Technical White Paper

Designing a Power Supply for a Safety MCU to Meet Functional Safety ASIL B

Harvey Chen

ABSTRACT

Functional safety is important in automotive applications such as advanced driver assistance systems (ADAS), battery management systems (BMS), digital cockpits, and instrument clusters. Designers often wonder how to design power supplies for safety microcontrollers (MCU) to achieve Automotive Safety Integrity Level (ASIL) B.

This article describes a TI design leveraging two TI Functional Safety-Capable devices – the LM63625-Q1 buck converter combined with the TPS37A-Q1 supervisor – to meet random hardware fault metrics for ASIL B in digital cockpit and cluster applications. This method can also be scaled to other automotive applications.

TI Functional Safety-Capable devices are not developed according to the requirements of any functional safety standard. TI provides failure-in-time (FIT) rate and failure mode distribution information to customers to aid in the calculation of random hardware fault metrics. TI recommends integrating these components into a system through the strategy of “evaluation of hardware element” (International Organization for Standardization [ISO] 26262-8:2018, clause 13).

Table of Contents

List of Figures

List of Tables

1 Introduction

Safety MCUs are widely used in safety-critical automotive systems such as digital cockpits and instrument clusters. The MCU collects safety-relevant information from various electronic control units and sensors through a Controller Area Network (CAN). The device then executes the corresponding signal processing and fault detection to achieve the system functional safety requirements. Keeping the power supply within the recommended operating range of the safety MCU is essential to prevent the MCU from running into an unsafe state.

There are four classifications of ASILs in the ISO 26262 standard based on the inherent safety risk: ASIL A, ASIL B, ASIL C, and ASIL D, with ASIL D being the most stringent requirement. The target for digital cockpit and cluster applications is typically ASIL B.

2 Power Designs for Safety MCUs With Functional Safety Requirements

Suppose that a safety MCU needs a 3.3-V power rail. Figure 2-1 illustrates the typical power architecture.

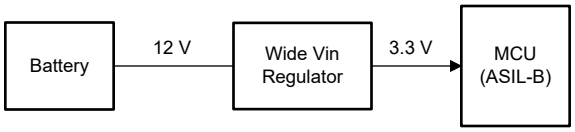

Figure 2-1. Typical Power Architecture for a Safety MCU

The 3.3-V power output needs to be monitored for faults such as supply undervoltage or overvoltage. If either occurs, the MCU is potentially operating in an unsafe state, so resetting the MCU to switch off and transitioning the system into a safe state is required.

Designers must consider how to design the power supply for a safety MCU to achieve the random hardware fault requirement for ASIL B at the system level. One recommended fix is to use an external supervisor to monitor the power-supply output. The supervisor is independent of the power-supply output, so there is no common-cause failure. Given the high performance and accuracy of the supervisor, the diagnostic coverage for power-supply over- and undervoltage is high.

Using the integrated PGOOD pin of a functional safety-capable regulator as the safety mechanism to monitor under- and overvoltage failures can be insufficient to meet ASIL B requirements. The PGOOD circuit is possibly not independent from the regulator circuit of the power supply, as the circuits potentially share the same internal band gap. If the band gap drifts out of specification, then PGOOD also fails and does not catch under- and overvoltage failures; this is known as a common-cause failure. The diagnostic coverage with PGOOD is possibly below 90%, which does not meet the single-point fault metric (SPFM) of ≥ 90% for ASIL B.

Figure 2-2 and Figure 2-3 depict reference designs targeting ASIL B using various supervisors.

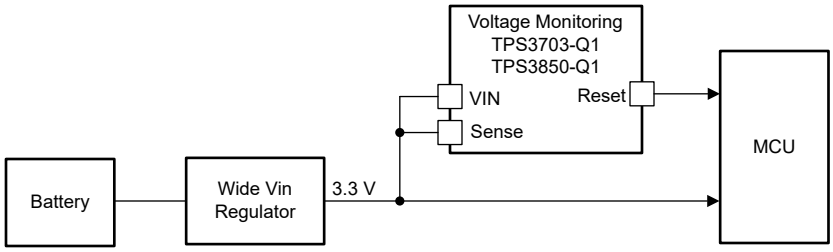

Figure 2-2. MCU Power-Supply Monitoring Using TPS3703-Q1 or TPS3850-Q1

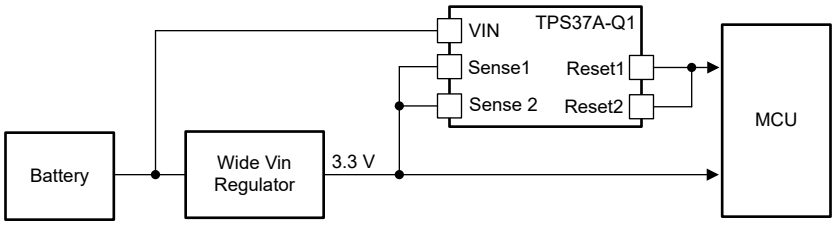

Figure 2-3. MCU Power-Supply Monitoring Using a Wide-V_{IN} Supervisor

In Figure 2-2, the TPS3703-Q1 is a window supervisor with a high-accuracy under- and overvoltage monitor. The TPS3850-Q1 is a window supervisor with an integrated window watchdog. Both devices support input voltages at the V_{IN} and SENSE pins of up to 6.5 V. If a regulator overvoltage fault results in more than 6.5 V_{OUT}, this overvoltage exceeds the absolute maximum voltage input range of the supervisor and renders the supervisor ineffective or damaged. However, usually this overvoltage also exceeds the maximum operating voltage of the MCU. The MCU has a gross malfunction or even damage. In a digital cockpit or instrument cluster, a damaged MCU results in a black screen, which is considered as a safe state.

If overvoltages above 6.5 V are a concern, then consider the TPS37A-Q1 instead. This device is a wide V_{IN} supervisor that supports voltages on the V_{IN} and SENSE pins of up to 65 V, so that V_{IN} can be directly connected to the battery. The supervisor monitors the power-supply output and resets the MCU into a safe state upon detection of an under- or overvoltage event.

3 ASIL B Power-Supply Design Example and FMEDA Analysis

The following example shows a power-supply design using the LM63625-Q1 wide-V_{IN} regulator and the TPS37A-Q1 supervisor to achieve ASIL B. This example is applicable to digital cockpits and instrument clusters, and is adaptable to other functional safety designs.

3.1 Functional Safety Requirements

Use the following functional safety requirements practices when designing with TI devices:

- Safety requirement: Design an ASIL B-compliant 3.3-V power supply for a safety MCU
- Safe state: Reset the safety MCU to a safe state upon detection of a power fault
- Fault-tolerant time interval: 500 ms
- Feature how to leverage TI's failure mode distribution (FMD) and pin failure mode analysis (FMA) data in the system's failure modes, effects, and diagnostic analysis (FMEDA)
- Prove that a TI Functional Safety-Capable regulator coupled with a supervisor meets ASIL B metrics through FMEDA analysis

3.2 Proposed Power Design

Figure 3-1 adopts the design shown in Figure 2-2, redrawing the diagram and including the part number for the regulator.

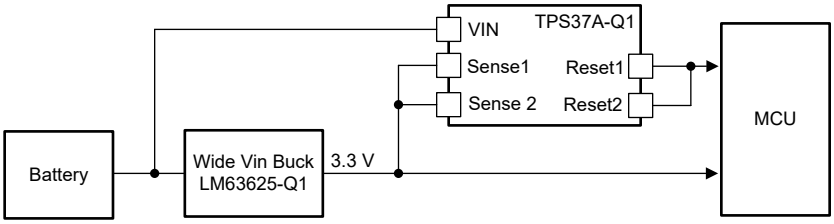

Figure 3-1. Power-Supply Design for an MCU to Meet ASIL B Criteria

The LM63625-Q1 is a 3.5-V to 36-V wide-V_{IN} buck converter; the power output is 3.3 V. The safety operating voltage of the MCU is from 3 V to 5 V. The TPS37A-Q1 monitors the 3.3-V power-supply output, and resets the safety MCU when the voltage is above 5 V or below 3 V. The TPS37A-Q1 therefore implements an over- and undervoltage detection safety mechanism (SM).

3.3 FMD and Pin FMA

TI products provide FIT rates derived from the reliability guides of Siemens (SN) 29500 or International Electrotechnical Commission (IEC) TR 62380. SN 29500 differs from IEC TR 62380 in accounting for failures caused by silicon and package interactions. SN29500 provides only a total FIT rate, while IEC TR 62380 distinguishes between die FIT rate and package FIT rate for analysis.

Functional safety standards recommend that semiconductor component manufacturers estimate failures caused by silicon interaction with package materials and silicon-to-package connection points (pins). For functional safety-capable devices such as pre-regulators, low-dropout regulators, and voltage supervisors, TI provides functional safety FIT rate, failure mode distribution, and pin FMA reports.

Using the LM63625-Q1 as a reference, Table 3-1 lists the failure modes and their respective distribution.

Table 3-1. Die Failure Modes and Distribution

Die Failure Modes	Failure Mode Distribution (%)
SW no output	35
SW output not in specification – voltage or timing	45
SW driver FET stuck on	10
$\overline{\text{RESET}}$ false trip or fails to trip	5
Short circuit any two pins	5

The die failure modes listed in Table 3-1 are described in the following list:

- *SW no output* means that there is no voltage output. The MCU is unpowered. This failure mode can be classified as a safe fault.
- *SW output not in specification – voltage or timing* means that the power-supply output is out of specification. The TPS37A-Q1 detects under- and overvoltage faults with an accuracy of ±1%, and resets the MCU into a safe state.
- *SW driver FET stuck on* can lead to a power output equal to V_{IN}. The TPS37A-Q1 detects this fault and outputs the reset signal to the MCU. In this example, the power output is not switched off to protect the MCU, so the MCU is potentially damaged resulting in a black screen in an instrument cluster, which is considered as a safe state. If a damaged MCU is a concern in more rigorous applications, an external metal-oxide semiconductor field-effect transistor (MOSFET) switch can switch off the power output to protect the MCU.
- The $\overline{\text{RESET}}$ output of LM63625-Q1 is not used in this example. Therefore the *$\overline{\text{RESET}}$ false trip or fails to trip* failure mode is considered not safety relevant.
- *Short circuit any two pins* is analyzed in the pin failure mode and effects analysis.

3.4 LM63625-Q1 and TPS37A-Q1 FMEDA Analysis at the Die Level

The calculations in the following sections are based on IEC TR 62380. The FMEDA tables list the die and package faults separately.

Table 3-2 shows the calculation of the single-point fault metric (SPFM) and latent fault metric (LFM) for the LM63625-Q1 and TPS37A-Q1 at the die level to prove that the design meets ASIL B criteria: SPFM ≥ 90% and LFM ≥ 60%, leaving any passive components needed for this circuitry out of consideration.

Table 3-2. LM63625-Q1 and TPS37A-Q1 FMEDA Analysis at the Die Level

					Single Point Fault				Latent Fault			
Component	**Failure Rate**	**Safety-related component to be considered in the calculation?**	**Failure Mode**	**Failure Mode Distribution**	**Failure mode that has the potential to violate the safety goal in absence of safety mechanisms**	**Safety mechanism allowing to prevent the failure mode from violating safety goal**	**Failure mode coverage with regard to violation of safety goal**	**Residual or Single-Point Fault Failure Rate**	**Failure mode that can lead to the violation of safety goal in combination with an independent failure of another component**	**Detection means? Safety mechanism allowing to prevent the failure mode from being latent?**	**Failure mode coverage with respect to latent failures**	**Latent multiple-point fault failure rate**
	FIT	**SR/NSR**		**%**	**V/NV**	**SM/NSM**	**%**	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**
LM63625-Q1	7.00	SR	SW no output	35%	NV			0.0000	NV			0.00
	7.00	SR	SW output not in specification - voltage or timing	45%	V	SM	99%	0.0315	V	SM	100%	0.00
	7.00	SR	SW driver FET suck on	10%	V	SM	99%	0.0070	V	SM	100%	0.00
	7.00	SR	RESET false trip or fails to trip	5%	NV			0.0000	NV			0.00
	7.00	SR	Short circuit any two pins	5%	V	SM	99%	0.0035	V	SM	100%	0.00
TPS37A-Q1	2.00	SR	RESET1/ fails to trip	8%	NV			0.0000	V	NSM	0%	0.16
	2.00	SR	RESET1/ false trip	8%	NV			0.0000	NV			0.00
	2.00	SR	RESET1/ trip outside specification (voltage or time)	31%	NV			0.0000	V	NSM	0%	0.62
	2.00	SR	RESET1/ delay outside specification	3%	NV			0.0000	NV			0.00
	2.00	SR	RESET2/ fails to trip	8%	NV			0.0000	V	NSM	0%	0.16
	2.00	SR	RESET2/ false trip	8%	NV			0.0000	NV			0.00
	2.00	SR	RESET2/ trip outside specification (voltage or time)	31%	NV			0.0000	V	NSM	0%	0.62
	2.00	SR	RESET2/ delay outside specification	3%	NV			0.0000	NV			0.00
	9.0000							0.0420				1.5600

Total failure rate (die): 9 FIT

Total residual and single-point failure rate: 0.042 FIT

Total latent fault: 1.56 FIT

SPFM = 1 – (0.042 / 9) = 99.5%

LFM = 1 – (1.56 / (9 – 0.042)) = 82.6%

$$\text{Single Point Fault Metric} = 1 - \frac{\sum(\lambda_{\mathbf{SPF}} + \lambda_{\mathbf{RF}})}{\sum(\lambda_{\mathbf{SR}})}$$

$$\text{Latent Fault Metric} = 1 - \frac{\sum(\lambda_{\mathbf{MPF,Latent}})}{\sum(\lambda_{\mathbf{SR}}) - \sum(\lambda_{\mathbf{SPF}} + \lambda_{\mathbf{RF}})}$$

3.5 LM63625-Q1 and TPS37A-Q1 FMEDA Analysis at the Pin Level

Table 3-2 shows the FMEDA analysis at the die level, while Table 3-3 and Table 3-4 detail the package (pin)-level analysis. Four failure modes are usually considered for each pin: pin open, pin short to GND, pin short to adjacent pin, and pin short to power supply. These four failure modes are evenly distributed, many TI products follow this empirical distribution. For the LM63625-Q1 and TPS37A-Q1 devices; however, the pin FMDs in Table 3-3 and Table 3-4 are adjusted based on the specific integrated circuit (IC) design and simulation results. The reason is that the *Pin short to V_{IN} fault* rate is very low, most likely resulting in a pin open failure mode in the LM63625-Q1 and TPS37A-Q1.

Table 3-3. LM63625-Q1 FMD at the Pin Level

Package FIT	5 FIT	
Pin numbers	12	
FIT for each pin	5 / 12 = 0.417 FIT	
Failure mode for each pin	**Distribution**	**FIT for each failure mode**
Pin open	70%	0.417 × 70% = 0.292 FIT
Pin short to GND	15%	0.417 × 15% = 0.063 FIT
Pin short to adjacent pin	15%	0.417 × 15% = 0.063 FIT

Table 3-4. TPS37A-Q1 FMD at the Pin Level

Package FIT	3 FIT	
Pin numbers	10	
FIT for each pin	3 / 10 = 0.3 FIT	
Failure mode for each pin	**Distribution**	**FIT for each failure mode**
Pin open	70%	0.3 × 70% = 0.21 FIT
Pin short to GND	15%	0.3 × 15% = 0.045 FIT
Pin short to adjacent pin	15%	0.3 × 15% = 0.045 FIT

Table 3-5 and Table 3-6 show the FMEDA of the LM63625-Q1 and TPS37A-Q1, respectively, at the pin level.

Table 3-5. LM63625-Q1 FMEDA Analysis at the Pin Level

					Single Point Fault				Latent Fault			
Pin Name	**Failure Mode**	**Effect of failure mode**	**Safety-related element to be considered in the calculations**	**Failure Rate**	**Failure mode that has the potential to violate the safety goal in absence of safety mechanisms**	**Safety mechanism allowing to prevent the failure mode from violating safety goal**	**Failure mode coverage with regard to violation of safety goal**	**Residual or single-point failure rate**	**Failure mode that can lead to the violation of safety goal in combination with an independent failure of another component**	**Detection means? Safety mechanism allowing to prevent the failure mode from being latent?**	**Failure mode coverage with respect to latent failures**	**Latent multiple-point fault failure rate**
			SR/NSR	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**
SW	Pin open	No voltage output	SR	0.292	NV			0.0000	NV			0.000
	Short to ground	No voltage output	SR	0.063	NV			0.0000	NV			0.000
	Short to BOOT	No voltage output	SR	0.063	NV			0.0000	NV			0.000
BOOT	Pin open	Loss of output regulation, low or no voltage output	SR	0.292	V	SM	99%	0.0029	NV			0.000
	Short to ground	No voltage output	SR	0.063	NV			0.0000	NV			0.000
	Short to VCC	Loss of output regulation, low or no voltage output	SR	0.063	V	SM	99%	0.0006	NV			0.000
VCC	Pin open	No voltage output	SR	0.292	NV			0.0000	NV			0.000
	Short to ground	No voltage output	SR	0.063	NV			0.0000	NV			0.000
	Short to RT	In this example, VCC shorts to GND, no voltage output	SR	0.063	NV			0.0000	NV			0.000
RT	Pin open	Switching frequency drops to zero, no voltage output	SR	0.292	NV			0.0000	NV			0.000
	Short to ground	No effect	NSR	0.063	NV			0.0000	NV			0.000
	Short to VSEL	No effect	NSR	0.063	NV			0.0000	NV			0.000
VSEL	Pin open	Incorrect output voltage	SR	0.292	V	SM	99%	0.0029	NV			0.000
	Short to ground	No effect	NSR	0.063	NV			0.0000	NV			0.000
	Short to SYNC/MODE	No effect	NSR	0.063	NV			0.0000	NV			0.000
SYNC/ MODE	Pin open	Internal pull-down place device in AUTO mode, no effect	NSR	0.292	NV			0.0000	NV			0.000
	Short to ground	No effect	NSR	0.125	NV			0.0000	NV			0.000

Table 3-5. LM63625-Q1 FMEDA Analysis at the Pin Level (continued)

					Single Point Fault				Latent Fault			
Pin Name	**Failure Mode**	**Effect of failure mode**	**Safety-related element to be considered in the calculations**	**Failure Rate**	**Failure mode that has the potential to violate the safety goal in absence of safety mechanisms**	**Safety mechanism allowing to prevent the failure mode from violating safety goal**	**Failure mode coverage with regard to violation of safety goal**	**Residual or single-point failure rate**	**Failure mode that can lead to the violation of safety goal in combination with an independent failure of another component**	**Detection means? Safety mechanism allowing to prevent the failure mode from being latent?**	**Failure mode coverage with respect to latent failures**	**Latent multiple-point fault failure rate**
			SR/NSR	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**
$\overline{\text{RESET}}$	Pin open	No effect	NSR	0.292	NV			0.0000	NV			0.000
	Short to ground	No effect	NSR	0.063	NV			0.0000	NV			0.000
	Short to FB	Output voltage incorrect or no output	SR	0.063	V	SM	99%	0.0006	NV			0.000
FB	Pin open	Output voltage can be out of specification	SR	0.292	V	SM	99%	0.0029	NV			0.000
	Short to ground	Regulator operates at maximum duty cycle. Output voltage rises to nearly V_{IN}	SR	0.063	V	SM	99%	0.0006	NV			0.000
	Short to AGND	Regulator operates at maximum duty cycle. Output voltage rises to nearly V_{IN}	SR	0.063	V	SM	99%	0.0006	NV			0.000
AGND	Pin open	No voltage output	SR	0.292	NV			0.0000	NV			0.000
	Short to ground	No effect	NSR	0.063	NV			0.0000	NV			0.000
	Short to EN	No voltage output	SR	0.063	NV			0.0000	NV			0.000
EN	Pin open	No voltage output	SR	0.292	NV			0.0000	NV			0.000
	Short to ground	No voltage output	SR	0.063	NV			0.0000	NV			0.000
	Short to NC	No effect	NSR	0.063	NV			0.0000	NV			0.000
NC	Pin open	No effect	NSR	0.292	NV			0.0000	NV			0.000
	Short to ground	No effect	NSR	0.063	NV			0.0000	NV			0.000
	Short to VIN	No effect	NSR	0.063	NV			0.0000	NV			0.000
V_{IN}	Pin open	No voltage output	SR	0.292	NV			0.0000	NV			0.000
	Short to ground	No voltage output	SR	0.125	NV			0.0000	NV			0.000
Total				5.000				0.0113				0.000

Table 3-6. TPS37A-Q1 FMEDA Analysis at the Pin Level

					Single Point Fault				Latent Fault			
Pin Name	**Failure Mode**	**Effect of failure mode**	**Safety-related element to be considered in the calculations**	**Failure Rate**	**Failure mode that has the potential to violate the safety goal in absence of safety mechanisms**	**Safety mechanism allowing to prevent the failure mode from violating safety goal**	**Failure mode coverage with regard to violation of safety goal**	**Residual or single-point failure rate**	**Failure mode that can lead to the violation of safety goal in combination with an independent failure of another component**	**Detection means? Safety mechanism allowing to prevent the failure mode from being latent?**	**Failure mode coverage with respect to latent failures**	**Latent multiple-point fault failure rate**
			SR/NSR	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**
VDD	Pin open	Device Unpowered, LOSS of OV/UV monitoring	SR	0.210	NV			0.0000	V	NSM	0%	0.210
	Short to ground	Device Unpowered, LOSS of OV/UV monitoring	SR	0.045	NV			0.0000	V	NSM	0%	0.045
	Short to SENSE1	3V3 short to VDD, OV detected	NSR	0.045	NV			0.0000	NV			0.000
SENSE1	Pin open	LOSS of OV monitoring	SR	0.210	NV			0.0000	V	NSM	0%	0.210
	Short to ground	LOSS of OV monitoring	SR	0.045	NV			0.0000	V	NSM	0%	0.045
	Short to SENSE2	No effect	NSR	0.045	NV			0.0000	NV			0.000
SENSE2	Pin open	LOSS of UV monitoring	SR	0.210	NV			0.0000	V	NSM	0%	0.210
	Short to ground	3V3 short to GND,UV detected	NSR	0.045	NV			0.0000	NV			0.000
	Short to RESET1	LOSS of UV monitoring	SR	0.045	NV			0.0000	V	NSM	0%	0.045
RESET1	Pin open	LOSS of OV monitoring	SR	0.210	NV			0.0000	V	NSM	0%	0.210
	Short to ground	RESET1 is LOW, which is safe state	NSR	0.045	NV			0.0000	NV			0.000
	Short to RESET2	No effect	NSR	0.045	NV			0.0000	NV			0.000
RESET2	Pin open	LOSS of UV monitoring	SR	0.210	NV			0.0000	V	NSM	0%	0.210
	Short to ground	RESET2 is LOW, which is safe state	NSR	0.090	NV			0.0000	NV			0.000
CTR1/MR	Pin open	No effect	NSR	0.210	NV			0.0000	NV			0.000
	Short to ground	RESET1 is LOW, which is safe state	NSR	0.045	NV			0.0000	NV			0.000
	Short to CTS1	Unreliable timing	SR	0.045	NV			0.0000	V	NSM	0%	0.045
CTS1	Pin open	No effect	NSR	0.210	NV			0.0000	NV			0.000
	Short to ground	RESET1 is LOW, which is safe state	NSR	0.045	NV			0.0000	NV			0.000
	Short to CTS2	Unreliable timing	SR	0.045	NV			0.0000	V	NSM	0%	0.045

Table 3-6. TPS37A-Q1 FMEDA Analysis at the Pin Level (continued)

					Single Point Fault				Latent Fault			
Pin Name	**Failure Mode**	**Effect of failure mode**	**Safety-related element to be considered in the calculations**	**Failure Rate**	**Failure mode that has the potential to violate the safety goal in absence of safety mechanisms**	**Safety mechanism allowing to prevent the failure mode from violating safety goal**	**Failure mode coverage with regard to violation of safety goal**	**Residual or single-point failure rate**	**Failure mode that can lead to the violation of safety goal in combination with an independent failure of another component**	**Detection means? Safety mechanism allowing to prevent the failure mode from being latent?**	**Failure mode coverage with respect to latent failures**	**Latent multiple-point fault failure rate**
			SR/NSR	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**	**V/NV**	**SM/NSM**	**%**	**FIT**
CTS2	Pin open	No effect	NSR	0.210	NV			0.0000	NV			0.000
	Short to ground	RESET2 is LOW, which is safe state	NSR	0.045	NV			0.0000	NV			0.000
	Short to CTR2/MR	Unreliable timing	SR	0.045	NV			0.0000	V	NSM	0%	0.045
CTR2/MR	Pin open	No effect	NSR	0.210	NV			0.0000	NV			0.000
	Short to ground	RESET2 is LOW, which is safe state	NSR	0.045	NV			0.0000	NV			0.000
	Short to GND	RESET2 is LOW, which is safe state	NSR	0.045	NV			0.0000	NV			0.000
GND	Pin open	Device Unpowered, LOSS of OV/UV monitoring	SR	0.210	NV			0.0000	V	NSM	0%	0.210
	Short to ground	No effect	NSR	0.090	NV			0.0000	NV			0.000
Total				3.00				0.00				1.53

3.6 Total FMEDA Analysis of the LM63625-Q1 and TPS37A-Q1

Adding the total FIT rate, residual or single-point faults, and latent faults of Table 3-2, Table 3-5, and Table 3-6 produces the overall FIT rate. From there, you can calculate the final SPFM = 99.55% and LFM = 81.74% for this design (Table 3-7), proving that a TI power-supply design with the LM63625-Q1 and TPS37A-Q1 meets ASIL B criteria.

Table 3-7. Total FMEDA Analysis for the LM63625-Q1 and TPS37A-Q1

		Die (LM63625)	Package (LM63625)	Die (TPS37A)	Package (TPS37A)	Overall
Total FIT	λ_S	7.0000	5.0000	2.0000	3.0000	17.0000
Residual and single point faults	λ_{SPF} and λ_{RF}	0.0420	0.0113	0.0000	0.0000	0.0533
Latent fault	$\lambda_{MPF,L}$	0.0000	0.0000	1.5600	1.5300	3.0900
Single point failure metric	SPFM	99.40%	99.77%	100.00%	100.00%	99.69%(1)
Latent failure metric	LFM	100.00%	100.00%	22.00%	49.00%	81.77%(2)

(1) SPFM = 1 – 0.0533 / 17 = 99.69%
(2) LFM = 1 – 3.09 / (17-0.0533) = 81.77%

4 Summary

Safety critical automotive applications must make sure that the system not only meets functional and performance requirements, but also functional safety standards. This article provides a TI design that adopts TI power ICs combined with supervisors to create high-performance and reliable ASIL-B-compliant products. This design can be scaled to end equipment such as ADAS, digital cockpit and cluster, and so forth.

5 Additional Resources

- Texas Instruments, *LM636xx-Q1 Functional Safety FIT Rate, FMD, and Pin FMA* Functional Safety Information
- Texas Instruments, *TPS37-Q1 and TPS38-Q1 Functional Safety FIT Rate, FMD and Pin FMA* Functional Safety Information

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

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