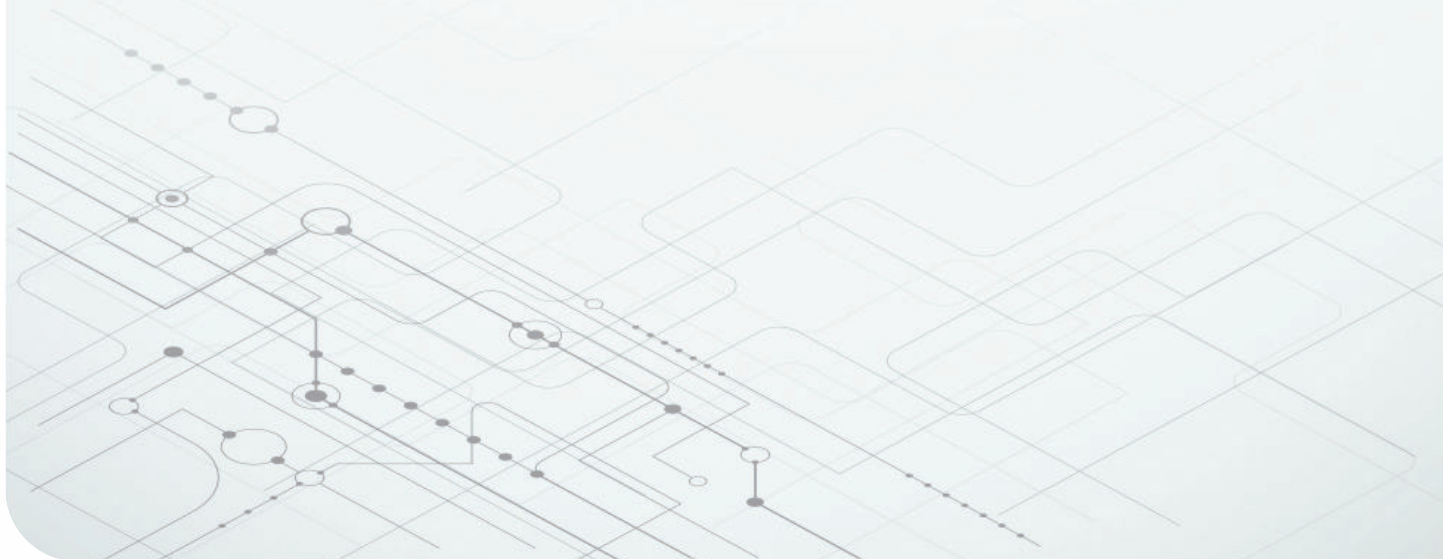


Integrating Voltage Monitoring for Safe Power Implementation in Industrial Stationary and Mobile Robots








Jackson Wightman
Applications Engineer
Voltage References and Supervisors

Kristen Mogensen
Systems Engineer
Robotics Systems



At a glance

-  **1 Safety considerations and potential failures in power-supply designs**
-  **2 Introduction to functional safety and standards in industrial systems**
-  **3 Voltage monitoring using voltage supervisor ICs**
-  **4 How voltage supervision affects functional safety ratings**
-  **5 Safe torque-off design example**

In this white paper, we'll explore how to design safe power supplies while adhering to International Electrotechnical Commission (IEC) 61508 standards. We will demonstrate power-supply monitoring design practices and why voltage supervision is essential for safe power up and smooth failure recovery. Voltage supervisor integrated circuit (IC) features such as built in self-test (BIST) and latch clear pins are new functions that, in addition to accurate voltage monitoring, can greatly improve functionally safe design practices.

Introduction

In modern manufacturing facilities, motor drives for industrial stationary and mobile robots can help increase factory output, efficiency and safety. But as employees in factories work alongside increasingly numerous (and increasingly powerful) automated robots, system designers must meet more strict safety requirements. Powering on and using standard or emerging technologies must be safe under any and all circumstances to enable true collaboration between employees and robots. Additionally, appropriately

powering off or making operating adjustments in the event of a failure is a primary element of safety. The safe power design for these robots or other electronics is essential to achieve system-level functional safety requirements.

Safety considerations and potential failures in power-supply designs

In a perfect world, a power supply will provide a constant voltage and current that never wavers or changes beyond the specific design requirements. But in the real world, that is not what happens. Not only do power supplies have inherent characteristics that introduce error, but they can also occasionally fail. These failures come in many forms. **Table 1** includes some examples of power-supply failures and their causes.

Power-supply failure effect	Cause
No output voltage	Failing power source
Power-supply voltage too high	Sudden change in load impedance, shorts to downstream
Power-supply voltage too low	Inadequate power supply, failing power source
Microcontroller (MCU) brownout	Inadequate power supply, failing power source

Table 1. Power-supply failures and their causes.

When designing devices and technologies that regularly operate around humans, you must take appropriate steps to mitigate the hazards of power-supply failures. This is true for a wide variety of applications, including industrial mobile robots, collaborative robots or any other technology where failures could be catastrophic. For example, in a motor-drive application, having a situation where the torque of the device is unpredictable could be incredibly dangerous and risky.

But how do you detect that a power supply has drifted out of its specifications? At what point do power-supply changes become a problem? And how is a potential fault communicated throughout the entire system for industrial applications?

Introduction to functional safety and standards in industrial systems

Defined functional safety standards help determine whether or not a system is safe. The most popular standards are IEC 61508 and International Organization for Standardization (ISO) 13849. Both standards look at the failure mode diagnostic coverage or safe failure fraction, as well as the hardware fault tolerance, to determine the safety integrity level (SIL) or performance level (PL) that a system meets. Table 2 summarizes these ratings.

Hardware fault tolerance (HFT)				Category				
IEC 61508				ISO 13849				
0	1	2	SFF	DC	1	2	3	4
-	SIL1	SIL2	<60%	None				
SIL1	SIL2	SIL3	60% to <90%	Low	c	c	d	
SIL2	SIL3	SIL4	90% to <99%	Medium		d	e	
	SIL4	SIL4	≤99%	High				e
Type B								

Table 2. IEC 61508 vs. ISO 13849 safety standards.

Using Table 2 as a guide, you can see that there are multiple ways to obtain each IEC 61508 SIL or ISO 13849 PL. By designing a system with the appropriate safe failure fraction or diagnostic coverage and hardware fault tolerance, you can reach one of these levels. In particular, monitoring the voltage of your power supply can increase your diagnostic coverage. The implementation of voltage monitoring can also increase your hardware fault tolerance.

Table 3 provides more information on each of these safety parameters.

As you can see, you must account for not just the number of failures possible but the likelihood of failures occurring. You can also see that by increasing your diagnostic coverage or safe failure fraction, you can move up in SIL or PL without changing your hardware fault tolerance, and vice versa. Voltage monitoring is an essential aspect of determining the diagnostic coverage or safe failure fraction of your system and reducing your residual FIT of the system solution.

Measurement	Definition
Hardware fault tolerance	Minimum number of tolerable failures for a system while also retaining safety functionality
Safe failure fraction	$\frac{\text{Total safe failures} + \text{Total detected dangerous failures}}{\text{Total safe failures} + \text{Total detected dangerous failures} + \text{Total undetected dangerous failures}} \quad (1)$
Diagnostic coverage	$\frac{\text{Total detected dangerous failures}}{\text{Total detected dangerous failures} + \text{Total undetected dangerous failures}} \quad (2)$
SIL	Functional safety rating system

Table 3. Important functional safety rating terms.

Voltage monitoring using voltage supervisor ICs

There are many methods for monitoring the voltage. Additionally, which voltage you are choosing to monitor can also vary. In any industrial application, you may need to monitor voltages as high as 48V or as low as 0.8V for overvoltage or undervoltage conditions. Thankfully, there are effective methods to monitor important voltage rails in your system that can enable a few aspects of any functionally safe design. With accurate voltage supervision, you'll know when to completely shut off a system, reset an MCU, or make another system-level choice to achieve the safe state. Without constant monitoring of the safety related voltage rails, the system cannot take action in the event of potentially dangerous situation.

There are ways to design a voltage monitoring circuit using discrete components, but in a functional safety-focused system, it becomes much easier to determine the diagnostic coverage if the voltage monitoring functionality is integrated into one sub-system circuit. That is why voltage supervisor ICs are especially helpful for functional safety – they include different combinations of threshold accuracy, quiescent current, reset time delay, latching capability, voltage hysteresis, output type and BIST.

Table 4 lists some voltage supervisor parameters and features.

Parameter or feature	Description
Threshold accuracy	The accuracy percentage around the nominal threshold voltage.
Maximum input voltage	The maximum voltage that the device can monitor.
Quiescent current	The amount of current the device consumes while idle.
Reset time delay	The amount of time it takes for the device to release from a fault condition once there is no longer a fault.
Voltage hysteresis	The difference between the threshold and the deasserting threshold. This parameter helps prevent false deassertion if the monitored voltage is oscillating.
Output topology	The output pin of the voltage supervisor (open drain or push pull) with either an active-low or active-high format.
Latch	Once a fault occurs, the pin indicating the fault remains asserted until the supervisor IC receives a signal to clear the logic.
BIST	Internal device diagnostics to check for internal faults.

Table 4. Important voltage supervisor parameters.

Voltage supervisor ICs monitor a voltage; once that voltage enters an undervoltage or overvoltage state, the voltage supervisor can notify an MCU, flip a power switch or drive a gate. A voltage supervisor can detect that a power supply has changed and quickly disconnect the power supply safely and effectively. Supervisors that monitor both undervoltage and overvoltage are also called window supervisors. Which type of voltage monitoring you are doing also affects the functional safety rating.

Table 5 lists these ratings.

Voltage monitoring type	Potential diagnostic coverage or safe failure fraction
Overvoltage	60%
Window (Overvoltage and Undervoltage)	90% to 99%

Table 5. How voltage monitoring affects DC.

When designing your safety circuit, is important to consider the level of diagnostic coverage. Additionally, using a voltage supervisor IC can decrease the number of necessary circuit components, allowing for a simpler design.

How voltage supervision affects functional safety ratings

When designing for a target SIL or PL, it is important to consider the hardware fault tolerance or safe failure fraction, which refers to the redundancy of your design as well has how you’ve implemented voltage monitoring into your system. The two most common standards define a few different ways to establish or increase your functional safety rating. Voltage monitoring is an essential part of making this determination or increasing functional safety. See Figure 1 and Figure 2, which illustrate a SIL 2-capable design using a voltage monitor.

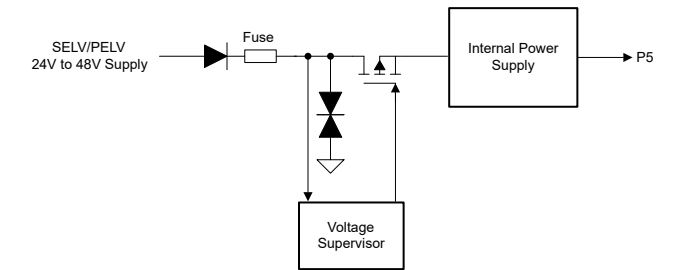


Figure 1. IEC 61800-5-2 implementation of a high-side safe power supply showing power supply and voltage monitoring.

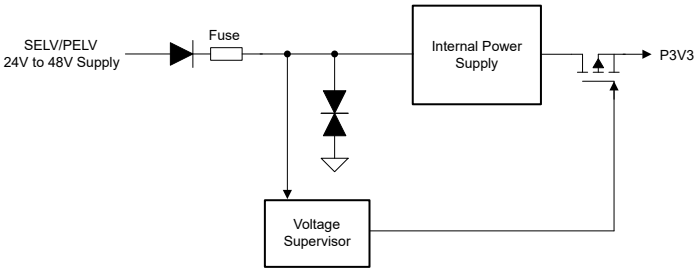


Figure 2. Another option for the IEC 61800-5-2 implementation would be a low-side safe power supply showing power supply and voltage monitoring.

In the Figure 2, the voltage supervisor serves as one single channel that can monitor overvoltage and undervoltage, if that is also of interest. The output of the voltage supervisor can disconnect a power supply that is outside the safe range of operation, or notify the MCU of a fault condition. The circuits in Figure 1 and Figure 2 has a hardware fault tolerance of 0 and can provide a safe failure fraction or diagnostic coverage of up to 90%. For this reason, Figure 1 are capable of providing up to a SIL 2 or PL d rating.

Using this same logic, increasing the hardware fault tolerance of your circuit configuration would increase the level of functional safety. Figure 3 shows an example of how you would increase the hardware fault tolerance of a circuit configuration while using voltage monitoring.

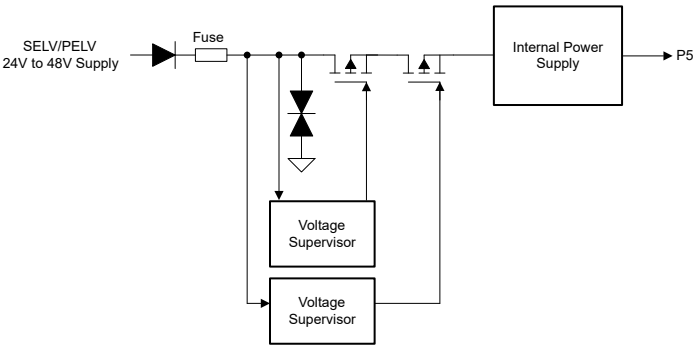


Figure 3. Block diagram for an SIL 3-capable power supply using voltage monitoring.

Using two voltage supervisors in parallel provides two channels for monitoring overvoltage or undervoltage conditions. Because these voltage monitors are each linked to their own method of disconnecting the power rail from the rest of the system, if one voltage supervisor

fails, the other will still be able to correctly and safely take the prescribed steps if the supply voltage moves out of specifications, enabling your design to achieve a rating as high as SIL 3.

Another method of improving the functional safety of a circuit configuration, such as the one shown in [Figure 3](#), is by using diversity in voltage supervisor implementation methods. Consider the instance of a common cause failure, as described in IEC61508 standards, between voltage supervisor devices. If two different voltage supervisor technologies are used to monitor the same supply rail, this would reduce the probability of a failure that is common mode.

For example, selecting two voltage supervisors with different voltage threshold values could provide increased diversity. For another example, in a circuit configuration such as the one shown in [Figure 3](#), using the TPS3762 from TI for one of the voltage supervisor functionality blocks and TPS37 from TI for the other would also provide additional functional diversity. This is because they are two different devices with two different designs.

One question you may ask at this point is what you should do if your voltage monitoring method fails, or if the components that make up the voltage monitoring circuitry cease to function properly. This is another instance where a voltage supervisor IC is especially helpful. Some voltage supervisor ICs include BIST functionality. These supervisors are window voltage monitors that also have an input pin where a user can request that the device test its own functionality. Upon request, the voltage monitor will perform internal tests and provide a signal to show that it is still operating as expected.

[Figure 4](#) shows such an implementation.

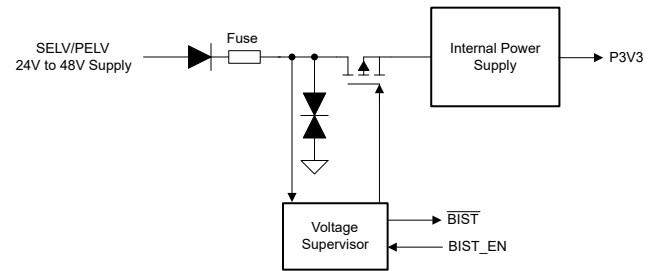


Figure 4. Voltage monitoring using a voltage supervisor IC with BIST features.

Providing diagnostic coverage of the voltage monitoring methods themselves, in this case being done by a voltage supervisor IC with a BIST feature, can increase the diagnostic coverage of your system to as much as 99%, which is a very high level of coverage. This high diagnostic coverage can enable your system to reach SIL 3 or PL e levels of functional safety when implemented in circuits with the appropriate hardware fault tolerance. An example of a device that has such integrated functionality is the TPS3762 from TI.

Another benefit of using a voltage monitoring device is that they can monitor high voltages. The TPS3762, for example, can monitor up to 65V, which enables it and similar devices with a wide input voltage range to connect directly to power rails and provide monitoring and other diagnostics. For example, some designs need extra low voltage (ELV) which is a defined voltage range in the standard IEC 60449-1. Now ELV definition has been reused to also define a SELV definition in the IEC 62368 standard where some electrical energy source levels do not allow higher than a certain voltage on the output of the power supply. For example, the electrical energy source level ES1 does not allow higher than 60V on the output of the power supply.

With this in mind, for safety extra low voltage power supplies, a safe maximum voltage level is set at 60V_{DC} maximum, and a safe power supply can only exceed this amount for a very short period before it does not meet safety extra low voltage standards. 60V_{DC} is a very common maximum voltage for safety standards, including safety extra low voltage and protective extra

low voltage. For this reason, wide input voltage devices such the TPS3762 have a maximum input voltage that can be monitored to 65V.

Safe torque-off design example

Motor-drive stages are essential for many industrial processes, and they are used in many environments where safety is of utmost importance. Many robots use motors as they work side by side with humans. In a motor-drive application, it is absolutely essential to take appropriate actions to shut down the system in the event of a potentially dangerous state. Circumstances such as

those listed in [Table 1](#) can lead to sudden dangerous motor operation.

One important aspect of safe motor drives is implementing a safe torque-off circuit. Every motor drive has a power stage that consists of gate drivers and potentially isolation in addition to a power-stage circuit. Using a voltage supervisor IC to monitor the power-supply rails for the gate drivers and power stage is extremely beneficial to determining the functional safety rating of your system. [Figure 5](#) is an example of a SIL 2- or PL d-rated safe torque-off system block diagram.

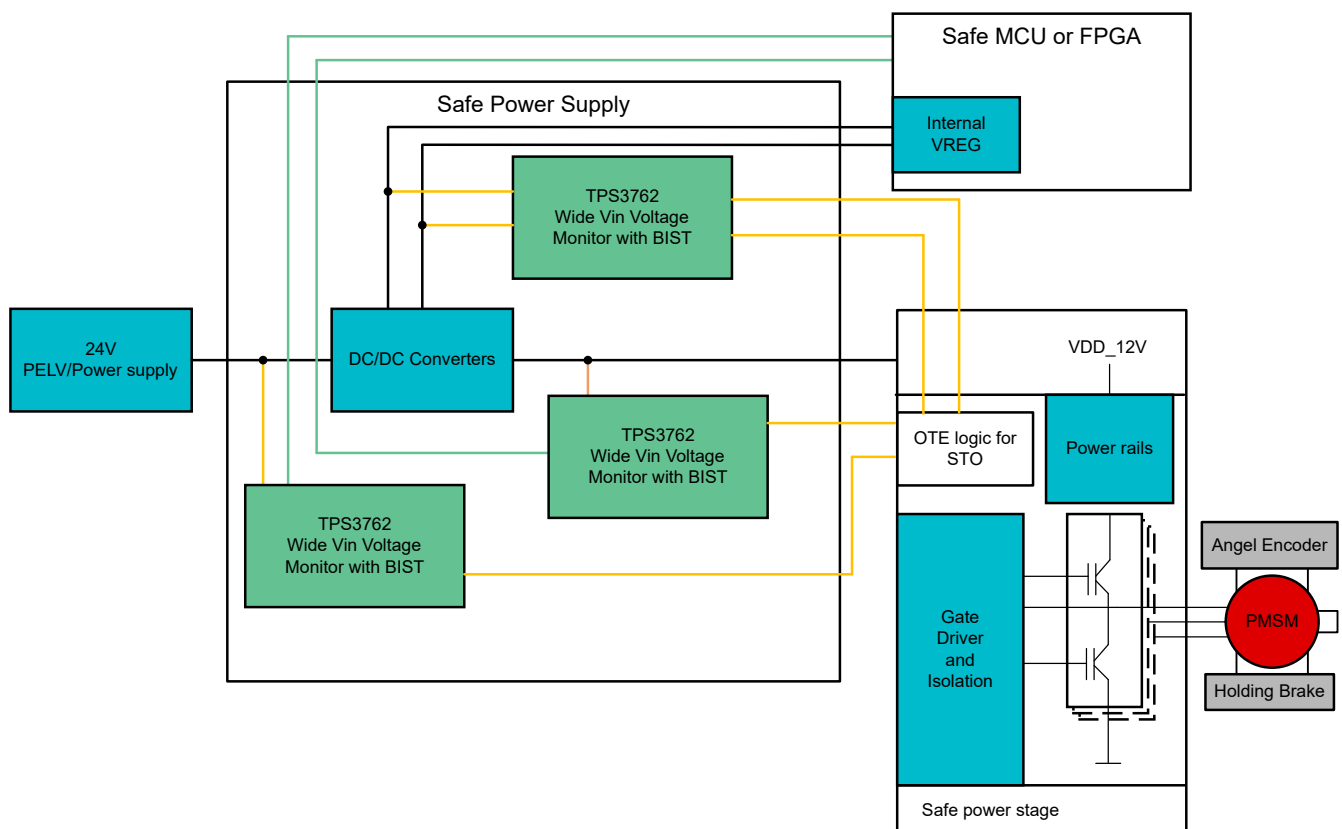


Figure 5. SIL 2- or PL d-rated safe torque-off system block diagram.

In **Figure 5**, there are a few instances of voltage monitoring: the 24V power supply and the various isolated inputs used in the power stage for an MCU or field-programmable gate array. These voltage monitoring schemes have a hardware fault tolerance of zero. But because of the high diagnostic coverage offered by the window voltage monitoring of the TPS3762 and its BIST feature, you can still obtain a SIL 2- or PL d-rated system.

Conclusion

As we become more advanced technologically, we must become more strategic about how such advances affect human lives. Safety is essential as we learn to effectively use new advances in machinery, robotics and electronics. Increasing the functional safety of any power-supply design will ultimately lead to more impressive and potent motor-drive applications. Thanks to advanced chips such as voltage supervisors, designers can safely determine when a system might see a safety fault and take the proper steps to ensure safety.

Functional safety will become increasingly important in the coming years. Using voltage monitoring to understand and improve the functional safety of any application can lead to a safer world.

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.

All trademarks are the property of their respective owners.

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
Copyright © 2024, Texas Instruments Incorporated