Application Report
SLVA681E–March 2015–Revised March 2019

# Safety Manual for TPS65917-Q1 Power Management Unit (PMU)

**ABSTRACT**

This document is a safety manual for the Texas Instruments TPS65917-Q1 power management unit (PMU). It provides information to help system developers create safety related system using a supported TPS65917-Q1 PMU.

**Contents**



**List of Figures**

**List of Tables**



## Trademarks

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 the 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 document is a safety manual for the Texas Instruments TPS65917-Q1 power management unit (PMU). It provides information to help system developers create safety related system using a supported TPS65917-Q1 PMU. 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 and 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

The separate Safety Analysis Report documents the following information, not covered in this document:

- Failure rates estimation Qualitative failure analysis (design FMEA and FTA)
- 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 TPS65917-Q1 PMU. This document is intended to be used in conjunction with the pertinent datasheets 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 as seen in IEC 61508:2010.

## 2 Product Overview

The TPS65917-Q1 component is a power management integrated circuits (PMIC), available in a 48-pin, 0.5-mm pitch, 7-mm x 7-mm QFN package. It is designed specifically for automotive applications. The PMU provides five configurable step-down converter rails, with two of the rails having the ability to combine power rails and supply up to 7 A of output current in multi-phase mode. It also provides five external LDO rails. The PMU also comes with a 12-bit GPADC with two external channels, seven configurable GPIOs, two $I^2C$ interface channels or one SPI interface channel, PLL for external clock sync and phase delay capability, and programmable power sequencer and control for supporting different processors and applications.

The five step-down converter rails consist of five high frequency switch mode converters with integrated FETs. They are capable of synchronizing to an external clock input and support switching frequency between 1.7 MHz and 2.7 MHz. The SMPS1 and SMPS2 can combine in dual phase configuration to supply up to 7 A. In addition, SMPS1, SMPS2, and SMPS3 support dynamic voltage scaling by a dedicated $I^2C$ interface for optimum power savings. The five LDOs support 0.9 V to 3.3 V output with 50-mV step. They can be supplied from either a system supply or a pre-regulated supply. All LDOs and step-down converters can be controlled by the SPI or $I^2C$ interface, or by power request signals. In addition, voltage scaling registers allow transitioning the SMPS to different voltages by SPI, $I^2C$, or roof and floor control.

The power-up and power-down controller is configurable and programmable through OTP. The TPS65917-Q1 PMU includes a 32-kHz RC oscillator to sequence all resources during power up and power down. An internal LDOVRTC generates the supply for the entire digital circuitry of the component as soon as the VSYS supply is available through the VCCA input.

The 7 configurable GPIOs on the TPS65917-Q1 PMU feature multiplexed functions. They can be configured and used as general purpose IO signals, or as system control signals such as NSLEEP or NRESWARM, or as enable signals for external resources which can be included into the power-up and power-down sequence. The general-purpose (GP) sigma-delta analog-to-digital converter (ADC) with two external input channels inside the TPS65917-Q1 PMU can be used as thermal or voltage and current monitors.

The TPS65917-Q1 functional safety architecture features die temperature monitoring and shutdown, over current and short detection, watchdog timer which sends periodic interrupts and requests acknowledgment from the attached application processor, input supply undervoltage monitor, CRC self-check for OTP registers, and so forth. These features will be described in greater detail later in this document.

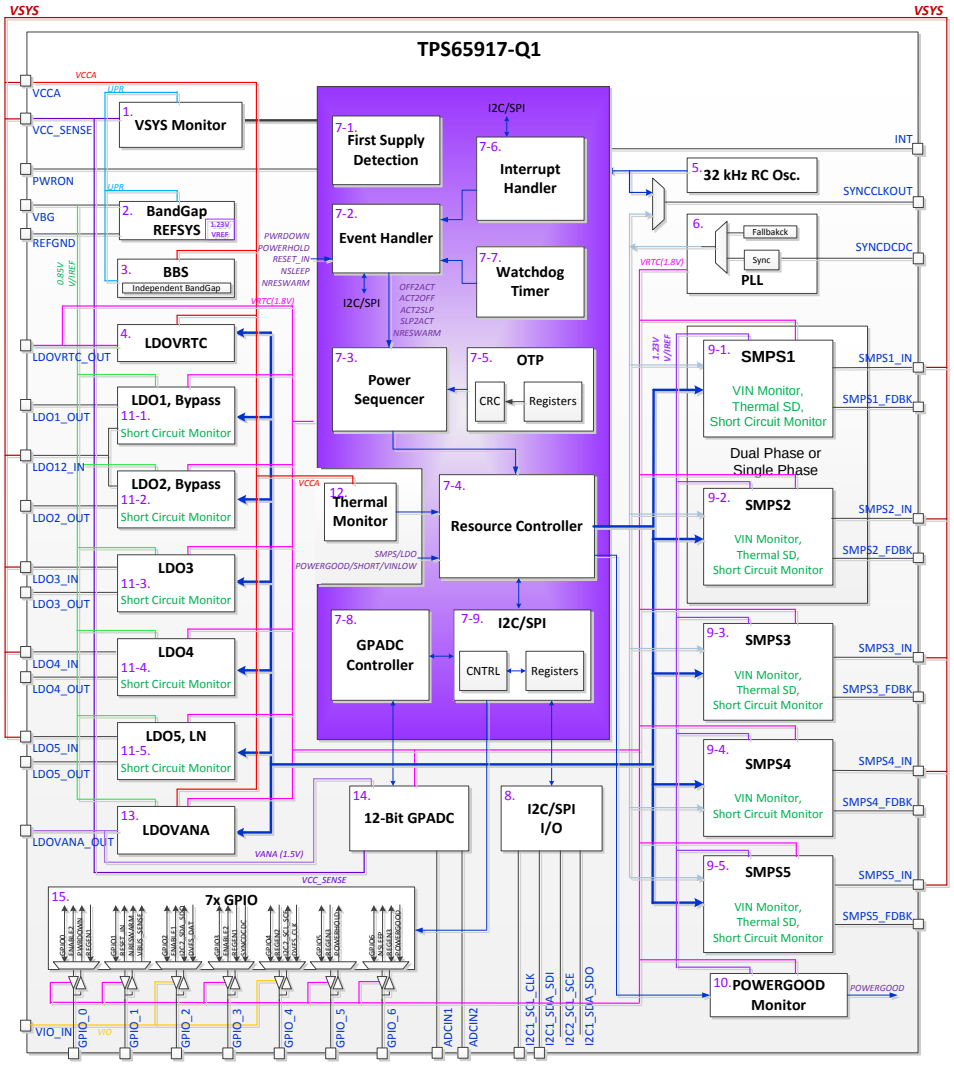



**Figure 1. TPS65917-Q1 Safety Architecture Diagram**

## 2.1 Target Applications

TPS65917-Q1 is designed for use as the PMU in the following automotive applications:

- Automotive Infotainment Systems
- Automotive Digital Cluster
- Advance Drive Assist Systems including Vision and Radar Sensors
- Industrial Vision and Radar Sensor 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. In designing this component, TI made various assumptions about how it could be used so as to address expected industry requirements for Advance Drive Assist Systems because these safety-critical systems are especially demanding.

Although TI has considered certain applications while developing these devices, 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 needs.

Figure 2 shows a presumed system configuration of an Advance Drive Assist System including Vision and Radar Sensors wherein TPS65917-Q1 is analyzed as a power management unit supporting the target application to achieve the safety level of ASIL-B.

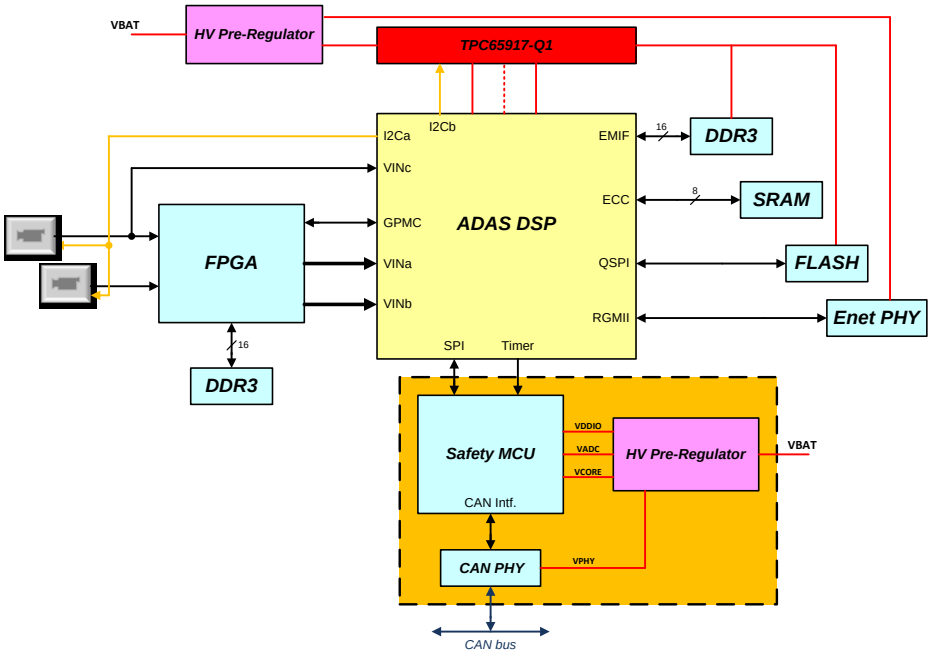



**Figure 2. Typical System Configuration for ADAS Systems Including Vision and Radar Sensors**

## 2.2 Product Safety Constraints

The TPS65917-Q1 safety analysis was performed under the following assumptions of system constrains:

- The VSYS input to the TPS65917-Q1 PMU is pre-regulated
- All inputs to the TPS65917-Q1 PMU meets the recommended operating conditions defined in the device data sheet and do not exceed absolute operating conditions defined therein
- The operating temperature of the TPS65917-Q1 PMU meets the ambient and junction temperature limits defined in the device data sheet
- All external components to the TPS65917-Q1 PMU meet the electrical characteristics defined in the device data sheet for the components in question
- The layout of the system board follows the layout guideline as defined in section 12.1 of the TPS65917-Q1 PMU data sheet, which particularly addresses the 9-Vpp restriction for all 5 SMPS supplies at the phase-node for both the high-side FETs (VIN – SWx) and the low-side FETs (SWx – PGND)
- The junction temperature of the TPS65917-Q1 PMU does not exceed the maximum value as specified in the TPS65917-Q1 PMU data sheet
- The safety MCU of the ADAS system is power independently from the TPS65917-Q1 PMU

# 3 TPS65917-Q1 Development Process for Management of Systematic Faults

For safety-critical development, it is necessary to manage both systematic and random faults. Texas Instruments has created a 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 applications developments targeting IEC 61508 and ISO 26262, then augments this process.

## *3.1 TI New-Product Development Process*

Texas Instruments 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 regarding quality management and product reliability. Though not explicitly developed for compliance to a functional safety standard, the TI new-product development process already featured many elements necessary to manage systematic faults.

The TPS65917-Q1 PMU was developed using TI's new product development process which has been certified as 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 3 shows the standard process

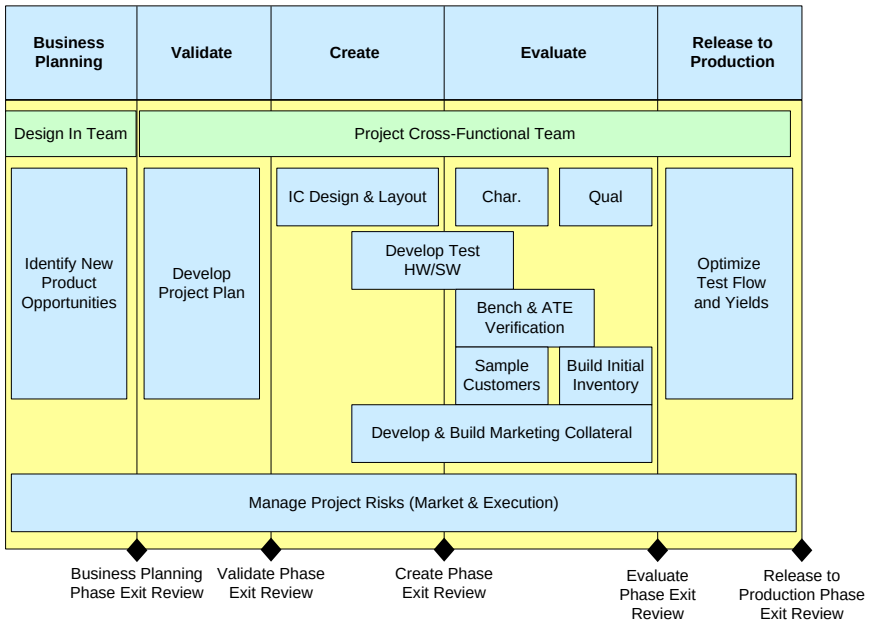



**Figure 3. TI New-Product Development Process**

## 3.2 TI Safety Development Flow

The TI 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 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. It aligns with the TI QRAS AP00210 enhanced-safety development process.

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

Key elements of the TI 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

Table 1 lists these activities overlaid atop the standard QM development flow.

**Table 1. TI New-Product Development Process**

| Business Opportunity Prescreen | Program Planning | Create | Validate, Sample, and Characterize | Quality | Ramp/Sustain |
|---|---|---|---|---|---|
| Determine if safety process execution is necessary | Define SIL/ASIL capability | Execute safety design | Validate safety design in silicon | Qualification of safety design | Implement plans to support operation and production |
| Execute development interface agreement (DIA) with lead customers and suppliers | Generate safety plan | Qualitative analysis of design (FMEA and FTA) | Release safety manual | Release safety case report | Update safety case report (if needed) |
| | Initiate safety case | Incorporate findings into safety design | Release safety analysis report | Update safety manual (if needed) | Periodic confirmation measure reviews |
| | Analyze assumed system to generate system level safety assumptions and requirements | Develop safety product preview | Characterization of safety design | Update safety analysis report (if needed) | |
| | Develop component level safety requirements | Validation of mixed-signal safety design at transistor, gate and RTL level | Confirmation measure review | Confirmation measure review | |
| | Validate component safety requirements meet system safety requirements | Quantitative analysis of design (FMEDA) | | | |
| | Implement safety requirements in design specification | Incorporate findings into safety design | | | |
| | Validate design specification meets component safety requirements | Validation of mixed-signal safety design at transistor/gate/physical layout level | | | |
| | Confirmation measure review | Confirmation measure review | | | |

## 3.3 Development Interface Agreement

The intent of a development interface agreement (DIA) is to define the responsibilities of the customer and supplier in facilitating the development of a functional safety system.

In custom developments, the DIA is a key document executed between customer and supplier early in the process of developing both the system and the custom TI component. As the TPS65917-Q1 family is a commercial, off-the-shelf (COTS) product, TI has prepared a standard DIA which describes the support 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 TPS65917-Q1 product is developed as a safety element out of context (SEooC) with a target safety goal of ASIL-B. Detailed safety requirements were not available from lead customers during development. Therefore, the safety requirements used were based on TI analysis of target safety applications.

TI is willing to discuss 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 2 lists the safety documentation for the TPS65917-Q1, which are made available either publicly or under a non-disclosure agreement (NDA):

**Table 2. 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 | Available |
| Safety manual | User guide for the safety features of the product, including system-level assumptions of use. | Public | Available |
| ISO 26262 Safety Analysis Report | Results of FTA, FMEA, and/or FMEDA safety analysis execution and resulting metrics per the ISO 26262 standard. For use in conjunction with the safety manual. | NDA material | Available |
| Safety Case Report | Detailed summary of the conformance of the product to the ISO 26262 and IEC 61508 standards. | NDA material | Available |

### 3.3.3 External Product Audits

TI has no current plans to perform an external audit of TPS65917-Q1 products to IEC 61508 or ISO 26262 standards. Detailed documentation can be made available after product qualification to support customer system audit/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 TPS65917-Q1 Product Architecture for Management of Random Faults

For safety-critical development, it is necessary to manage both systematic and random faults. The TPS65917-Q1 product architecture integrates several modules which can detect and respond to random faults by returning the device to a safe state. . Naturally, the effectiveness of fault management also depends on other elements of the safety system and how they are interconnected as described in part below.

TPS65917-Q1 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 will introduce these operation modes and safety mechanisms of the TPS65917-Q1:

- Embedded power controller (EPC)
- Programmable Reset levels of the TPS65917-Q1
- Resource state assignment and emergency switch-off
- Warm reset function

## *4.1 Device Operating States*

The operating states of TPS65917-Q1 can be monitored by the system software via $I^2C$ or SPI interface and register sets. The EPC of the device fully manages the state of the device during power transitions. According to four defined types of requests (ON, OFF, WAKE, and SLEEP), the EPC executes one of the five predefined power sequences (OFF2ACT, ACT2OFF, SLP2OFF, ACT2SLP, and SLP2ACT) to control the state of the TPS65917-Q1 resources. Any power resource can be included in any power sequence; when a resource is not controlled or configured through a power sequence, it is left in its default state (from OTP).

### 4.1.1 Embedded Power Controller

The EPC is composed of three main modules:

- An events arbitration module used to prioritize ON, OFF, WAKE, and SLEEP requests.
- A power state-machine used to determine which power sequence to execute, based on the system state (supplies, temperature, and so forth) and requested transition (from the event arbitration module).
- A power sequencer that fetches the selected power sequence from OTP and executes it. The power sequencer sets up and controls all resources accordingly, based on the definition of each sequence.

Figure 4 shows the EPC block diagram.

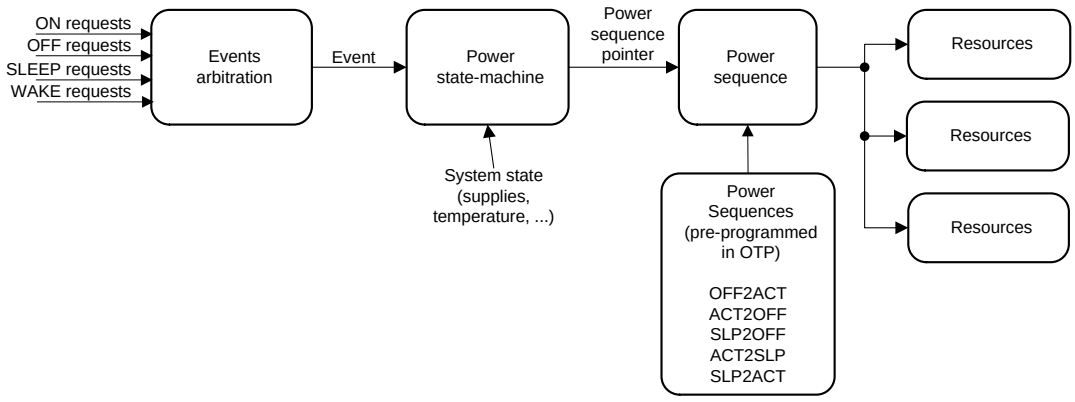



**Figure 4. EPC Block Diagram**

Each power transition consists of a sequence of one or several register accesses that controls the resources according to the EPC supervision. Because these sequences are stored in nonvolatile memory (OTP), they cannot be altered.

## 4.2 Resource Operating Mode Management and Reset Mechanism

The operating mode of the power resources on TPS65917-Q1 can be programmed to allow control through external signals. In the event of systematic or random system malfunction, the reset mechanism of the TPS65917-Q1 will also ensure all of the power resources return to the programmed default state. The following sections briefly describe the architecture of these mechanisms. For more information on each of these mechanisms, refer to the *TPS65917-Q1 Power Management Unit for Processor* data sheet.

### 4.2.1 Resource State Assignment and Emergency Switch-Off

The power resources SMPS1 through SMPS5 and LDO1 through LDO5 in the TPS65917-Q1 can be assigned to three external control pins NSLEEP, ENABLE1, and ENABLE2. These three control pins can directly control the mode of the assigned power resources while the TPS65917-Q1 goes through the ACT2SLP or the SLP2ACT power sequences.

The control register of each power resource allows the user to assign the power resource to a specific power mode while it is under ACTIVE or SLEEP state. For example, under the control register SMPS1_CTRL, MODE_ACTIVE and MODE_SLEEP bits allow the user to program SMPS1 to either OFF, FORCE PWM, or ECO mode while SMPS1 is in ACTIVE or SLEEP state.

A power resource can be assigned to the NSLEEP pin through the NSLEEP_SMPS_ASSIGN, NSLEEP_LDO_ASSIGN1, or the NSLEEP_LDO_ASSIGN2 registers. Once it is assigned to the NSLEEP pin, an activation of this pin will cause the power resource to transition between the modes which was programmed in the MODE_ACTIVE and the MODE_SLEEP bits under the resource control register. The timing of the transition will follow the SLEEP and WAKE (ACT2SLP or SLP2ACT) power sequence as programmed in the OTP.

The user can bypass the SLEEP and WAKE power sequencing by having resources assigned to the ENABLE1 or the ENABLE2 pins through the ENABLE1/2_SMPS_ASSIGN, ENABLE1/2_LDO_ASSIGN1, or the ENABLE1/2_LDO_ASSIGN2 registers. When these pins are activated, the assigned power resource will transition immediately between the modes which was programmed in the MODE_ACTIVE and the MODE_SLEEP bits under the resource control register. The timing of the transition will be immediate and will not be controlled by the power sequencer. Therefore these external control pins can be used as emergency switch-off of the power resources during system critical condition.

Table 3 lists the logic arbitration of the ENABLE1, ENABLE2, and NSLEEP pin assignments and their effect on the state transition of the assigned power resources.

**Table 3. Resources SLEEP and ACTIVE Assignments**

| ENABLE1 Assignment | ENABLE2 Assignment | NSLEEP Assignment | ENABLE1 Pin State | ENABLE2 Pin State | NSLEEP Pin State | State | Transition |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | Don't care | Don't care | Don't care | ACTIVE | None |
| 0 | 0 | 1 | Don't care | Don't care | 0 ↔ 1 | SLEEP ↔ ACTIVE | Sequenced |
| 0 | 1 | 0 | Don't care | 0 ↔ 1 | Don't care | SLEEP ↔ ACTIVE | Immediate |
| 0 | 1 | 1 | Don't care | 0 | 0 ↔ 1 | SLEEP ↔ ACTIVE | Sequenced |
| | | | | 1 | 0 ↔ 1 | ACTIVE | None |
| | | | | 0 ↔ 1 | 0 | SLEEP ↔ ACTIVE | Immediate |
| | | | | 0 ↔ 1 | 1 | ACTIVE | None |
| 1 | 0 | 0 | 0 ↔ 1 | Don't care | Don't care | SLEEP ↔ ACTIVE | Immediate |
| 1 | 0 | 1 | 0 | Don't care | 0 ↔ 1 | SLEEP ↔ ACTIVE | Sequenced |
| | | | 1 | | 0 ↔ 1 | ACTIVE | None |
| | | | 0 ↔ 1 | | 0 | SLEEP ↔ ACTIVE | Immediate |
| | | | 0 ↔ 1 | | 1 | ACTIVE | None |

**Table 3. Resources SLEEP and ACTIVE Assignments (continued)**

| ENABLE1 Assignment | ENABLE2 Assignment | NSLEEP Assignment | ENABLE1 Pin State | ENABLE2 Pin State | NSLEEP Pin State | State | Transition |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 ↔ 1 | Don't care | SLEEP ↔ ACTIVE | Immediate |
| | | | 1 | 0 ↔ 1 | | ACTIVE | None |
| | | | 0 ↔ 1 | 0 | | SLEEP ↔ ACTIVE | Immediate |
| | | | 0 ↔ 1 | 1 | | ACTIVE | None |
| 1 | 1 | 1 | 0 | 0 | 0 ↔ 1 | SLEEP ↔ ACTIVE | Sequenced |
| | | | 0 | 1 | 0 ↔ 1 | ACTIVE | None |
| | | | 1 | 0 | 0 ↔ 1 | ACTIVE | None |
| | | | 1 | 1 | 0 ↔ 1 | ACTIVE | None |
| | | | 0 | 0 ↔ 1 | 0 | SLEEP ↔ ACTIVE | Immediate |
| | | | 0 | 0 ↔ 1 | 1 | ACTIVE | None |
| | | | 1 | 0 ↔ 1 | 0 | ACTIVE | None |
| | | | 1 | 0 ↔ 1 | 1 | ACTIVE | None |
| | | | 0 ↔ 1 | 0 | 0 | SLEEP ↔ ACTIVE | Immediate |
| | | | 0 ↔ 1 | 0 | 1 | ACTIVE | None |
| | | | 0 ↔ 1 | 1 | 0 | ACTIVE | None |
| | | | 0 ↔ 1 | 1 | 1 | ACTIVE | None |

### 4.2.2 Reset Levels of the TPS65917-Q1

The TPS65917-Q1 includes three levels of device reset:

**Power-on reset (POR) —** A POR occurs when the device receives supplies and transition from the NO SUPPLY state to the BACKUP state. The POR is the global device reset which resets all registers. The values of the registers in this domain will retain their value under HWRST and SWORST event. This ensures the information which contains the cause of the switch off event is retained when the device is reset to its default operating state.
The following registers are reset only during POR event:

- SMPS_THERMAL_STATUS
- SMPS_SHORT_STATUS
- SMPS_POWERGOOD_MASK
- LDO_SHORT_STATUS
- SWOFF_STATUS

This list is indicative only; a full list and bit details can be found in the *TPS65917-Q1 Register Map*.

**Hardware reset (HWRST) —** A HWRST occurs when any OFF request is configured to generate a hardware reset. Configuration of the reset level is programmed in the SWOFF_HWRST register. This reset triggers a transition to the OFF state from either the ACTIVE or SLEEP state, and therefore executes the ACT2OFF or SLP2OFF sequence.
A HWRST will reset all registers in the HWRST and the SWORST domain, but leave the registers in the POR domain unchanged.
The following registers are in the HWRST domain:

- SMPS control registers expect MODE_ACTIVE and MODE_SLEEP bits
- LDO control registers expect MODE_ACTIVE and MODE_SLEEP bits
- VSYS_LO Threshold
- PMU_CONFIG and PMU_CTRL
- NSLEEP, ENABLE1, and ENABLE2 resource assignment registers

- Input and Output, including the GPIO pins, Configuration and Control registers
- Interrupt Control, Status and Mask Registers
- OTP CRC results register
- GPADC Configuration and Results registers

This list is indicative only; a full list and bit details can be found in the *TPS65917-Q1 Register Map*.

**Switch-off reset (SWORST) —** A SWORST occurs when any OFF request is configured to not generate a hardware reset. Configuration is done in the SWOFF_HWRST register. This reset acts like the HWRST, except only the SWO registers are reset. The TPS65917-Q1 goes into the OFF state, from either ACTIVE or SLEEP, and therefore executes the ACT2OFF or SLP2OFF sequence.
A SWORST will reset only registers in the SWORST domain, but leave the registers in the HWRST and POR domains unchanged.
The following registers are in the SWORST domain:

- SMPS control registers for voltage levels and operating mode control
- LDO control registers for voltage levels and operating mode control
- DEV_CTRL and POWER_CTRL registers
- VSYS_MON enable and result register
- WATCHDOG configuration register
- PLL and REGEN Control registers

This list is indicative only; a full list and bit details can be found in the *TPS65917-Q1 Register Map*.

Table 4 lists the reset levels, and Figure 5 shows the reset levels versus registers.

**Table 4. Reset Levels**

| Level | Reset Tag | Registers Affected | Comment |
|---|---|---|---|
| 0 | POR | POR, HW, SWO | This reset level is the lowest level, for which all registers are reset. |
| 1 | HWRST | HW, SWO | During hardware reset (HWRST), all registers are reset except the POR registers. |
| 2 | SWORST | SWO | Only the SWO registers are reset. |

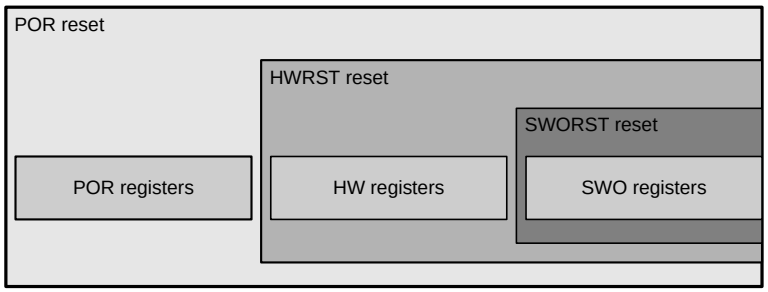



**Figure 5. Reset Levels versus Registers**

### 4.2.3 Warm Reset Function

The TPS65917-Q1 can execute a warm reset. The main purpose of this reset is to recover the device from a locked or unknown state by reloading default configuration without switching off all of the power resources. The warm reset is triggered by the NRESWARM pin. During a warm reset, the OFF2ACT sequence is executed regardless of the state (ACTIVE or SLEEP) and the TPS65917-Q1 returns to or remains in the ACTIVE state. Resources which are not part of the OFF2ACT sequence are not impacted by warm reset and keep their previous state. Resources which are part of power-up sequence go to active mode, and output voltage level is reloaded from OTP or kept in the previous value depending on the WR_S bit in the SMPSx_CTRL or LDOx_CTRL register. The total time for the warm reset execution is system dependent and will vary based on the number of resources which are part of the OFF2ACT sequence and the settling time based on the output loading.

# 5 TPS65917-Q1 Architecture Safety Mechanisms and Assumptions of Use

This section summarizes the safety mechanisms for each major functional block of TPS65917-Q1 architecture and provides general assumptions of use. The product data sheet contains the details of each safety mechanism. The safety analysis report notes the effectiveness of these safety mechanisms. Naturally, the system integrator must comprehensively assess effectiveness in the context of the specific end use.

The TPS65917-Q1 Architecture Safety Mechanisms includes the following:

- Interrupt mechanism serving as pre-warning
- CRC self-check for OTP registers
- Supply Voltage (VSYS) Monitor
- Watchdog Timer
- Load Current Monitor for SMPS
- Thermal Monitors and Shutdown
- POWERGOOD indicator for SMPS outputs
- GPADC as Secondary Analog Monitoring
- Short Circuit Detection for each SMPS and LDO rails
- Thermal Monitors and Shutdown
- GPIOs have separate internal and external voltage of IO buffers
- Input voltage monitoring of SMPS while in ECO-mode

## 5.1 Interrupt Mechanism Serving as Prewarning

TPS65917-Q1 uses an INT output signal to warn the host processor of any interrupt event that has occurred within the TPS65917-Q1. The host processor must read the interrupt status registers (INTx_STATUS) through the control interface ($I^2C$ or SPI) to identify the interrupt source. Any interrupt source can be masked by programming the corresponding mask register (INTx_MASK). When an interrupt is masked, its associated event detection mechanism is disabled. Therefore the corresponding STATUS bit is not updated and the INT line is not triggered if the masked event occurs. If an event occurs while its corresponding interrupt is masked, that event is lost. If an interrupt is masked after it has been triggered (the event has occurred and has not been cleared), then the STATUS bit reflects the event until it is cleared, and it does not trigger again if a new event occurs (because it is now masked).

The polarity of the INT line and clearing method of interrupts can be configured using the POLARITY_CTRL register. The INT output is active low and is a push-pull output by default, but is configurable as an open-drain output. To reset the INT output line, all status registers must be cleared. The clearing of all status registers can be achieved by using a clear-on-read or a clear-on-write by default method. When the PMU is switched-off due to an interrupt event, the INT pin will remain in low state.

For more information on the device interrupt mechanism, refer to the *TPS65917-Q1 Power Management Unit for Processor* data sheet.

## 5.2 CRC Self-Check for OTP Registers

There are 6 banks of EPROM registers residing in TPS65917-Q1, each with 64 bytes of One Time Programmable (OTP) memory. These OTP registers holds the silicon trimming data along with default power sequencing and device configuration data. As a safety measure, an OTP bit integrity error detection routine can be enabled to ensure the bit integrity of the OTP memory before these data are used to power up the device in its default configuration. If enabled, this routine will be executed to compare the current OTP values with the pre-programmed values at the beginning of every OFF2ACT power sequence. When an OTP bit integrity error is detected, the pre-programed value in the CRC_CONTROL OTP register will determine the next action of the event handler based on the following options:

- Skip Error Detection and execute all power sequence
- Execute Error Detection and execute all power up sequence, even if an error is detected
- Execute Error Detection. If an error is detected, execute power up sequence until VIO supply rail is up
- Execute Error Detection. If an error is detected, stop power up sequence altogether

For a safety-critical system design, it is recommended that the OTP CRC self-check is always executed and not skipped at the beginning of every OFF2ACT power sequence. It is also recommend that the power sequence is stopped when an error is detected.

When an error is detected, an interrupt (INT2.OTP_ERROR) is sent to the host processor regardless of the CRC_CONTROL setting. The result of the CRC self-check will be recorded in the CRC_RESULTS register. The CRC_RESETS register is defined as:

**Bit0 —** CRC_RESULTS_TRIM (CRC Results for Trimming Data): 0 - Good, 1 - Error

**Bit1 —** CRC_RESULTS_SEQ (CRC Results for Power Sequence Data): 0 - Good, 1 - Error

**Bit2 —** CRC_RESULTS_CFG (CRC Results for Configuration Data): 0 - Good, 1 - Error

**Bit3 —** CRC_FORCE_OFF: 0 - Power Sequence is executed through the end, 1 - Power Sequence is forced off

**Bit7:4 —** Reserved

Figure 6 shows the OTP register map indicating the data allocations and the locations of the CRC control and result bits.

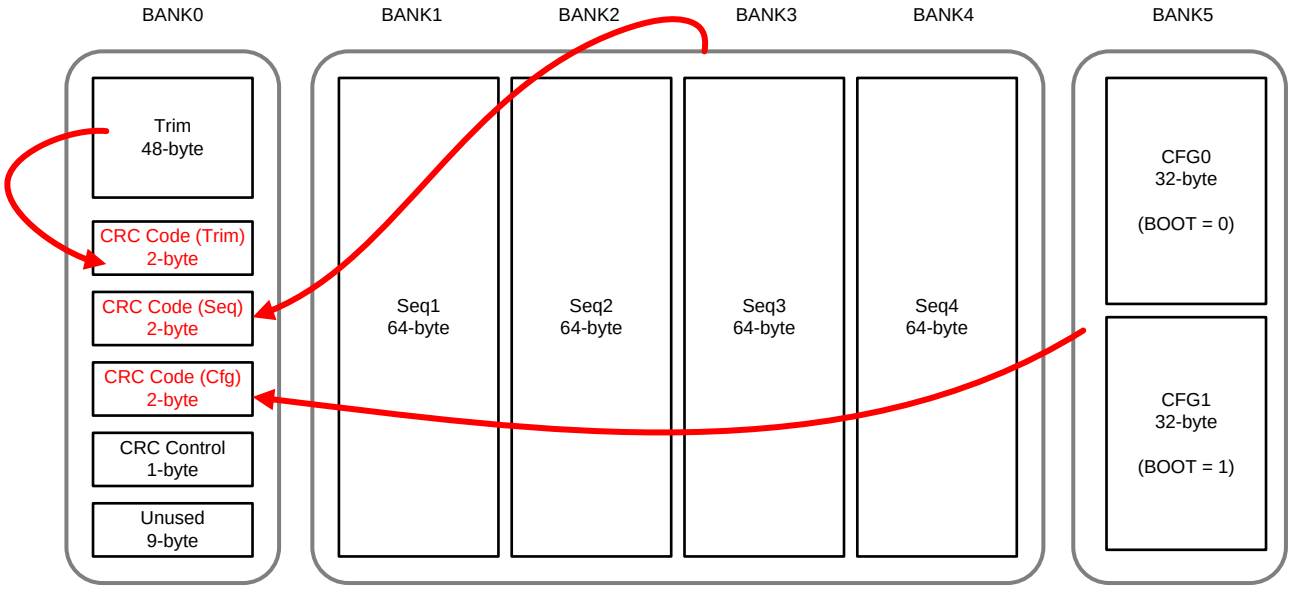



**Figure 6. OTP Register Map Diagram**

## 5.3 Supply Voltage Monitor (VSYS_MON)

The TPS65917-Q1 PMU is designed to work with an analog supply voltage range of 3.135 V to 5.25 V. The input supply should be well regulated and connected to the VCCA pin, as well as SMPS and LDO input pins with appropriate bypass capacitors. The battery supply voltage is monitored for undervoltage condition via VSYS_MON and VSYS_LO comparators.

Analog comparators are used to monitor the voltage on the VCC_SENSE and VCCA pins. The output of the voltage monitor controls the power state-machine of the TPS65917-Q1. It also provides early warning to the attached application processor (through the VSYS_MON interrupt) when the supply voltage falls below the pre-programmed threshold voltage.

During power up, the value of VSYS_HI OTP is used as a threshold for the VSYS_MON comparator which is gating PMIC start-up (that is, as a threshold for transition from the OFF state to the ACTIVE state). The VSYS_MON comparator monitors the VCC_SENSE pin. After power up, the VSYS_MON comparator is automatically disabled. Software can select new threshold levels using the VSYS_MON register to a threshold value between VSYS_HI and VSYS_LO and then enable the comparators. When the supply voltage drops below threshold value, a VSYS_MON interrupt will be triggered and require the processor to acknowledge the interrupt . The processor will therefore have additional time to react to the falling supply voltage and take appropriate actions prior to system shut down.

Figure 7 shows the implementation and the operating state of the VSYS_MON comparator. For more information on the operation of the VSYS_MON, refer to *TPS65917-Q1 Power Management Unit for Processor*.

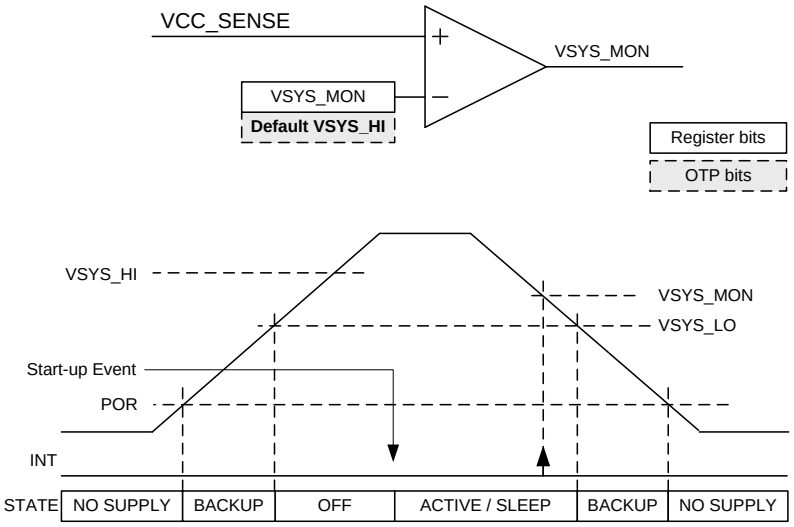



**Figure 7. System Voltage Monitor and System State Diagram**

## 5.4 Watchdog Timer

A watchdog timer is included in TPS65917-Q1 to monitor the state of the attached processor. The watchdog timer on this device has two modes of operation, periodic mode and interrupt mode.

In periodic mode, an interrupt is generated with a regular period N, defined by the setting of WATCHDOG.TIMER. This interrupt is generated at the beginning of the period (when the watchdog internal counter equals 1). The IC initiates a shutdown at the end of the period (when the internal counter reaches N) only if the interrupt is not cleared within the defined timeframe (0 to N). In this mode, when the interrupt is cleared, the internal counter is not reset. The counter keeps counting until it reaches its maximum value (defined by the TIMER setting) and automatically rolls over to 0 to start a new counting period. Regardless of when the interrupt is cleared within a given period (N), the next interrupt is generated only when the ongoing period completes (reaches N). The internal watchdog counter is initialized and kept at 0 as long as the RESET_OUT pin is low, and it starts counting when the RESET_OUT pin is released.

In interrupt mode, any interrupt sources reset the watchdog counter and start the counting. If the sources of the interrupts are not cleared (meaning the INT line released) before the end of the predefined period N (set by WATCHDOG.TIMER setting), then the IC initiates a shutdown. If the sources of the interrupts are cleared within the predefined period, then the watchdog counter is discarded (dc) and no shutdown sequence is initiated.

By default, the watchdog is disabled. The watchdog can be enabled by setting the ENABLE bit of the WATCHDOG register to 1, and this selection is write protected by setting the LOCK bit to 1. Reset of the device will return these bits to default values.

Figure 8 shows the watchdog timings.

WTD (bit 5) in the SWOFF_STATUS Register will be set if the OFF request was due to watchdog timeout.

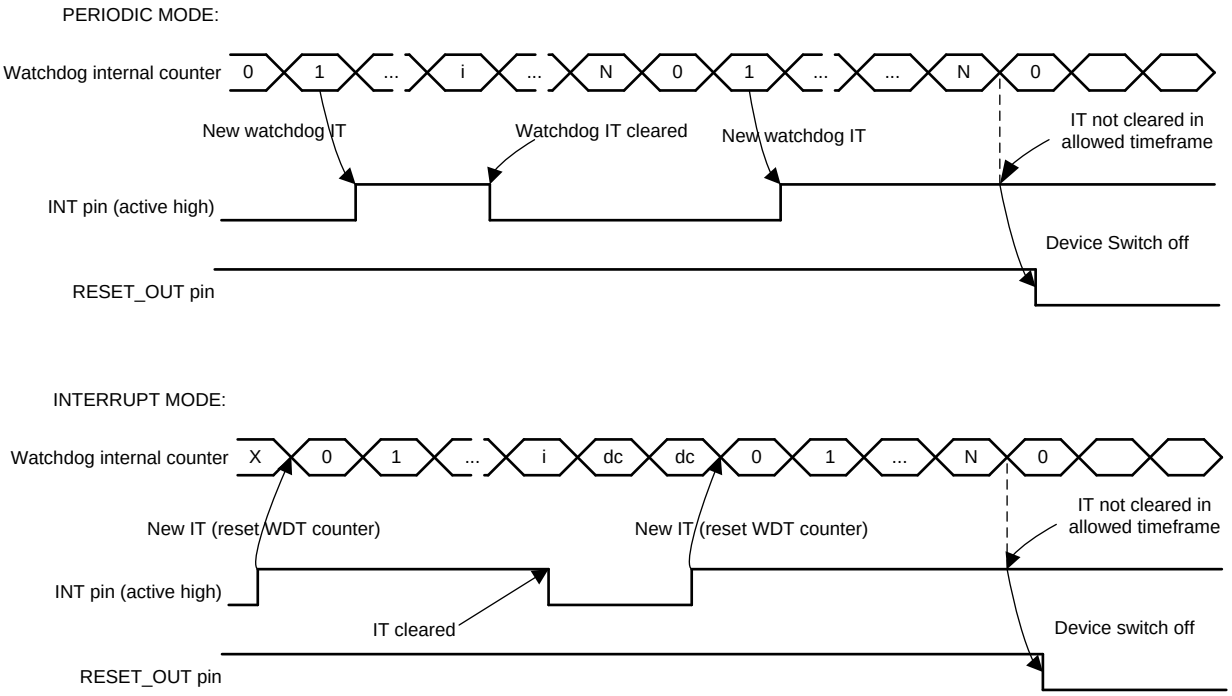



**Figure 8. Watchdog Timings**

For both the periodic mode and the interrupt mode, the shortest period N which can be programmed by the WATCHDOG.TIMER setting is 1 second. For safety critical systems which require more frequent monitoring of the processor, an external watchdog timer is recommend.

## 5.5 Load Current Monitor for SMPS

Serving as an early warning to the attached processor for over current conditions, Channel 4 of the GPADC on TPS65917-Q1 can be used to monitor the output current of SMPS1, SMPS2, SMPS1&2, SMPS3, or SMPS5. Load current monitoring is enabled for one SMPS at a time, assigned in the SMPS_ILMONITOR_EN register. SMPS output power monitoring is intended to be used during the steady state of the output voltage, and is supported in PWM mode only.

The basic equation for the SMPS output current result is:

$$I_{LOAD} = I_{FS} \times \text{GPADC code} / (2^{12} - 1) - I_{OS}$$

where

- $I_{FS} = I_{FS0} \times K$
- $I_{OS} = I_{OS0} \times K$
- K = the number of SMPS active phases (1)

Temperature compensated result:

$$I_{LOAD} = I_{FS} \times \text{GPADC code} / ( [2^{12} - 1] \times [1 + TC\_R0 \times (TEMP-25)]) - I_{OS} \quad (2)$$

Values of output current measurement gain factor, $I_{FS0}$, and Output current measurement current offset, $I_{OS0}$, can be found in the device data sheet for TPS65917-Q1 under the Electrical Characteristics table for the 12-Bit Signal-Delta ADC.

For all the SMPS rails, including SMPS4 , the sink current limitation is controlled can be enabled by setting the SMPS_NEGATIVE_CURRENT_LIMIT_EN register. The limitation is enabled by default.

## 5.6 POWERGOOD Indicator for SMPS Outputs

The TPS65917-Q1 includes an external POWERGOOD pin which indicates if the outputs of the SMPS are within the range of the programmed output voltage, and if the current loading for the SMPS is less than the current limit. The POWERGOOD signal can be output through GPIO6 when it is programmed as the POWERGOOD pin. It is an open drain output with programmable polarity, so users can combine it with other gating signals to create an enable signal for the attached processor.

Users can select whether POWERGOOD will report the result of both voltage and current monitoring or only current monitoring. This selection applies to all SMPSs in the SMPS_POWERGOOD_MASK2.POWERGOOD_TYPE_SELECT register. When both voltage and current are monitored, the POWERGOOD signal indicates whether or not all SMPS outputs are within a certain percentage, as defined by the $V_{SMPSPG}$ parameter, of the programmed value while the load current is below $I_{LIM}$.

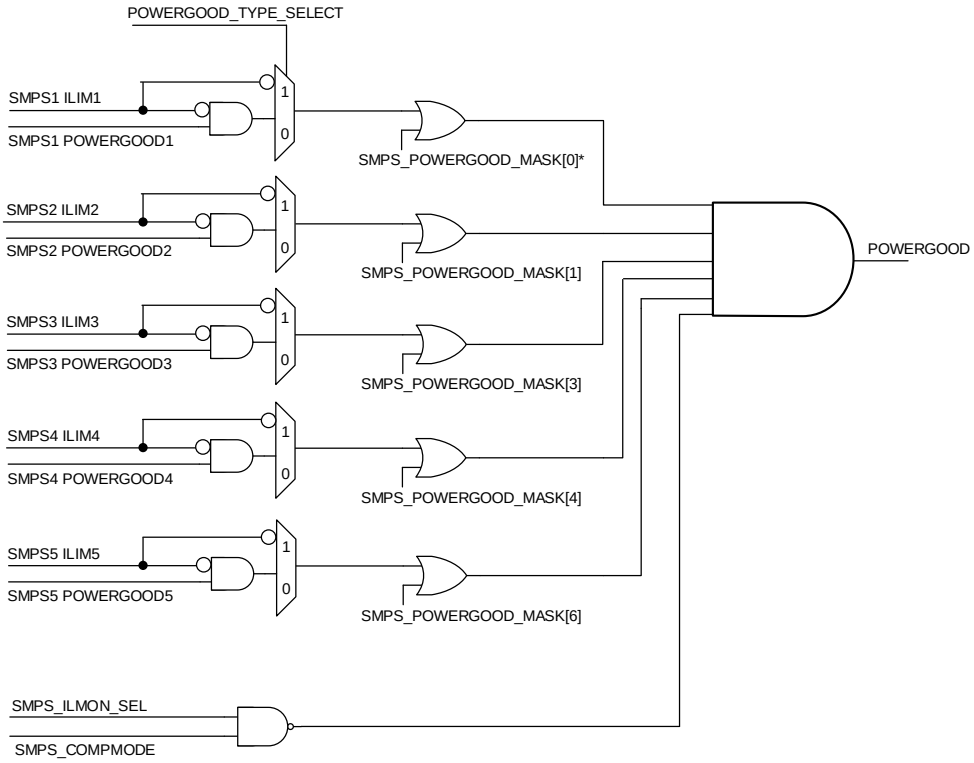
All POWERGOOD sources can be masked in the SMPS_POWERGOOD_MASK1 and SMPS_POWERGOOD_MASK2 registers. When an SMPS is disabled, it should be masked from the POWERGOOD monitor. When SMPS voltage transitions from one target voltage to another due to DVS command, voltage monitoring is internally masked and POWERGOOD is not impacted.

It is also possible to include in POWERGOOD the GPADC result for SMPS output current monitoring by setting the SMPS_COMPMODE bit to 1. The GPADC can monitor only one SMPS current loading at a time.

The POWERGOOD threshold for the SMPS outputs -2 typically -4% for rising output, and -16% for falling output. If more accurate under voltage monitoring is required, we recommend utilizing the two external GPADC channels as described in Section 5.7, or using an external voltage monitor with the required accuracy.

**NOTE:** When operating SMPS1 and SMPS2 in dual-phase (for a combined 7 A maximum output current), it is required that external monitoring is used on the SMPS12 output to achieve system voltage monitoring requirements. Additionally, if using the POWERGOOD signal, it is recommended that SMPS12 is masked from POWERGOOD monitoring. Monitoring SMPS12 on the POWERGOOD rail could result in a false detection of a POWERGOOD event under certain loading conditions.

Figure 9 shows the construction of the POWERGOOD monitoring and indicator.




*When operating in dual phase, SMPS_POWERGOOD_MASK[0] controls the monitoring of SMPS12. SMPS_POWERGOOD_MASK[1] is masked internally with dual phase operation.

**Figure 9. POWERGOOD Block Diagram**

## 5.7 GPADC as Secondary Analog Monitoring

The GPADC on TPS65917-Q1 provides an alternative solution to voltage monitor. In the case when the output of a particular SMPS needs to be monitored with greater precision, the output of the SMPS can be looped back to ADCIN1 or ADCIN2 pin of TPS65917-Q1. The input channel can be setup by the software for automatic conversion in time intervals as short as 31.25 mS.

If the conversion result triggers the pre-programmed threshold level, an INT interrupt is generated and the conversion result is stored. If the interrupt is not cleared or the results are not read before another auto-conversion is completed, then the registers store only the latest results, discarding the previous ones. The auto-conversion is never stopped by an uncleared interrupt or unread registers. The system software can also program the threshold level to trigger a platform shutdown. By programming the SHUTDOWN bits in the GPADC_AUTO_CTRL register, two GPADC channels can be selected to independently shutdown the TPS65917-Q1 device if the conversion result triggered an interrupt, and the interrupt is not is not cleared within the periodic delay time. The off request to shutdown the TPS65917-Q1 through this mechanism can be configured to generate a hardware a reset (HWRST) or switch-off reset (SWORST) through OTP pre-programming. More details regarding HWRST and SWORST was described in section Section 4.2.2.

For more information on the operation of the GPADC on the TPS65917-Q1 device, refer to *TPS65917-Q1 Power Management Unit for Processor*.

## 5.8 Short Circuit Detection for Each SMPS and LDO Rails

In addition to the load current monitoring for each SMPS via the POWERGOOD indicator, all SMPS and LDO regulators on TPS65917-Q1 also have a detection for load current above $I_{LIM}$ to indicate overcurrent or shorted LDO output. The SMPS_SHORT_STATUS register indicates any SMPS short condition, while the LDO_SHORT_STATUS register indicates any LDO short condition. Depending on the interrupt short line mask bit register (INT2_MASK.SHORT), an interrupt is generated upon any shorted SMPS or LDO rail. If a short condition occurs while the SMPS or the LDO is in operation, a switch-off signal is sent to the corresponding power source to prevent possible damages to the system due to the current overload. The corresponding short status bit is set in the SMPS_SHORT_STATUS or the LDO_SHORT_STATUS registers, therefore enables the software to identify the power source which suffered the short condition.

## 5.9 Thermal Monitors and Shutdown

Each SMPS on TPS65917-Q1 except SMPS4 includes the independent thermal monitoring feature. The SMPS thermal monitoring is enabled by default, and can be disabled with the SMPS_THERMAL_EN register. When enabled, the SMPS thermal status can be monitored by the system software by ready the the SMPS_THERMAL_STATUS register.

In addition to the independent thermal monitors for 4 of the 5 SMPS, TPS65917-Q1 also integrates two thermal detection modules to monitor the temperature of the die. These modules are placed on opposite sides of the chip and close to the LDO and SMPS modules. Over temperature at either module first generates a warning to the system through the HotDie interrupt; if the temperature continues to rise, the PMIC device shuts down before damage to the die can occur. Thus, here are two protection levels:

- A hot-die (HD) function sends an interrupt to software. Software is expected to close any noncritical running tasks to reduce power.
- A thermal shutdown (TS) function immediately starts to switch-off the TPS65917-Q1 device.

For more information on the hot-die interrupt and thermal shutdown functions, refer to *TPS65917-Q1 Power Management Unit for Processor*.

## 5.10 Input Voltage Monitoring of SMPS While in ECO-mode

To ensure proper operation of the converter while it is in ECO-mode, the output voltage level must be less than 70% of the input supply voltage level. If the Vo of the converter is greater than 2.8V, a safety feature of the device will monitor the supply voltage of the converter, and automatically shut down the converter if the input voltage falls below 4V. The purpose of this safety mechanism is to prevent damage to the converter due to design limitation while the converter is in ECO-mode.

# 6 Application Diagrams and Safety Analysis

This section contains a Safety Element out of Context (SEooC) analysis of TPS65917-Q1. 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 TPS65917-Q1 to assist the system designer in achieving a given ASIL level. Customers are responsible for putting this device into the context of their system and analyze the ASIL coverage achieved therein. The TPS65917-Q1 was designed to support several different systems that require multiple configurable power rails. However, of all these systems, only Advanced Driver Assistance Systems (ADAS) have been identified to have safety requirements. The TPS65917-Q1 has been designed to perform/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. Please note that the system designer may chose to use this TPS65917-Q1 in other safety-critical systems including systems with safety goal higher than ASIL-B if the system analysis is done which may require ASIL decomposition, external monitoring, fault metric calculations, and more.

## 6.1 TPS65917-Q1 Supplying a Typical ADAS Processor

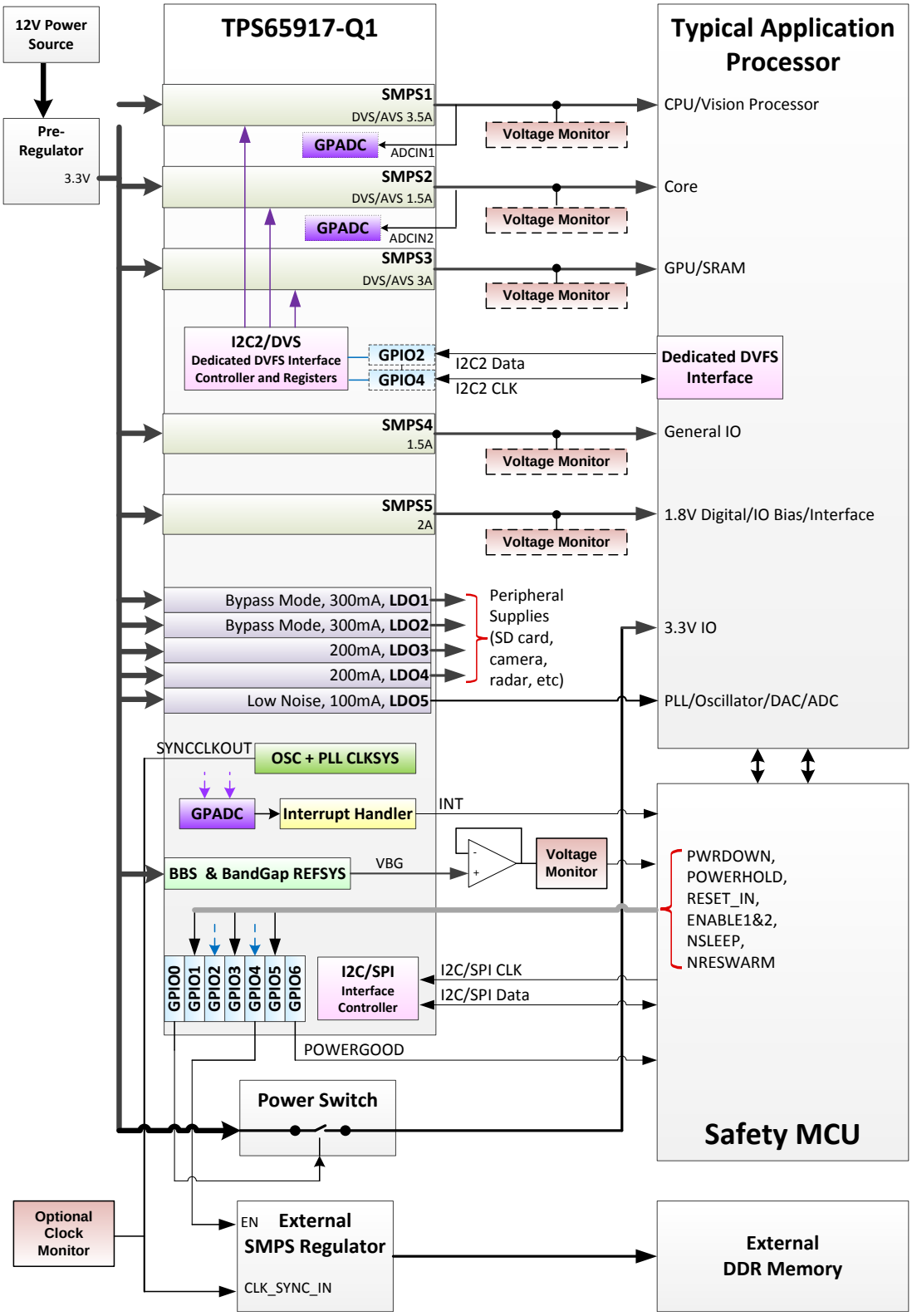



**Figure 10. Applications Diagram for TPS65917-Q1 Supplying a Typical ADAS Processor**

To achieve a target safety goal of ASIL-B in this system the following settings and external components were used in this safety analysis:

- The Safety MCU is supplied independently from the TPS65917-Q1 device
- Every LDO and SMPS rail that is supplying a safety-critical component in the system are looped back to and monitored by channel 1 or 2 of the GPADC, or connected to an external voltage monitor. If a dual-phase configuration of the device is used, SMPS12 is also monitored by the GPADC or and external voltage monitor.
- Load current monitoring and POWERGOOD indicators are enabled for SMPS1-5
- Short circuit detection is enabled for LDO5
- Vref is measured at the VBG output pin with a voltage follower circuit and an external voltage monitor
- The CRC self-check is programmed to execute error detection and if an error is detected, stop power up sequence altogether.
- When a failure is detected in the bandgap (including loss of voltage, undervoltage, and over-voltage) through an external voltage monitor circuitry, the Safety MCU of this ADAS system will force the PMIC to the safe shut down state.
- The Safety MCU of this ADAS system is capable of handling errors reported by the interrupt handler of the PMIC.
- Errors of the GPADC can be detected with a startup procedure by setting one of the non-critical SMPS at several voltages and comparing the output with the values given by the GPADC to the set values. This can provide latent coverage for GPADC failures.
- Mechanisms are implemented in the safety system to ensure the data integrity of the $I^2C$/SPI communication channels
- The software must acknowledge successful powerup events through the powerhold pin

## 6.2 Example System Fault Analysis

This section provides an example of several different types of failures that could happen in the system and is not considered to be a complete analysis. This analysis is highly dependent on each specific system implementation. Please refer to the Failure Mode and Effects Diagnostic Analysis (FMEDA) when performing this analysis for more information on how to claim coverage with this device.

### 6.2.1 Fault 1 - VSYS 3.3-V Supply from Preregulator Shorted to Ground or Open

Impact of the fault:

- Affects the entire PMIC and any device or system that receives power from it

Fault Detection/Prevention:

- VSYS supply dropping below the VSYS_MON threshold (programmable) will cause an interrupt to the MCU
- VSYS_LO Detection will cause the PMIC to power down

### 6.2.2 Fault 2 - Bandgap REFSYS Voltage Too High or Too Low

Impact of the fault:

- Affects the entire PMIC and any device or system that receives power from it

Fault Detection/Prevention:

- External voltage monitor will detect and signal the Safety MCU to place the system into a safe state

### 6.2.3 Fault 3 - PLL Synchronization Fails / Loss Of External Clock

Impact of the fault:

- Affects the SMPS outputs of the PMIC and any device or system that receives power from them

Fault Detection/Prevention:

- M Loss of the external clock will cause the PMIC to automatically default to using the 2.2 MHz free run clock for SMPS switching

### 6.2.4 Fault 4 - I²C / SPI Short or Open

Impact of the fault:

- Affects the ability of the Safety MCU to communicate with the PMIC

Fault Detection/Prevention:

- I²C / SPI startup and shutdown communication test will detect error
- Watchdog Timer interrupt will not be acknowledged and PMIC will be put into safe state

### 6.2.5 Fault 5 - SMPS Outputs Short

Impact of the fault:

- Affects the devices connected to the SMPS output

Fault Detection/Prevention:

- Undervoltage detection via the POWERGOOD pin or an external voltage monitor if greater accuracy is required
- Over-voltage condition can be clamped externally or detected by an external over-voltage monitor
- Over-voltage conditions of 2 safety critical channels can also be monitored by Channel 0 and 1 of the GPADC. When a threshold is crossed, a device/platform shutdown can be generated by enabling the SHUTDOWN bits in the GPADC_AUTO_CTRL register, as described in section Section 5.7 If a system nuisance shutdown is not desired, GPADC can also be configured to report threshold violations only via the INT pin
- Over-current/Short detection mechanism of each SMPS will shut down the corresponding rail and send an interrupt to the Safety MCU. The incident will be recorded in the SMPS_SHORT_STATUS register

### 6.2.6 Fault 6 - LDO Outputs Short

Impact of the fault:

- Affects the devices connected to the LDO output

Fault Detection/Prevention:

- If the output of the LDO is connected to a safety critical rail, an external voltage monitor may be used to trigger an over-voltage or an undervoltage detection
- Over-current/Short detection mechanism of each LDO will shut down the corresponding rail and send an interrupt to the Safety MCU. The incident will be recorded in the LDO_SHORT_STATUSx register

# Revision History

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

**Changes from D Revision (March 2017) to E Revision** **Page**

- Updated POWERGOOD Block Diagram and added Dual Phase Operation Note ..... 19
- Added requirement for dual-phase device configurations to use external monitor on SMPS12 ..... 23

**Changes from C Revision (March 2015) to D Revision** **Page**

- First public release of document ..... 3

**Changes from B Revision (May 2015) to C Revision** **Page**

- Added input voltage monitoring and separate GPIO IO buffers to the Architecture Safety Mechanisms list..... 15
- Added text about setting of WTB bit if an OFF request occurs due to watchdog timeout to the *Watchdog Timer* section 17
- Added the *Input Voltage Monitoring of SMPS While in ECO-mode* section ..... 21
- Added GPADC error detection text to the settings and external components list for safety analysis in the *TPS65917-Q1 Supplying a Typical ADAS Processor* section ..... 24
- Added software acknowledge text to the settings and external components list for safety analysis in the *TPS65917-Q1 Supplying a Typical ADAS Processor* section ..... 24

**Changes from A Revision (April 2015) to B Revision** **Page**

- Added comments under the Product Safety Constraints section to link the layout constraint to the Layout guideline section of the datasheet ..... 7
- Added additional assumption under the Product Safety Constraints section for independent power supply of the safety MCU ..... 7
- Added typical accuracy of the POWERGOOD comparators, and include recommendation for using the GPADC external channels or external voltage monitor if tighter accuracy is required. ..... 19
- Re-word the paragraph to list all assumptions in the Safety Fault Analysis in bullet format ..... 24

**Changes from Original (March 2015) to A Revision** **Page**

- Added timing limitation of current Watchdog Timer and suggesting for external solution if the safety critical system requires a more frequent monitoring. ..... 18
- Added GPADC as a secondary analog monitoring feature for SMPS outputs. ..... 20
- Added GPADC as alternative monitoring solution for detecting SMPS output overvoltage or undervoltage conditions. .. 25

## IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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, 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 (www.ti.com/legal/termsofsale.html) 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.

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