q1 high-voltage power-management IC. This document contains:

- An overview of the superset product architecture
- An overview of the development process used to reduce systematic failures
- An overview of the safety architecture for management of random failures
- The details of architecture partitions, implemented safety mechanisms, and recommended usage

The Safety Analysis Report documents the following information which is **not** covered in this document:

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

The safety case documents the following information which is **not** covered in this document:

- Evidence of compliance to targeted standards
- Results of assessments of compliance to targeted standards

TI expects that the user of this document has a general familiarity with the TPS65311-Q1 product family. 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 a safety manual as seen in IEC 61508:2010.

# 2 Product Overview

The TPS65311-Q1 device is a high-voltage power-management IC designed to supply microcontrollers and DSPs in safety-critical applications, such as those found in automotive applications.

The TPS65311-Q1 device integrates one high-voltage buck controller for pre-regulation combined with two buck and one boost converter for post regulation. Another integrated low-dropout regulator (LDO) rounds up the power supply concept and offers a flexible system design with a total of five independent voltage rails. All regulated outputs are protected against overload and over temperature. Each regulated power-supply output voltage is adjustable with the external resistor network settings. Internal soft start ensures controlled startup for all supplies.

The TPS65311-Q1 device combined with an external PMOS is capable of sustaining voltage transients up to 80 V (a protection feature). The external PMOS is used in safety critical applications to protect the system in case malfunction of one of the rails (undervoltage, overvoltage, or overcurrent).

The TPS65311-Q1 device supports two low-power states (LPM1 with an active buck controller or LPM0 with all rails off) to reduce current consumption when the system is constantly connected to the battery.

The TPS65311-Q1 device monitors all regulator outputs, supply voltage (VIN) and digital IO supply (VIO). A second band-gap reference, independent from the main band-gap reference, is used as voltage reference for monitoring circuit. The second band-gap reference prevents the band-gap voltage reference from being a common-cause failure for both regulator and monitoring circuits (for example: regulator going out of regulation and not being detected by monitoring circuit). In addition, the TPS65311-Q1 device implements current limits, over-temperature detection, and protection for all regulated supply rails, and self-test diagnostics for monitoring circuits.

The TPS65311-Q1 device features a window-watchdog function with an external watchdog trigger input, CRC on non-volatile memory, MCU supervisor with reset generation, and a current-limited high-side switch for an external PMOS control with overtemperature protection.

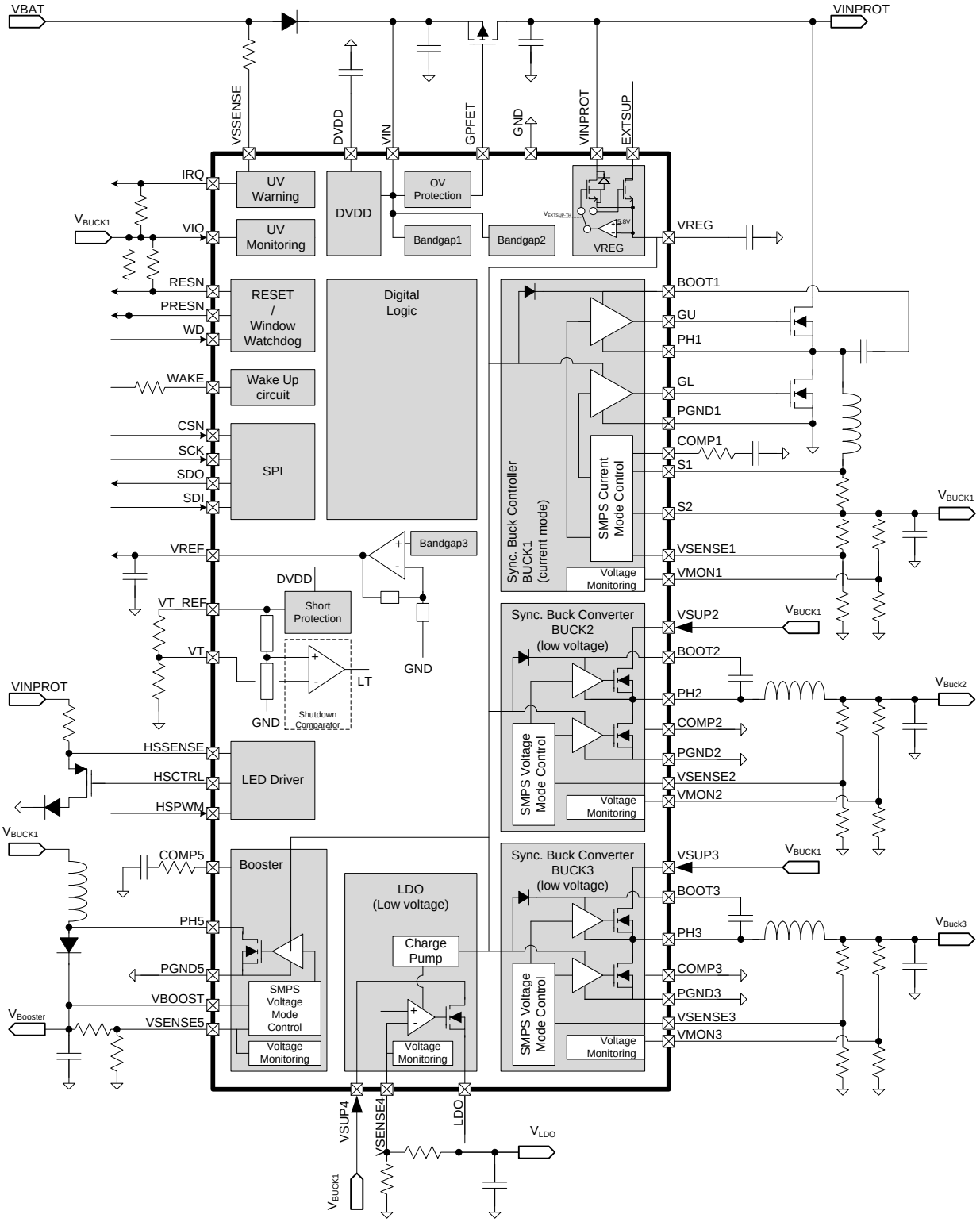



**Figure 1. TPS65311-Q1 Architecture Overview**

### 2.1 Target Applications

The TPS65311-Q1 device targets general-purpose safety applications. Analysis of multiple safety applications during concept phase enabled support of Safety Element out of Context (SEooC) development according to ISO 26262-10:2011. Example target applications include:

- Adaptive cruse control (ACC)
- Lane departure warning
- Collision avoidance
- Industrial safety applications

In the case of overlapping requirements between target systems, TI Mixed-Signal Automotive (MSA) has attempted to design the device respecting the most stringent requirement.

Although TI MSA has considered certain applications while developing these devices, this document 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 the system safety.

### 2.2 Product Safety Constraints

For safety components developed according to many safety standards, the expectation is that the component safety manual provide a list of product safety constraints. For a simple component, or more complex components developed for a single application, this document is a reasonable response. However, the TPS65311-Q1 device is not developed targeting a single, specific application. Therefore a single set of product safety constraints cannot govern all viable uses of the product. The safety analysis report provides an example implementation of the TPS65311-Q1 device in a common system, with relevant product safety constraints.

## 3 TPS65311-Q1 Development Process for Management of Systematic Faults

For safety-critical development, managing both systematic and random faults is necessary. Texas Instruments MSA has created a unique development process for safety-critical semiconductors, which greatly reduces the probability of systematic failures. This process builds on a standard quality-managed development process as the foundation for safety-critical development. A second layer of development activities, which are specific to safety critical developments targeting IEC 61508 and ISO 26262, then augments this process.

TI MSA first saw the need to augment our standard new-product development process in order to develop products according to IEC 61508. In 2007, TI updated the new-product development process according to IEC 61508.

By mid-2009, it became clear that the emerging IEC 61508 2nd edition and ISO 26262 functional safety standards would require enhanced process-flow capabilities. Because of the lack of maturity of these draft standards, it was not possible to implement a development process which ensured compliance before final drafts were available. TI joined the ISO 26262 working group in mid 2009 as a way to better understand and influence the standard with respect to microcontroller hardware component development. As part of the US Technical Advisory Group (TAG) and international working group for ISO 26262, TI has notable contributions to:

- ISO 26262:5-2011, Annex D - informative section describing failure modes and recommended diagnostics for hardware components, enhanced by TI's detailed knowledge of silicon failure modes and effectiveness of diagnostic methods
- ISO 26262:10-2011, Clause 9 - informative section describing development of safety elements out of context, a technique which legitimizes and enables the use of commercial off-the-shelf (COTS) safety-critical components
- ISO 26262:10-2011, Annex A - informative section describing how to apply ISO 26262 to microcontrollers, influenced by TI's lessons learned in application of IEC 61508 to microcontroller development

In early 2011, TI MSA began development of a process flow compliant to IEC 61508 secondnd edition and ISO 26262 draft baseline 18. The process applied to the first TPS65311-Q1 silicon covered by this document incorporates all changes through ISO 26262 draft baseline 21 (July 2011).

### 3.1 TI MSA New-Product Development Process

Texas Instruments MSA has been developing mixed-signal automotive ASICs for safety-critical and non-safety critical automotive applications for over fifteen years. Automotive markets have strong requirements on quality management and high reliability of product. Though not explicitly developed for compliance to a functional safety standard, the TI MSA new-product development process already featured many elements necessary to manage systematic faults.

The TI MSA new-product development process is certified compliant to ISO TS 16949 as assessed by Det Norske Veritas Certification, Inc.

The standard development process breaks development into phases:

- Business planning
- Validate
- Create
- Evaluate
- Process to production

Figure 2 shows the standard process.

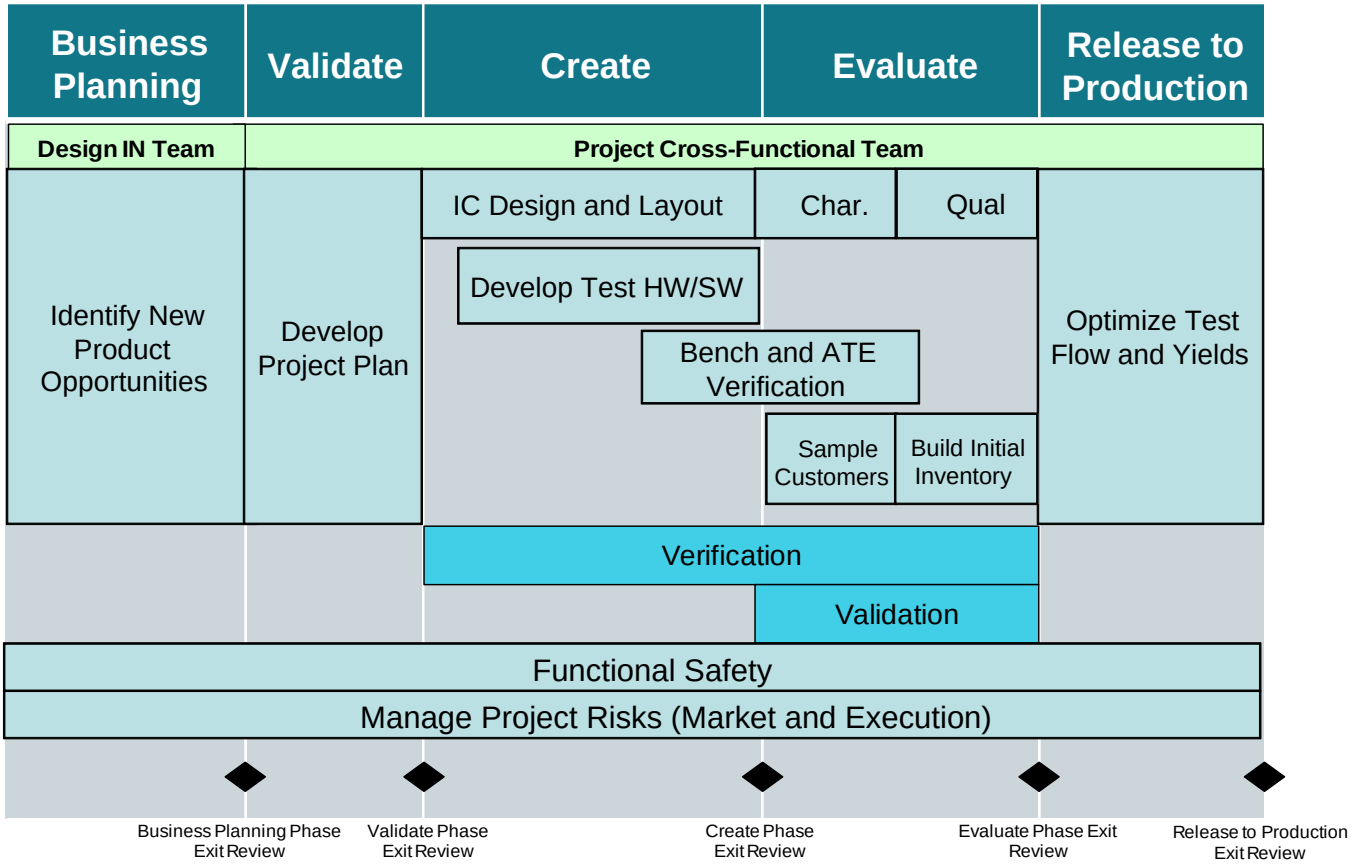



**Figure 2. TI MSA New-Product Development Process**

## 3.2 TI MSA Safety Development Flow

The TI MSA safety-development flow derives from ISO 26262 as a set of requirements and methodologies to be applied to mixed-signal circuit safety-development flow. This flow is an integrated part of the TI MSA new-product development process. The goal of the safety-development flow is to reduce systematic faults.

The safety-development flow targets compliance to IEC 61508 second edition and ISO 26262 baseline 21, and is under a process of continuous improvement to incorporate new features of future ISO 26262 working-group drafts. This flow aligns with the TI MCU enhanced-safety development process.

While the safety-development flow is not directly targeted at other functional safety standards, TI expects that other functional safety systems can readily use products developed to industry state-of-the-art.

Key elements of the MSA Safety Development flow are:

- Assumptions on system-level design, safety concept, and requirements based on TI's expertise in safety critical systems development
- Combined qualitative and quantitative or similar safety analysis techniques comprehending the sum of silicon failure modes and diagnostic techniques
- Fault estimation based on multiple industry standards as well as TI manufacturing data
- Integration of lessons learned through multiple safety critical developments to IEC 61508 and participation in the ISO 26262 international working group

Figure 3 shows these activities overlaid atop the standard QM development flow.

| Phase 0<br>Bussiness Planning | Phase 1<br>Program Planning | Phase 2<br>Create | Phase 3<br>Evaluate | Phase 4<br>Ready for Production | Phase 5<br>Sustaining |
|---|---|---|---|---|---|
| Is Safety Process required? | Generate Safety Plan | Device Design Specification | Validation of Safety Elements in Silicon | Plans for Support of operation and production | Ongoing production support |
| Nominate Safety Manager | Initiation of the Safety Case | Qualitative Analysis of Design Specification | Characterization of Safety Elements | Release of final safety case | End of Life Production |
| Execution of Development Interface Agreement | Identify System and component safety requirements | Validation of Safety Design implementation at transitor/schematicand RTL level | Qualification of safety related design features | Confirmation review | Decommissioning of products in the field |
| | Confirmation Review | Quantitative analysis of design | Release of safety manual | | Periodic confirmation reviews |
| | | Re-validation of Safety Design with back-annotated circuit parasitics | Release of safety analysis report | | |
| | | Confirmation Review | Confirmation Review | | |

**Figure 3. Key Elements of the MSA Safety Development Flow**

## 3.3 Development Interface Agreement

The intent of a development interface agreement (DIA) is to capture an agreement between a customer and supplier toward the management of shared responsibilities in developing a functional safety system. In custom developments, the DIA is a key document executed between customer and supplier early in the development process. Because the TPS65311-Q1 device is a commercial, off-the-shelf (COTS) product, TI has prepared a standard DIA which describes the support that TI can provide for customer developments. Refer requests for custom DIAs to your local TI sales office for disposition.

The following sections highlight key points of the standard DIA.

### 3.3.1 Requirements Transfer

The TPS65311-Q1 device is developed as a safety element out of context (SEooC) with ASIL-B process capability. Detailed safety requirements were not available from lead customers during development. Because these requirements were not available, the safety requirements used were based on TI analysis of target safety applications.

To discuss the acceptance of new customer safety requirements for future designs please contact your local TI sales office for further information.

### 3.3.2 Availability of Safety Documentation

**Table 1. Safety Documentation**

| Deliverable Name | Contents | Availability | Delivery |
|---|---|---|---|
| Safety Product Preview | Overview of safety considerations in product development and product architecture. Delivered ahead of public product announcement. | NDA material | May 2012 |
| Safety Manual | User guide for the safety features of the product, including system-level assumptions of use. | Public | November 2012 |
| ISO 26262 Safety Analysis Report | Results of FTA, FMEA, and FMEDA safety analysis execution and resulting metrics per the ISO 26262 standard. For use in conjunction with the safety manual. | NDA material | November 2012 |
| Safety Case Report | Detailed summary of the conformance of the product to the ISO 26262 and IEC 61508 standards. | NDA material | 2Q2013 |

### 3.3.3 External Product Audits

TI has no current plans to perform an external audit of TPS65311-Q1 products to IEC 61508 or ISO 26262 standards. Detailed documentation can be made available after product qualification to support customer system audit and certification.

Forward any request for an independent audit of a TI product by an external assessor to your local TI sales office for disposition.

## 4 TPS65311-Q1 Product Architecture for Management of Random Faults

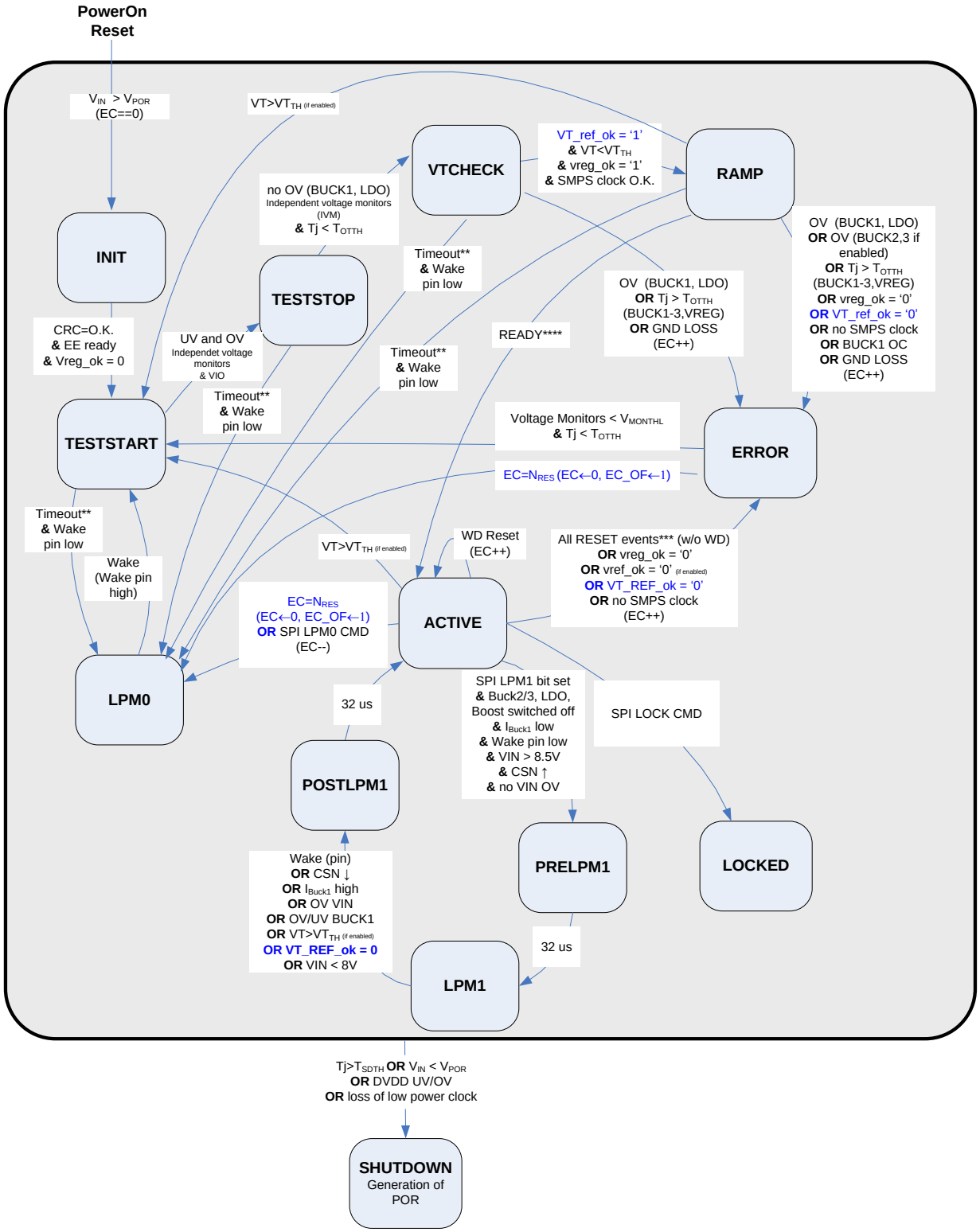
For safety-critical development, managing both systematic and random faults is necessary. The TPS65311-Q1 product architecture includes many safety mechanisms which can detect and respond to random faults when used correctly.

The device has a core set of modules allocated for continuously operating hardware safety mechanisms:

- Device state controller or supervisor (wake-up, power down, standby, and lock state detection circuit)
- Time-limited start-up time
- System MCU and system peripherals reset supervisors
- Independent band-gap reference voltages for regulator, monitoring circuits
- Independent regulated supplies and monitoring circuits
- Independent buffered band-gap reference as external system voltage reference output
- High-side switch pre-driver with overcurrent monitoring and protection
- Loss of GND detection
- System-error interrupt output
- Window-watchdog function
- Overtemperature detection and shutdown
- Switch-mode power-supply clock and low power-mode clock monitors
- SPI communication monitor

### *4.1 Device State Controller and Operating States*

The TPS65311-Q1 operating states must be monitored by the system developer in their software and system-level design concepts. Figure 4 and the following sections describe the operating-states state machine.




* GPFET is turned on in VTCHECK, RAMP, ACTIVE, POSTLPM1, LPM1, PRELPM1 and VIN < $VIN_{OV}$.

** TIMEOUT counter is reset with every state transition.

*** **Reset Events**: WD, GROUND LOSS, VOLTAGE MONITOR BUCK1, MONITOR BUCK2-3 (if enabled), VOLTAGE MONITOR VIO, OVERTEMPERATURE BUCK1-3 or VREG, BUCK1 OVERCURRENT.

**** READY = VREF_OK and not Buck1_UV and Power-up sequence complete.

**Figure 4. Device Controller State Diagram**

### 4.1.1 INIT State

- Default state after a power-on reset event
- Analog trim data stored in EEPROM is loaded to trim registers
- Device transitions to TESTSTART state if the following occurs:
  - IEEPROM CRC check is correct
  - Internal VREG comparator self-test diagnostic passed without failure
- Device remains in INIT state if one or both of the following occurs:
  - EEPROM CRC check failed
  - Internal VREG comparator self-test failed

  **NOTE:** EEPROM contains analog component trim values.

  **NOTE:** EEPROM content is re-loaded with every power-on reset event.

### 4.1.2 TESTSTART State

- ESTSTART state is entered
  - From INIT state (coming from power on)
  - After detecting that VT > $VT_{TH}$
  - From ERROR state when fail condition is removed
  - After a wake event in LPM0 state
- In this state self-test diagnostics for undervoltage and overvoltage comparators are performed:
  - BUCK1/2/3
  - BOOST
  - LDO
  - LDO
- The device transitions to TESTSTOP state if self-test diagnostics pass without failure.

### 4.1.3 TESTSTOP State

- Undervoltage and overvoltage comparators are switched into normal operating mode
- The device transitions to VTCHECK state when the following occurs:
  - No over-voltage condition is detected
  - No over-temperature condition is detected
  - Start-up pulse is driven on WAKE input pin
- If above conditions are not met, after a time-out event, the device transitions to LPM0 state

### 4.1.4 VTCHECK State

- This mode is used to:
  - Switch on external GPFET in case VIN < $V_{OVTH\_L}$
  - Turn on VREG regulator and VT_REF
  - Check if voltage on pin VT < $VT_{TH}$
  - Check if SMPS clock is running correctly
  - Check if VREG,VT_REF exceed the minimum voltage
- The device enters RAMP state if all checks are valid
- The device enters LPM0 state after timeout event if one of checks failed or WAKE input is low. This helps reduce device current consumption.
- The device enters ERROR state when the following occurs:
  - BUCK1/2/3 over-voltage is detected
  - BUCK1/2/3 or VREG over-temperature is detected

– Loss of GND is detected

### 4.1.5 RAMP State

- The device runs through power-up sequencing (see Figure 5)

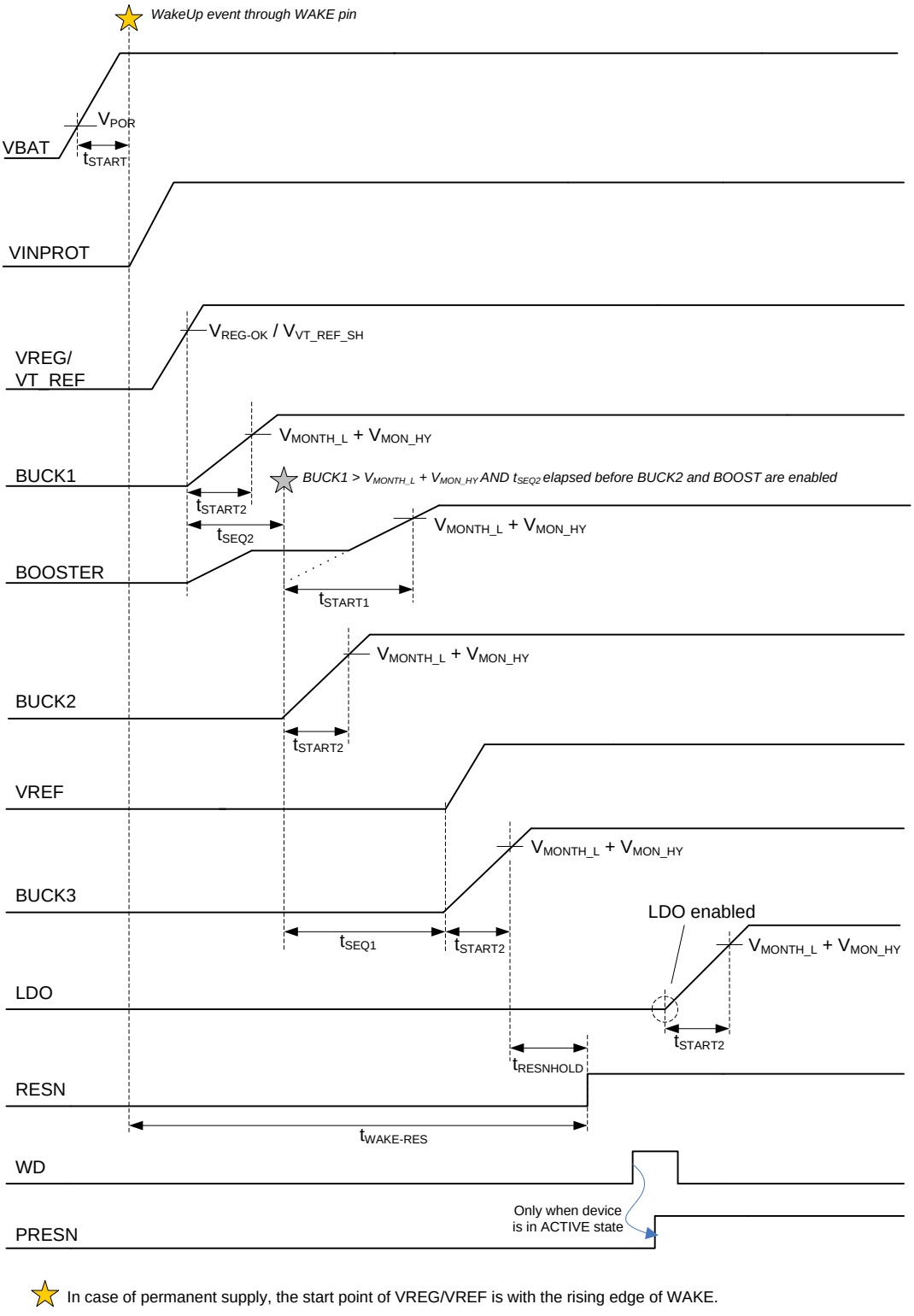



**Figure 5. Power-Up Sequence**

- The device transitions to ACTIVE state if no error condition is detected.
- The device transitions to ERROR state when the following occurs:
  - Over-temperature on BUCK1-3 or VREG
  - Over-voltage on BUCK1-3 or LDO
  - Over-current on BUCK1
  - SMPS clock fail
  - VT_REF/VREG under-voltage
  - Loss of GND
- The device transitions to TESTSTART state if VT > $VT_{TH}$

  **NOTE:** There is no dedicated power-down sequence; all rails are switched off at the same time.

### 4.1.6 ACTIVE State

- ACTIVE state is the normal operating state
- The device transitions to ERROR state when the following occurs:
  - Any valid reset event is detected
  - VREG, VREF, VT_REF undervoltage event is detected
  - SMPS clock failed
- The device transitions to a LOCKED state if the MCU sends an SPI lock command (SPI_LOCK_CMD)
- The device transitions to a TESTSTART state after detecting VT < $VT_{TH}$
- The device transitions to an LPM0 state when the following occurs:
  - The MCU sends an SPI LPM0 command
  - The error counter reaches the NRES value
- The device transitions to an LPM1 state when the following occurs:
  - LPM1 is enabled
  - BUCK2/3, LDO, BOOST are disabled
  - IBUCK1 is low,
  - Wake Pin is low
  - CSN is low
  - VIN > 8.5 V
- Watchdog failure does not cause the device to change state, it only increments device-error count

### 4.1.7 ERROR State

- In this state all power stages and GPFET are switched off
- Error counter is incremented each time device transitions to ERROR state.
- The device transitions to LPM0 state if error counter reached NRES value
- The device transitions to TESTSTART state when the following occurs:
  - All rails indicate an undervoltage condition
  - No GND loss is detected
  - No overtemperature condition is detected

### 4.1.8 LOCKED State

- The device is disabled in this state, and the only way to exit this state is when the following occurs:
  - Power-on reset event
  - Thermal shutdown event
  - Loss of low-power-mode (LPM) clock
- The error counter is incremented each time the device transitions to ERROR state.

#### 4.1.9 LPM0 State

- LPM0 State is a low-power-mode state which is intended to reduce system quiescent-current consumption.
- In this state, system functions are powered down, and NRES and PRES are asserted low.
- The device transitions to TESTSTART state if valid wake event is detected.

#### 4.1.10 LPM1 State

- LPM1 State is a low-power-mode state, intended to reduce system quiescent-current consumption, while device minimum functionality is still maintained.
- The device can enter the LPM1 state only from the ACTIVE state
  - LPM1 is enabled by LPM1 bit in DEV_CONFIG register
  - BUCK2/3, LDO and BOOST is disabled
  - $I_{BUCK1}$ < 1% of the set maximum load current
  - WAKE pin is low
  - CSN is high
  - VIN > 8.5 V
- In this state, GPFET and BUCK1 are still active with reduced load currents.
- The device transitions from LPM1 state to ACTIVE state when the following occurs:
  - Voltage on WAKE pin > $V_{WAKE\_ON}$ for minimum of $t_{WAKE}$
  - A falling edge on the CSN pin
  - $I_{BUCK1}$ > 10% of the set max load current
  - An overvoltage condition on VIN (GPFET shutdown)
  - VIN < 8 V
  - VT_REF_ok = 0 or VT > $VT_{TH}$

#### 4.1.11 SHUTDOWN State

- The device enters the SHUTDOWN state from any state
  - Thermal shutdown event ($T_J$ > $T_{SDTH}$ – $T_{SDHY}$)
  - VIN < VPOR
  - DVDD under-voltage event
  - DVDD over-voltage event,
  - Loss of Low Power Mode (LPM) clock is detected
- When the device exits the SHUTDOWN state and enters the INIT state a power-on reset event generates

### *4.2 Time-Limited Start-up Time*

A timer is used to limit the time in INIT mode. The device enters the LPM0 state after $t_{timeout}$ is elapsed and the Wake pin is low if device is in INIT state, VIN or VT is not in a proper range, and Wake pin is low. This timeout event causes the device to enter a safe state which prevents any irregular power-up sequence that can lead to an unknown or uncontrollable system state.

### *4.3 System MCU and System Peripherals Reset Supervisors*

RESN and PRESN are open-drain outputs which are active if one or more of the conditions listed in Table 2 are valid. $\overline{\text{RESN}}$ is extended for $t_{RESNHOLD}$ after a reset was triggered. RESN is the main processor reset and also asserts PRESN as a slave signal.

PRESN is latched and is released when the window-trigger mode of the watchdog is enabled (1st rising edge at WD pin).

**Table 2. RESN and PRESN Conditions**

| Header 1 | Header 2 |
|---|---|
| Power-on reset, or loss of low-power-mode clock, or thermal shutdown | The device reinitializes all register with their default values. Error counter is cleared. |
| BUCK 1/2/3 voltage monitoring | Input voltage at VMON1-3 pin out-of-bounds : $V_{VMON1-3} < V_{MONTH\_L}$ or $V_{VMON1-3} > V_{MONTH\_L}$ |
| VIO voltage monitoring | Input voltage at VMVIO pin out-of-bounds : $V_{VMVIO} < V_{VIOMON\ TH}$ |
| Loss of GND | Open at PGNDx or GND pin |
| BUCK1/2/3 over-temperature, VREG over-temperature | Over-temperature on BUCK1-3 or VREG |
| Watchdog Reset | Watchdog Window violation |

In case of improper supply voltages or under critical failure condition, RESN and PRESN must keep the main processor and peripheral devices in a defined state during power-up and power down. Therefore, for low supply voltages, the topology of the reset outputs also ensures that RESN and PRESN are always held at a low level when RESN and PRESN are asserted even VIN falls below VPOR or the device is in STANDBY state.

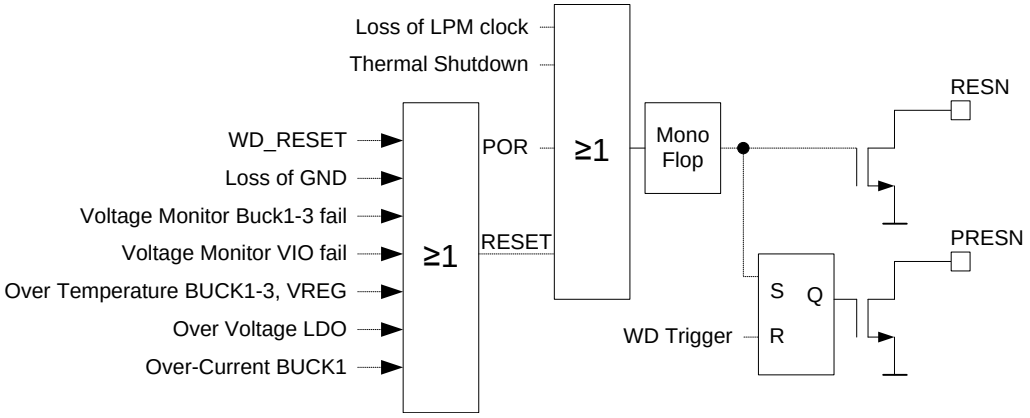



**Figure 6. RESN and PRESN Conditions**

## *4.4 Independent Regulating Circuits, Voltage References, and Voltage Monitoring*

The TPS65311-Q1 device integrates independent voltage monitoring for BUCK1/2/3, LDO, VIO and BOOST rails. The reference voltages are derived from independent band-gaps. BUCK 1/2/3 use a separate input pins for monitoring. The voltage monitoring is implemented as a window comparator with an upper and lower threshold.

To prevent false supply-rail failure detection in case system application does not use BUCK2/3 or BOOST supply rails, the VMON2/3 or VSENSE5 pins must be connected to VMON1 pin. Voltage monitoring self-test diagnostics is performed every time the device enters TESTSTART state.

The TPS65311-Q1 device enters ERROR state in case of upper threshold violation (for LDO in RAMP or VTCHECK states, and for BUCK1/2/3) or lower threshold violations (for BUCK1/2/3 and VIO). RESN and PRESN are asserted low and the external PMOS (main system safing switch) is switched off, and the error counter is incremented.

VIN supply under-voltage is monitored for POR generation. Two VIN overvoltage-shutdown thresholds (VOVTH) are selected through SPI. The lower threshold is selected after a POR event. Only a POR condition is monitored when the device is in LPM0 state.

An integrated filter avoids false reaction because of spikes on the VIN supply line. The external PMOS safing switch is turned off to protect the device and system in case of an overvoltage condition. The BUCK1 controller is not switched off and continues to run until under-voltage on VREG or BUCK1 supply rail is detected.

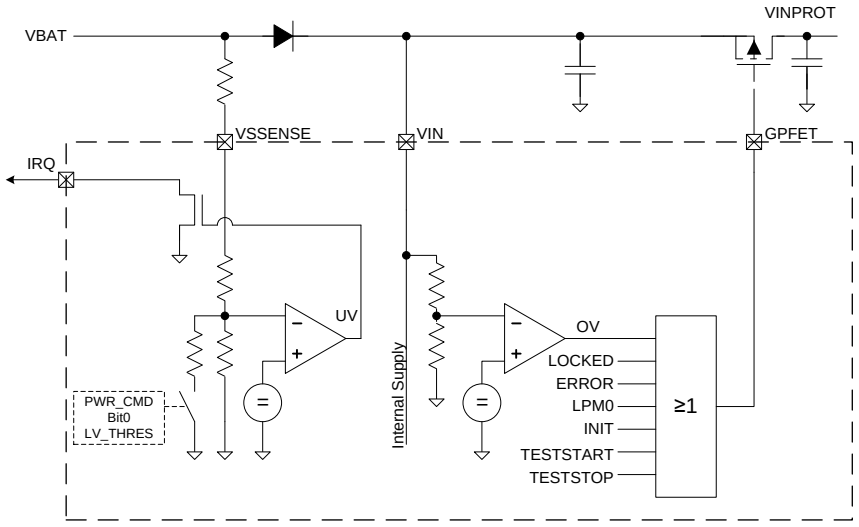



**Figure 7. Overvoltage and Undervoltage Detection Circuit, and System Safing Protection**

Low battery condition on VSSENSE asserts IRQ output (interrupt to external MCU). Sense input can directly connect to VBAT through a resistor. The detection threshold for an undervoltage warning is selected through SPI. An integrated filter avoids false reaction because spikes on the VBAT line.

The IRQ pin has two different functions. In normal operating state the IRQ pin is forced low in case the voltage on the battery line is below $V_{SSENSETHx}$ threshold. In LPM1 the pin indicates a wake-up event. The IRQ pin is low as long as PRESN is low. In case PRESN goes high and the battery line is already below $V_{SSENSETHx}$ threshold the IRQ pin is forced high for $t_{VSSENSE\_BLK}$.

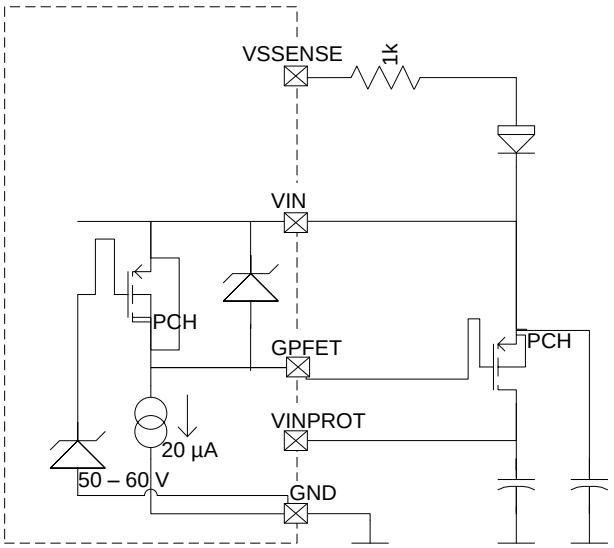



**Figure 8. PMOS Safing-Switch Control Circuit**

### 4.5 Independent Buffered Bandgap Reference as System Voltage Reference Output

The device includes a precise voltage-reference output to supply a system ADC. The VREF output is enabled in RAMP state, and is disabled with SPI. The output is protected against short to GND.

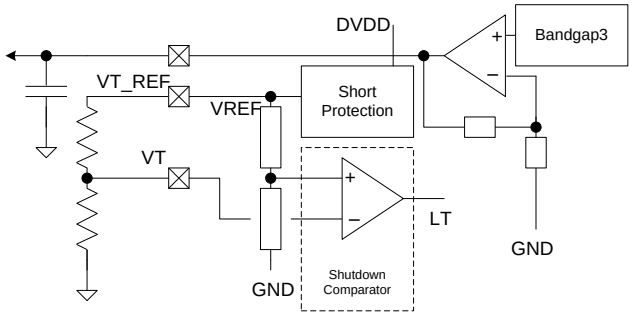



**Figure 9. Buffered Bandgap Output Reference**

### 4.6 High-Side Switch Pre-Driver

The high-side switch pre-driver controls an external PMOS current-limited high-side switch. The current levels are adjusted with an external sense resistor. The HS_EN bit enables and disables the switch. The switch is controlled by the HSPWM input pin. Driving HSPWM high turns on the external FET.

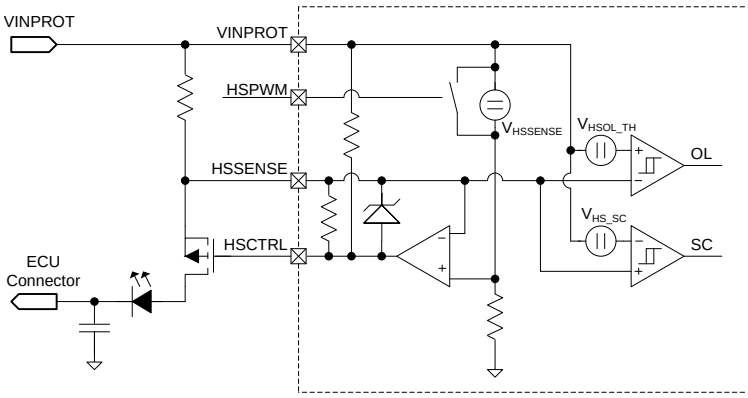



**Figure 10. High-Side Pre-Driver**

The high-side pre-driver integrates an open-load diagnostic circuit with the HS_OL status flag bit in the SPI register PWR_STAT. Open Load is also detected in case the voltage on VINPROT-VSSENSE does not drop below the threshold, when PWM is low (self-test).

A counter monitors the overcurrent condition to detect the risk of overheating. While HSPWM is high and HS_EN is high, the counter is incremented during overcurrent conditions and decremented if the current is below the overcurrent threshold at a sampling interval of $t_{S\ HS}$, like shown in Figure 11. When a net current-limit time of $t_{HSS\ CL}$ is reached, the driver turns off and the HS_EN bit clears. This feature is disabled by the SPI bit HS_CLDIS. The counter resets when HS_EN is cleared.

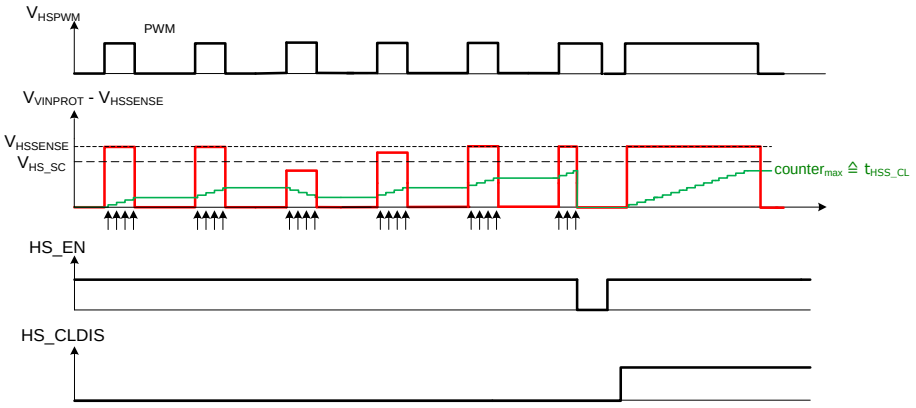



**Figure 11. HS Overcurrent Counter**

## 4.7 Loss of GND Detection

All power grounds PGNDx are monitored. If the voltage difference between PGNDx and GND exceeds $V_{GLTH\text{-}low}$ or $V_{GLTH\text{-}high}$ the device enters ERROR mode. RESN and PRESN are asserted low, the external PMOS (main system switch) is switched off, and the device error counter is incremented.

## 4.8 System-Error Interrupt Output

In OPERATING mode the IRQ pin is forced low in case the voltage on the battery line is below $V_{SSENSETHx}$ threshold. In LPM1mode the IRQ pin indicates a wake-up event.

The IRQ pin is low as long as PRESN is low. In case PRESN goes high and the battery line is already below $V_{SSENSETHx}$ threshold the IRQ pin is forced high for $t_{VSSENSE\_BLK}$.

## 4.9 Window-Watchdog Function

The watchdog function detects a malfunction of the MCU/DSP. The watchdog operates in two different modes:

- Timeout trigger mode with long timing starts with rising edge at RESN
- Window trigger mode with fixed timing after the first and each subsequent rising edge at WD pin.

A watchdog reset occurs when the following occurs:

- A trigger pulse outside the WD Trigger open window
- No trigger pulse during window time

After the RESN pin is released (rising edge) the DSP/MCU has to trigger the WD, by a rising edge on WD pin within a fixed time $t_{timeout}$. With this first trigger the Window Watchdog functionality is released. In case LPM1 is selected and all power rails except BUCK1 are manually switched off the WD is disabled.

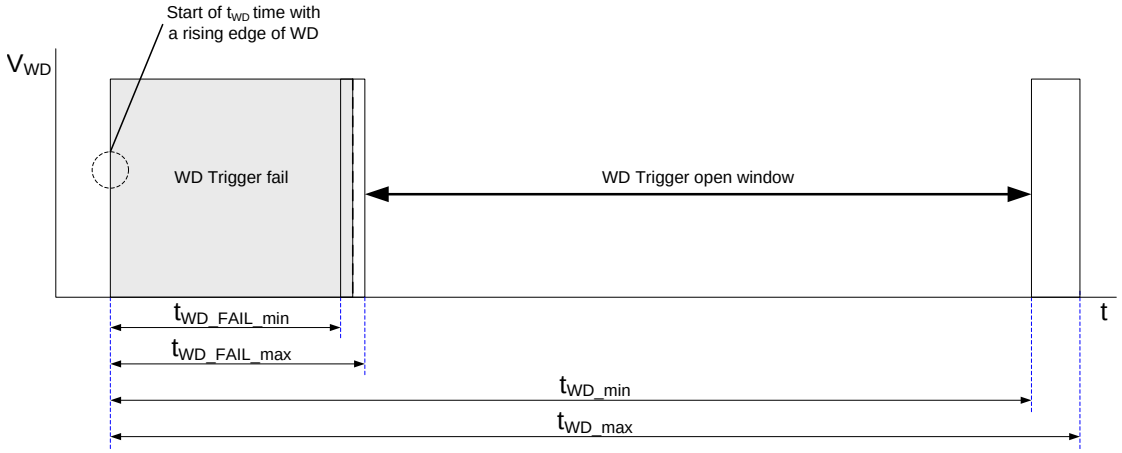



**Figure 12. Window-Watchdog Function**

## 4.10 Over Temperature Detection and Shutdown

There are two levels of thermal protection for the device. Over-temperature is monitored locally on each regulator.

1. Over-temperature for BUCK1-3
   - If a thermal monitor on the buck rails reaches a threshold higher than $T_{OTTH}$ the device enters ERROR mode. Leaving ERROR mode is only possible if the temperature is below $T_{OTTH}$ -$T_{OTHY}$.
2. Over-temperature for BOOST/LDO
   - If the temp monitor of the Boost or the LDO reaches the TOTTH threshold, the corresponding regulator switches off

**Over temperature Shutdown** is monitored on a central die position. In case the TSDTH is reached the device enters shutdown mode. Exiting shutdown when the TSD sensor is below TSDTH – TSDHY. This event internally generates a POR.

## 4.11 Switch-Mode Power-Supply Clock and Low-Power-Mode Clock Monitors

The SMPS-clock and LMP-clock sources are monitored as a cross check of these two clock domains. Detected clock failures are latched as status bits and main function disabled.

## 4.12 SPI Communication

The serial peripheral interface (SPI) provides a communication channel between the TPS65311-Q1 device and a controller, while the TPS65311-Q1 device is always the slave and the controller is always the master.

The TPS65311-Q1 SPI is enabled by the SPI master asserting CSN (Chip Select) low. Each communication consist of 16 bits

- 1-bit Parity (odd) (parity is built over all bit incl. R/W, CMD_ID[5:0], DATA[7:0])
- 1-bit read-write (read = 0, write = 1)
- 6-bits CMD identifier
- 8-bits data

Each command is valid if:

- A valid CMD_ID was sent
- The parity bit (odd) was correct
- Exactly 16 SPI clocks have been counted between falling and rising edge of CSN

The response to each master command is given in the next following SPI cycle. The response address is the CMD_ID of the previous sent message and the corresponding data byte. The response data is latched with the previous cycle such that a response to a write command is the status of register before the write access (same response as a read access).

The response to an invalid command is the original command with the correct parity bit. The response to an invalid number of SPI clock cycles is a SPI_SCK_FAIL communication (CMD_ID=0x03). Write access to a read only register is not reported as an SPI error and is treated as a read access. The initial answer after the first SPI command sent is CMD_ID[5:0]=0x3F and Data[7:0] 0x5A.

The slave transmits an FSI bit between the falling edge of CSN and the rising edge of SCK. If the SDO line is high during this time a failure has occurred in the system and the MCU must use the PWR_STAT to get the root cause. A low level of SDO indicates normal operation of the device.

The FSI bit is set in case PWR_STAT != 0x00 or (SYS_STAT & 0x98) !=0x00 or SPI_STAT != 0x00. FSI is cleared in case all status flags are cleared.

## 5 TPS65311-Q1 Architecture Safety Mechanisms and Assumptions of Use

As a system and equipment manufacturer or designer, you are responsible to ensure that your systems (and any TI hardware or software components incorporated in your 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. You understand and agree that your use of TI components in safety-critical applications is entirely at your risk, and that you (as the buyer) agree to defend, indemnify, and hold harmless TI from any and all damages, claims, suits, or expense resulting from such use.

## 6 Application Diagram

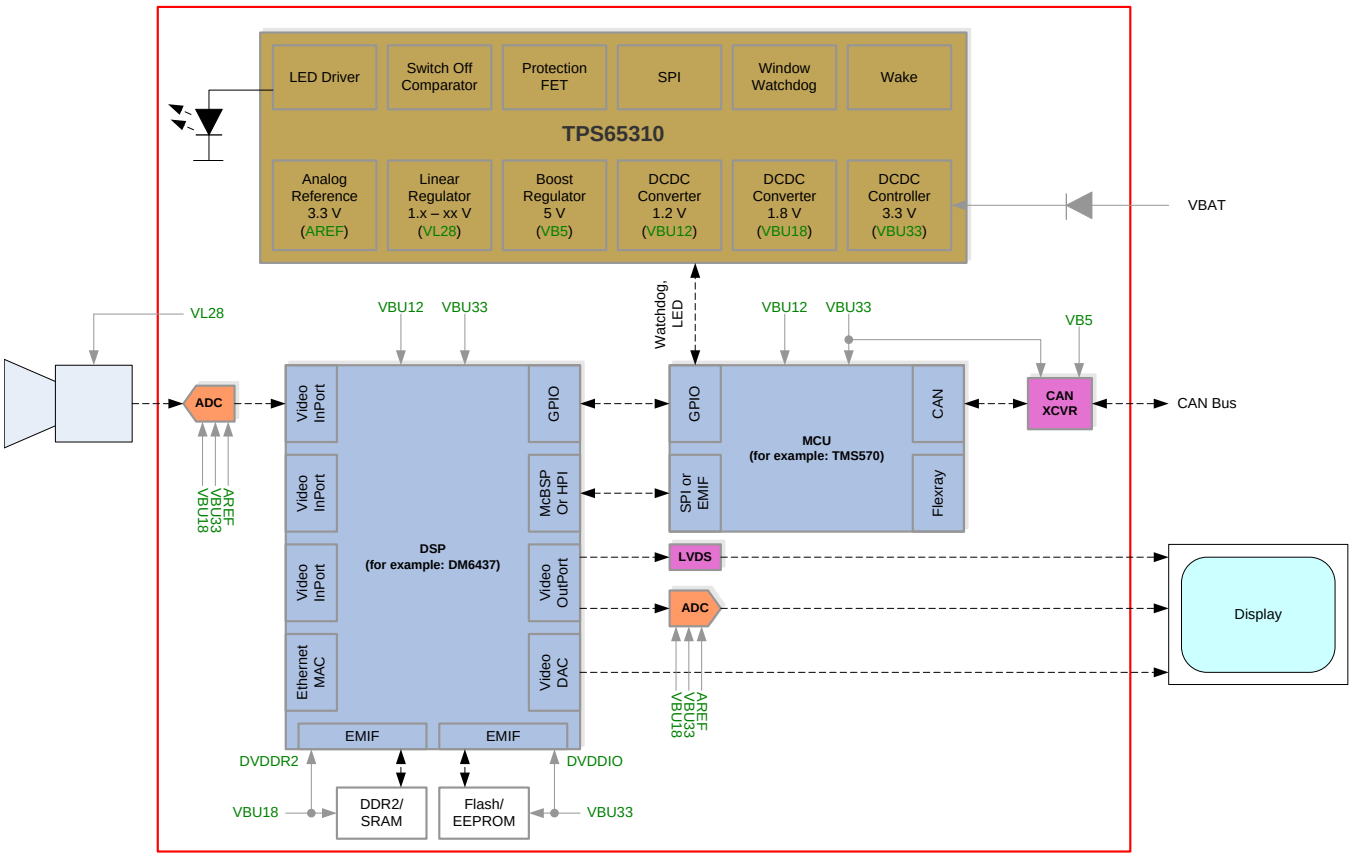



**Figure 13. Vision PMU Example**

# 7 Functional Safety Disclaimer for Safety Critical Solutions

TI's safety critical solutions, including integrated circuits, software and tools help TI's customers create end products that may be used in appropriately designed safety-critical applications to comply with functional safety standards or requirements.

Buyers represent and agree that they have all the necessary expertise to design, manage and assure effective system-level safeguards to anticipate, monitor and control system failures in safety-critical applications. Buyers agree and accept sole responsibility to meet and comply with all applicable regulatory standards and safety-related requirements concerning their systems and end-products which use TI's safety-critical applications. Buyers will fully indemnify TI and its representatives against any damages arising out of the use of TI products in safety-critical applications.

TI integrated circuits are not authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

## IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

| **Products** | | **Applications** | |
|---|---|---|---|
| Audio | www.ti.com/audio | Automotive and Transportation | www.ti.com/automotive |
| Amplifiers | amplifier.ti.com | Communications and Telecom | www.ti.com/communications |
| Data Converters | dataconverter.ti.com | Computers and Peripherals | www.ti.com/computers |
| DLP® Products | www.dlp.com | Consumer Electronics | www.ti.com/consumer-apps |
| DSP | dsp.ti.com | Energy and Lighting | www.ti.com/energy |
| Clocks and Timers | www.ti.com/clocks | Industrial | www.ti.com/industrial |
| Interface | interface.ti.com | Medical | www.ti.com/medical |
| Logic | logic.ti.com | Security | www.ti.com/security |
| Power Mgmt | power.ti.com | Space, Avionics and Defense | www.ti.com/space-avionics-defense |
| Microcontrollers | microcontroller.ti.com | Video and Imaging | www.ti.com/video |
| RFID | www.ti-rfid.com | | |
| OMAP Applications Processors | www.ti.com/omap | **TI E2E Community** | e2e.ti.com |
| Wireless Connectivity | www.ti.com/wirelessconnectivity | | |

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