TECHNICAL ARTICLE

Improving Industrial Functional Safety Compliance with High Performance Supervisory Circuits: Using SIL-Rated Components—Part 2

Bryan Angelo Borres, Product Applications Senior Engineer

Abstract

Diagnostic functions, such as power supply monitors, play a crucial role in identifying hazardous failures in electronic, electrical, and programmable electronic safety-related systems (SRS). While such components are not mandatory to be functional safety rated for compliance with IEC 61508 under the current revision, utilizing a functional safety-compliant part when designing an SRS offers several advantages. For this reason, this second part of the series discusses six benefits of using a SIL-rated power supply monitor when designing a system covering industrial functional safety.

Introduction

This is the second article of the series discussing industrial functional safety compliance through high performance voltage supervisory circuits is discussed. This article explores the significance of employing functional safety-compliant diagnostic functions for compliance. It will cover six key aspects: availability of failure mode, effects, and diagnostics analysis (FMEDA) information; integrated safety features; on-chip diagnostics; future-proofing against the upcoming revision of the IEC 61508; consideration of other standards; and the views of external assessors, all underscoring the benefits of using SIL-rated power supply monitors such as the MAX42500.

The Basic Functional Safety Standard and Beyond

Part 1 of this series highlighted the role of diagnostics in meeting both the qualitative and quantitative demands of the basic functional safety standard as seen in Figure 1. For qualitative considerations, the implementation of power supply monitors is mandatory regardless of the safety integrity level (SIL). But for quantitative requirements, there are two main considerations: reliability predictions and architectural constraints. Reliability predictions assess the system's average probability of dangerous failure rate, which can either be the average probability of dangerous failure on demand (PFDavg) for low demand operation

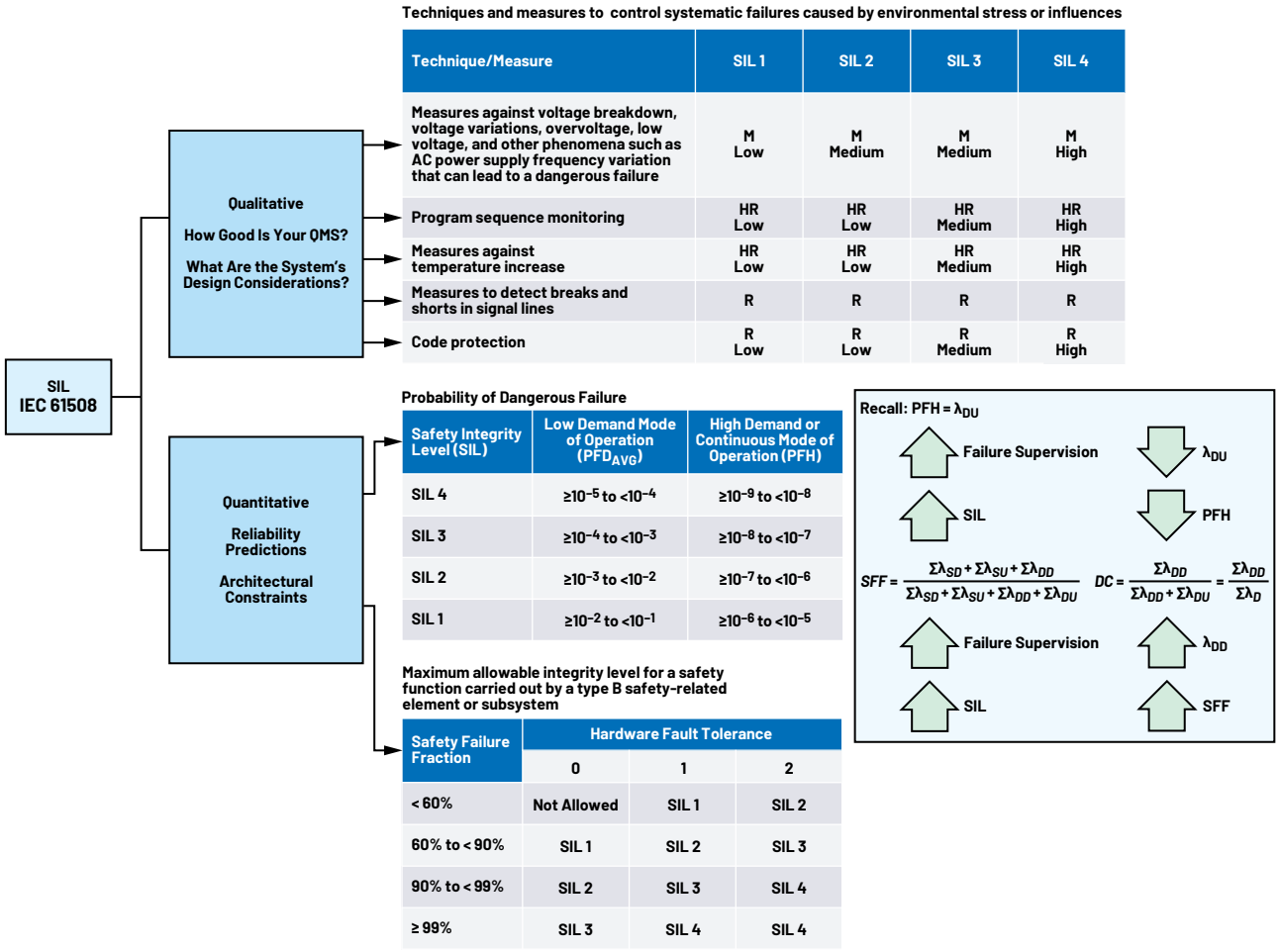


Figure 1. Diagnostics through the lens of IEC 61508:2010.[1]

or the average frequency of dangerous failure per hour (PFH) for high demand operation. For the purpose of discussion, PFH is used. Meanwhile, architectural constraints are affected by the safe failure fraction (SFF) and redundancy requirements. The integration of diagnostic functions enhances these metrics by identifying random hardware failures. Consequently, any supervisory IC that meets the required specifications can be used, as SIL ratings are determined at the system level.

Implementing a safety project often requires more effort compared to a nonsafety project due to the stringent demands of the safety lifecycle. However, there are effective strategies that can enhance both the project timeline and functional safety compliance. One such strategy is the use of components that have already been developed according to the IEC 61508. Although not mandatory under IEC 61508, this approach offers several advantages that exceed the basic functional safety standard requirements. These advantages include the following.

It Has Its Own FMEDA

Power supply monitors that adhere to IEC 61508 standards include a safety manual detailing their FMEDA. The FMEDA process involves examining the failure modes of a system to identify the potential failure causes and their effects on the system (Figure 2). Whether applied at the component level or at the system level, an FMEDA facilitates the demonstration of compliance with a functional safety standard such as the IEC 61508, addressing both its qualitative and quantitative requirements.

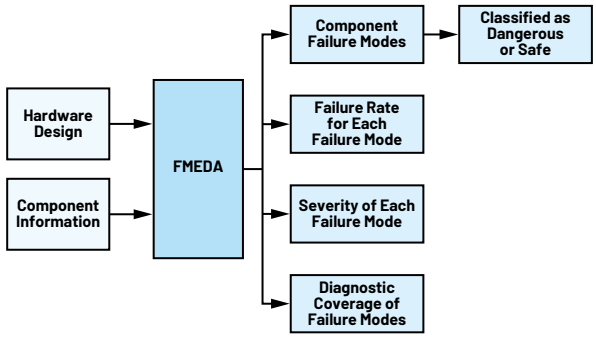


Figure 2. An FMEDA block diagram.[2]

The requirements for a safety manual for compliant items are outlined in IEC 61508-2:2010. This information facilitates the IC integrator to more easily complete their FMEDA.

Annex D Section D.2.2 states that for every function, the safety manual shall:

(d) contain the failure modes of the diagnostics, internal to the compliant item (in terms of the behavior of its outputs), due to random hardware failures, that result in a failure of the diagnostics to detect failures of the function;

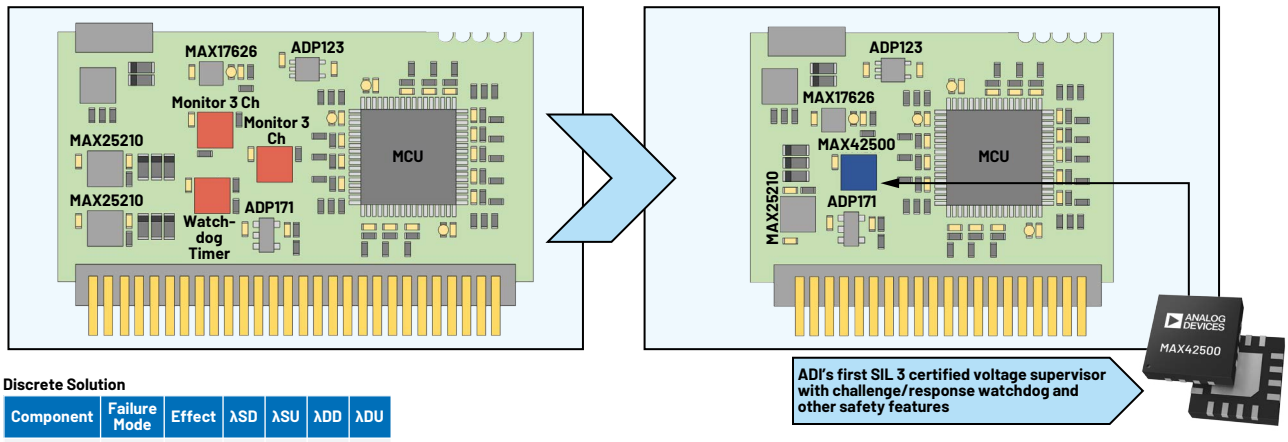
(e) for every failure mode in (c) and (d) the estimated failure rate.

Section 7.4.9.4 Item (j) states that the failure rate of the diagnostics due to hardware failures information shall be available for each safety-related element that is liable to random hardware failure requirements for E/E/PE system implementation.

This information streamlines the safety analysis process for system architects, as the failure rates provided in the safety manual can be directly applied to create the system-level FMEDA. If the component FMEDA's assumptions differ from the system designer's use case, the existing analysis documents can be adapted for recalculations and further analysis at the system level.

It Has Integrated Safety Features Scoping Several Diagnostic Functions

Selecting the right part for an application usually involves considering factors such as component cost, board size, system operation, and features. With functional safety compliance in mind, another factor comes into play—the complexity of the safety analyses such as those found in the FMEDA. Figure 3 shows how a highly integrated part reduces board size and component count as well as simplifies the system's FMEDA. Discrete solutions, which involve more components, necessitate a more extensive consideration of failure modes and rates in the analyses. On the other hand, integrated solutions that comply with functional safety standards tend to have fewer rows in the FMEDA document. For instance, the MAX42500 shown on the right of Figure 3 consolidates the functionalities of the three separate parts on the left. Being a SIL 3-rated device already has its lambda values available in its FMEDA, thus simplifying the necessary analyses and calculations for the system's FMEDA.



Discrete Solution

Component	Failure Mode	Effect	λSD	λSU	λDD	λDU
Diagnostic IC1						
Diagnostic IC2						
Diagnostic IC3						

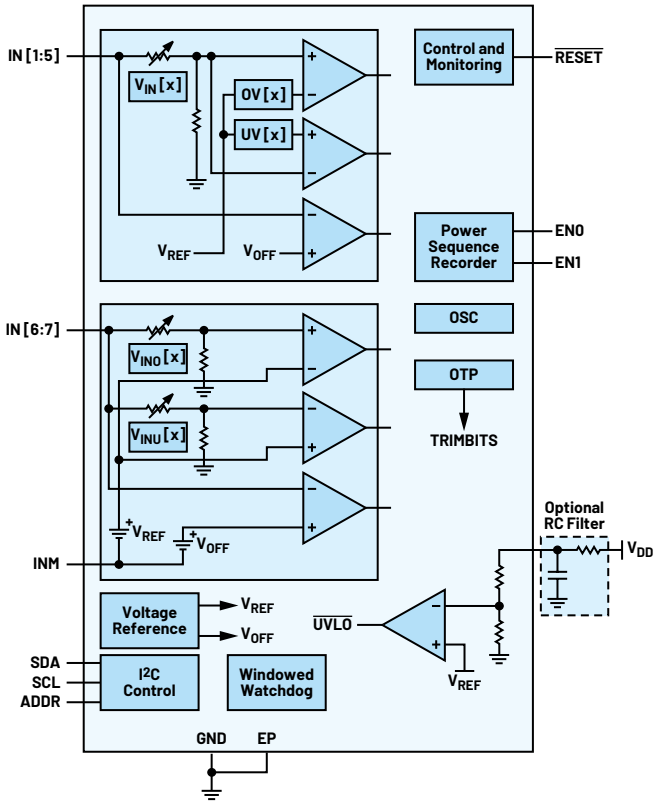
Integrated Solution

Component	Failure Mode	Effect	λSD	λSU	λDD	λDU
Diagnostic IC1						

Compliant Integrated Solution

Component	Failure Mode	Effect	λSD	λSU	λDD	λDU
Diagnostic IC1						

Figure 3. Discrete solution vs. integrated solution.



Fault	Diagnostic Coverage
Short to GND/V_{DD} on IN_X Pins	OV/UV comparators assert depending on voltage.
Open on IN_X Pins	UV/OFF comparators assert.
Short to GND on V_{DD} Pin	Loss of I²C communications.
Open on V_{DD} Pin	Loss of I²C communications.
Open/Short to GND EN0/EN1 Pins	Sequencing is not detected. This is detectable by reading the EN0/EN1 state through the I²C and by the loss of sequencing information in the status register.
Open/Short on SDA/SCL	No I²C communications. Communication attempts result in a NACK response. Watchdog fault will flag due to inability to update the watchdog.
Open GND Pin	$\overline{RESET}$ can still assert down to one body diode above system ground. Persistent UV conditions occur if any voltage monitors are active.
Short to V_{DD} on $\overline{RESET}$	Test at power-on can verify that $\overline{RESET}$ pins are low.
Open on $\overline{RESET}$ Pin	This can be detected by reading the state of the $\overline{RESET}$ pin through I²C. If the $\overline{RESET}$ pin should be high but is low (due to 2 µA pulldown current), the pin is open. This is also detectable if a power-on watchdog test is performed.
Internal Watchdog Block Failure	Can be detected through a host-induced test.

(b)

Figure 4. The MAX42500's (a) functional block diagram and (b) diagnostics.

It Has Its Own Diagnostics to Detect Its Own Random Hardware Failures

Components developed in compliance with IEC 61508 incorporate a specific SFF, λ_{DU} (dangerous undetected failure rate), and systematic capability, which significantly enhance its reliability over noncompliant devices, particularly in terms of either PFDavg and/or PFH, thanks to on-chip diagnostics. These diagnostics are engineered to minimize dangerous undetected failures that are considered during the part's development, targeting compliance with a SIL. Consequently, parts without such diagnostics typically exhibit significantly worse reliability predictions due to the absence of mechanisms to detect and mitigate internal failures.

Consider the MAX42500 shown in Figure 4. This highly integrated device features multiple blocks and pins, and it is equipped with diagnostics to identify random hardware failures that could affect these components. The first part of this series discussed how high performance voltage supervisors such as power supply monitors contribute to enhancing functional safety compliance by improving failure detection, which in turn boosts systematic integrity, PFH, and SFF. Similarly, compliant devices demonstrate enhanced performance with lower rates of dangerous undetected failures.

Figure 5 shows a typical budget allocation for the PFH requirement for a safety function within a safety-related system aiming to comply with IEC 61508. This shows that diagnostic components with a lower rate of dangerous undetected failures not only improve a system's reliability but also permit a more flexible allocation of the PFH budget across other system components.

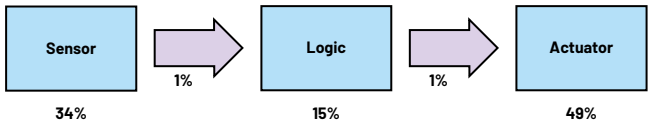


Figure 5. A PFH budget allocation example.[2]

It Is Future-Proof Against IEC 61508's Upcoming Revision

Currently, the basic functional safety standard—IEC 61508:2010—does not mandate a diagnostics on diagnostics for nonredundant systems nor a systematic capability (SC) that is one level below that required for the safety function for diagnostics.[3] However, the upcoming revision of the standard is expected to introduce several significant changes:

- Explicit warnings about the use of on-chip diagnostics to detect failures on the same chip unless the IC was developed in compliance with IEC 61508.
- Requirements that align with the automotive ISO 26262 standard concerning latent fault metrics.
- A specific SFF for diagnostic functions.
- An SC requirement for diagnostic circuitry.

Therefore, using ICs developed in compliance with IEC 61508, such as the MAX42500, will help future-proof the design in anticipation of these potential updates.

It Considers Other Countries' Safety Standards and Directives

System designers who want their products to be used in a specific country must ensure compliance with the respective national laws and regulations. Different countries have their unique safety regulations, and many have already adopted their versions of the IEC 61508 standard, such as Australia's AS 61508,[4] the United Kingdom's BS EN 61508,[5] and Canada's CSA 61508.[6] As the basic functional safety standard undergoes revisions, related sector-specific standards and national laws and regulations are expected to be updated accordingly.

Notably, the use of SIL-rated monitors is mandated in some countries, especially within the European Union. This requirement stems from the Machine Directive 2006/42/EC Recommendations for Use,[7] which necessitates SIL-rated monitors for single-channel systems. The directive specifies that failures in diagnostic functions, which could directly lead to a failure in the safety function or element, should be treated as if they were failures in the safety function or element itself. Additionally, in scenarios involving two or more faults that cause a critical state related to the safety function or element, one of the following approaches shall be applied:

1. The diagnostic functions are considered as separate functions and must meet the criteria as shown in Table 1.

Table 1. Systematic Capability Requirements for the Application of Diagnostic Functions[7]

Safety Function	Diagnostic Function
SIL 1	Basic safety principles
SIL 2	SIL 1
SIL 3	SIL 2

2. A failure in a diagnostic function that increases the probability of the safety function does not operate correctly when required shall be classified as a dangerous failure according to IEC 61508-4:2010, clause 3.6.7. A failure in a diagnostic function that leads directly to the safe state shall be classified as a safe failure according to IEC 61508-4:2010, clause 3.6.8.[7]

See Tom Meany's blog post "Diagnostics on Your Diagnostics" for insights on how various sector-specific standards perceive SIL-rated diagnostics.

It Eases Functional Safety Assessment

Applications requiring higher SIL levels also necessitate greater independence. This is shown in IEC 61508-1:2010 Table 4 and Table 5, which show that the required degree of independence for functional safety assessments varies based on the consequence or SIL/SC requirement, ranging from an independent person to an independent organization. Thus, the highest degree of independence requires an independent organization, such as external assessors, to verify functional safety compliance. In turn, this emphasizes the importance of understanding the perspectives of external assessors on functional safety.

Take, for instance, TÜV SÜD, a recognized independent assessor in Functional Safety. The organization says that the SIL requirements for the entire safety function shall apply to diagnostics as well.[8] Similarly, Exida emphasizes the importance of developing safety-critical components according to the IEC 61508-compliant process.[9] With diagnostics central to functional safety compliance as discussed in part 1 of this series, selecting SIL-rated monitors not only improves FS compliance but also expedites the certification process through faster external assessment.

Conclusion

The primary objective of this article is to explore the importance of using functional safety-rated monitors when complying with functional safety standards. Initially, it delves into the fundamental requirements of the IEC 61508's standard, emphasizing the significance of accessible component-FMEDA information in the safety manual of the compliant parts. Secondly, it illustrates the advantage of integrating a SIL-rated power supply monitor, which not only reduces the board size but also simplifies safety analysis compared to discrete solutions. Thirdly, the article discusses the role of extensive on-chip diagnostics in a SIL-rated diagnostic IC in minimizing the rate of dangerous undetected failures and its influence on the overall system's PFH budget. Fourthly, it demonstrates how using such parts can

future-proof safety-related system designs in anticipation of the upcoming revision to the IEC 61508 standard. Fifthly, it connects the need for SIL-rated monitors with the growing adoption of the basic functional safety standard by various countries and the perspectives of sector-specific standards such as the Machinery Directive. Lastly, it references the positions of renowned functional safety assessors on the use of IEC 61508-compliant diagnostics.

Stay tuned for the next article in the series where we will discuss features of diagnostic functions that are crucial in designing an SRS.

References

[1] *IEC 61508 All Parts, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. International Electrotechnical Commission, 2010.

[2] Marvin Rausand. *Reliability of Safety Critical Systems: Theory and Applications*. John Wiley & Sons, January 2014.

[3] Brian Condell. "Designing a Functionally Safe SIL 3 Analog Output Module with SIL 2 Components." Analog Devices, Inc., September 2023.

[4] *AS 61508 All Parts, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. Australian Standard, 2011.

[5] *BS EN 61508 All Parts, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. British Standards Document, 2010

[6] *CSA C22.2 No. 61508 All Parts, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. Standards Council of Canada, 2017.

[7] *Coordination of Notified Bodies—Machinery Directive 2006/42/EC—Recommendation for Use*. 2015.

[8] "Top Misunderstandings About Functional Safety." TÜV SÜD, 2024.

[9] John Yozallinas. "So What Does Interference-Free Mean? And Why Do We Care?" exida, February 2017.

About the Author

Bryan Angelo Borres is a power applications senior engineer taking up the functional safety engineer role in his group, the Multi-Market Power-East. Working with Tom Meany regarding several functional safety initiatives, he helps customers design functionally safe systems compliant to industrial functional safety standards such as the IEC 61508. He holds a postgraduate degree in power electronics from the Mapua University, where he currently takes his master's degree in electronics engineering. Bryan has more than six years of extensive experience in designing efficient and robust power electronics systems.