Using voltage supervisors for rail monitoring in functional safety applications

By Mathew Jacob
Applications Engineering

Introduction

Functional safety is a concept that requires any safety-related system to operate correctly or fail in a predictably safe way. It's a broad topic, with standards focused on electronics in automotive applications (International Organization for Standardization 26262) and industrial applications (International Electrotechnical Commission 61508).

The growing demand for advanced electronic systems in autonomous vehicles or collaborative robots is driving concerns around functional safety, which has lead engineers to seek a greater understanding of various failure modes and how to design fail-safe systems.

The focus of this article is specifically on voltage-rail monitoring for an automotive camera system. Voltage supervisors offer power, size and failure-in-time (FIT) rate advantages over other discrete solutions and can help engineers meet higher safety ratings in designs. Automotive camera systems or domain controllers typically require significant voltage-rail monitoring across the power architecture.

Voltage-rail system faults

Voltage-rail monitoring is part of every electronics system and ensures that critical components work within their recommended operating voltages. Voltage-rail faults can occur for many reasons, including internal failures in power supplies that lead to incorrect voltage regulation, passive failures that lead to short or open faults, or even an unexpected load current that causes a power rail to dip. Voltage supervisors monitor voltage rails for incorrect voltages and allow them to respond with an output that a safety system can use for diagnostics.

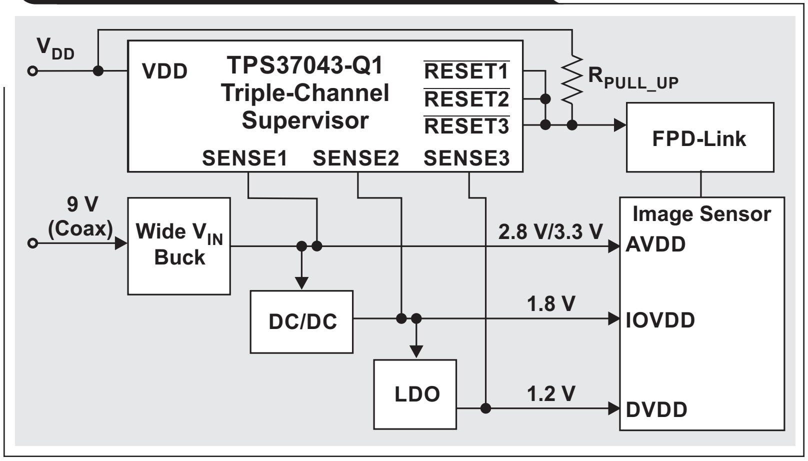
A common example of a point-of-load fault is a brownout at the microcontroller (MCU). A brownout happens when the voltage rail powering the MCU is lower than expected, which can cause an undefined state at the MCU. One common way to resolve an MCU brownout is to monitor the voltage rails going into the MCU for an undervoltage condition and provide a reset output to the MCU. The reset output turns off the MCU until the brownout is resolved.

Figure 1 is an example of a basic power architecture for an automotive camera system, featuring the TPS37043-Q1 voltage supervisor, which is a Functional Safety-Compliant device that can meet the ISO 26262 requirements and automotive safety integrity levels. The goal of the supervisor in this power architecture is to identify potential faults in the system and prevent any maloperation of the image sensor or camera system. Voltage-rail faults without coverage can lower the fault metrics rating, thus lowering overall system safety, whereas voltage-rail monitoring can help increase the fault metrics rating of any power architecture. This capability gives the system more information to enable a controlled decision-making process and avoid safety violations that can lead to hazards.

In Figure 1, safe operation means that the automotive camera in use works reliably all the time, every time without putting the user at risk of serious injury. There are two types of faults that can potentially happen: systemic and random faults. Adhering to proper design rules during the development of the parts used in the power architecture helps eliminate systemic faults; however, random faults are by definition random. No one knows if and when they will happen.

Now consider a failure example with a backup camera. If a random fault occurs in any of the parts of the power architecture and the display for the driver goes blank, the event is considered a perceptible failure; the driver can still look in the rearview mirror to back up safely. When using this camera in a lane-keeping assist function or obstacle detection scheme, however, the user isn't aware of a failure, which can lead to danger. The failure could have been triggered by one of the rails to the image sensor going lower than the absolute maximum or minimum of the image sensor, causing it to go into a hung state. The

Figure 1. An automotive-camera power architecture with supervision



job of the voltage supervisor in this case is to cause a reset of the image sensor if a hung state occurs so that the system reboots.

An obvious question is whether the time taken to reboot could in itself be considered a safety hazard? This is where the fault-tolerant time interval (FTTI) comes into play. This is the time that the system has to make a correction without putting the driver or others in danger. A reset time delay for the supervisor would be a design parameter chosen based on the FTTI. During system reset, the safe course of action would be to give a visual and audible alert to the driver as soon as the fault triggers. This alert would make the driver alert, and avoid imperceptible failures leading to a hazard.

The next question is what is the assurance that the voltage supervisor is working reliably all the time? This is where latent faults come into the picture. As an example, assume that the most critical rail that would trigger a direct maloperation is 1.2 V. What happens if the comparator (SENSE3) of the TPS3704 monitoring the 1.2-V rail is not working properly? There are four possible reasons the fault detection does not work (this is called failure-mode distribution):

- The threshold for overvoltage is too high.
- The threshold for undervoltage is too low.
- The comparators are not working at all.
- The comparators are working but the reset line is stuck high, so the fault cannot be communicated.

If the comparator goes into one of these failure modes, there is no indication in the system until the supervisor acts. This undetected supervisor fault could create a maloperation that if not caught within the FTTI, a driver could potentially be injured. Thus, the fault to the comparator is latent and lies dormant until it's time for the supervisor to act.

Applying a mechanism called built-in self-test (BIST) prevents the supervisor fault scenario. Ideally, a BIST should be automatic and run every time power is applied to the supervisor (key on). Figures 2 shows a manual self-test for an undervoltage fault and Figure 3 shows a manual check of over- and undervoltage trip points.

In Figure 2, SENSE4 overvoltage (V_{IT+}) is set at 5.5 V and undervoltage (V_{IT-}) is set at 2 V. V_{IT+} is the overvoltage trip point set and V_{IT-} is the undervoltage trip point set. It is possible to design the startup mechanism so that every time the ignition key is turned on, it triggers a manual undervoltage, which pulls SENSE4 below its undervoltage trip point and asserts RESET2 low. This process confirms that the undervoltage comparator and RESET logic are working properly. It is a low-coverage self-test scheme, since it is checking only one SENSE channel and is a pseudo-representation of the other channels.

Figure 3 shows a scheme that checks the over- and undervoltage trip points above or below their thresholds and implements the check on the SENSE channel that is the most critical for the operation of the automotive camera. In this scheme, LM10011 is used along with a voltage-identification (VID) interface. Different logic combinations of the VID interface change the internal DAC output current (I_{DAC_OUT}) of the LM10011 between three values: nominal, overvoltage test and undervoltage test. Equations 1, 2 and 3 show how the LM10011 can be used to trigger over and undervoltage faults.

$$V_{SENSEx} = \frac{1.2}{R1+R2} \times R2 - I_{DAC(nom)} \times R2 = 0.8 \quad (1)$$

where V_{SENSEx} is the sense voltage and 1.2 V is the monitored voltage.

Figure 2. Manual self-test for an undervoltage fault

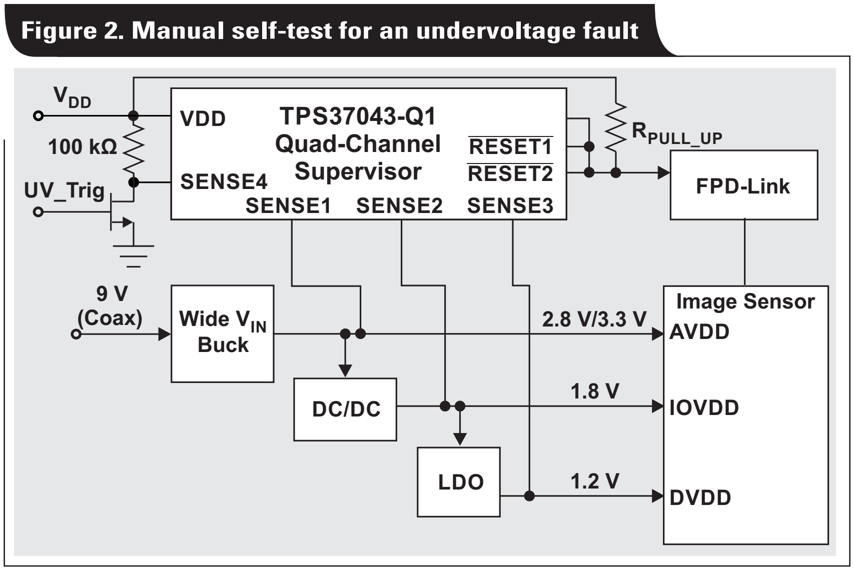


Figure 3. Manual check of over- and undervoltage trip points

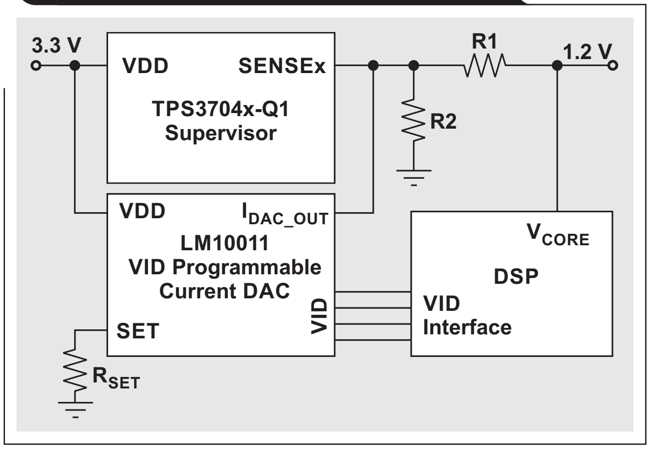
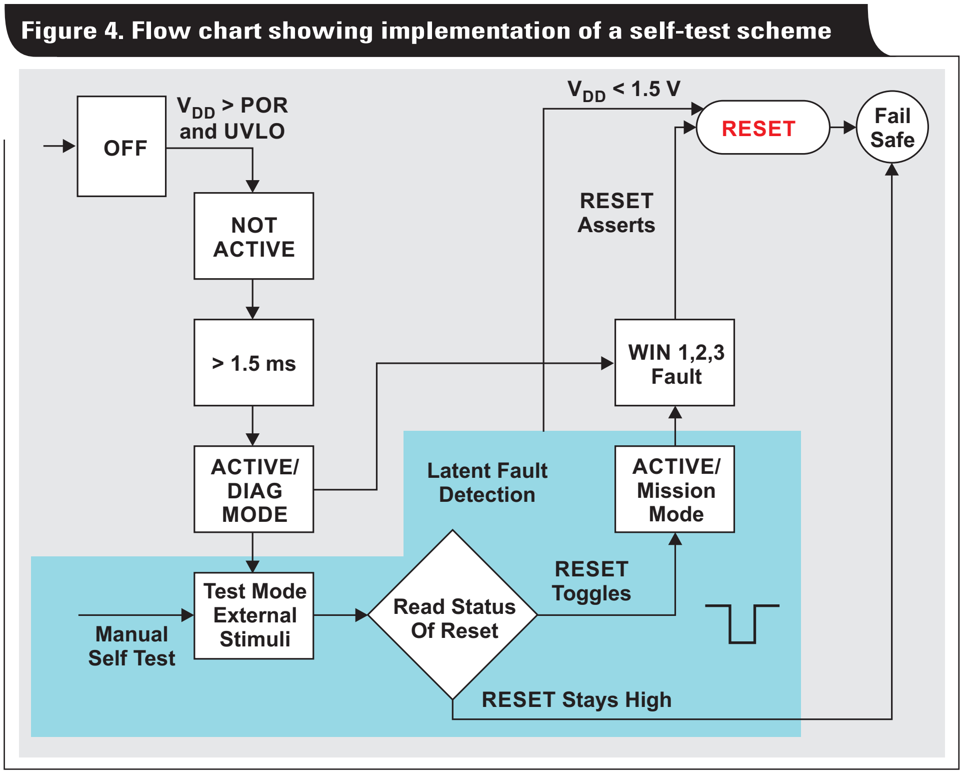


Figure 4. Flow chart showing implementation of a self-test scheme



Equation 1 shows that R1 and R2 are selected to get 0.8 V at the SENSEx pins for the nominal output voltage being checked.

Set Equation 2 values such that chosen overvoltage trip point of the 1.2-V rail is crossed when I_{DAC_OUT} is set for the overvoltage test.

$$I_{DAC(ovtest)} \quad R2 \tag{2}$$

Set Equation 3 values such that the chosen undervoltage trip point of 1.2-V rail is crossed when I_{DAC_OUT} is set for the undervoltage test:

$$I_{DAC(uvtest)} \quad R2 \tag{3}$$

where $I_{DAC(ovtest)} > I_{DAC(nom)} > I_{DAC(uvtest)}$.

Now consider the functional safety metrics that the implemented BIST scheme shown in Figure 3 directly affects. There are two key aspects that come into play when functional safety metrics are calculated: single point of failure diagnostic coverage and latent-fault diagnostic coverage. Since the window supervisor is used for diagnostic coverage for single-point failures scores high, the latent-fault diagnostic coverage jumps from 0% to 60% with a BIST scheme implemented. This helps reduce the latent fault FIT.

Various self-test methods can improve latent fault metrics to be sure that the supervisor is always on duty. To claim the self-test as a safety mechanism, the test needs to occur once every time at key on or a drive cycle or any time the function of the camera system is activated. The flow chart shown in Figure 4 illustrates the scheme. The goal would be to perform the self-test scheme before the system gets into its active or mission mode of operation. The shaded region in Figure 4 shows the additional blocks for the self-test scheme that make it possible to claim the increased latent fault metrics.

Conclusion

It is important to pick the right supervisor based on the application and once chosen, there are simple mechanisms that can be used to improve the latent fault metrics and avoid having failures of the power rails propagate into a hazard.

Related Web sites

Product information:
TPS3704x-Q1
LM10011

TI Worldwide Technical Support

TI Support

Thank you for your business. Find the answer to your support need or get in touch with our support center at

www.ti.com/support

China: http://www.ti.com.cn/guidedsupport/cn/docs/supporthome.tsp

Japan: http://www.tij.co.jp/guidedsupport/jp/docs/supporthome.tsp

Technical support forums

Search through millions of technical questions and answers at TI's E2E™ Community (engineer-to-engineer) at

e2e.ti.com

China: http://www.deyisupport.com/

Japan: http://e2e.ti.com/group/jp/

TI Training

From technology fundamentals to advanced implementation, we offer on-demand and live training to help bring your next-generation designs to life. Get started now at

training.ti.com

China: http://www.ti.com.cn/general/cn/docs/gencontent.tsp?contentId=71968

Japan: https://training.ti.com/jp

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.

A011617

Texas Instruments

SLYT814

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 (https: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