Electronic Design

BRYAN ANGELO BORRES, Senior Functional Safety Engineer,
Analog Devices Inc., https://www.analog.com/

The Principles of Safe Industrial Power Design

This article examines how to eliminate systemic and random failures that can cause unsafe conditions in power supplies.

In safety-related industrial systems, the power supply is one of the most critical pieces of the puzzle, and it must be protected against failures that could prevent the system from achieving or maintaining a safe state. However, as outlined by the IEC 61508 standard for functional safety, different failures can prevent safety-related systems from reaching a safe state during startup or operation. Understanding these failure modes — and how to mitigate them — is fundamental to safe power-supply design.

A safety function can either carry out positive actions to avoid hazardous situations or prevent actions from being taken to maintain a safe state. In terms of failures, a safety function could either have a systematic failure or a random one as shown in *Figure 1*.

Systematic failures include both hardware and software. These failures occur in a deterministic way due to a certain cause and must be eliminated through design modifications, such as implementing component derating, robust overvoltage protection, and proper power-supply monitoring. For instance, IEC 61508 provides normative techniques and measures so that systematic failures can be avoided and controlled.

On the other hand, random failures only occur in hardware. These types of failures result from one or more of the possible degradation mechanisms in the hardware happening at a random time. Thus, random hardware failures can only be controlled using diagnostic measures and architectural design, primarily quantified through failure modes, effects, and diagnostics analysis (FMEDA).

Effective management of both failure types — eliminating systematic weaknesses and controlling random hardware failures — is essential to meet the required safety integrity level (SIL).

How to Control Systematic Failures in Power Supplies

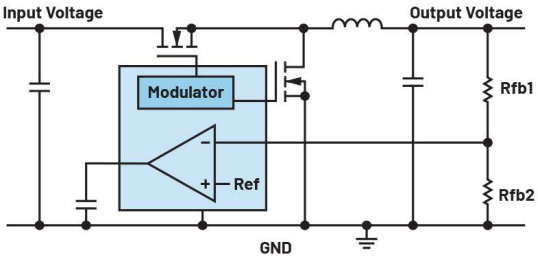
Regardless of the SIL, measures against voltage breakdowns, and other power supply-related dangerous failures, are mandatory to control systematic failures.

These can come in the form of passive protection devices like fuses and Zener diodes or other passive approaches such as implementing proper derating of components and allotting sufficient operating margins. Or designers can

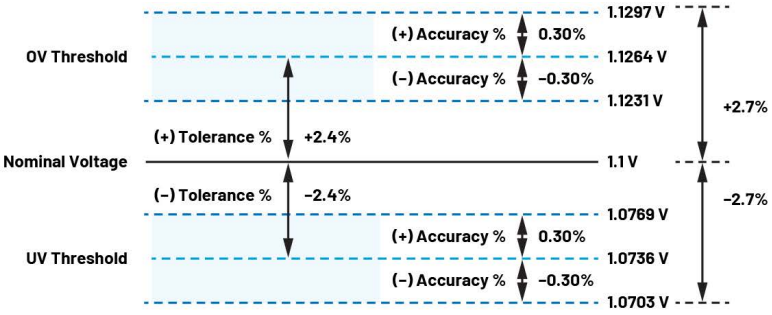
Systemic Failures	Random Hardware Failures

Avoid:
▸ IEC 61508-2 (Hardware) Annex B
▸ IEC 61508-3 (Software) Annex A, B
▸ Other Requirements in Text (IEC 61508-1, IEC 61508-2, IEC 61508-3)
 	
Control:
▸ IEC 61508-2, Annex A
  ▸ Table A.15
  ▸ Table A.16
  ▸ Table A.17
	Control:
	▸ Diagnostic Measures
	  ▸ Fault Models with Diagnostic Coverage — 60%/90%/99%
	  ▸ IEC 61508-2, Table A.1
	  ▸ Recommendation of Concrete Diagnostic Measures
	  ▸ IEC 61508-2, Table A.2 to Table A.14
	▸ Architecture
	  ▸ Redundancy/Hardware Fault Tolerance (HFT)
	  ▸ Homogenous or Diverse
	  ▸ Common-Cause Failures
	  ▸ Safe Failure Fraction (SFF)
	  ▸ PFDavg/PFH

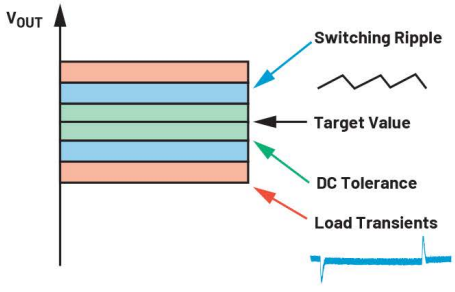
1. The IEC 61508 standard outlines the differences between systematic failures and random hardware failures.



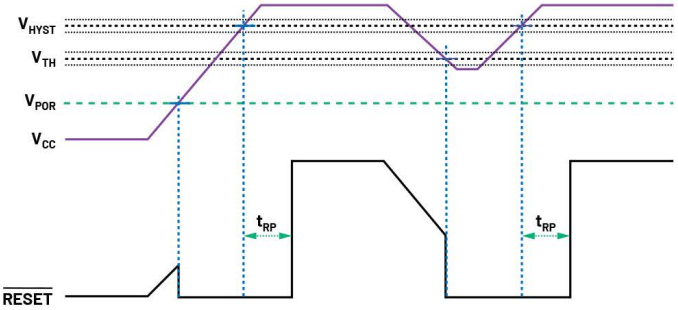
(a) Switch-Mode Power Supply Circuit Example



(c) Power Supply Monitor Accuracy and Tolerance Example



(b) Factors Affecting the Accuracy of Power Supply Output



(d) A Timing Diagram of a Monitored Voltage V_{CC} and Reset Output Signal of a Voltage Supervisor

2. When setting the power-supply monitor's overvoltage (OV) and undervoltage (UV) thresholds, the power supply's output accuracy must be taken into account.

take more direct action in the form of power-supply diagnostic measures, e.g., adding overvoltage protections, windowed power-supply monitoring, secondary voltage control, current limiting, and other active protection circuitries.

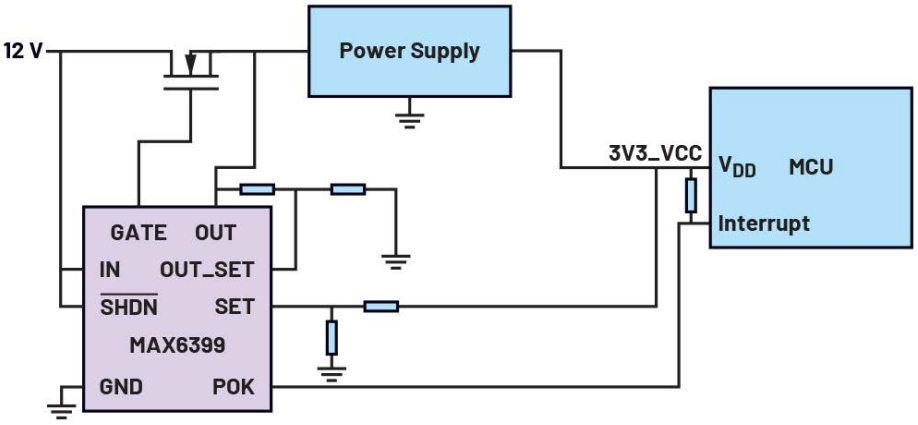
Aside from complying with performance requirements spanning from electrical, thermal, and mechanical to electromagnetic compatibility (EMC) and safety, some questions to ponder include:

Are all voltages properly monitored to enable proper power sequence?

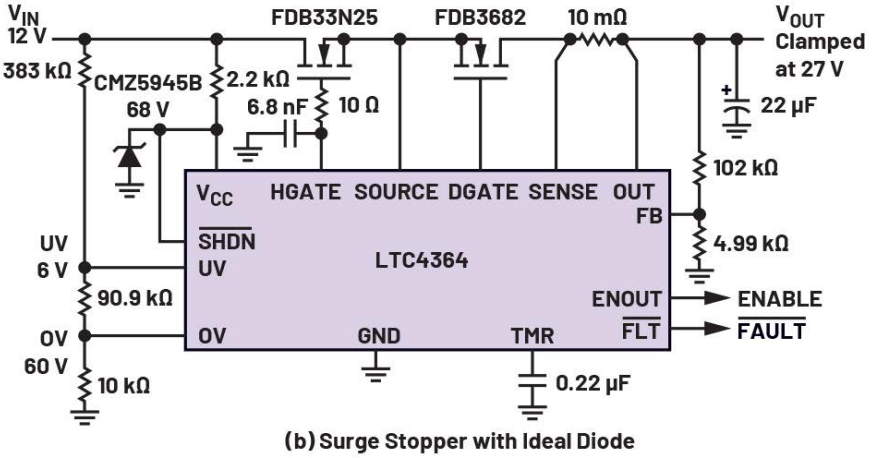
Consider different factors affecting a power supply's output accuracy when setting the power-supply monitor's overvoltage (OV) and undervoltage (UV) thresholds to enable seamless sequencing and diagnostics. This can be seen in *Figure 2*.

Are sufficient protections — for example, surge protections — or

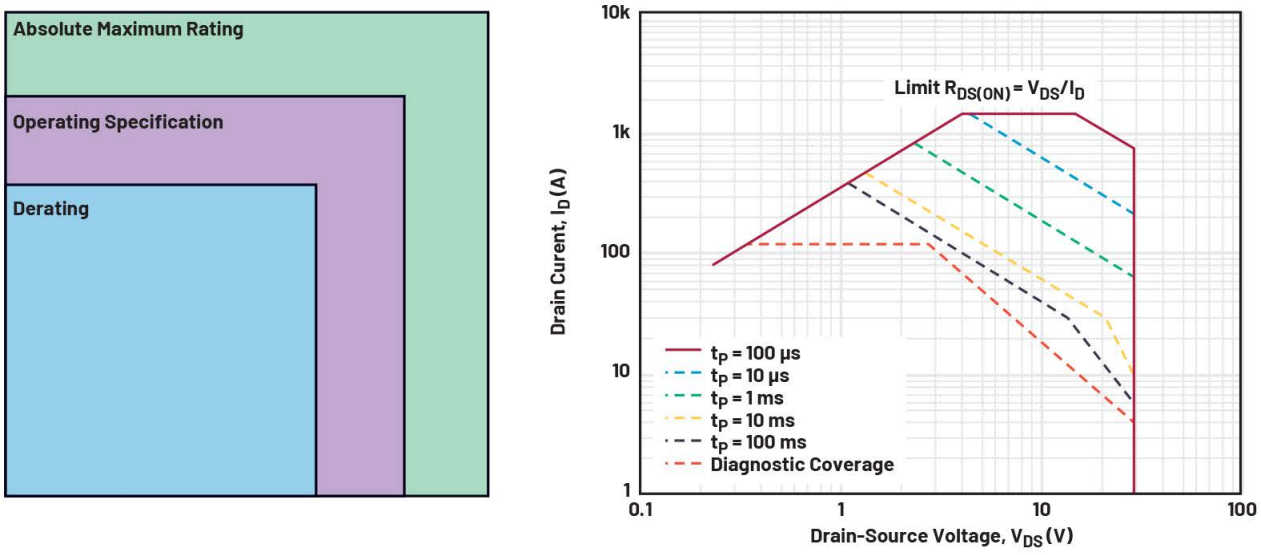
3. Safe power supplies leverage protection measures such as OV/UV protection, surge stoppers, reverse-input protection, reverse current, and current limiting.



(a) OV/UV Protection



(b) Surge Stopper with Ideal Diode



(a) Component Derating Illustration

(b) MOSFET Safe Operating Area (SOA)

4. Sufficient derating improves electromagnetic immunity and ensures components operate in their safe operating area.

other measures employed to improve electromagnetic immunity?

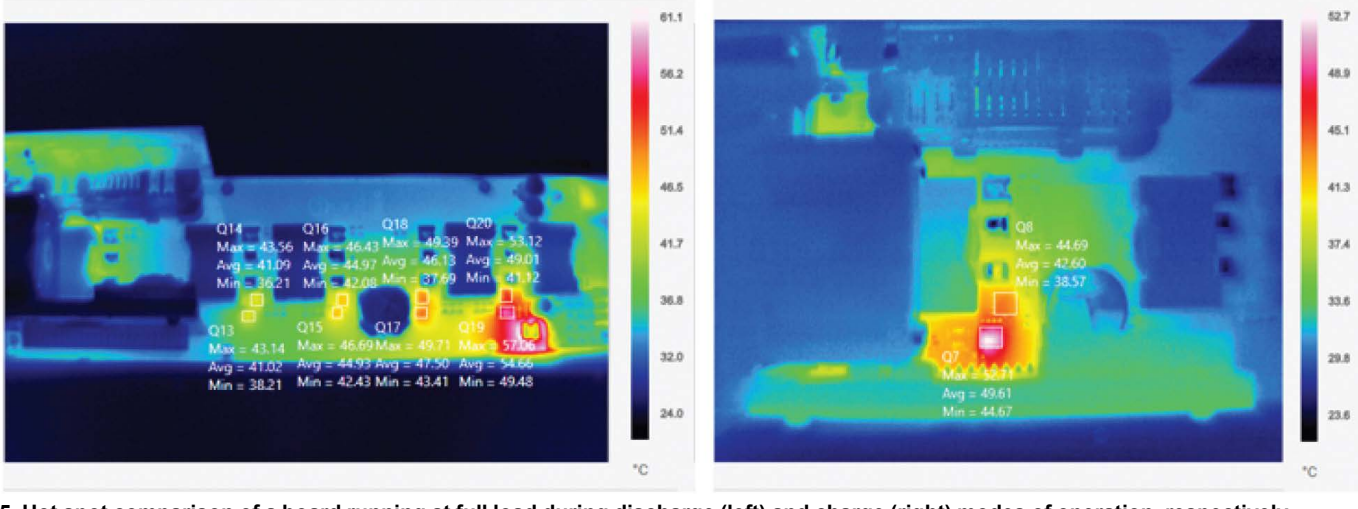
Consider protection measures such as OV/UV protection as in the MAX6399 and surge stoppers like those in the LTC4364. Reverse-input protection, reverse-current, and current-limiting can also be implemented *(Fig. 3)*.

Are well-tried components used according to their specifications with sufficient derating, such as 67% of loading conditions?

Sufficient derating involves ensuring components operate in their safe operating area as well as employing additional operating margins *(Fig. 4)*. For instance, a 125°C-rated part provides sufficient derating when used to operate at 55°C ambient operating temperature with junction temperature rising to 85°C.

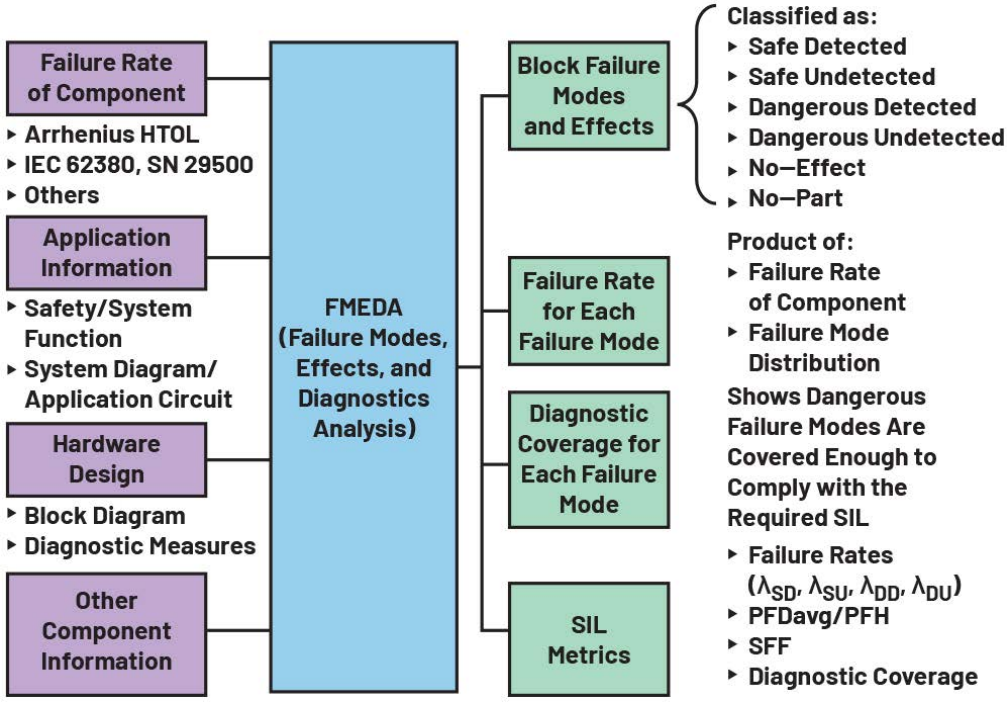
What other systematic failure modes need to be addressed in the power-supply design?

These can include back EMF (electromotive force) that can damage input circuit; timing or pulse-width modulation (PWM) issues that can cause cross-conduction; and hot spot issues that could cause thermal runaways as shown in *Figure 5*.



5. Hot spot comparison of a board running at full load during discharge (left) and charge (right) modes of operation, respectively.

6. The components of FMEDA.



Reducing the Risk of Random Hardware Failures

A FMEDA document is used to analyze and quantify the impact of random hardware failures on the performance of safety-related systems. Its input includes failure rate, application, and hardware design information. Meanwhile, its output shows block failure modes and effects; failure rates λ_{SD}, λ_{SU}, λ_{DD}, and λ_{DU}; diagnostic coverage for each failure mode; and the SIL metrics. These are shown in *Figure 6*.

Evaluating a product against these FMEDA principles includes other requirements:

- Analyzing the failure modes of components used to implement the safety function.
- Employing additional safety (diagnostic) measures/ built-in self-tests (BISTs) against dangerous undetected failures to improve SIL metrics accordingly.
- Doing iterations until the required safe failure fraction (SFF) and probability of dangerous failure (PFH/PFDavg) metrics are met.

Other considerations include using functional-safety compliant components, which offer several benefits, or using Analog Devices' FS-enabled parts, which provide safety application notes to show an IC's failure rate information, failure mode distribution (FMD), and pin failure modes and effects analysis (FMEA) information to help speed up the system FMEDA.

Conclusion

The foundation of a robust and safe power-supply design lies in a rigorous approach to failure management as prescribed by IEC 61508. Addressing systematic failures is paramount; these deterministic faults must be eliminated through proactive design choices, such as implementing windowed voltage monitoring, using sufficient component derating, and integrating surge protection.

By adopting both passive and active measures early in the development cycle, engineers can mitigate risks like thermal runaway and voltage breakdowns. This ensures the power system remains within its defined safe operating area even under stress.

On top of that, engineers need to account for the unpredictable nature of random hardware failures. While these can't be eliminated through design changes alone, they're effectively managed by quantifying risks via FMEDA. By meticulously analyzing failure rates and incorporating diagnostic coverage like BISTs, designers can control hardware degradation impacts to meet stringent SIL requirements.

Ultimately, eliminating both systematic weaknesses and controlling random hardware failures ensures that the power supply functions not just as a power source, but as a reliable backbone for functional-safety systems.

Bryan Angelo Borres is a TÜV-certified functional-safety engineer who focuses on industrial functional safety. As a senior power applications engineer, he helps component designers and system integrators design functionally safe power products that comply to industrial functional safety standards such as the IEC 61508. Bryan is a member of the IEC National Committee of the Philippines to IEC TC65/SC65A and IEEE

Functional Safety Standards Committee. He also has a post-graduate diploma in power electronics and more than seven years of extensive experience in designing efficient and robust power electronics systems.

References

Frederik Dostal. "Determining Voltage Accuracy of Switch-Mode Power Supplies." *Electronic Design*, October 2025.

Bryan Borres and Christopher Macatangay. "Improving Industrial Functional Safety Compliance with High Performance Supervisory Circuits: Safety Critical Features—Part 3." *Analog Dialogue*, Vol. 59, June 2025.

Noel Tenorio and Anthony Serquiña. "High Performance Voltage Supervisors Explained—Part 1." *Analog Dialogue*, Vol. 58, April 2024.

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

Tom Meany. "De-rating: Advice from NASA & Irish Legend." January 2019.

Dan Eddleman. "MOSFET Safe Operating Area and Hot Swap Circuits." *LT Journal of Analog Innovation*, April 2017.

Building a Better Stepper Motor System with StallGuard and CoolStep Technologies. Analog Devices

Christian Cruz, Gary Sapia, and Marvin Neil Cabueñas. "Smart Battery Backup for Uninterrupted Energy Part 1: Electrical and Mechanical Design." *Analog Dialogue*, Vol. 57, December 2023.

Bryan Borres. "Improving Industrial Functional Safety Compliance with High Performance Supervisory Circuits: Using SIL-Rated Components—Part 2." *Analog Devices*, March 2025.

Bryan Borres. "Know Your Safety Application Notes—Part 2: Failure Mode Distribution." *Analog Dialogue*, Vol. 59, October 2025.