



COMPLIANCETM

MAY 2025

THE COMPLIANCE INFORMATION RESOURCE FOR ELECTRICAL ENGINEERS

Implementing Robust Watchdog Timers for **Embedded Systems**

INCLUDING

Recalls Can Create a
Multitude of Legal Problems

Developing the Dynamic
Hazard-Based Safety
Engineering by Introducing the
Control-Oriented Model

EMC Concepts Explained

Hot Topics in ESD

Troubleshooting EMI
Like A Pro

On Your Mark

WHO SAYS YOU CAN'T HAVE IT ALL?

and with next-day, on-time delivery



You Can Have It All when it comes to EMC/EMI testing. A.H. Systems is proud to bring you exciting new products, and many reliable favorites for your evaluation and compliance applications. Our antennas are unique and distinctive with broadband frequency ranges between 20 Hz up to 40 GHz. This enables us to specialize in various sales, rentals and, re-calibrations of test Antennas throughout the world. To view our products and get quick answers to your questions, access our comprehensive online catalog. Search for various information about product descriptions, typical AF plots, VSWR, power handling capabilities and links to product data sheets. Or simply request a catalog be sent to you. Not only have we been developing EMI Antennas for over 30 years, we also have organized worldwide sales representation. You can find your local knowledgeable representative in over 27 countries via our website. For quality products, excellent service and support with next-day, on-time delivery.

Antennas...

And Kits too.



Innovation

Quality

Performance

Phone: (818)998-0223 • Fax (818)998-6892
<http://www.AHSystems.com>

A.H. Systems



Sometimes only a **tailored** **RF Solution will do!**

At AR we can design and build a tailor-made EMC test system to precisely fit your test requirements, budget and time frame.

Our RF engineering team are able to provide customers with a complete design and system implementation to meet the requirements of RF immunity standards.

Peace of mind

A fully compliant system from AR includes an engineered design that is guaranteed to meet field strength requirements for the tests. Contact our design team to discuss your requirements and get a custom proposal.

TAILORED SOLUTIONS

- Immunity Systems for IEC products
- Automotive ISO 11452-2, 3, 4, 5 & 9
- Airborne and Military applications
- MIL-STD-461 & RTCA DO-160
- Emission Systems for disturbance current, voltage, power & field strengths
- Reverb Chamber Solutions

STANDARD SYSTEMS

- GTEM systems for immunity and emissions
- IEC61000-4-6 for conducted RF-immunity
- IEC61000-4-3 for radiated RF-immunity
- IEC61000-4-4-41 complex modulated signals
- ISO 11452-2 and 4 for radiated RF-immunity on vehicle components
- BCI for Automotive, Airborne & Military
- Strip Lines for Automotive immunity



Visit our website to learn more about AR tailored RF Solutions.



THE POWER OF **3**
emtest / TSEQ / ar



IN COMPLIANCE

ELECTRONIC DESIGN, TESTING & STANDARDS

AT WORK.

AT HOME.

ON THE GO.

**In Compliance
is here for you.**

[HTTPS://INCOMPLIANCEMAG.COM](https://incompliancemag.com)

The **EERC**TM

Electrical Engineering
Resource Center

white paper

Mastering High Voltage: The Importance of Accurate Test Equipment

Navigate the dangerous world of high-voltage testing with precision instruments that prevent catastrophic failures—where accurate calibration means the difference between reliable operation and deadly flashover.

offered by

VITREK

application note

Use of a PC-Based Digitizer in Medical Acoustic Microscopy System

Unlock hidden structures with ultrasonic visualization powered by advanced PC digitizers—where 70 MHz sound waves and streaming gigabytes of data reveal what microscopes can't see beneath tissue surfaces.

offered by

GaGe
by VITREK

application note

Common Test & Calibration Uses of a Portable Signal Generator in The Field

Unlock field testing potential with this rugged, dual-channel signal generator that simulates everything from jet engine rotations to piezoelectric sensors—all in a two-pound, battery-powered package.

offered by

mti instruments
by VITREK

<https://incompliancemag.com/EERC>

In Compliance Magazine Same Page Publishing Inc.
ISSN 1948-8254 (print) 451 King Street, #458
ISSN 1948-8262 (online) Littleton, MA 01460
is published by tel: (978) 486-4684
fax: (978) 486-4691

© Copyright 2025 Same Page Publishing, Inc.
all rights reserved

Contents may not be reproduced in any form without
the prior consent of the publisher. While every attempt
is made to provide accurate information, neither the
publisher nor the authors accept any liability for errors
or omissions.

**publisher/
editor-in-chief** Lorie Nichols
lorie.nichols@
incompliancemag.com
(978) 873-7777

**business
development
director** Sharon Smith
sharon.smith@
incompliancemag.com
(978) 873-7722

**production
director** Erin C. Feeney
erin.feeney@
incompliancemag.com
(978) 873-7756

**marketing
director** Ashleigh O'Connor
ashleigh.oconnor@
incompliancemag.com
(978) 873-7788

**circulation
director** Alexis Evangelous
alexis.evangelous@
incompliancemag.com
(978) 486-4684

features editor William von Achen
bill.vonachen@
incompliancemag.com
(978) 486-4684

**senior
contributors** Bogdan Adamczyk
Keith Armstrong
Ken Javor
Kenneth Ross
Christopher Semanson
Min Zhang

**columns
contributors** Bogdan Adamczyk
Erin Earley
Min Zhang
EOS/ESD Association, Inc.

advertising For information about
advertising, contact
Sharon Smith at
sharon.smith@
incompliancemag.com

subscriptions In Compliance Magazine
subscriptions are free to qualified
subscribers in North America.
Subscriptions outside North
America are \$149 for 12 issues.
The digital edition is free.

Please contact our
circulation department at
circulation@
incompliancemag.com

FEATURE ARTICLES

8 Implementing Robust Watchdog Timers for Embedded Systems

By Christopher James Semanson, Senior Contributor

20 Recalls Can Create a Multitude of Legal Problems

By Kenneth Ross, Senior Contributor

26 Developing the Dynamic Hazard-Based Safety Engineering by Introducing the Control-Oriented Model

By Shun Zhang, Haiwen Lu, Brent Taira, and Daniel Barsotti

COLUMNS

37 EMC Concepts Explained

By Bogdan Adamczyk, Patrick Cribbins, and Khalil Chame

41 Hot Topics in ESD

By Eleonora Gevinti, Michael Khazhinsky, Ali Muhammad, Dolphin Abessolo Bidzo, Nicolas Richaud, Peter Koeppen, Kuo-Hsuan Meng, Vladislav Vashchenko, Andrei Shibkov, and Matthew Hogan, WG18
on behalf of EOS/ESD Association, Inc.

44 Troubleshooting EMI Like A Pro

By Dr. Min Zhang

46 On Your Mark

By Erin Earley

DEPARTMENTS

6 Compliance News

50 Upcoming Events

48 Product Showcase

50 Advertiser Index

FDA Warns Against Unauthorized Modifications to Medical Devices

The U.S. Food and Drug Administration (FDA) is stepping up its efforts to identify FDA-cleared medical devices that have been subsequently modified and that no longer fall within the scope of their original clearance.

An article posted to the website of JD Supra summarizes a recent FDA investigation of the facility of a California-based medical device manufacturer (Q'Apel Medical, Inc.), during which inspectors identified several concerns regarding a previously cleared medical device. The issues included design

modifications and misbranding concerns, each of which required the company to obtain a new 510(k) notification to reflect these changes.

Under FDA regulations, manufacturers seeking to make changes to medical devices originally cleared under the 510(k) process must conduct a risk-based assessment to determine whether the proposed changes alter the device sufficiently to affect the safety or efficacy of the device or lead to a significant change in its intended use. If so, the manufacturer is required to make a new FDA 510(k) submission.

FCC to Investigate CCP-Aligned Entities

The U.S. Federal Communications Commission (FCC) has launched a major investigation into entities operating in the U.S. that are aligned with China's Communist Party (CCP) and whose communications equipment has been placed on the FCC's Covered List.

According to a press release issued by the Office of FCC Chair Brendan Carr, some of the entities on the Covered List may still be operating within the U.S., in violation of the prohibitions under FCC regulations.

The FCC has already sent Letters of Inquiry to each of the listed entities to determine what, if any, further actions are required.

The FCC's investigation will be conducted by the Commission's new Council on National Security.

The FCC's Covered List includes those companies whose equipment or services "pose unacceptable risks to America's National Security." The List was originally created in early 2021 and currently includes 11 separate entities.

EU Commission Releases Its Consumer Conditions Scoreboard

The Commission of the European Union (EU) has published its biennial report monitoring consumer sentiment across the EU in connection with consumer conditions in the Union.

According to a press release issued by the Commission, the data shows that the majority (70%) of EU consumers believe that retailers and service providers respect consumer rights, while 61% of consumers trust public organizations to protect those rights.

However, other results complicate those top-level findings. For example, more than 60% of online shoppers say they are more likely to experience problems with their purchases than those who shop

offline. Further, 93% of online shoppers worry over online targeted advertising, including the collection of personal data and excessive advertising, while 45% have encountered online scams and other unfair practices, including fake reviews and misleading discounts.

And, in the uncertain global economy, 38% of consumers expressed concerns about their ability to pay their bills, as well as 35% who worry about affording their preferred foods.

The latest Biennial Consumer Conditions Scorecard is based primarily on data from the Commission's Consumer Conditions Survey conducted in November 2024.

Thank you to our Premium Digital Partners



FCC Warns Consumers of “Grandparent Scam” Robocalls

The U.S. Federal Communications Commission (FCC) is raising awareness among consumers about a new robocall scam targeting vulnerable older Americans.

In a Consumer Alert, the FCC warns consumers to pay particular attention to a new, so-called “Grandparent Scam” robocall scheme, intended to trick older people to part with their money. According to the Alert, scam callers falsely claim to be a relative of the call recipient and use personal information

about the recipient’s relatives and acquaintances (such as the travel plans of grandchildren) to support their identity claim.

Then, the caller claims to need money for an emergency purpose,

such as for bail in the case of an arrest and advising the call recipient to give cash to a “bail bondsman” who will come to the target’s home to collect the money.

Leveraging the latest technology, some callers even use artificial intelligence (AI) technology to clone the voice of the real relative being impersonated by the caller.

The U.S. Department of Justice has reportedly indicted 25 individual Canadian nationals for participating in the fraudulent robocall scheme for defrauding elderly individuals in more than 40 U.S. states.



Your One-Stop Product Safety Shop – Everything You Need for Product Safety!

ED&D

**PRODUCT
SAFETY
SOLUTIONS**

www.ProductSafeT.com

**IEC/ISO 17025
Accredited Calibrations**



Equipment Calibrated **in SCOPE!**

ED&D is the worlds leading source for precision product safety test equipment. Our engineers are the most qualified in the industry. We'll show you how to save time & money in the regulatory process. Test in advance to be sure you pass the first time!



Call Us Today!

USA/Canada Toll Free:

800.806.6236

International:

+1.919.469.9434

Website:

www.ProductSafeT.com

Research Triangle Park • North Carolina • USA



**Force
Gauges**

**Finger
Probes**

**Save Time...
Save Money...
Get Smart...**



**Impact
Hammers**



**JET-01
& JET-02
Jet Nozzles**

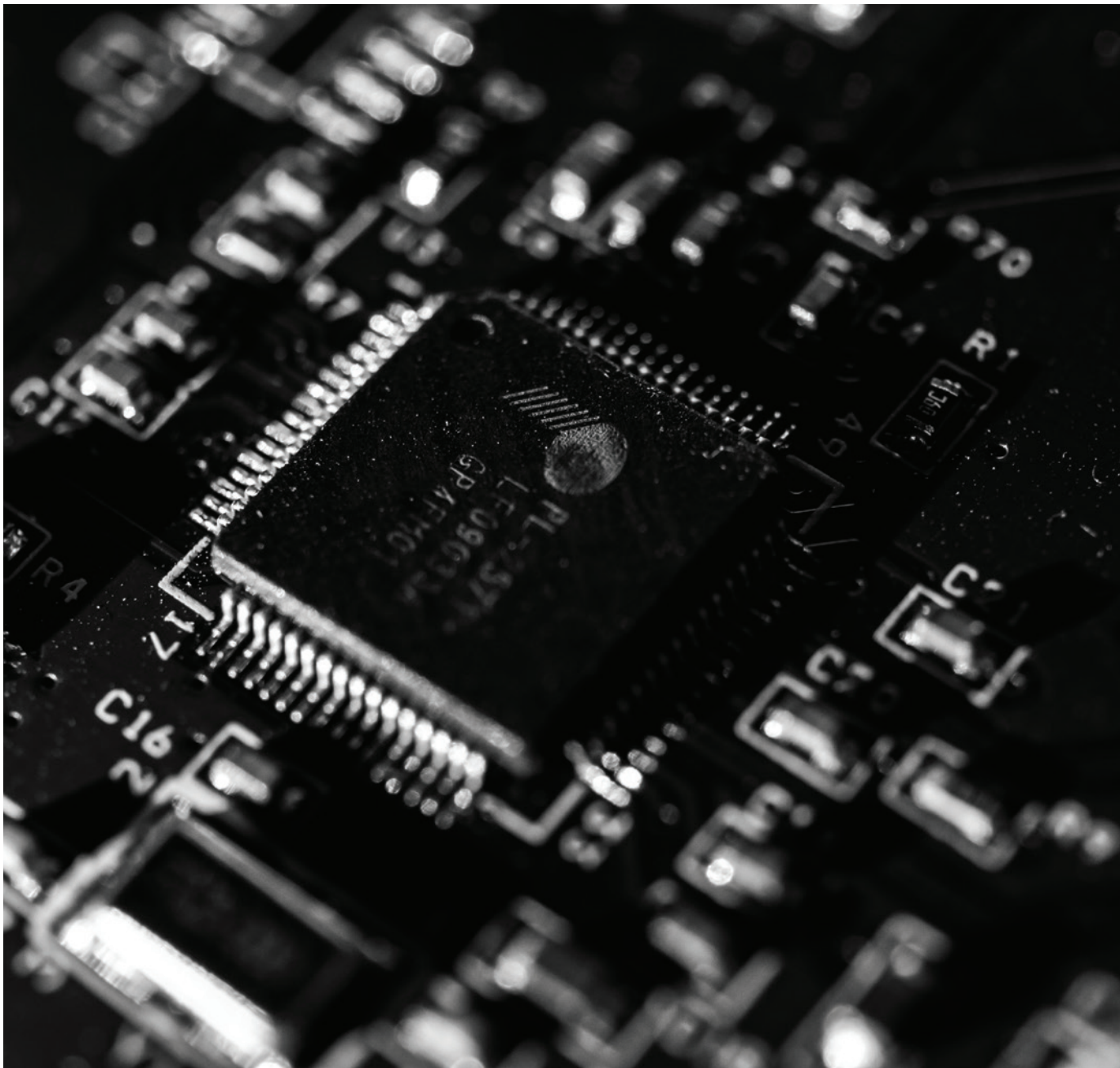


WTR01 Water Tank & Pump System



IMPLEMENTING ROBUST WATCHDOG TIMERS FOR EMBEDDED SYSTEMS

Design Principles, Configuration Strategies, and Fault Recovery Methods Using Watchdogs for Modern Systems



Christopher Semanson is a Senior Contributor to *In Compliance Magazine* and System and Solution Engineer at Renesas Electronics America, Inc, supporting a wide variety of general-purpose applications dealing with MCU, MPU, and Electrical System Design. He has previous experience in EMC Education at the University of Michigan, teaching EMC and Electronics with Mark Steffka and in Software Systems at John Deere and Ford Motor Company. Semanson has a bachelor's degree in electrical and computer engineering and a master's degree in electrical engineering from the University of Michigan Dearborn. He can be reached at chris.semanson.yf@renesas.com.



By Christopher James Semanson, Senior Contributor

Watchdogs have long been a standard, if slightly esoteric, element of system design, often receiving only secondary consideration after the primary application has been planned out. At their core, they serve a straightforward purpose: providing a graceful means of recovery in the event of abnormal system behavior. At their origin, watchdog timer architectures were simple, implemented via a dedicated application-specific integrated circuit (ASIC), positioned adjacent to the system's processor (see Figure 1).

In that early form, interaction with the watchdog was typically limited to a simple general-purpose input/output (GPIO) pin. However, as systems have grown in complexity and adopted stricter safety requirements, watchdog implementations have also evolved. In more modern setups (see Figure 2), a watchdog may be integrated into the microcontroller itself, reside in a voltage monitor or supervisory device, or be part of a power management integrated circuit (PMIC), often refreshable through GPIO, I²C, or SPI.

Two major standards, ISO 26262 and IEC 61508, which outline functional safety requirements, are now driving the design for these

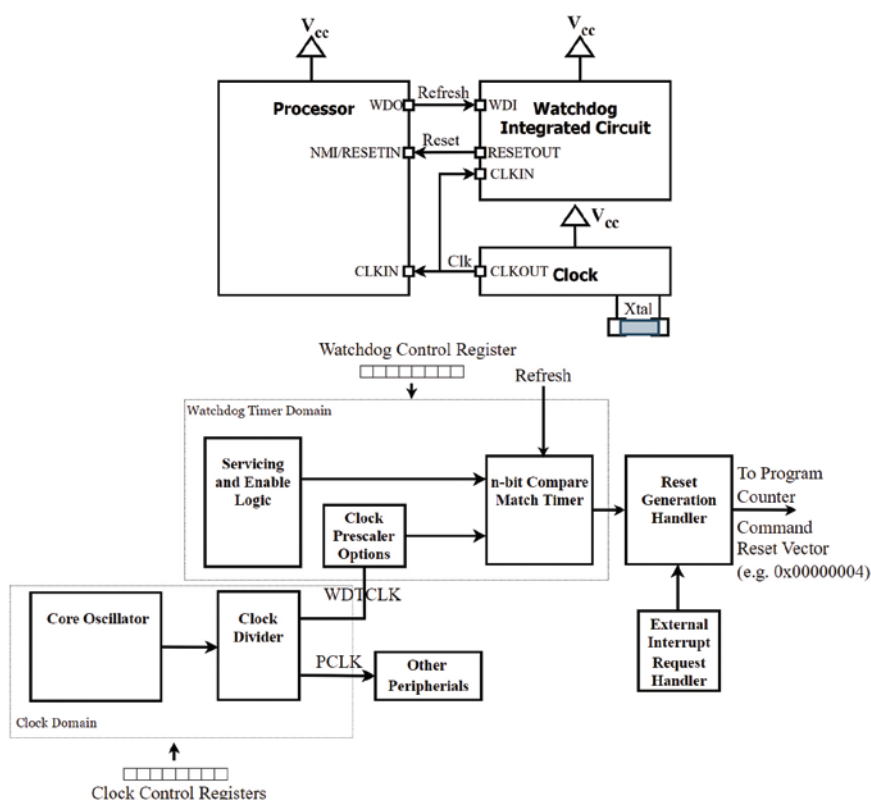


Figure 1: Basic ASIC watchdog architecture (top); basic internal watchdog architecture (bottom)

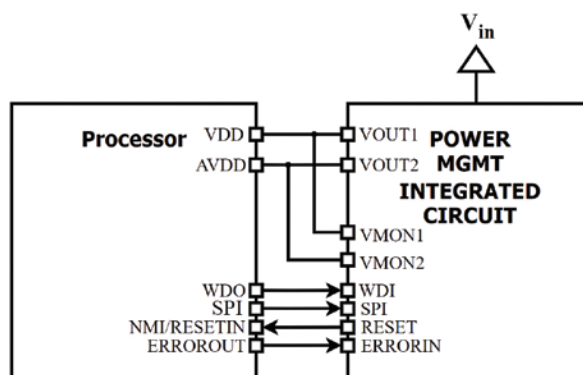


Figure 2: Advanced watchdog architecture with power management device

watchdog architectures. This has led to additional complexity in an already mature device category, introducing new mandates such as:

- The system watchdog must be able to operate independently, mitigating the risk of dependent failures between the device being protected and the device doing the protecting and
- The system watchdog must be capable of accurately monitoring the timing of individual tasks and reporting a hung task to a higher-level application, all while remaining fault tolerant, allowing for maximum uptime.

With these new requirements, watchdogs may include advanced features such as challenge-response mechanisms and, in other system designs, multiple watchdogs that feed into a “master” watchdog to present an overall health status.

In the following sections, we’ll first trace the evolution of watchdog timers, starting with the basic refresh mechanism, moving on to windowed watchdogs, and finally examining challenge-response (Q&A) watchdogs, complete with real-world application

examples. We’ll then delve into safety analyses, explore various system architectures showing how multiple watchdogs can coexist in a robust design, and ultimately highlight the key reporting features to look for when selecting a watchdog solution. This holistic approach will equip you with a comprehensive understanding of modern watchdog systems and how they’re meeting the demands of functional safety in increasingly complex, multicore environments.

EVOLUTION OF THE WATCHDOG TIMER

Before diving into the complexities of modern watchdogs designed for high-safety systems—those requiring Automotive Safety Integrity Level (ASIL) B or higher, or Industrial Safety Integrity Level (SIL) 2 or higher—it helps to first examine the fundamental watchdog timer and its inner workings. This begins with the simplest form of watchdog refresh, progresses through window-based watchdogs, and culminates in challenge-response (Q&A) watchdogs.

The Basic Watchdog Refresh Driven by Pin

In its classic incarnation, a watchdog timer is often implemented as a separate ASIC sitting alongside the main processor (see Figure 3).

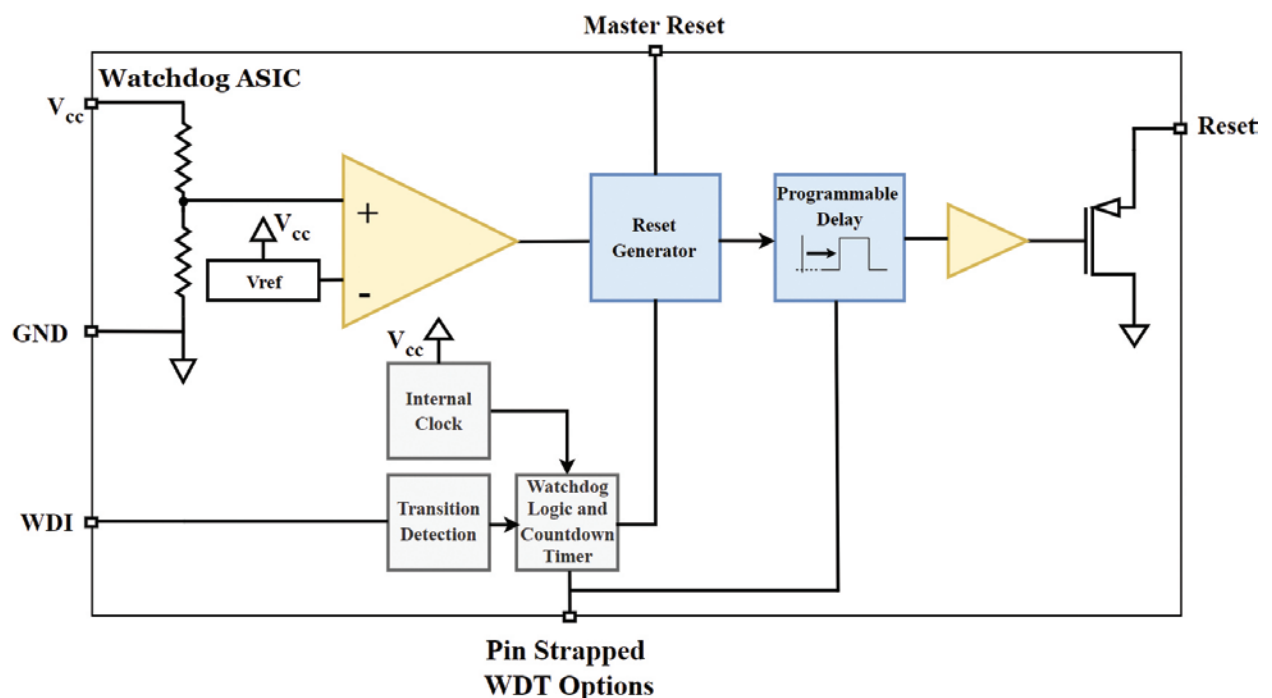


Figure 3: Example internals of a basic WDT ASIC

Because it's relatively straightforward, this type of watchdog can also be integrated directly into the system microcontroller (MCU). In its simplest form, it uses a GPIO pin (or similar) to detect if the system is "alive." If a refresh signal isn't received within a predefined interval, the watchdog times out and triggers a reset or error condition.

Key features of this basic watchdog include:

- *Edge-triggered input:* Responds to rising edges, falling edges, or both
- *Programmable timeout:* Defines how much time may pass between refresh events and
- *Reset delay (or grace period):* Specifies the time from a missed refresh to an actual reset.

These parameters may be configured via special function registers (SFRs, if the watchdog is onboard the MCU) or through one-time programmable (OTP) memory (if it's an external device). Typically, engineers choose a maximum refresh interval that comfortably accommodates the longest atomic task—or aligns with a system's fault-tolerant time interval—plus some margin. While that broad coverage is helpful for catching major system stalls, a basic pin-driven watchdog does have drawbacks. It can't determine

whether individual tasks are running within their expected timeframes, and it only detects a complete system hang which results in a missed refresh.

To address the need for more precise timing checks, the next evolution introduces the window-based watchdog.

The Window-Based Watchdog

As systems grew more complex, the desire to pinpoint abnormal task durations led to the development of window-based watchdogs (WWDT, see Figure 4). These watchdogs monitor refresh signals within a defined "window" of acceptable timing. Conceptually, there are three critical calibratable time limits:

1. *Lower time limit:* If the refresh comes early, the watchdog flags an error

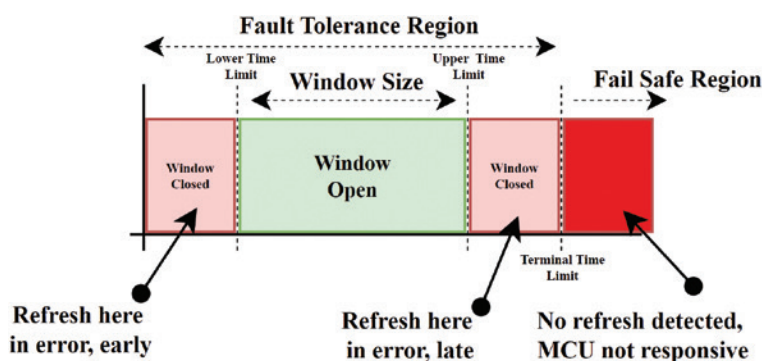


Figure 4: Window watchdog window depiction



EMI Power Choke Impedance Finder

Coilcraft



- Find off-the-shelf, high-current inductors for your EMI noise-filtering applications
- Quickly analyze and compare one or more part numbers of your choice
- Review performance curves at your desired frequency, including L vs. F and Z vs. F

Try it today @ coilcraft.com

- 2. *Upper time limit:* If the refresh comes late, the watchdog flags an error and
- 3. *Terminal limit:* Much like the basic watchdog’s timeout, this defines the point at which the system will be reset if no valid refresh is seen; this is often referred to as too late or non-responsive time limit.

By imposing both lower- and upper-time constraints, a window watchdog offers two primary benefits:

- 1. *Granular fault tolerance:* You can configure different potential responses based on whether the refresh was too early or too late, potentially allowing the system to log errors and continue running for minor timing violations and
- 2. *Monitoring task health:* Some designs allow you to keep track of how often these individual limits are breached. A higher-level supervisor could read an “error count” register and spot if certain tasks are chronically missing their timing. Over time, this data helps diagnose performance bottlenecks or failing components.

User-defined features in a window-based watchdog typically include:

- *Setting the three-time limits:* Specified in base clock counts or milliseconds and
- *Defining an error tolerance:* An “error accumulator” or similar mechanism (Figure 5) decides how many errors trigger a reset.

By returning to correct timing within the defined window, the system can “self-heal” from minor hiccups while still triggering a reset for persistent or major faults (see Figure 6). This improves coverage in functionally safe designs and allows tighter timing constraints compared to the basic watchdog.

However, while the window watchdog accounts for tasks running too long or too short, it still doesn’t confirm that each task is performing the correct operations. That gap is filled by a more advanced mechanism, either the challenge-response or Q&A watchdog.

THE QA WATCHDOG, 4QA AND 16QA

For systems demanding the highest levels of safety, such as those requiring ASIL-D or SIL 4, engineers often use a challenge-response watchdog (also called a question-and-answer watchdog). This design (see Figure 7) builds upon the window concept by actively

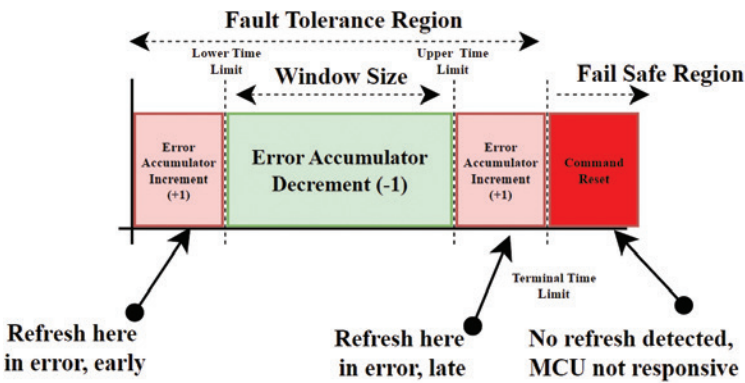


Figure 5: Fault accumulator depiction

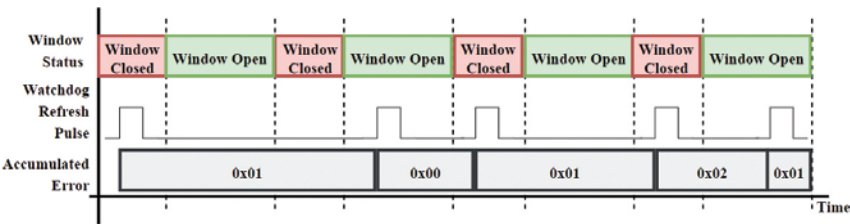


Figure 6: Flow of a window watchdog accumulating and clearing errors

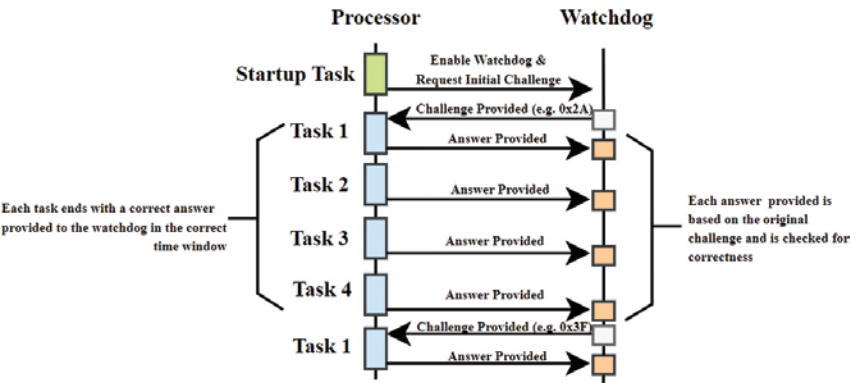


Figure 7: Example of the process a multiple challenge, response watchdog follows

verifying that the MCU or SoC is not only responding within the correct timeframe but also providing the correct *response* to a given *challenge*.

In this scheme, the watchdog issues a “token” or “challenge” that the monitored device (MCU or SoC) must process before returning the result, either by doing arithmetic or applying a bitwise transformation. By expecting a specific and sequential response, the watchdog effectively tests whether the system is running the right code in the right order. Below are three common variants:

- **4-question-and-answer (4QA):** The watchdog provides four sequential challenges (often simple operations on an 8-bit value), and each must be answered correctly in the right time window (see Figure 8).
- **16-question-and-answer (16QA):** The watchdog uses a seed token that defines the next four responses. Additional seeds can chain together to create longer challenge sequences (see Figure 9). This allows for more in-depth program-flow monitoring across multiple tasks.
- **LFSR (linear feedback shift register)-based:** A polynomial is used to generate a pseudo-random challenge (Figure 10 on page 14). The monitored device must compute the correct response for each step in the sequence. This approach can create a large number of possible challenge-response pairs, further increasing system robustness.

Typically implemented in advanced ASICs, voltage supervisors, or PMICs, these watchdogs have moved away from simple pin refreshes, instead relying on I²C, SPI, or dedicated serial interfaces to send and receive challenge tokens. This more sophisticated interaction allows for:

- **Program flow verification:** Ensuring tasks and subroutines execute in the proper sequence and
- **Advanced error accounting:** An error accumulator or register can keep track

of how many challenges were missed or answered incorrectly, letting the system react gracefully to minor issues while still triggering a hard reset when conditions warrant it.

Each type of watchdog (basic pin-driven, window-based, and challenge-response) has its place in the

4 Challenge Response Table Implementation

WDT Challenge	Correct MCU Response	Bit Operation
0x7F (b01111111)	0x55 (b01010101)	Preserve Odd Bits in Challenge and Send back, make even bits 0
0x80 (b10000000)	0x2A (b00101010)	Invert Even Bits in Challenge and Send back, make odd bits 0
0xC0 (b11000000)	0xCF (b11001111)	Invert Lower Nibble and send back
0x00 (b00000000)	0xFF (b11111111)	Invert all bits and send back

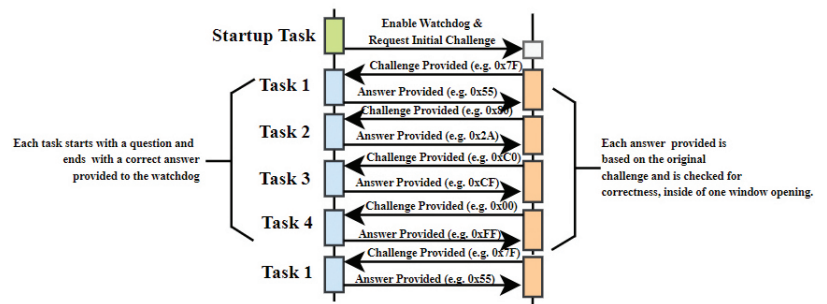


Figure 8: Example of a 4QA response table and sequence

16 Challenge Response Table Implementation

WDT Challenge	Correct MCU Response 1	Correct MCU Response 2	Correct MCU Response 3	Correct MCU Response 4
0x00	0xFF	0x0F	0xF0	0x00
0x01	0xB0	0x40	0xBF	0x4F
...				
0x0E	0x4E	0xBE	0x41	0xB1
0x0F	0x01	0xF1	0x0E	0xFE

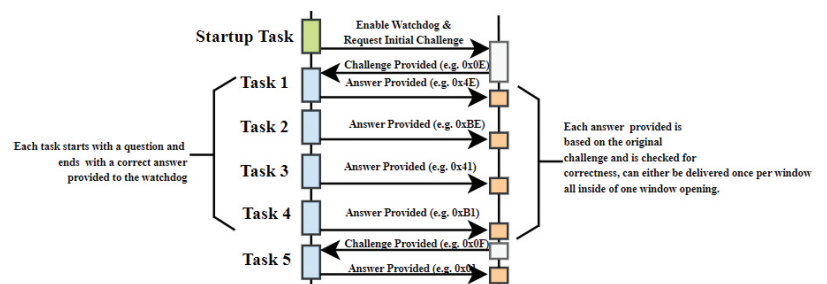


Figure 9: Example of a 16QA Response table and sequence

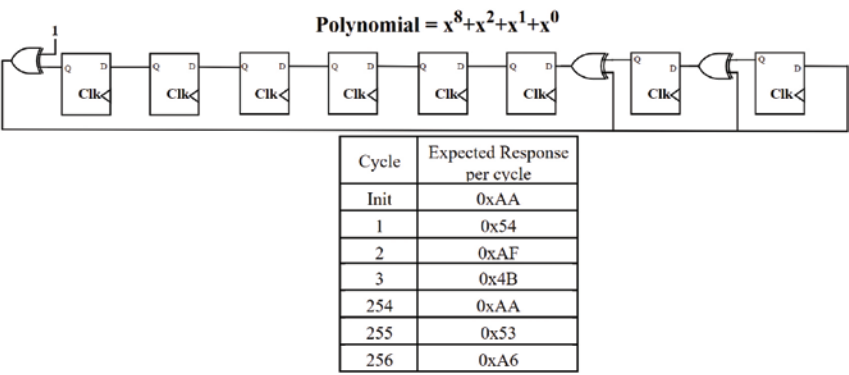


Figure 10: Digital representation of a watchdog implemented as an LFSR polynomial, along with the expected sequential response from the processor

design of reliable, safe, and functionally robust systems. Selecting the right one depends on your application’s criticality, performance requirements, and tolerance for fault conditions. Understanding where your system stands in terms of safety (e.g., ASIL-B vs. ASIL-D, SIL-2 vs. SIL-4) is often the first step in deciding which watchdog functionality you’ll need. Now that the function of these different watchdog timers has been investigated, the next step is focusing on their proper implementation into your system architecture.

SYSTEM REQUIREMENTS

When choosing a watchdog to integrate into an application, it is essential to identify the specific requirements driving its selection. Such requirements often include understanding the types of faults the watchdog is expected to detect, the hardware or software resources the watchdog might share with the device it protects, and the nature of the reporting mechanisms the system must support. All of these considerations can be distilled into four major areas:

- The safety analysis of relevant fault types
- The avoidance of undesirable system dependencies
- The proper integration of multiple watchdogs (if necessary) and
- The selection of reporting features that align with the application’s diagnostic needs

Watchdog and Functional Safety

At its core, a watchdog must provide a graceful means of recovery to the system if the application stops responding. This task generally protects against two principal failure modes.

- The first relates to random hardware faults, such as an oscillator becoming stuck or running at an incorrect frequency or issues arising from miscounted edges on a communication interface like I²C or SPI.
- The second concerns systematic failures, where tasks fail to execute correctly because of software defects—examples include memory corruption due to an errant pointer or semaphore mismanagement that leaves a task waiting indefinitely.

One common example of a systematic failure involves an I²C or SPI interface that becomes stuck because unexpected clock pulses are generated in the presence of high-power transients or noise (see Figure 11). In a system requiring low-voltage interfacing, transient electrical noise can elevate reference voltages beyond VIH/VIL limits, causing the digital state machine inside an ASIC or MCU to miscount edges and wait indefinitely.

Another widespread systematic issue, usually caught in design reviews, involves pointers that exceed array bounds or function pointers that jump to invalid memory locations, leaving the program “off in the weeds.”

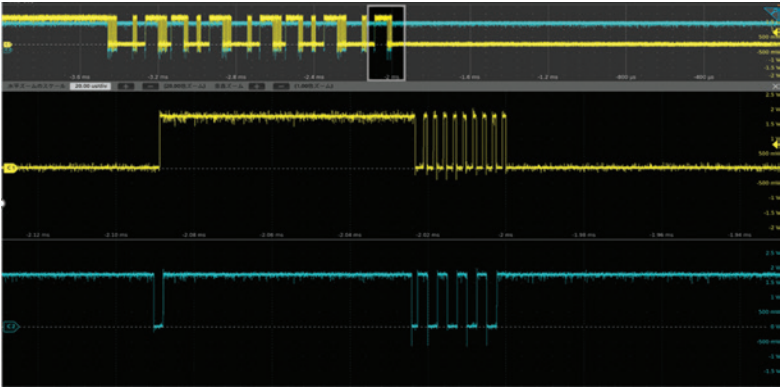


Figure 11: An example of a stuck I²C line, halting system processing

Although these two categories illustrate typical random and systematic errors, a thorough failure mode, effects, and diagnostic analysis (FMEDA) is recommended to examine the system's fault modes. The diagnostic analysis portion of this activity often identifies coverage the watchdog can provide to a specific subsystem. For example, a challenge-response watchdog can address more sophisticated problems by verifying correct arithmetic operations, monitoring individual cores in a multi-core architecture, and detecting clock-frequency irregularities or hardware communication issues as opposed to a simple windowed response watchdog.

In general, the watchdog is expected to catch single-point faults that might otherwise violate the system's safety goals.

Achieving this level of protection requires that the watchdog remains free from dependencies that could prevent it from detecting application errors. A dependent failure analysis (DFA) helps uncover situations where the watchdog relies on shared resources or design elements that might also be subject to failure. In Figure 12, the core oscillator and clock divider provide one clock domain to the peripherals, core, and watchdog timer. Additionally, all system memory is shared, as well as all powered from one power domain. Failure in any one of these areas would prevent the WDT from functioning properly in addition to impacting the ability of the device to achieve the safety goal.

Often, this analysis shows the watchdog must:

1. Use an independent clock source that remains unaffected if the main system clock fails
2. Maintain reliable power or voltage supervision so that

it does not lose state information during dips or brownouts and

3. Operate offboard, which keeps it isolated from defects in the MCU pipeline or CPU core and ensures that it continues running even when the MCU is compromised.

The need for watchdog independence is widely recognized, and achieving it typically involves selecting suitable reporting features and designing the system so that multiple watchdogs can operate without compromising each other's functions (see Figure 13).

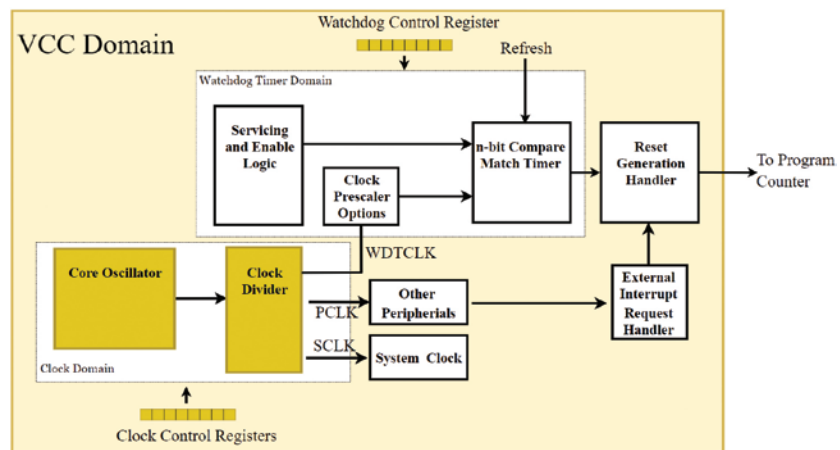


Figure 12: A watchdog diagram, full of dependencies (colored in dark yellow). Clock, memory/registers, and VCC are all identified here.

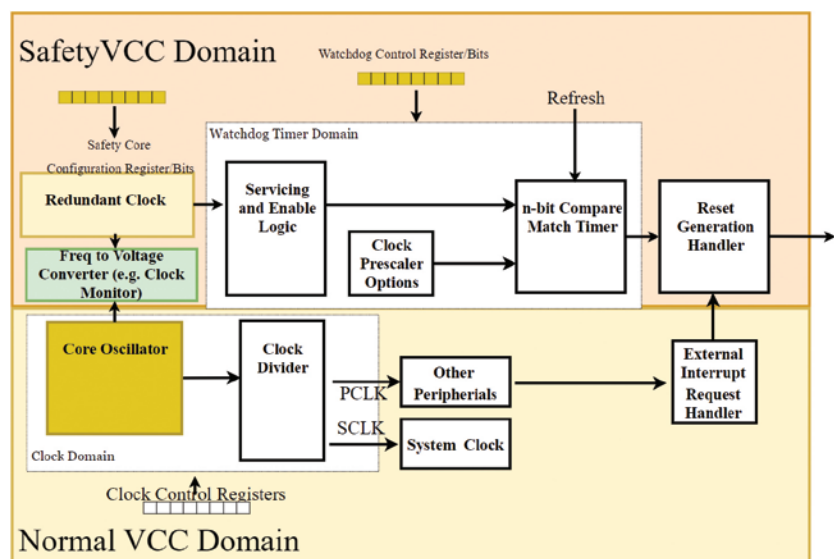


Figure 13: A distributed domain with two clocks, a clock monitor, and two separate VCC domains to remove dependencies

Examining Watchdog Architectures

In the previous section, the DFA was introduced as an analysis that aids in ensuring that a watchdog is free from dependency. In this section, we can apply that thinking to various situations to determine the advantages given three general-use cases.

Hierarchical Watchdogs for Dependency Avoidance

When a system has multiple watchdogs available to them it is up to the designer how to structure their function in such a way that each watchdog can exist at a different level in the system. This allows them to provide evidence that their watchdogs are free from dependency over the domain they’re monitoring and will operate in a predictable way to avoid a boot lock.

This situation is best found in applications with watchdogs per core on a multicore processor and an offboard watchdog either on an associated PMIC or voltage monitor integrated circuit. To start this design, the watchdogs are separated into two groups: the subordinate watchdogs found on a per-core basis and the master watchdog found offboard (see Figure 14).

At its base function, each watchdog will watch its own core, providing localized monitoring, usually in the form of a normal single refresh watchdog or a window-based one. Generally, if that watchdog is not refreshed under the correct parameters, that individual core will issue an interrupt to a specific space in memory and execute a subroutine that will often restart that specific core, leaving the others independent. While this

works well for individual tasks that have hung, such as I²C or SPI, it does not work well for clock and voltage independencies as it relies on a functioning program counter and CPU bus to issue the interrupt and load the program counter with the correct spot in memory. By adding a master watchdog that is refreshed along with individual ones, you’re able to address dependencies such as:

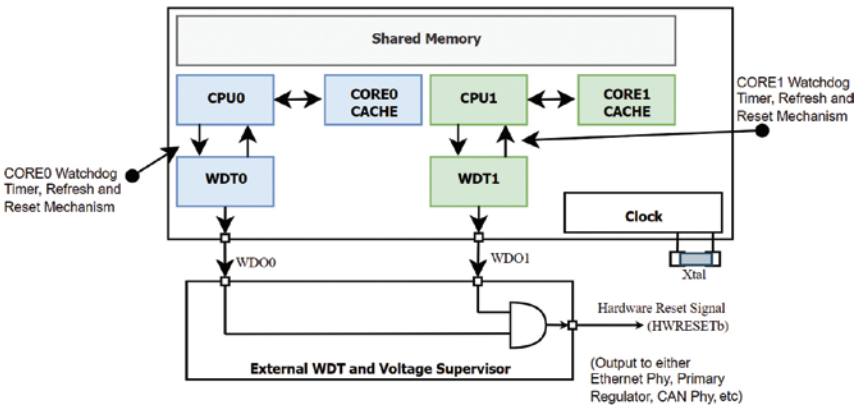


Figure 14: A block diagram of a multicore MCU, with WDT from each core reporting to a system supervisor

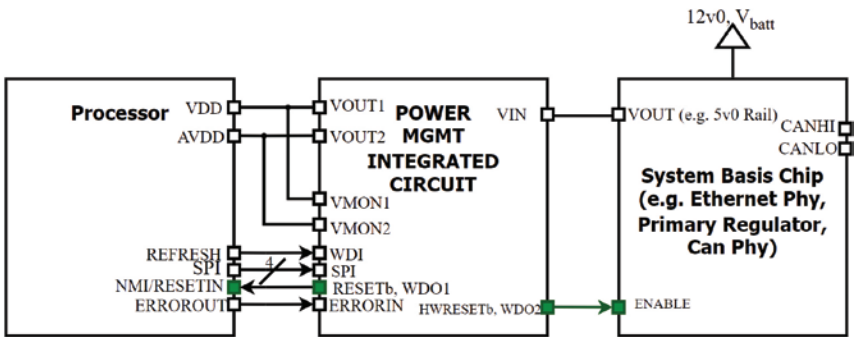


Figure 15: Previously depicted PMIC circuit with 2 reset lines (in green)

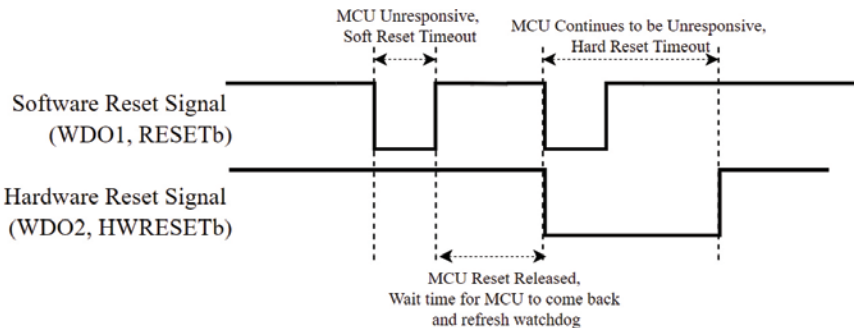


Figure 16: Labeled timing diagram of both reset lines

- **Clock independence:** The external master watchdog relies on its own clock source. If any single core's clock fails, the core's own watchdog stops refreshing, and eventually, the master sees an issue. This separation ensures that one domain's fault does not compromise the entire watchdog infrastructure.
- **Fault isolation:** Each subordinate watchdog can trigger a localized reset or interrupt for its core. If that fails or the core remains hung, the master watchdog takes further action, like forcing a full power cycle.
- **Resource separation:** Subordinate watchdogs rely on the MCU's internal registers and clock domains, while the master watchdog uses an offboard resource (such as a separate oscillator). This avoids the problem of a single clock or memory bus dominating the entire safety mechanism.

The main advantage of this layered approach is that the system offers simplified debugging, allowing each core to issue a refresh and subsequently log irregularities specific to each core while still allowing a master watchdog timer to issue a system-wide reset should errors continue. The downside is that the fault limits need to be chosen correctly to fit inside of the module's fault-tolerant timer interval while still allowing some fault tolerance for the watchdog of each core. This is best used for instances where an SPI, I²C, or a systematic error causes an individual core to hang.

Dual-Output Watchdog: Separating Peripheral Resets from Full System Reboots

In some systems, it's useful for a watchdog to be in control of both a hardware as well as a software reset, passing the responsibility of resetting the module or communications interface to the watchdog timer if the system processor is unable to respond, even after a software reset (see Figure 15). This type of watchdog architecture requires the watchdog to have two output pins, referred to below as WDO1 and WDO2.

In architectures like these, the MCU will communicate with the offboard watchdog and, in the event of a missed refresh, can be programmed to issue a reset to the system controller through a non-maskable interrupt pin. If the offboard watchdog does not receive a signal from the processor indicating a successful recycle, it can toggle the second output, which can either reset the power or communications to the device (see Figure 16). This two-tiered approach allows for:

**In Compliant with
IEC 61000-4-2: 2025**



Electrostatic Discharge (ESD) Simulator

EDS MAX20



- > Test voltage 20 kV;
- > Changeable discharge tips;
- > 1.25 kg (incl. battery);
- > Support fiber-optic communication;
- > Changeable RC modules & automatically identified;
- > Ergonomic design and intuitive user interface;
- > Functions of discharge threshold setting and counter;
- > Up to 18 working hours for rechargeable battery;
- > Built-in 3 test modes: standard test, sequence test and easy test.

IEC/EN 61000-4-2:2025, IEC/EN 61000-6-1/-6-2,
IEC/EN 61326, IEC 61340-3-1, ISO 14304,
ITU-T K.20, Bellcore GR-1089-Core

EDS MAX30



- > EDS MAX30;
- > Test voltage 30 kV;
- > Changeable discharge tips;
- > Changeable RC modules & automatically identified;
- > Power supply AC 100 V~250 V;
- > Support fiber-optic communication;
- > Ergonomic design and intuitive user interface;
- > Functions of discharge threshold setting and counter;
- > Built-in 3 test modes: standard test, sequence test and easy test.

ISO 10605, ISO 14304, IEC/EN 61000-4-2:2025,
IEC/EN 61000-6-1/-6-2, IEC 61340-3-1,
IEC/EN 61326, ITU-T K.20/ K.21

SUZHOU 3CTEST ELECTRONIC CO., LTD.

Add: No.99 E'meishan Road, SND,
Suzhou, Jiangsu Province, China
Email: globalsales@3ctest.cn
Ph: + 86 512 6807 7192
Web: www.3c-test.com



SUBSCRIBE: 3CTEST

- *Reduced downtime:* Resetting a single peripheral requires less re-initialization time than rebooting the entire system, improving availability in real-time or mission-critical applications and
- *Dual timeout domains:* The shorter timeout for WDO1 (e.g., 100 ms) might be enough to catch process stalls. The longer WDO2 timeout (e.g., 500 ms) covers system-level lockups. While the watchdog remains decoupled from the processor clock domain, this also reduces the chance of a single clock failure compromising both outputs.

One such use case for this architecture is in a motor-control system that communicates with multiple sensor ICs via SPI. Occasional electrical noise can cause the SPI bus to freeze due to miscounted clock edges, causing the controller and peripheral to get out of sync. The watchdog's WDO1 toggles a hardware reset line if the bus remains idle or locked for 50 ms, allowing immediate recovery. If the system fails to refresh WDO2 for 500 ms (perhaps because the main control loop is hung), the watchdog triggers a full system reset by either toggling power to the module or the communications interface to the processor.

The key advantage here is that not only the clock but also the way to a safe system state is physically isolated from the processor's main reset domain but still allows some fault tolerance in the case of a non-critical error.

Cross-Monitoring with a Co-Processor

While an offboard watchdog integrated into a supervisor chip or PMIC is quickly becoming popular due to cost, some systems still rely on a co-processor, either be it a simpler MCU or a field programmable gate array (FPGA). This architecture offers the most flexibility, albeit for the

most price, as it allows a user to create a custom response either via a companion MCU or FPGA (see Figure 17).

In this architecture, it is best to separate the domains into a local domain and a companion processor domain. The local domain is where each core on the MCU is being watched internally. However, instead of being given the authority to toggle a hardware reset line, or preempt the CPU with an interrupt, it's given a GPIO or SPI message to a neighboring processor.

At the co-processor layer, the device collects these signals and tracks their failures applying custom behavior allowing pin-based refreshing to lower-level tasks, and challenge-response type logic for higher-level, critical tasks.

Additionally, in this scenario, we gain the benefits of a dual watchdog output in addition to customizable reset requirements. Examples of these custom requirements are:

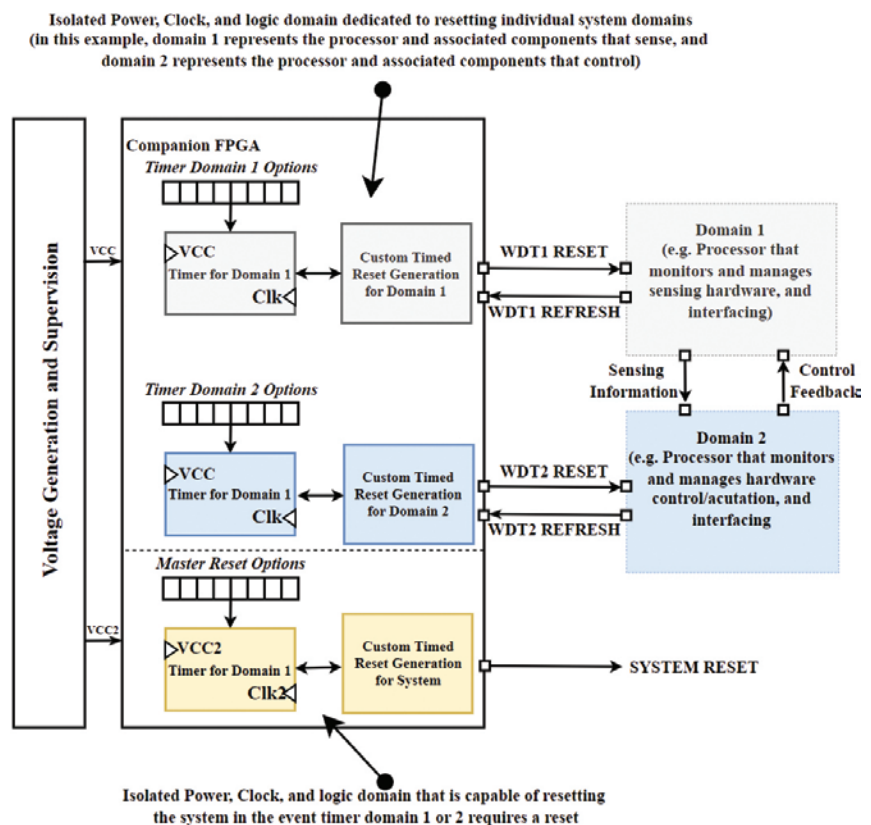


Figure 17: Example system focusing on a custom FPGA that monitors the health of two logical domains, with a master reset with little to no dependencies

- This would allow the system to log a custom number of errors in different situations, resulting in increased uptime and visibility into which tasks have stalled or are otherwise causing system instability.
- Custom responses to reset specific physical interfaces. In an automotive module, there might be multiple interfaces (e.g., CAN, LIN, and an Ethernet PHY). Depending upon the task that is stalled, you may want to either cycle power to or otherwise disable a specific function while still offering reduced functionality (this is often referred to as failing functional).

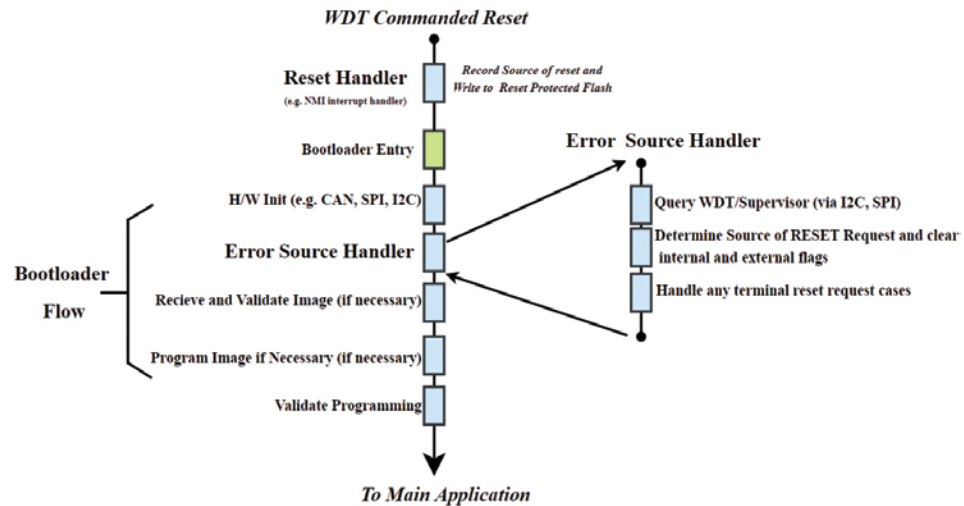


Figure 18: Flow diagram of a system reset, boot loader, and error reporting

Overall, this type of architecture allows the system designer to consider which tasks and domains are suitable for a hard reset where power must be cycled, or a soft reset where just the program counter in the CPU must be modified. Additionally, this scheme offers physical separation of function, which is also desirable when it comes to failure mode analysis as one physical failure will no longer guarantee failure in the monitoring hardware. However, care must be taken in this example to avoid voltage dependency, if the same voltage source is feeding both the co-device and the main MCU there runs a risk of voltage anomalies disturbing the ability for both the watchdog aggregator and the MCU to malfunction similar resulting in the negation of this complex architecture.

Reporting and Error Handling


A final, often overlooked topic involves how complex watchdogs handle faults and generate reports. In many designs, once the watchdog resets the main controller or toggles power to the module, the watchdog's internal memory (often a form of RAM) preserves status flags indicating the nature of the reset that is often cleared upon read, or when written to (see Figure 18). At startup, the system bootloader can read

this information and decide whether to log an event, increment a counter in non-volatile memory, or alter its initialization routine.

Additionally, systems that require more comprehensive tracking benefit from watchdogs capable of distinguishing between different causes for a reset. For instance, some devices maintain separate flags for time-based refresh failures, invalid challenge-response answers, or total non-responsiveness. Placing these flags in an easily accessible register allows a bootloader to implement custom strategies, such as reloading a firmware image or initiating a safe-mode startup if too many consecutive resets occur.

Ideally, the system would offer a simple communication channel built into the boot loader (for example, CAN or LIN in automotive applications) to facilitate external queries about the reset cause. When done properly it aids engineers in finding the cause for reset by highlighting persistent errors.

CONCLUSION

Overall, today's watchdogs can do more than simply catch hung processes; they can precisely monitor task timing, validate code execution, and accumulate valuable diagnostic data. And as safety standards continue to evolve, so will watchdog timers and their architectures, ensuring they remain informative, independent, and, most importantly, reliable in today's functionally safe systems. 

RECALLS CAN CREATE A MULTITUDE OF LEGAL PROBLEMS

Minimizing These Problems Can Be Difficult



When a recall is implemented, it hopefully solves the safety issue. But that doesn't always happen. First, you rarely are 100% successful in retrieving the product or repairing it. And, of course, the occurrence of an accident involving a recalled product can be very difficult to defend. Even worse, an accident involving a product that was unsuccessfully repaired by the manufacturer can be even harder to defend.

The number of lawsuits involving recalled products and products that haven't been recalled has been proliferating recently. And the verdicts and settlements have been significant.

This article will describe the difficulty of defending the adequacy of a recall, the types of remedies that are offered, and a recent trend of class action lawsuits being filed alleging that the remedy instituted by the manufacturer is inadequate and resulted in economic loss to the consumer or owner of the product.

DEFENDING THE ADEQUACY OF THE RECALL

Injuries or deaths resulting from unsuccessful recalls or repair programs can result in litigation and huge verdicts. It can be difficult to argue that a 10% response rate was adequate and could not be improved by the manufacturer doing more. In that case, the jury could believe that the manufacturer negligently performed the recall.

In addition, if a repair is performed and an accident still occurs, that can also cause a jury to get mad and believe that the manufacturer was grossly negligent. In August 2024, a jury rendered a huge award against Harley-Davidson for allegedly failing to adequately repair faulty software on one of its recalled motorcycles. Unfortunately, there was an accident on the repaired motorcycle that resulted in catastrophic injuries and one death. The jury awarded \$240 million in punitive damages and \$47 million for pain and suffering, medical expenses, and loss of consortium.

Kenneth Ross is a Senior Contributor to *In Compliance Magazine* and a former partner and now Of Counsel to Bowman and Brooke LLP. He provides legal and practical advice to manufacturers and other product sellers in all areas of product safety, regulatory compliance, and product liability prevention, including risk assessment, design, warnings and instructions, safety management, litigation management, post-sale duties, recalls, dealing with the CPSC, contracts, and document management. Ross can be reached at 952-210-2212 or at kenrossesq@gmail.com. Ken's other articles can be accessed at <https://incompliancemag.com/author/kennethross>.



By Kenneth Ross, Senior Contributor

Of course, Harley believes that the accident had nothing to do with the original repair and they plan to appeal. The message here is that if you repair or replace the product instead of refunding the purchase price, you had better be confident that the fix or replacement is adequate and that you have good evidence that it is safe.

Given the variables for determining the adequacy and effectiveness of a recall program, it is difficult to come up with definite strategies for defending the recall. The best recall most likely will not cut off liability for the manufacturer for selling a defective product. And, given the fact that most recall notices admit that the product is defective, defense counsel needs to look elsewhere for a good defense.

Of course, the best approach would be to keep the recall from being introduced into evidence. While you can argue that the recall is a “subsequent remedial measure” and should not be allowed into evidence to prove that the product was defective, a good plaintiff’s attorney can somehow get the recall into evidence or find an expert to argue that the product should have been recalled. In fact, it may be beneficial to the manufacturer to affirmatively place the recall into evidence as proof of the manufacturer’s commitment to safety and the well-being of its consumers.

Having the recall in evidence would be necessary to use some of the other possible defenses. The best one is that the recalled product or part of the recalled product that was defective did not cause the injury or damage. Of course, the existence of the recall, if it gets into evidence, will muddy the facts, and may result in liability even without causation.

The next good defense would be that the consumer saw the message or received the notice and ignored the recall. While it may be hard to prove that the injured

party assumed the risk, this argument should at least help establish some contributory fault on the part of the injured party. When using this defense, it is imperative to be able to prove that the “warning” in the letter or notice was adequate, using general warning principles.

If the recall is to be performed by an intermediary such as a dealer or retailer, and they did not do it adequately, the manufacturer might be able to pass along some or all the liability to that entity. For example, in one case that I worked on, a propane gas dealer was held liable, and the manufacturer was absolved because the dealer did not send out the manufacturer’s recall letters to their customers after promising to do so.

The dealer’s failure to send out the letters constituted a superseding, intervening cause. Similarly, a retailer’s failure to remove recalled products from the shelves and warehouse, or failure to place the recall notice in a conspicuous place may also constitute some contributory fault or intervening cause, thus reducing or eliminating liability for the manufacturer of the defective product.

If you cannot break the causal link, then you must defend the adequacy of the specific recall or post-sale program. Since the recall was presumably not effective for the injured party, the plaintiff will argue that the manufacturer could have and should have done more. The manufacturer will have to evaluate the techniques it employed, the effectiveness rates as compared to others for comparable products, explain the effectiveness rate in the context of limitations to increasing the rate, and discuss why doing more would not have necessarily increased the rate or guaranteed that the recall notice would have been received and heeded.

An analysis of past punitive damage awards clearly shows that the basis for most such awards is that the jury believed that the manufacturer failed to undertake

adequate post-sale remedial measures such as a recall. Hopefully, at a minimum, the manufacturer can develop and implement a reasonably effective recall which will minimize or prevent the possibility that punitive damages will be awarded.

U.S. PIRG REPORT ON RECALL REMEDIES

On January 11, 2024, U.S. Public Interest Research Group (PIRG), a public interest advocate, issued a report¹ describing how difficult some companies make it to get a refund or repair on a recalled product. The report starts off by saying that in 2023, there were 323 consumer product recalls done in cooperation with the U.S. Consumer Product Safety Commission (CPSC).

PIRG claims that more than half of these recalls required consumers to undertake what they deem unnecessary actions to get a refund. These actions include returning the product to the store or shipping it back to the manufacturer. They also include registering the product on the company's website, sending a photo and maybe proof of purchase to confirm that the product is among those being recalled, and then disabling the product in some fashion so it can't be used in the future and sending the company a photo of the disabled product. And then the consumer may only get a partial refund or a credit or voucher towards the purchase of another product from the manufacturer. These actions need to be approved by the CPSC and imposed on the consumer to ensure that they have disabled or discarded the unsafe product.

Of the 323 recalls studied by PIRG, half offered just a refund and half offered a replacement or repair. Also, manufacturers offered any of the three remedies in only around 10% of these recalls. PIRG found that of these 323 recalls, only about 6-10% of the recalled products were returned or discarded. They attribute this partly to the difficult requirements imposed by the manufacturer.

PIRG gave an example of this difficulty as follows:

Burdensome recall processes have been a problem for many years. The outrage accelerated in 2019 after Fisher-Price recalled 4.7 million Rock 'n Play Sleepers after 30 infant deaths were connected to the inclined sleeper. Fisher-Price ordered refunds only to customers who'd purchased the product within the last six months if they sent pieces of the sleeper and proof of purchase. Families with products

older than six months were given vouchers to use toward buying another Fisher-Price product. The sleepers cost \$40 to \$149. Consumers, advocates, and policymakers found the vouchers offensive and insensitive, considering the sleepers were linked to infant deaths.

For a variety of reasons, the number of sleepers returned was astonishingly low. The belief was that at least some consumers didn't want the hassle of returning the sleepers, only to get a voucher for another product. Because of the low return numbers, the recall was reannounced in January 2023. By that time, an additional 70 infant deaths were connected to the Fisher-Price sleepers, for a total of about 100. That included at least eight deaths that happened after the April 2019 recall.

PIRG goes on to analyze in detail the remedies offered by companies and concludes with recommendations for manufacturers, retailers, the CPSC, and Congress to make the remedies easier to obtain in a timely fashion.

As we've already discussed, one of the defenses to these cases is that the consumer received the recall notice but did not follow through with the proposed remedy. The more difficult the company makes it for the consumer to obtain the remedy, the less viable this defense might be in front of a jury.

NO-INJURY CLASS ACTIONS

Another series of lawsuits that have been filed because of recalls involve class actions alleging that the recall remedies are inadequate and do not make them whole, and therefore the consumer has suffered some economic loss. These lawsuits can be filed even though there have been no incidents resulting in injury or damage. Most of the class-action lawsuits filed for an "inadequate remedy" have been against automobile manufacturers who have recalled their products. However, there have been a number of cases filed against consumer product manufacturers and the number seems to be growing in the U.S. and also in Canada.²

In August 2024, a class action was filed in New York against Samsung Electronics America. Samsung had announced a recall six days before this lawsuit was filed. The recall concerned the front-mounted heat control knobs of recalled ranges that can be activated by accidental contact by humans or pets, posing a fire hazard. The remedy provided by Samsung was as follows:

Consumers should contact Samsung to receive a free set of knob locks or covers compatible with their model of electric slide-in range to install. Consumers using the recalled ranges without knob locks or covers are cautioned to keep children and pets away from the knobs, to check the range knobs to ensure they are off before leaving the home or going to bed, and to not leave objects on the range when the range is not in use.

The plaintiffs allege that the ranges are still dangerous and seem to be asking for a full refund for the range instead of just receiving new covers.

Another case filed in 2023 was brought against a bicycle parts manufacturer. The complaint states:

Even though Shimano has finally acknowledged the widespread issue, it is working hard to limit the cost of fixing the issue at the expense of consumers. Rather

than offering to issue refunds or replacements for all of the Defective Cranksets, Shimano has taken the unconscionable position that only “(c)onsumers whose cranksets show signs of bonding separation or delamination during (an) inspection will be provided a free replacement crankset . . . that the dealer will professionally install.”

The plaintiffs go on to allege:

This proposed remedy is a nightmare for riders and bike shops. Owners are left without usable bicycles while they get in line with hundreds of thousands of other impacted cyclists to schedule and await an inspection. When the inspection finally happens, a local bicycle mechanic is tasked with making a complex engineering judgment to determine whether the crankset shows sufficient deterioration to merit replacement.



UNRIVALLED PRODUCT SAFETY TESTING CAPABILITY REDUCE RISK AND TIME TO MARKET



Element is a world-leading testing and certification provider for product safety. From consumer electronics to medical devices, our global network of local experts support manufacturers navigating the complexity of global regulations, simplifying and streamlining your products journey to market.



SCAN ME

The plaintiffs conclude by alleging that:

Plaintiffs and the other Class members were deprived of having a safe, defect-free crankset installed on their bicycles, and Defendants unjustly benefited from the sale of these products and from the unconscionable limitations on the recall remedy now offered.

Plaintiffs are asking for reimbursement of all their expenses because of this recall, which would include a refund for the purchase price of the defective crankshaft. Of course, the bigger part of any settlement or verdict will be for attorney's fees.

There was a recent settlement of class action lawsuits filed against Fisher-Price for its recall of Rock 'n Play Sleepers in 2019. There had been sixteen class actions filed in thirteen states all alleging, in part, that the recall was deficient because a full refund was not offered to all consumers. For some consumers, Fisher-Price offered vouchers for other Fisher-Price products. The settlement established a fund of \$19 million to reimburse consumers who are being asked to disable their product and file a claim to receive a cash refund of some of the purchase price.

Most recently, in a recall by Fisher-Price announced on October 10, 2024, CPSC Commissioner Trumka issued a statement criticizing the details of the recall. Fisher-Price is asking consumers to remove parts of the product and if they do, they can receive a \$25 cash payment. Commissioner Trumka says that this offer is not adequate because the product is still unsafe, and that Fisher-Price should be offering a full refund of \$160 and ask the consumer to destroy the entire product.

Not surprisingly, on October 17, 2024, a class action lawsuit was filed in New York, alleging in part that:

Despite the recall involving companies with billions of dollars in revenue each year (Mattel and Fisher-Price) and an incredibly dangerous safety hazard (suffocation/death), the recall provides only \$25 in potential relief to consumers, and that is only if consumers "remove and destroy the headrest and body support insert."

It goes on to say:

This recall was immediately panned by consumer safety experts. CPSC Commissioner Richard Trumka stated that "the flawed recall that Fisher-Price is announcing today is doomed to fail and will keep many babies in harm's way...", noting that Fisher-Price was continuing to urge consumers to use the swing so long as infants are not sleeping in it and the headrest and body support inserts are removed. Commissioner Trumka wrote that he had "no doubt that if these products remain in homes, many consumers will still use these products for sleep because they have received conflicting instructions over time," citing a Fisher-Price YouTube video from 2015 stating that the Products were safe for naps.

He ended his letter thusly: "Fisher-Price can do more to save babies' lives—I think it needs to. And I firmly believe that consumers should demand more from this company."

There are other significant class actions described in a blog posting by a law firm that specializes in filing class actions for recalled products.³ The blog posting is titled *The Relationship Between Recalls and Class Action Lawsuits* and it describes in detail a class action that involves a \$758 million settlement in 2020 concerning engine fires in Hyundai and Kia vehicles and claims that the recall was too narrow and the remedy not adequate.

And food sellers are also seeing class actions filed after most food recalls are undertaken.⁴ These lawsuits typically seek reimbursement of the purchase price of the product, various penalties available to consumers who have allegedly been defrauded, and exorbitant attorneys' fees.

WHAT SHOULD YOU DO?


Obviously, you need to do whatever is necessary to not have a recall. However, once a recall or other post-sale program is being developed, the manufacturer must make a serious assessment of what can be done to minimize the risk of future incidents and what program will be most effective and defensible. This is difficult in that a full refund program can be very expensive and many times, not necessary. However, it may make sense to consider offering a refund as one option to head off any criticism of the recall by a plaintiff's attorney, a CPSC commissioner or a consumer publication like Consumer Reports.⁵



CONCLUSION

Manufacturers need to be prepared to recall their products even if they have never had to do so in the past. Once a product safety issue arises, it is too late to develop a plan. Preparing for a recall before it occurs can significantly increase its effectiveness and lessen the costs and disruption. Of course, the manufacturer also needs to employ proactive pre-sale product liability prevention techniques so that a recall is not necessary in the first place.

It is clear that governments around the world will focus more on identifying product safety problems and forcing or encouraging manufacturers to do something about them. Keeping up with the state of the art will require paying attention to what other companies are doing and what government agencies are requiring.

This vigilance will pay large dividends. Manufacturers should not assume that their effectiveness rates are static and can't be improved. Technology is available today that could increase their ability to quickly communicate with the distribution chain and even consumers about the recall. They should continually look for ways to significantly improve the success of their recalls and other post-sale remedial programs. Hopefully, this will minimize risks and the potential for accidents and provide some type of defense if an accident happens. 

ENDNOTES

1. <https://pirg.org/edfund/resources/too-much-to-recall>
2. <https://www.osler.com/en/insights/updates/what-if-you-face-a-class-action-even-though-no-one-was-harmed>
3. <https://www.classaction.org/blog/the-relationship-between-recalls-and-class-action-lawsuits>
4. <https://www.food-safety.com/articles/10115-widening-recalls-and-class-action-lawsuits-alarmed-recall-trends-in-2024>
5. <https://www.foley.com/insights/publications/2024/08/can-a-voluntary-consumer-product-safety-commission-recall-short-circuit-costly-class-action-litigation>

SGS

When you need to be sure



**We'll be at
IEEE ISPCE
May 13-15
Booth #8**

When it comes to **product safety and compliance**, you can't afford to take shortcuts

As the world's leading Testing, Inspection and Certification company, we help organizations to comply with safety and EMC standards for US, Canada, EU and regions worldwide. Our testing services include:

- EMC
- Medical EMC
- Medical Device Safety
- Wireless Coexistence
- RF Exposure (SAR)
- EMC On-Site
- General Product Safety
- IP Testing
- CE
- Field Evaluation

Contact us to learn more about our product safety and compliance services at **ee.global@sgs.com**.



DEVELOPING THE DYNAMIC HAZARD-BASED SAFETY ENGINEERING BY INTRODUCING THE CONTROL-ORIENTED MODEL

By Shun Zhang, Haiwen Lu, Brent Taira, and Daniel Barsotti



Editor's Note: The paper on which this article is based was originally presented at the 2024 IEEE Product International Symposium on Product Compliance Engineering (ISPCE), held in Chicago, IL in April-May 2024, where it received the 2024 Best Paper Award. It is reprinted here with the gracious permission of the IEEE. Copyright 2025, IEEE.

INTRODUCTION

The International Electrotechnical Commission (IEC) has established the IEC 62368-1 standard, grounded in hazard-based safety engineering (HBSE) principles, as a pivotal framework for the design and evaluation of audio, video, and information and communication technology (ICT) equipment. HBSE emphasizes the identification and mitigation of risks by evaluating the safety of a product under normal operating, abnormal operating, and single-fault conditions, as well as acknowledges a variety of potential hazards. This standard organizes energy sources into categories—

electrical energy sources (ES), thermal energy sources (TS), mechanical energy sources (MS), radiation energy sources (RS), and power sources (PS)—based on their capacity for energy transfer and potential harm [1-2].

IEC 62368-1 addresses numerous hazards, including electric shock, mechanical, heat, radiation, chemical, and fire risks. Yet, its current iteration primarily presumes that safety mechanisms are built-in or are physical hardware safeguards, with minimal explicit focus on control-based safety, especially where hazard prevention significantly depends on or is facilitated by software. In the digitalization and Internet of Things (IoT) era, where software increasingly governs devices—including vital safety functions like overtemperature protection, fire prevention, and other types of hazard monitoring and control—this oversight in considering software's role in safety assurance demands thorough examination [3-4].

Shun Zhang is a hardware engineer at Cisco Systems (China) Research and Development and can be reached at shunzhan@cisco.com.

Haiwen Lu is a compliance program manager at Cisco Systems (China) Research and Development and can be reached at haiwlu@cisco.com.

Brent Taira is an engineering manager, NEBS, Safety and Homologation at Cisco Systems and can be reached at btaira@cisco.com.

Daniel Barsotti is a technical leader of hardware engineering at Cisco Systems, and can be reached at dbarsott@cisco.com.

After an extensive literature review [5-14], the authors first propose a concept of the “Composition-Based Safety View” in this field, which explains the nature and characteristics of safety at a product level. Figure 1 provides an overlap infographic to illustrate the connotation of this concept.

As it shows, there are three overlapped areas that still need to be covered by IEC 62368. More specifically, the ① represents those functional-safety related software not affected by remote communications through the public network; the ② represents those functional-safety related software that also can be affected by remote communications through the public network; the ③ represents those non-functional-safety related software that can affect the HBSE evaluation results, and also can be affected by remote communications through the public network, e.g., the remote software update involves the changes of the safety-critical operating parameters (e.g., the RPM or duty cycle) of DC fan which running at a constant speed during normal operating condition.

This paper argues that the current HBSE standard exhibits a deficiency in encompassing software or control-oriented safety assessments, leaving a vital facet of product safety unexplored and heightening the potential for safety incidents arising from software malfunctions or systemic failures. The exploration of introducing the control-oriented model into HBSE is essential for achieving comprehensive product safety in the software-

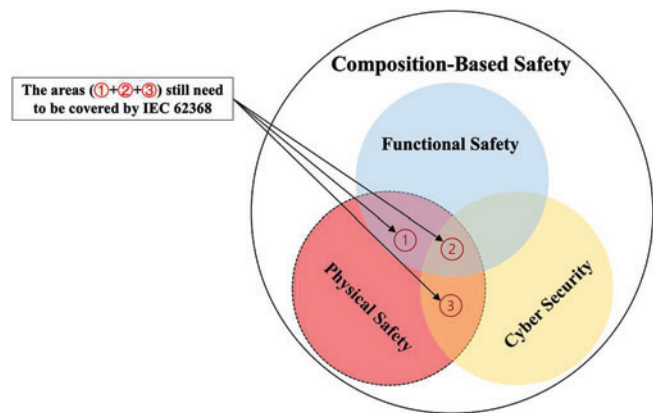


Figure 1: Overlap infographic to illustrate the concept of “composition-based safety view” (Source: proposed by the authors)

driven era. This investigation aims to address this fundamental oversight and bridge the identified gap.

TYPICAL MODULAR SWITCHING FAN TRAY DESIGN AND HAZARD ANALYSIS

Figure 2 is a typical modular switching fan tray control board design. Based on the current IEC 62368-1 requirement, individual fan locking should be conducted. Generally, for the usual stuck and single fan disable cases, one fan failure doesn't impact other fans' functioning; the system will continue to operate without

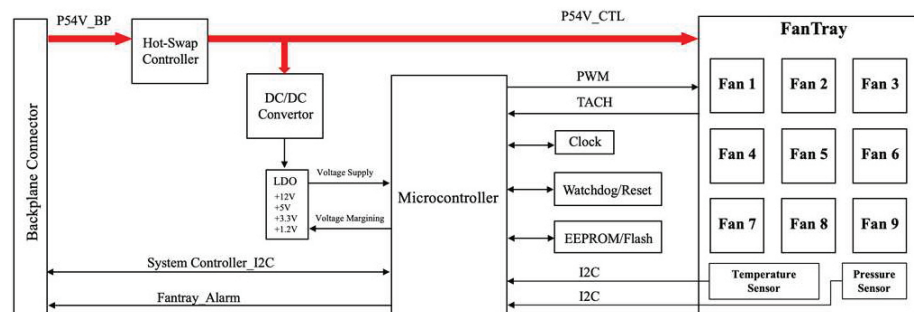


Figure 2: Block diagram of the fan tray (Source: drawn by the authors)

significant degradation in cooling. However, if the fan is short internally, the power bus (i.e., P54V_CTL) will be short as well. To protect the whole system, the hot-swap acts to turn off the whole fan tray’s power entry, which makes all fans stop spinning.

In this situation, the temperature of the chassis will increase rapidly as there is no forced cooling, and overheating will happen. To avoid fire hazard or thermal hazards, the microcontroller must report the issue to the system (global) controller (i.e., CPU) through I²C (inter-integrated circuit) immediately, then the CPU makes the decision and sends a power-off command to the power supply via PMBus (power management bus), shuts down the chassis timely. The fact is that more and more protection designs in ICT equipment rely on the microcontroller/processor, which involves a “hardware + software” combination protection. Unfortunately, IEC 62368 doesn’t provide any information regarding how to evaluate the integrity and robustness of such control-based protection.

Based on ISO/IEC Guide 51 [15], the definition of safety is “freedom from unacceptable risk,” while risk is a “combination of the probability of occurrence of harm and the severity of that harm.” Harm is “injury or damage to the health of people, or damage to property or the environment,” and hazard is “potential source of harm.” Therefore, during the product safety evaluation, all hazards should be identified first, then the risk caused by the hazard should be assessed quantitatively or qualitatively. Finally, appropriate technical and management measures should be implemented to reduce the risk to an acceptable level. Many methods are available for hazard analysis and risk

assessment (HARA). The current mainstream hazard analysis methods or tools include bow-tie analysis (BTA), event tree analysis (ETA), and layer protection analysis (LOPA). Moreover, some time-dependent approaches are suitable for capturing dynamic states and complex systems like Markov Analysis, Petri Nets, and Monte Carlo simulation. However, as this paper focuses on ICT equipment safety assessment,

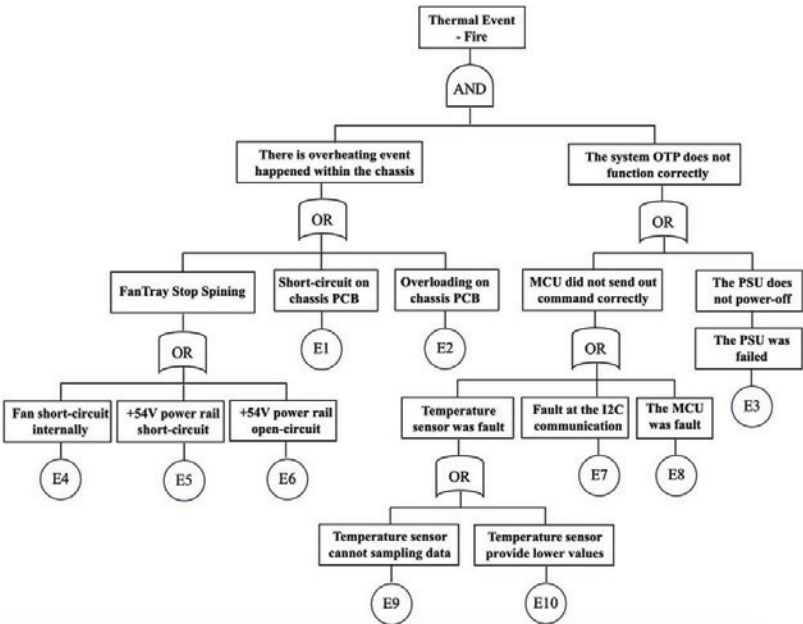


Figure 3: An example of fault tree analysis (FTA) for the thermal event of fire (Source: created by the authors)

Fault Identifier	Items/ Functions	Potential Failure Modes	Potential Failure Effects	Severity (S)	Potential Failure Causes	Occurrence (O)	Current Preventions	Current Detections	Detection (D)	RPN (1-9)	Fault Recovery Measure
1	Backplane Connector	Pin Short-circuit	FanTray power off, no cooling for system	Critical	Incorrect installation, overstress	Low	HIG, connector derating	I2C NACK	Always	3	Send alarm, and shutdown chassis when necessary
2	Backplane Connector	Pin Open-circuit	FanTray power off, no cooling for system	Critical	Component damaged, overstress	Low	Derating guidelines per IPC9592	I2C NACK	Always	3	Send alarm, and shutdown chassis when necessary
3	54V Hotswap Controller	Breakdown	FanTray power off, no cooling for system	Critical	Component damaged, overstress	Low	Derating guidelines per IPC9592	I2C NACK	Always	3	Send alarm, and shutdown chassis when necessary
4	DC/DC converter	Breakdown	No power for MCU	Major	Component damaged, overstress	Low	Derating guidelines per IPC9592	I2C NACK	Always	2	Send alarm, monitor temp, shutdown chassis
5	LDO	Breakdown	No power for MCU	Major	Component damaged, overstress	Low	Derating guidelines per IPC9592	I2C NACK	Periodic	2	Send alarm, monitor temp, shutdown chassis
6	Microcontroller	Breakdown	Registers stuck at 0 or 1	Critical	HW random failure or SW fault	Low	Follow MCU application guideline	POST or periodic BIST	Always	3	Reset, send alarm, shutdown chassis if necessary
7	DC Fan	Fan stucked and cannot spin	Increase other Fans' speed	Major	Bearing damaged due to random aging effect	Random	Qualified by IPC9591 and Safety Agency	TACH feedback	Always	4	Send alarm, and shutdown chassis when necessary
8	Temperature Sensor	Breakdown	Sampling out of range, Fan run abnormally	Critical	Environment, random failure	Low	Application per Spec/Datasheet	Temp readout via I2C	Periodic	6	Send alarm, and shutdown chassis when necessary
9	Pressure Sensor	Breakdown	Sampling out of range, performance degraded	Minor	Extream Environment, random failure	Low	Application per Spec/Datasheet	Altitude readout via I2C	Periodic	2	Send warning
10											

Table 1: An example of failure modes and effects analysis (FMEA) for the fan tray (Source: created by the authors)

the following three approaches will be introduced as they are more suitable in practice: fault tree analysis (FTA); failure modes and effects analysis (FMEA); and hazard and operability studies (HAZOP).

Fault Tree Analysis (FTA)

Fault tree analysis (FTA) is a systematic, deductive, and hierarchical risk assessment method used to identify potential causes of system failures within safety engineering [16]. This analytical technique visualizes the pathways through which various subsystems or components can lead to a top-level failure event, using a tree-like structure of logical symbols that represent the interrelationship between failures, external factors, and human errors.

In the HBSE context, FTA can provide a rigorous means to dissect the large core switching fan-tray architecture design and its associated failure modes. By mapping out all or most conceivable failure scenarios, FTA aids in pinpointing critical control points where the control-based model can effectively mitigate risk. It enables the identification of both random hardware failures and systematic failures that may arise from hardware and software interactions, thereby offering a comprehensive view of potential hazards. The figure below shows the FTA for the thermal event of fire by the modular switching chassis.

Failure Modes and Effects Analysis (FMEA)

Failure modes and effects analysis (FMEA) is another popular engineering technique for identifying potential failure modes and evaluating their impact on system safety [17]. It prioritizes risks based on severity, occurrence, and detectability. Despite its efficacy, FMEA encounters challenges in complex, control-oriented systems like the large core switching fan-tray architecture. Specifically, it may not fully capture concurrent failures or the intricate interactions between hardware and software, which are critical in modern systems.

Nonetheless, FMEA is invaluable for creating a comprehensive inventory of possible failure modes for each component within the system, facilitating an in-depth analysis of their causes and effects. This process enables the identification of critical controls and safeguards to mitigate system failures.

To address its limitations, integrating FMEA with other methodologies, such as FTA or simulation tools, can provide a more holistic understanding of system vulnerabilities, including those from hardware-software interplay and concurrent failures. While FMEA faces limitations in analyzing the control-oriented model, it remains integral to identify failure modes, and guiding effective mitigation strategies is crucial for hazard-based safety engineering, ensuring safety through comprehensive risk management strategies.

Hazard and Operability Studies (HAZOP)

Hazard and operability studies (HAZOP) is a tool used to identify potential system hazards and operational issues that cause deviations (or failure points) from design objectives. It was initially used to analyze process control systems in chemical plants but has since extended to other types of systems, including complex control systems and software-intensive designs [18]. HAZOP is a qualitative hazard analysis technique based on specific guide words (GW) such as “more,” “less,” “no,” “reverse,” and “delay,” alongside various critical parameters (e.g., power, speed, temperature, pressure). This approach allows for the thorough and systematic identification of design flaws that could lead to hazards or operational issues early in the product development phase. Guide words are utilized at each node or function, serving as a catalyst

EMC PARTNER **A STRONG PARTNERSHIP** **HVT TECHNOLOGIES, Inc.**

INS SERIES

FOR THE SAFETY OF ELECTRIC VEHICLE CHARGING SYSTEMS

PRECISION YOU CAN TRUST

The IEC 61851-1 Ed.3 standard ensures the safety and reliability of EV charging systems. The INS-1250 from EMC PARTNER simplifies compliance by delivering precise insulation testing, ensuring system integrity.

www.emc-partner.com

- 7.5kV, 15 kV or 30kV Version available
- For IEC 61851-1 Safety Testing
- 1.2/50µs Insulation Test as per IEC 60664-1
- Current & voltage integral measurements
- Integrated report handling

HVT TECHNOLOGIES, Inc. Your contact for North America **www.hvtechnologies.com** Mail emcsales@hvtechnologies.com Phone 703-365-2330

for team members to identify any possible causes and consequences and determine whether existing safeguards protect the product well.

Table 2 provides an example to illustrate the HAZOP application for the fan speed-up function. The HAZOP can be applied for any safety-critical functions.

In summary, based on the above-mentioned hazard analysis results, lots of hazard prevention depends on the related control functions being executed correctly. Therefore, introducing control-oriented safety analysis into the existing HBSE framework is imperative and necessary, to ensure comprehensive safety assessment in the new era.

INTRODUCING THE CONTROL-ORIENTED MODEL INTO HBSE

Time–The Key Element for Control-Oriented Safety

The element of “time” is foundational for the control-oriented models and functional safety assessments [19–25], acting as a pivotal element in ensuring timely responses to hazardous events. Time factors such as fault-tolerant time interval (FTTI), fault detection time interval (FDTI), and diagnostic test intervals (DTI) are integral to designing safety functions or products that prevent hazardous accidents. The product or system must detect and respond to potential hazards within defined time limits to mitigate risks effectively. Some existing safety standards have defined and listed these time-related parameters. Key temporal factors include:

Fault tolerant time interval (FTTI): Originally defined by ISO 26262-1, FTTI represents the maximum allowable time between the occurrence of a fault and the point at which the system must detect and respond to the fault to prevent unsafe conditions. This interval is critical for safety applications and reflects the urgency and efficiency of the safety mechanisms activated.

ID.	HAZOP GW	Malfunction	Product-Level Hazard
F1-1	No	No change on Fan speed	Overheating
F1-2	More	Fan speed-up more than intended	No Hazard
F1-3	Less	Fan speed-up less than intended	May Overheating
F1-4	Reverse	Fan speed-down	Overheating or Fire
F1-5	Too-late	Fan start speed-up later than intended	May Overheating
F1-6	Too-early	Fan start speed-up earlier than intended	No Hazard
F1-7	Unexpected	Fan speed intermittently changes	May Overheating
...

Table 2: An example of hazard and operability (HAZOP) studies application for the fan speed-up function

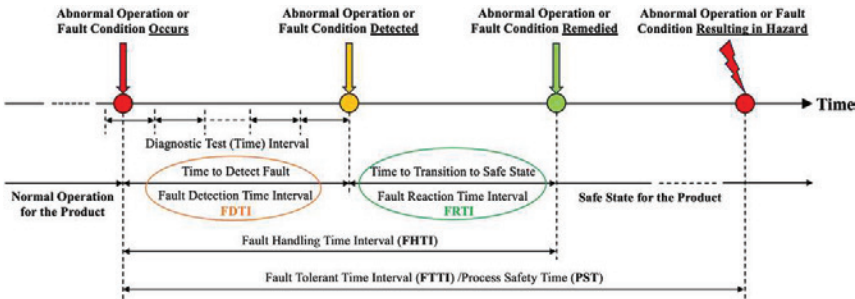


Figure 4: Illustration of several time concepts related to safety (Source: summarized by the authors based on ISO 26262-1 and IEC 61508-4)

Energy Source Types	Classification parameter	Contains “Time”?	Potential gaps (define Hazard duration or Response time)
Electrical energy source	“Prospective touch voltage + Touch current” for steady state ES1 and ES2 classification	No (except pulse duration for single pulses and pulses off times for repetitive pulses)	Can refer IEC 60479 to determine the duration limit for steady state ES1 and ES2
Power source	“Power available + Duration” for PS1 and PS2 classification	Yes	Can use 3s and 5s to determine the FTTI
Hazardous substance	No classification yet	No	Can refer to research from other disciplines or conduct experiments to use “concentration + exposure duration” to define each type of hazardous substances and classification
Mechanical energy source	“RPM + K-factor” for moving fan blades MS1 and MS2 classification; “Equipment mass + mounted height” for Wall/ceiling mount MS1 and MS2 classification	No	Can add the definition for Energy Degrade Time and Hazard Exposure Time for the moving parts such as fan blades
Thermal energy source	“Accessible parts material + Expected touch duration” for TS1 and TS2 classification	Yes	Can use the expected touch durations (e.g., 8h, 1min, 10s, 1s) to determine FTTI
Radiation energy source	Mainly rely on the original safety standard of specific radiation, such as IEC 60825 for Laser, IEC 62471 for Lamps and LED	No (except the sound exposure for dose-based systems)	Can refer to the specific radiation source safety standards (e.g., IEC 60825 specifies the “time base” for Laser classification) to determine the duration of maximum permissible exposure (MPE) or accessible emission limit (AEL) for each type of radiation source and classification

Table 3: Summary of the “time” element consideration in each energy source classification (Source: created by the authors)

Process safety time (PST): As outlined by IEC 61508-4, PST refers to the time available to bring a process to a safe state before the hazardous event occurs. This interval is crucial in industrial control systems, where delays in response times can lead to significant safety incidents.

Fault handling time interval (FHTI): This metric quantifies the time taken to manage and mitigate a fault once detected, encompassing the processes of fault identification, isolation, and system recovery or failover to a safe state.

Fault detection time interval (FDTI): This interval measures the time from the onset of a fault to its detection by the system's diagnostic mechanisms. Rapid fault detection is essential to minimize the exposure to potential hazards and initiate timely corrective actions.

Fault reaction time interval (FRTI): This denotes the time required for a system to react to a detected fault, implementing necessary measures to maintain safety. This interval is critical for ensuring systems can effectively counteract faults before they escalate into unsafe conditions.

Diagnostic test (time) interval: This refers to the scheduled or on-demand execution of diagnostic tests designed to detect latent faults within the system. The frequency and timing of these tests are vital for maintaining an ongoing assessment of system health and ensuring high safety availability.

Figure 4 provides a clear illustration of several time concepts related to control-oriented safety.

"Time" Consideration in HBSE

In the current hazard-based safety engineering (HBSE) standard (i.e., IEC 62368-1), the consideration of the element of "time" shows a fragmented state when conducting hazard analysis and risk assessment (HARA). This inconsistency is evident in the definition and classification of different hazardous energy sources within the standard. While "time" is explicitly considered in the context of certain hazards, such as those associated with fire (power sources) and thermal risks (thermal energy sources), it is notably absent

or not directly emphasized in the definitions and classifications of other hazard sources. These include electric shock hazards (electric energy sources), the dissemination and contact with hazardous substances, mechanical injury (mechanical energy sources), and radiation injury (radiation energy sources) [26–27].

Although some static energy sources, such as the surface sharpness of equipment, are difficult to relate to the concept of "time." There is a clear opportunity for the other dynamic energy sources to incorporate "time" into risk evaluations more systematically. This would involve acknowledging the temporal dynamics of hazard exposure, energy change, personal response, etc. Table 3 summarizes the "time" element consideration in each energy source classification by IEC 62368-1, which also provides insight for extending and refining the existing energy source classification in the future standard development and update.

Comparisons Between Traditional HBSE and D-HBSE

As Figure 5 on page 32 shows, the current HBSE framework does not fully account for the temporal dynamics of energy sources. It fails to capture the "state changes" that occur either due to autonomous changes in the energy sources over time or due to the enforced changes imposed by control models. This oversight can lead to an incomplete assessment of the dynamic characteristics of hazards.



PERMANENT ESD PROTECTION

- Meets ANSI / ESD specifications for ESD protection
- Operating temp of -60° to 250° F
- Inherent fiberglass strength and durability

A VARIETY OF ESD - SAFE TRAYS & CONTAINERS AVAILABLE

Made in the USA PH 814-683-4500
www.mfgtray.com

MFG TRAY

Developing the new dynamic hazard-based safety engineering (D-HBSE) by introducing the control-oriented model which acts as a safeguard. It forms a closed control loop by connecting energy transfer paths with signal transfer paths together. The D-HBSE enhanced the original HBSE model as it allows for:

Continuous monitoring and adjustment: The control model can continuously monitor the state of the energy sources and adjust their operation to maintain safety, accounting for the temporal variability of hazards.

Predictive analysis: By incorporating time-based data and control model outputs, the D-HBSE can predict potential hazard states before they occur, enabling preemptive action.

Adaptability and flexibility: The control model enables the system to adapt to both anticipated and unforeseen changes over time, ensuring long-term safety and reliability.

To facilitate a clearer and more intuitive understanding of the features of existing HBSE and the D-HBSE, Table 4 provides a detailed comparison of their respective protection mechanisms. While the HBSE offers a more diverse array of protection mechanisms, they are predominantly confined to physical forms, which are more passive and reactive. On the other hand, the control-oriented protection added by D-HBSE is more straightforward and direct, with simplicity and proactivity.

It is important to emphasize that dynamic hazard-based safety engineering (D-HBSE) does not seek to replace the existing HBSE framework. Rather, it is fully compatible with and inherits

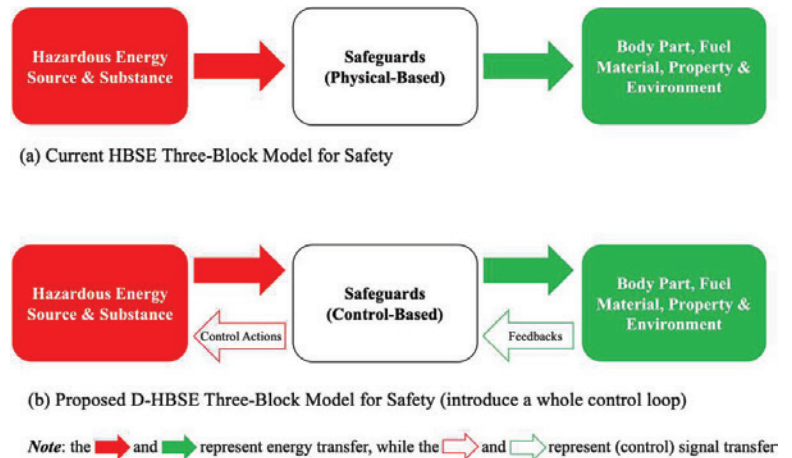


Figure 5: Three-block model comparisons between current HBSE and proposed D-HBSE (Source: created by the authors)

Hazardous Energy Source (Response to energy class)	Protective Means (Safeguards) Comparisons	
	HBSE Model (Reactive, and Reliability-based)	D-HBSE Model (Proactive, and Control-oriented)
Electrical energy source (Electric shock)	<ul style="list-style-type: none"> • Electrical enclosure • Spacing (clearance, creepage) • Insulation materials (solid, liquid) • SPD to reduce overvoltage/transient • Bleed resistor for capacitor discharge • Add impedance of energy transfer to body • Protective conductors • Etc. 	e.g., Monitor and diagnostic the circuit condition via periodic checks, could sense a fault or accident and disconnect the energy source within a determined brief period (less than FTTL, usually several hundred milliseconds level), to avoid harm (shock) to human.
Power source (Electrically-caused fire)	<ul style="list-style-type: none"> • Fire enclosure • Overcurrent limiters like Fuse, Circuit breaker • High thermal resistance material • Reliable electrical connection • Flammability class (V-0, VW-1, etc.) • Separate combustible material by distance • Separate combustible material by fire barrier • Etc. 	e.g. For a PS3 circuit, monitor the load current and voltage of the power rail continuously; when a short-circuit or overloading happens, both sampling values are over the thresholds set previously, the microcontroller will send a command to the power chip to shut down the power source circuit within 3 seconds.
Hazardous substance (Chemical reaction)	<ul style="list-style-type: none"> • Container integrity and robustness • Personal protective equipment (PPE) • Avoid/reduce the use of hazardous substances • Adequate room ventilation for hazardous gas • Etc. 	e.g., Dedicated gas sensors monitor concentrations of hazardous gases in real-time, when hazardous levels are detected, the control system triggers an alarm, activates the ventilation system, or takes other measures to reduce the risk of exposure
Mechanical energy source (Mechanically-caused injury)	<ul style="list-style-type: none"> • Mechanical enclosure • Finger guards for fan blades • Safety interlock • Manually activated stopping device • Emergency stop system • Etc. 	e.g., The MS3 Fan is designed with an e-Break function; once it is power-off, the fan blades will be forced to stop spinning immediately; it is faster than the action time when a person unplugs the Fan from chassis, which means it is safe enough even without finger guard.
Thermal energy source (Skin burn)	<ul style="list-style-type: none"> • Equipment enclosure • Overtemperature limiters like PTC/PPTC, Thermal-cutoff, Thermal-links, Thermostat, • High thermal resistance material • Etc. 	e.g., use sensors to on-line monitor the temperature for several hot spots on equipment surface, the microcontroller will shut down the corresponding power rail once trigger the temperature limit, to avoid thermal/burn hazard.
Radiation energy source (Radiation-caused injury)	<ul style="list-style-type: none"> • Equipment enclosure • Safety interlock • Dose-based system for sound exposure • Etc. 	e.g., Automatic Laser Shutdown (ALS): In optical fiber communication systems, the state of the optical fiber link was continuously monitored, it will immediately shut down the laser source if detect a broken fiber or disconnected cable, to avoid dangerous levels of laser light exposure
Note: 1. This table only includes equipment safeguards, installation safeguards, and personal safeguards, does not list behavioral safeguards and instructional safeguards as they are not suitable for ordinary person. 2. The item with bold words indicates it is similar or already adopted to the principle of the control-oriented model.		

Table 4: Protective means (safeguards) comparisons between HBSE and D-HBSE (Source: created by the authors)

everything from the existing HBSE, just simply extending the scope by adding the possibility of an additional type of protection mechanism. The D-HBSE enhances the established HBSE by incorporating dynamic elements that are especially relevant in the context of modern systems, which often involve complex interactions between hardware and software.

GUIDELINES FOR IMPLEMENTING AND EVALUATING D-HBSE

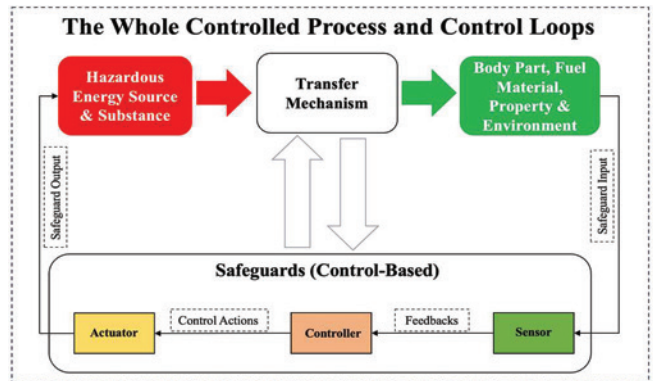
This part will provide guidelines for the implementation of control-based safety, it will be discussed from both hardware and software perspectives. This dual perspective is essential because the integration and interaction between hardware and software are critical to the overall safety of the control-based model.

Hardware Design (Safety Mechanism) and SIL Calculation

Hardware-related safety mechanisms are a crucial aspect of hardware functional safety design and constitute a significant component of the overall safety strategy. Table 5 summarizes the content from IEC 61508-2 Annex A and ISO 26262-5 Annex D, outlining the safety mechanisms and diagnostic coverage rates for potential faults in different components. This provides a foundational basis for subsequent calculations of hardware probability metrics.

Figure 7 is the schematic of temperature sensing circuits, which are part of the fan tray controller board and against the fire hazard.

During the hardware safety development stage, implementing safety mechanisms in the hardware design is just one aspect of ensuring safety. It is also essential to perform probabilistic measures of hardware random failures to ensure that the residual risk associated with the safety



Note: The above model and illustration are just an example. Theoretically, the whole control-based safeguard (i.e., sensor + controller + actuator) can be placed anywhere in the energy transfer path, all 3 parts can even

Figure 6: A simple "control-based safeguard" (i.e., E/E/PE-based safety function loop) (Source: created by the authors)

Components	Safety mechanism/measure (Diagnostic technique/ measure)	Typical diagnostic coverage	See overview of techniques
Sensors	Failure detection by on-line monitoring	90%	IEC 61508-7 A.1.1
Sensors	Input comparison/voting (1oo2, 2oo3 or better redundancy)	99%	IEC 61508-7 A.6.5
Sensors	Sensor valid range	60%	ISO 26262-5 D.2.8.1
Sensors	Sensor rationality check	90%	ISO 26262-5 D.2.8.3
Actuators	Failure detection by on-line monitoring	90%	IEC 61508-7 A.1.1
Actuators	Monitoring of relay contacts	99%	IEC 61508-7 A.1.2
Actuators	Cross-monitoring of multiple actuators	99%	IEC 61508-7 A.13.2
Power supply	Voltage or current control (input)	60%	ISO 26262-5 D.2.6.1
Power supply	Voltage or current control (output)	99%	ISO 26262-5 D.2.6.2
Power supply	Watchdog with separate time base without time-window	60%	ISO 26262-5 D.2.7.1
Power supply	Watchdog with separate time base and time-window	90%	ISO 26262-5 D.2.7.2
Communication	One-bit hardware redundancy	60%	ISO 26262-5 D.2.5.1
Communication	Multi-bit hardware redundancy	90%	ISO 26262-5 D.2.5.2
Communication	Complete hardware redundancy	99%	ISO 26262-5 D.2.5.3
Communication	Timeout monitoring	90%	ISO 26262-5 D.2.5.8
Program sequence (watchdog) & Clock	Watchdog with separate time base without time-window	60%	ISO 26262-5 D.2.7.1
Program sequence (watchdog) & Clock	Watchdog with separate time base and time-window	90%	ISO 26262-5 D.2.7.2
Program sequence (watchdog) & Clock	Combination of temporal and logical monitoring of programme sequence	99%	ISO 26262-5 D.2.7.4
Processing units	Stack over/under flow Detection	60%	ISO 26262-5 D.2.3.8
Processing units	Self-test supported by hardware (one-channel)	90%	ISO 26262-5 D.2.3.2
Processing units	Software diversified redundancy (one hardware channel)	99%	ISO 26262-5 D.2.3.4
Processing units	HW redundancy (e.g. dual-core lockstep)	99%	ISO 26262-5 D.2.3.6

Table 5: Summary of safety mechanism/measure or diagnostic technique/measure for HW design (Source: summarized by the Authors based on IEC 61508-2 Annex A and ISO 26262-5 Annex D)

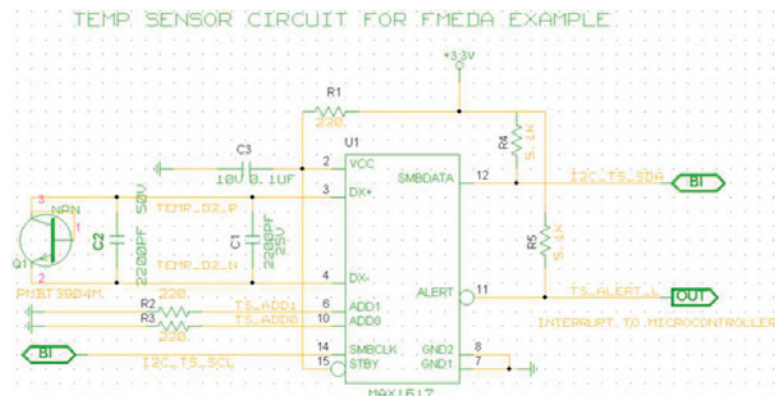


Figure 7: Example schematic of watchdog circuits (Source: drawn by the authors)

function is acceptably low. Failure modes effects and diagnostic analysis (FMEDA) is a valuable tool for performing these quantitative calculations. Table 6 illustrates how FMEDA is used to calculate probabilistic hardware metrics. This paper selects the SFF (safe failure fraction) and PFH (probability of dangerous failure per hour), which are from IEC 61508, as the metric indicator; besides this, the SPFM (single point fault metric) and PMHF (probabilistic metric for random hardware failures) from ISO 26262 can also be used as they are similar.

Software Design and Assessment

The software development should follow the V-model as Figure 8. The V-model is a best practice in the safety-critical software development lifecycle, emphasizing a methodical approach to developing electronic control systems. It delineates a process that begins with the establishment of system requirements and progressively drills down to more granular software requirements, architectural designs, and module designs, forming the descending limb of the “V.” This progression embodies the decomposition of requirements, with each step laying the groundwork for the subsequent phase, ensuring that development is aligned with safety goal and corresponding safety functional requirement.

As the lifecycle advances to the ascending limb of the “V,” the focus shifts towards validation and verification, mirroring the earlier stages of development with corresponding levels of testing. Unit testing examines the smallest parts of the application in isolation, followed by integration testing where these parts are combined and evaluated as a whole. System testing then assesses the complete, integrated system against the defined requirements to ensure compliance. The end of this process

is validation, which ensures the final product meets the intended safety goals and related requirements, the model emphasizes thorough testing and safety assurance from concept to completion.

In the V-model, the concepts of validation and verification are distinct yet frequently conflated. Validation is the process of evaluating software at the end of the development process to ensure

Comp onent	FIT	Safety- related?	Failure model	Distributi on	Failure mode violates safety if no Safety mechanisms?	Have Safety mechanisms?	DC [%]	Dangerous failure rate/FIT	Dangerous undetected failure rate/FIT
R1	5	Yes	Open	20%	Yes	None	0	1	1
			Closed	60%	No				
			Drift 0.5	10%	No				
			Drift 2	10%	No				
R2	3	Yes	Open	20%	Yes	None	0	0.6	0.6
			Closed	80%	No				
R3	3	Yes	Open	20%	Yes	None	0	0.6	0.6
			Closed	80%	No				
R4	2	Yes	Open	20%	Yes	None	0	0.4	0.4
			Closed	80%	No				
R5	2	Yes	Open	20%	No	None	0	1.6	1.6
			Closed	80%	Yes				
C1	4	No	Open	20%					
			Closed	80%					
C2	2	No	Open	20%					
			Closed	80%					
C3	2	Yes	Open	30%	No				
			Closed	70%	Yes	None	0	1.4	1.4
Q1	4	Yes	Open	20%	Yes	None	0	0.8	0.8
			Closed	80%	No				
U1	20	Yes	Safe	50%	No				
			Danger	50%	Yes	SM1	90	10	1
....				
uC	100	Yes	Safe	50%	No				
			Danger	50%	Yes	SM2	90	50	5
Σ 389		Σ 354							Σ 32.6

Total failure rate: 389 FIT
Total Safety-Related: 354 FIT
Total Non-Safety-Related: 35 FIT

$SFF = (\Sigma \lambda_S + \Sigma \lambda_{DO}) / (\Sigma \lambda_S + \Sigma \lambda_{DO} + \Sigma \lambda_{DOE}) = 1 - (32.6/354) = 0.908$
PFH total = 3.26×10^{-8}

Table 6: FMEDA HW architecture metric and random failure assessment calculation (Source: created by the authors)

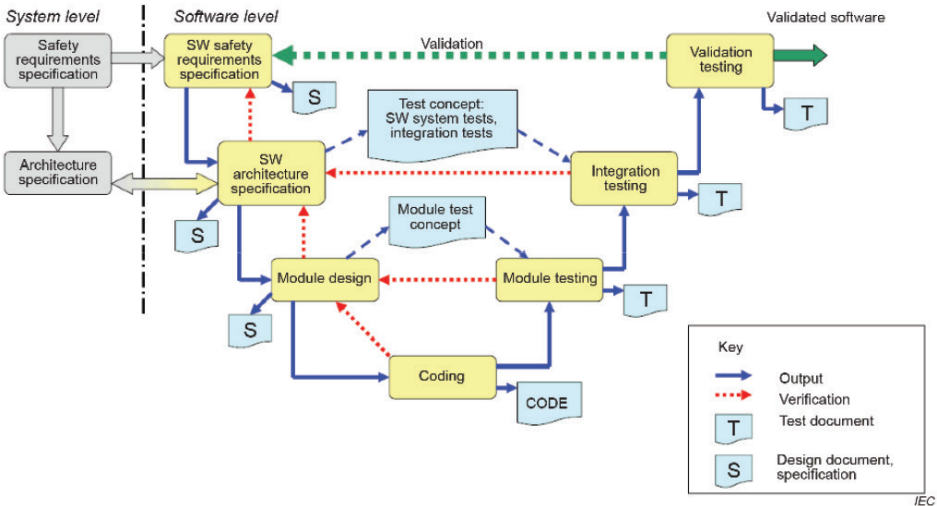



Figure 8: V-Model for the software development lifecycle (Source: reproduced from IEC 60730-1 Figure H.1)

it meets the requirements (safety) for the end user. Verification, on the other hand, occurs throughout the development process. It involves checking that the product is built correctly according to the specifications and design documents. Figure 9 illustrates the differences between verification and validation.

CONCLUSION

The rapid evolution of technology necessitates a reevaluation of product safety principles to establish a more encompassing framework. Upgrading HBSE to dynamic HBSE (D-HBSE) by integrating a control-oriented model is crucial to maintaining the efficacy of safety standards for ICT equipment in light of technological advances.

This paper contributes in three significant ways. First, this is the first time to propose the concept of dynamic HBSE (D-HBSE) and develop the new three-block model by adding the feedback path to implement the whole control loop, which makes the existing HBSE eligible to evaluate those products with software-controlled safety functions. Second, even though the authors have explored how to integrate functional safety into HBSE previously [4], it mainly focuses on the rationale and assessment process, and lacks in-depth gap analysis from a design technical and practical perspective, this paper conducts a detailed and comprehensive comparison of the protective means (i.e., safeguards) between HBSE and D-HBSE, and highlight the “time” element is the key for “dynamic” characteristic in the D-HBSE, meanwhile, propose the potential gaps and future extension directions for each energy source (ES) classification and definitions which were listed in existing HBSE standard. Last, it offers detailed guidelines for implementing and evaluating control-oriented safety functions within the D-HBSE framework, serving as a valuable resource for engineering design. 

LIMITATIONS

This study, while offering insights into the integration of a control-oriented model with HBSE, recognizes its preliminary nature and identifies avenues for further research. First, the application of control-oriented

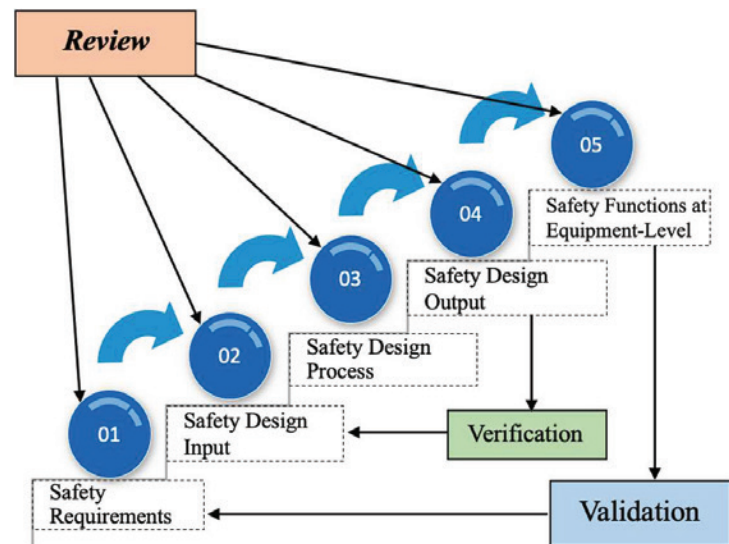


Figure 9: Illustration of the verification and validation process (Source: drawn by the authors)

safety, a relatively novel concept among the increasing complexity of hardware-software fusion in product design, presents challenges. Traditional safety analysis methods like FTA and FMEA may not fully address these complexities, and incorporating advanced methods like STPA into HBSE is a promising yet underexplored area. Second, the current assessment primarily references IEC 61508 and ISO 26262 standards. Future research could extend to other industry-specific standards, such as IEC 60730-1, ISO 13849-1, and IEC 62061 [28-30], which may offer more streamlined evaluation approaches under the IEC 62368 context. Last, as the lines between (cyber)security and functional safety begin to blur, particularly with the increased use of remote-control functions in ICT equipment, integrating cybersecurity evaluations into HBSE frameworks remains an essential research topic, especially where safety-related data communication is concerned.

ACKNOWLEDGMENT

The authors are very grateful to the International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) for permission to reproduce information from their publications, including IEC 62368, IEC 61508, and ISO 26262 series. IEC and ISO copyright all such extracts, they have no responsibility for the placement and context in which the authors reproduced.

REFERENCES

1. Audio/video, Information and Communication Technology Equipment - Part 1: Safety Requirements, IEC 62368-1, Edition 3.0, 2018.
2. Audio/video, Information and Communication Technology Equipment - Part 2: Explanatory information related to IEC 62368-1, IEC/TR 62368-2, Edition 3.0, 2019.
3. Nancy G. Leveson. Engineering a safer world: Systems thinking applied to safety. The MIT Press, 2016.
4. Shun Zhang and Haiwen Lu. Integrating Functional Safety into Hazard-Based Safety Engineering: Towards a Comprehensive Framework. 2023 IEEE International Symposium on Product Compliance Engineering - Asia (ISPCE-ASIA), Shanghai, China, 2023, pp. 1-8, doi: 10.1109/ISPCE-ASIA60405.2023.10365871.
5. Lin Xie, et al. Performance analysis of safety barriers against cascading failures in a battery pack. Reliability Engineering & System Safety, 228 (2022).
6. Yiliu Liu. Risk management of smart healthcare systems: Delimitation, state-of-arts, process, and perspectives. Journal of Patient Safety and Risk Management, 27.3 (2022): 129-148.
7. Sergio Jimeno Altelarrea, et al. STPA enabled safety assessment in the architecting of complex systems. Safety and Reliability. Vol. 41. No. 4., Taylor & Francis, 2022.
8. Ivo Friedberg, et al. STPA-SafeSec: Safety and security analysis for cyber-physical systems. Journal of information security and applications 34 (2017): 183-196.
9. Aibo Zhang, et al. Investigation of the compressed air energy storage (CAES) system utilizing systems-theoretic process analysis (STPA) towards safe and sustainable energy supply. Renewable Energy 206 (2023): 1075-1085.
10. David Marcos, et al. Functional safety BMS design methodology for automotive lithium-based batteries. Energies 14.21 (2021): 6942.
11. Hatice Ceren Ates, et al. End-to-end design of wearable sensors. Nature Reviews Materials 7.11 (2022): 887-907.
12. Yue Wang, et al. Privacy risk assessment of smart home system based on a STPA-FMEA method. Sensors 23.10 (2023): 4664.
13. Marvin Rausand and Ingrid Bouwer Utne. Product safety-Principles and practices in a life cycle perspective. Safety Science 47.7 (2009): 939-947.
14. Nancy G. Leveson. Rasmussen's legacy: A paradigm change in engineering for safety. Applied ergonomics 59 (2017): 581-591.
15. Safety aspects - Guidelines for their inclusion in standards, ISO/IEC Guide51, Edition 3.0, 2014.
16. Fault tree analysis (FTA), IEC 61025, Edition 2.0, 2006.
17. Failure modes and effects analysis (FMEA and FMECA), IEC 60812, Edition 3.0, 2018.
18. Hazard and operability studies (HAZOP studies) - Application guide, IEC 61882, Edition 2.0, 2016.
19. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, IEC 61508-1, Edition 2.0, 2010.
20. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, IEC 61508-2, Edition 2.0, 2010.
21. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, IEC 61508-3, Edition 2.0, 2010.
22. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations, IEC 61508-4, Edition 2.0, 2010.
23. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels, IEC 61508-5, Edition 2.0, 2010.
24. Road vehicles - Functional safety - Part 1: Vocabulary, ISO 26262-1, Edition 2.0, 2018.
25. Road vehicles - Functional safety - Part 5: Product development at the hardware level, ISO 26262-5, Edition 2.0, 2018.
26. Safety of laser products - Part 1: Equipment classification and requirements, IEC 60825-1, Edition 3.0, 2014.
27. Safety of laser products - Part 2: Safety of optical fibre communication systems (OFCs), IEC 60825-2, Edition 4.0, 2021.
28. Automatic electrical controls - Part 1: General requirements, IEC 60730-1, Edition 6.0, 2022.
29. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design, ISO 13849-1, Edition 3.0, 2015.
30. Safety of machinery - Functional safety of safety-related control systems, IEC 62061, Edition 2.0, 2021.

INDUCTOR IMPEDANCE EVALUATION FROM S-PARAMETER MEASUREMENTS

Part 2: S_{21} Two-Port Shunt and Two-Port Series Methods

By Bogdan Adamczyk, Patrick Cribbins, and Khalil Chame

This is the second of two articles devoted to the topic of inductor impedance evaluation from the S parameter measurements using a network analyzer. The previous article [1] described the impedance measurements and calculations from the S_{11} parameters using the one-port shunt, two-port shunt, and two-port series methods. This article is devoted to the impedance measurements and calculations from the S_{21} parameters using the two-port shunt and two-port series methods.

The overall conclusion of the previous article was that the inductor impedance evaluation from the S_{11} parameter measurements is not accurate. This article concludes that the two-port series method is the most accurate method for the inductor impedance evaluation from S_{21} parameters when using a network analyzer.

TWO-PORT SHUNT METHOD

The two-port shunt configuration is shown in Figure 1.

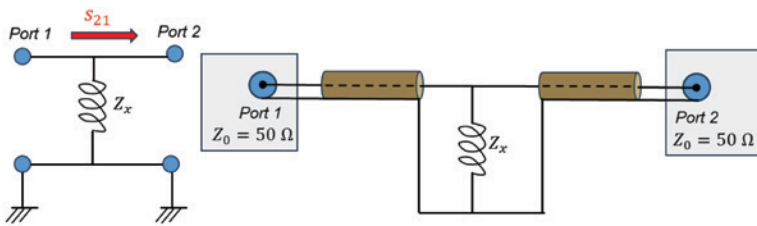


Figure 1: Two-port shunt configuration

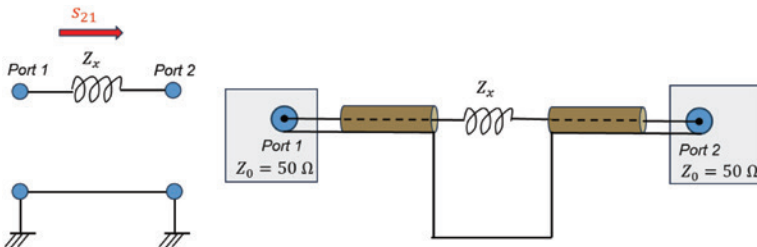


Figure 2: Two-port series configuration

Dr. Bogdan Adamczyk is professor and director of the EMC Center at Grand Valley State University (<http://www.gvsu.edu/emccenter>) where he performs EMC educational research and regularly teaches EM/EMC courses and EMC certificate courses for industry. He is an iNARTE-certified EMC Master Design Engineer. He is the author of two textbooks,



"Foundations of Electromagnetic Compatibility with Practical Applications" (Wiley, 2017) and "Principles of Electromagnetic Compatibility: Laboratory Exercises and Lectures" (Wiley, 2024). He has been writing "EMC Concepts Explained" monthly since January 2017. He can be reached at adamczyk@gvsu.edu.

Patrick Cribbins is pursuing his Bachelor of Science in Electrical Engineering at Grand Valley State University. He currently works full time as an Electromagnetic Compatibility Engineering co-op student at E3 Compliance, which specializes in EMC and high-speed design, pre-compliance testing and diagnostics. He can be reached at patrick.cribbins@e3compliance.com.



Khalil Chame is pursuing his Bachelor of Science in Electrical Engineering at Grand Valley State University. He currently works full time as an Electromagnetic Compatibility Engineer co-op student at E3 Compliance, which specializes in EMC and high-speed design, pre-compliance and diagnostics. He can be reached at khalil.chame@e3compliance.com.



For this configuration, the inductor's impedance in terms of the S_{21} parameter was derived in [2] as

$$Z_x = Z_0 \frac{S_{21}}{2(1-S_{21})} \quad (1)$$

TWO-PORT SERIES METHOD

The two-port series configuration is shown in Figure 2.

For this configuration, the inductor's impedance in terms of the S_{21} parameter was derived in [3] as

$$Z_x = 2Z_0 \frac{1-S_{21}}{S_{21}} \quad (2)$$

IMPEDANCE MEASUREMENT
SETUP AND RESULTS

The impedance measurement setup and the PCB boards are shown in Figure 3. The boards were populated with RF inductors [4] of the values 47 nH, 150 nH, and 270 nH.

Figure 4 shows the impedance curves for a 47 nH inductor using a two-port shunt and two-port series methods. The shunt measurements were taken at 50 dB and self-resonant frequencies. The series measurements were taken at 60 dB and self-resonant frequencies.

Figure 5 shows the inductor impedance curve obtained from support software [5].

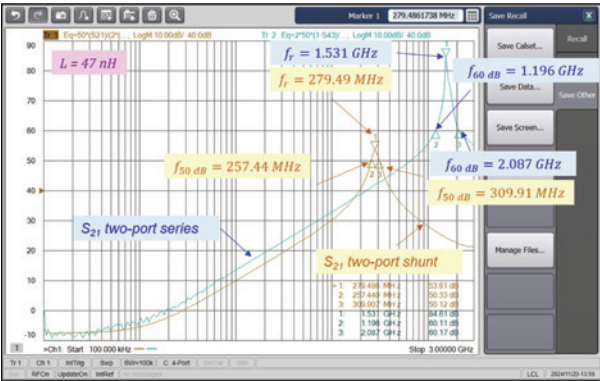


Figure 4: S_{21} -based impedance curves - two-port shunt vs. two-port series ($L = 47\text{ nH}$)

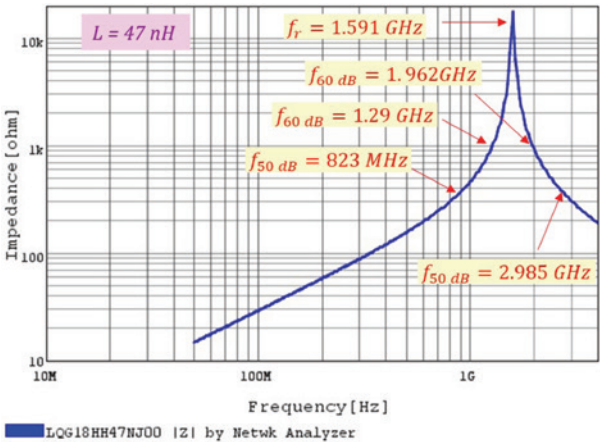


Figure 5: Support software impedance curve for 47 nH inductor

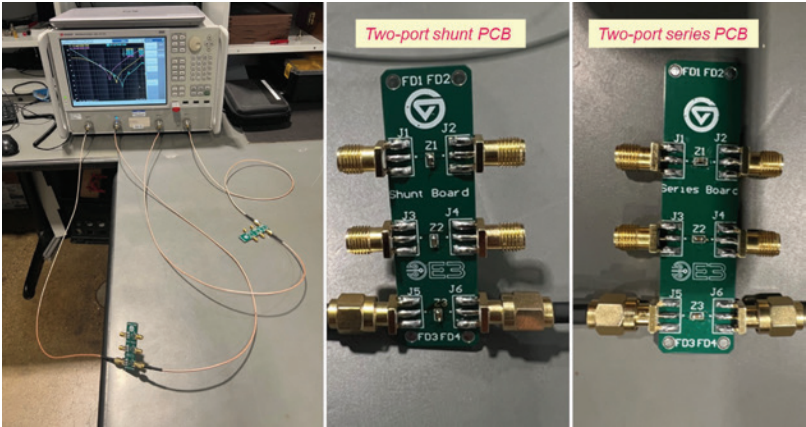


Figure 3: Measurement setup and PCBs

The two-port shunt, two-port series measurements, and the support software results are shown in Table 1.

It is apparent that the two-port series measurements are significantly closer to the support software results than the two-port shunt measurements.

Figure 6 shows the impedance curves for a 150 nH inductor using a two-port shunt and two-port series methods. The shunt measurements were taken at 50 dB and self-resonant frequencies. The series measurements were taken at 60 dB and self-resonant frequencies.

Figure 7 shows the inductor impedance curve obtained from the support software

The two-port shunt, two-port series measurements, and the support software results are shown in Table 2.

$L = 47\text{ nH}$	Two-port shunt	Support Software
1 st 50 dB frequency	257.44 MHz	823 MHz
Resonant frequency	279.49 MHz	1.591 GHz
2 nd 50 dB frequency	309.91 MHz	2.985 GHz
$L = 47\text{ nH}$	Two-port series	Support Software
1 st 60 dB frequency	1.196 GHz	1.29 GHz
Resonant frequency	1.531 GHz	1.591 GHz
2 nd 50 dB frequency	2.087 GHz	1.962 GHz

Table 1: Impedances at 50 dB, 60 dB, and self-resonant frequencies (S_{21} methods)

Again, the two-port series measurements at 50 dB and self-resonant frequencies are significantly closer to the support software results than the two-port shunt measurements.

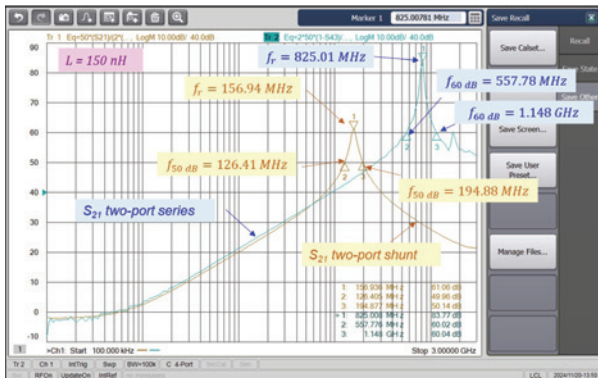


Figure 6: S_{21} -based impedance curves - two-port shunt vs. two-port series ($L = 150$ nH)

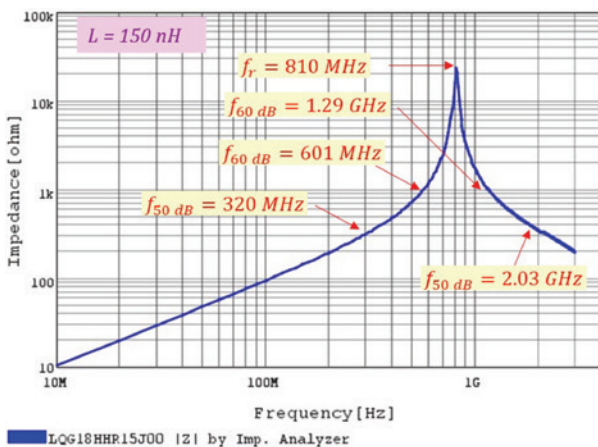


Figure 7: Support software impedance curve for 150 nH inductor

$L = 150$ nH	Two-port shunt	Support Software
1 st 50 dB frequency	126.41 MHz	320 MHz
Resonant frequency	156.94 MHz	810 MHz
2 nd 50 dB frequency	194.88 MHz	2.03 GHz
$L = 150$ nH	Two-port series	Support Software
1 st 60 dB frequency	557.78 MHz	601 MHz
Resonant frequency	825.01 MHz	810 MHz
2 nd 50 dB frequency	1.148 GHz	1.29 GHz

Table 2: Impedances at 50 dB, 60 dB, and self-resonant frequencies (S_{21} methods)

REGISTRATION IS OPEN!



JOIN YOUR COLLEAGUES
RALEIGH, NORTH CAROLINA
AUGUST 18 – 22, 2025

EMC+SIPI 2025 leads the industry in providing state-of-the-art education on EMC and Signal Integrity and Power Integrity techniques. The Symposium features five full days of innovative sessions, interactive workshops and tutorials, “Ask the Experts” panel discussions, experiments and demonstrations, and social networking events.

BENEFITS & FEATURES

- Learn EMC, Signal Integrity and Power Integrity (SIPI) techniques
- Three days of expert technical papers
- Two full days of practical EMC and SIPI workshops and tutorials
- Experiments and demonstrations of fundamental and advanced topics
- Add-on educational courses to expand your knowledge of EMC and SIPI.
- Find out the latest development in IEEE EMC and SIPI standards
- Exhibits! New Technologies, Instrumentation and Solutions
- Social gathering, connecting, and the Southern hospitality of Raleigh, NC



#IEEE_ESP25



IEEE

EMC
SOCIETY®


www.emc2025.org

Figure 8 shows the impedance curves for a 270 nH inductor using a two-port shunt and two-port series methods. The shunt measurements were taken at 50 dB and self-resonant frequencies. The series measurements were taken at 60 dB and self-resonant frequencies.

Figure 9 shows the inductor impedance curve obtained from the support software.

The two-port shunt, two-port series measurements, and the support software results are shown in Table 3.

Once again, the two-port series measurements at 50 dB and self-resonant frequencies are significantly closer to the support software results than the two-port shunt measurements.

The overall conclusion is that the two-port series method is the most accurate method of the inductor’s impedance evaluation from the S_{21} parameter measurements. 

REFERENCES

1. Bogdan Adamczyk, Patrick Cribbins, and Khalil Chame, “Inductor Impedance Evaluation from S Parameter Measurements – Part 1: S_{11} One-Port Shunt, Two-Port Shunt, and Two-Port Series Methods,” *In Compliance Magazine*, April 2025.
2. Bogdan Adamczyk, Patrick Cribbins, and Khalil Chame, “Capacitor Impedance Evaluation from S Parameter Measurements – Part 1: S_{11} One-Port Shunt, Two-Port Shunt, and Two-Port Series Methods,” *In Compliance Magazine*, February 2025.
3. Bogdan Adamczyk, Patrick Cribbins, and Khalil Chame, “Capacitor Impedance Evaluation from S Parameter Measurements – Part 2: S_{21} Two-Port Shunt and Two-Port Series Methods,” *In Compliance Magazine*, March 2025.
4. Murata RF inductors LQG18HH47NJ00 (47 nH), LQC18HH15J00 (150 nH), and LQG18HH27J00 (270 nH).
5. Murata Design Support Software, “SimSurfing.” <https://ds.murata.co.jp/simsurfing/index.html?lcid=en-us>

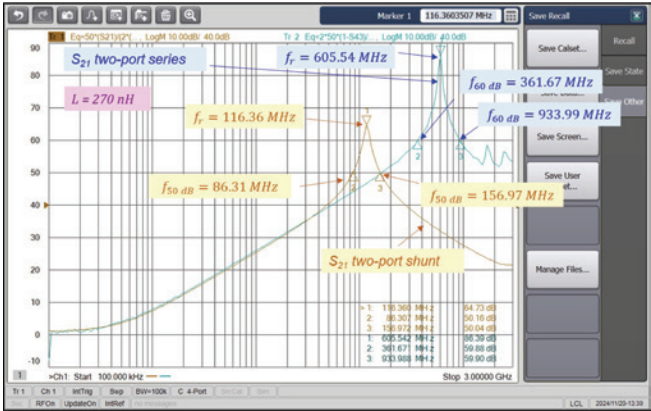


Figure 8: S_{21} -based impedance curves - two-port shunt vs. two-port series ($L = 270$ nH)

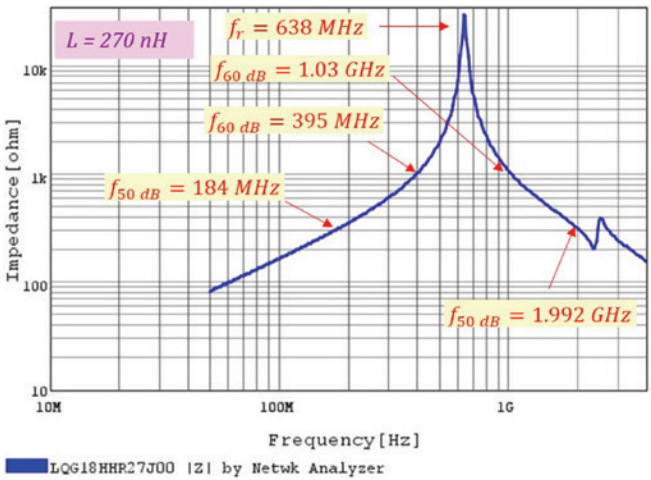


Figure 9: Support software impedance curve for 270 nH inductor

$L = 270$ nH	Two-port shunt	Support Software
1 st 50 dB frequency	86.31 MHz	184 MHz
Resonant frequency	116.36 MHz	638 MHz
2 nd 50 dB frequency	156.97 MHz	1.992 GHz
$L = 270$ nH	Two-port series	Support Software
1 st 60 dB frequency	361.67 MHz	395 MHz
Resonant frequency	605.54 MHz	638 MHz
2 nd 50 dB frequency	933.99 MHz	1.03 GHz

Table 3: Impedances at 50 dB, 60 dB, and self-resonant frequencies (S_{21} methods)

WHY ESD ELECTRONIC DESIGN AUTOMATION CHECKS ARE SO CRITICAL: PART 1

On behalf of EOS/ESDA Association, Inc.

By Eleonora Gevinti, Michael Khazhinsky, Ali Muhammad, Dolphin Abessolo Bidzo, Nicolas Richaud, Peter Koeppen, Kuo-Hsuan Meng, Vladislav Vashchenko, Andrei Shibkov, and Matthew Hogan, WG18

A new version of Technical Report TR18.0-01-25 (TR18) on ESD Electronic Design Automation (EDA) Checks by the ESD Association's Working Group 18 is about to be released. This article provides an overview of TR18, which offers guidelines for the EDA industry and the ESD design community to establish a comprehensive ESD verification flow. This flow addresses ESD design challenges in modern ICs, including common terminology and required check types. The main requirements are broad check coverage, manual checking limitations, transparency, and integration into the design flow for clear and actionable violation reporting. The document covers generic checks, EDA toolsets, and databases, allowing IC design companies, IDMs, or foundries to implement specific rules in their design and verification flows for automated checking.

ESD CHECKS THROUGHOUT THE IC DESIGN FLOW

ESD checks for an IC product design are performed at multiple phases throughout the product design. These checks need to be coordinated with the ESD development and implementation flow, supported by an ESD check flow. The main phases of the product design flow are:

- Technology Enablement Phase
- Product Definition Phase
- Product Architecture Phase
- Product Design Phase
- Product Verification Sign-off Phase
- Product Validation Phase

Founded in 1982, EOS/ESD Association, Inc. is a not for profit, professional organization, dedicated to education and furthering the technology Electrostatic Discharge (ESD) control and prevention. EOS/ESD Association, Inc. sponsors educational programs, develops ESD control and measurement standards, holds international technical symposiums, workshops, tutorials, and foster the exchange of technical information among its members and others.



The main ESD checks include:

- Schematic-based Topological ESD Checks
- Layout-based ESD Checks
- Package-level ESD Checks
- System-level ESD Checks
- ESD Circuit Simulation (SPICE)
- ESD TCAD Simulation

The timing of EDA check execution throughout the design flow is indicated with grey shapes in Figure 1 on page 42. Most ESD checks must be run during all design phases, with accuracy depending on design data maturity and completeness. Standardization of input and output data and interfaces is crucial for ESD EDA verification. The ESD engineer should consider the complexity and size of the checked database to build an efficient ESD verification flow.

SCHEMATIC-BASED STATIC TOPOLOGICAL ESD CHECKS

Static topological checks include verifications implemented with commercial or customized EDA tools capable of analyzing netlist topologies.

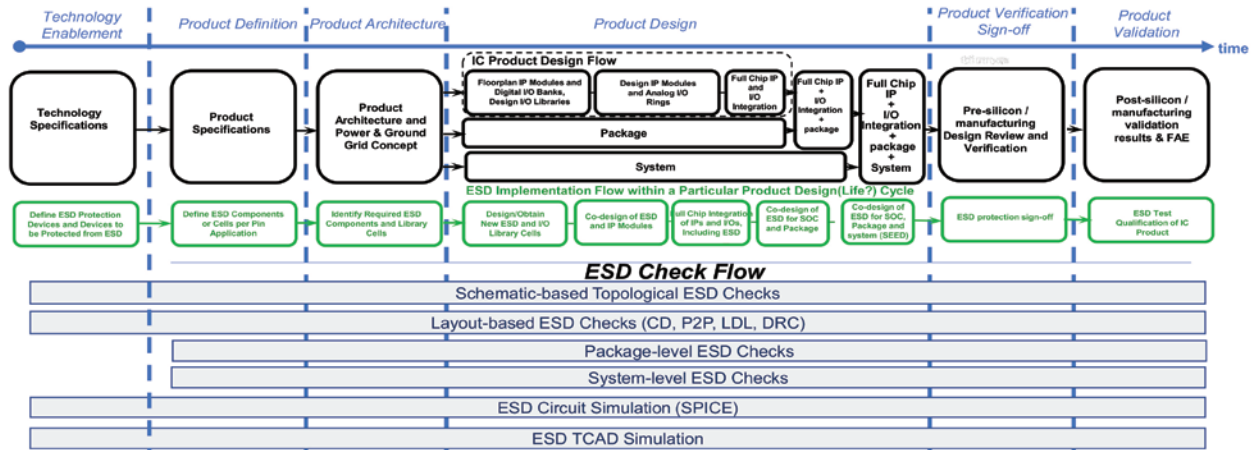


Figure 1: ESD verification flow mapped to IC design flow

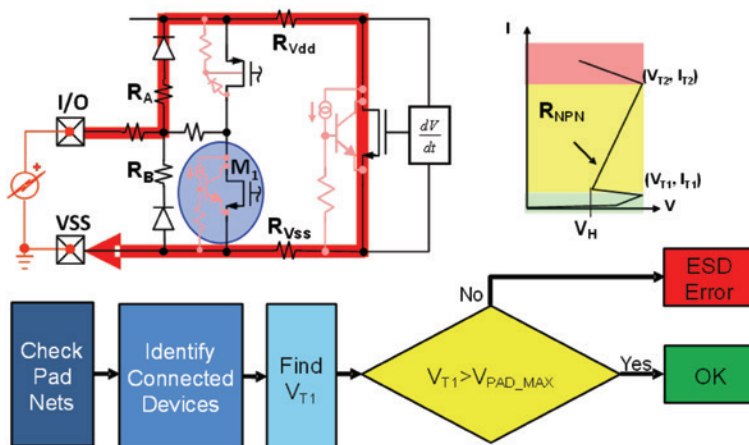


Figure 2a: Protected devices checks - Objective: Report ESD-vulnerable devices

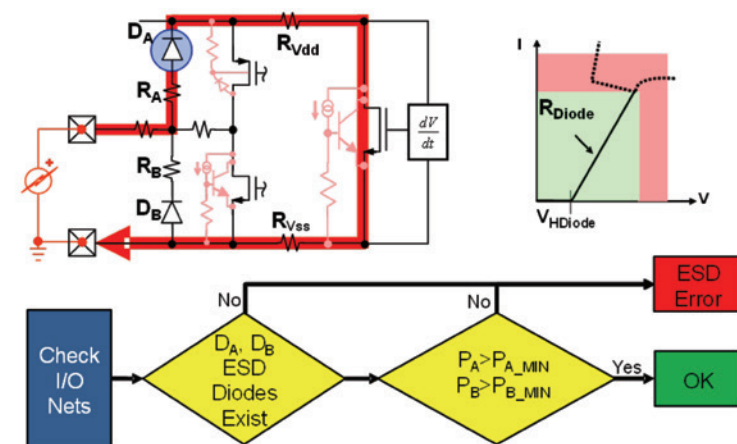


Figure 2b: ESD network checks – Objective: Report missing ESD diodes and diodes with insufficient perimeter

These checks verify devices that need ESD protection and ESD protection networks (Figure 2a and 2b). They consider schematics information and the electrical behavior of the circuit. Topological checks are typically run on netlists derived from schematic views but can also be run on layout-extracted netlists, including RLC parasitics for analysis.

ESD integration rules can be derived from SPICE and TCAD simulations or (VF)-TLP measurements to match required ESD industry standard levels. Topological checks ensure IC design compliance with predefined integration parameters and appropriately sized circuit structures for desired protection. These checks need additional ESD-specific input information for analysis. They are especially useful at early design stages when databases are partial and schematic views are available while layout information is limited. Topological checks accompany all IC product design flow phases with suitable verifications, depending on available data and completeness.

LAYOUT-BASED ESD CHECKS

ESD verification must also include layout-based checking to verify the

construction of ESD protection devices, identify weak ESD paths due to the creation of unintended parasitic devices, and perform a detailed analysis of back-end metallization. Layout-based ESD checks include broad classes of checks (Figure 3a and 3b):

- Geometrical Design Rule Checks (DRC)
- Logic Driven Layout (LDL) checks
- Current Density (CD) checks
- Metal routing Point to Point (P2P) resistance

The design database should include geometric information of the target circuit under check (e.g., layout or floorplan) and annotation of relevant metallization (e.g., IO/power/ground net type, voltage level, etc.). The tool flow may involve one or more commercial EDA vendor solutions plus additional means developed in-house for customized ESD robustness analysis. ESD devices are at the core of the ESD protection schemes and are the most critical elements in the discharge paths. They are often characterized by TLP/VFTLP measurements. Verification rule files (often from a foundry) are used to describe the relevant portion of the system to analyze and the constraints to be checked. The final output is used to visualize and confirm whether the design violates the design constraints.

CONCLUSION

In this first part of the article, the concept of ESD checks throughout the IC design flow was covered, together with schematic-based and layout-based ESD checks sections.

In Part 2, package-level and system-level checks sections, together with ESD circuit simulation and ESD TCAD simulation sections, will be handled, completing the coverage of all ESD EDA checks described in the Technical Report. [EN](#)

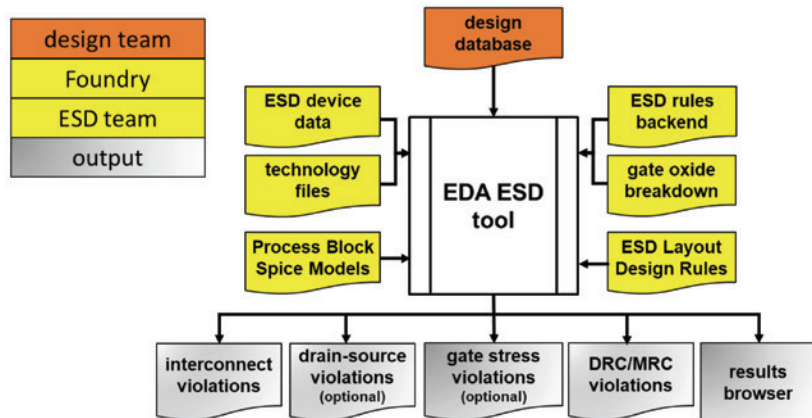


Figure 3a: Layout-based ESD checks flow

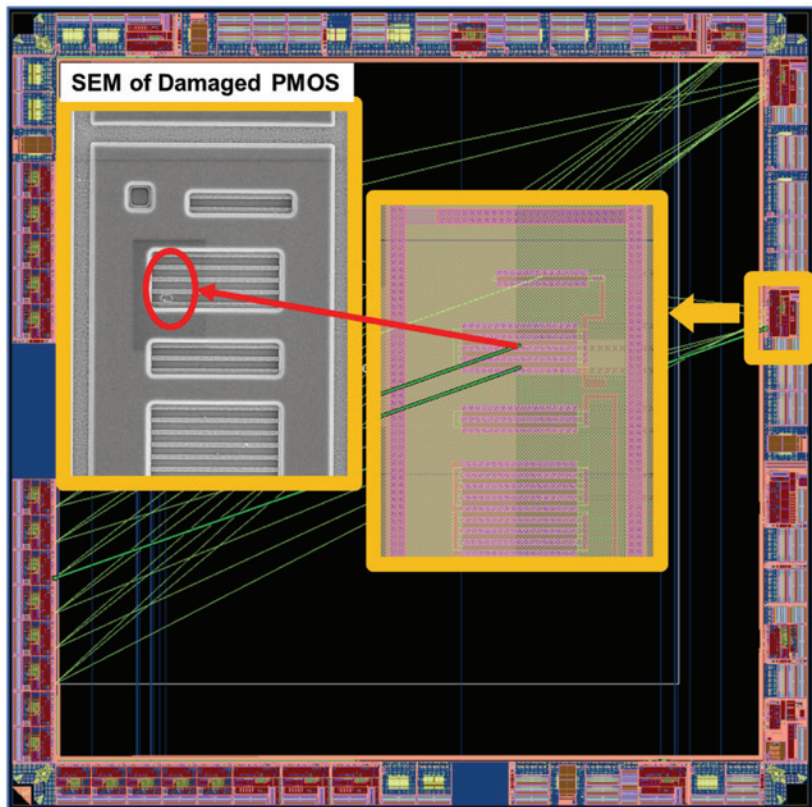


Figure 3b: Predictive CDM simulations fly lines between driver/receiver pairs fails confirmed by failure analysis.

POOR POWER DISTRIBUTION NETWORK LEADS TO UNEXPECTED RADIATED EMISSIONS

By Dr. Min Zhang

Recently, I worked on a radiated emissions case involving narrowband emission failures in the 100 MHz to 1 GHz range. Identifying the source of such narrowband noise is usually straightforward, and, in this case, a near-field sniffing probe quickly led us to the culprit: the clock signal of a high-speed SPI line between the microcontroller and the flash drive on the PCB. This is demonstrated in Figure 1.

However, during troubleshooting, I discovered something unexpected—other I/O lines, much slower by nature (such as an I²C line running at just tens of kHz), were also exhibiting the same 100 MHz harmonics. This became evident when I used an RF current probe to measure common-mode noise on the wires connected to the PCB, shown in Figure 2.

To mitigate the noise on the other I/O lines, I initially used high-impedance ferrite beads. When selecting ferrite beads, a simple rule applies:

- Their impedance should be low enough at the signal's operating frequency to avoid signal integrity issues and
- Their impedance should be high at the noise frequency to effectively suppress unwanted emissions.

In this case, the solution seemed straightforward, as the I/O lines

Dr. Min Zhang is the founder and principal EMC consultant of Mach One Design Ltd, a UK-based engineering firm that specializes in EMC consulting, troubleshooting, and training. His in-depth knowledge in power electronics, digital electronics, electric machines, and product design has benefitted companies worldwide. Zhang can be reached at info@mach1desgin.co.uk.



operated at relatively low frequencies compared to the 100s of MHz noise we were trying to suppress. But while the ferrite beads helped, I was eager to understand the underlying mechanism behind this unexpected harmonic behavior.

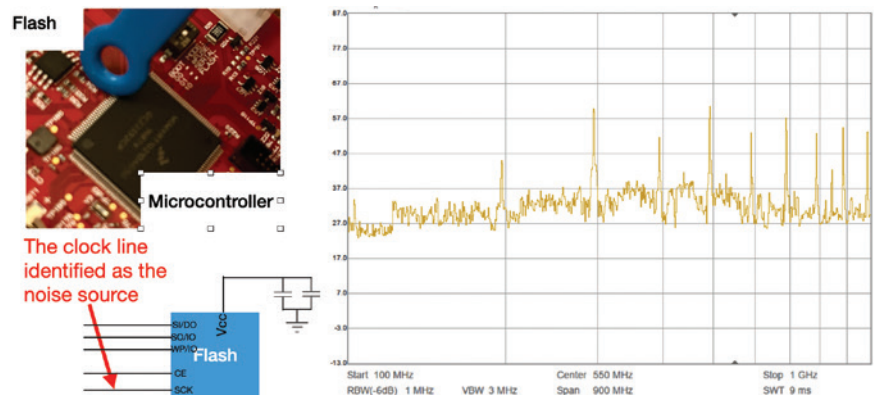


Figure 1: Near-field probing results identifying the noise source

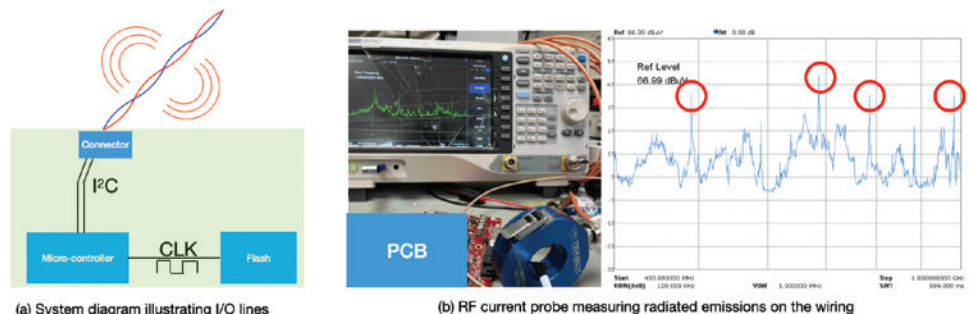


Figure 2: (a) System diagram illustrating I/O lines radiating harmonics of the clock frequency; (b) RF current probe measuring radiated emissions on the wiring

The best resource I found that explains this in detail is Prof. Todd Hubing's presentation¹ (downloadable link provided in the endnote).

Prof. Hubing explains that while DC power and low-speed digital signals do not usually have enough power at radiated emission frequencies to be problematic, they often carry strong high-frequency currents that can contribute to emissions. A poor power distribution network (PDN) design can result in high-frequency voltage fluctuations on every input and output trace connected to the IC.

In his presentation slide, page 17 shows that more current is being drawn from the DC power supply pins than from the signal pins. Page 18 highlights that significant high-frequency currents appear on low-speed I/O, including outputs that never change state during normal operation.

It seems that the issue arises due to two main factors:

- *IC design*—Some ICs handle internal noise containment better than others and
- *PCB layout and PDN design*—Poor layout can cause unintended noise propagation.

I then followed a great conversation with Dan Becker, Technical Director at NXP, and his perspective was fascinating.² Dan emphasized that poor PDN design is often the root cause of these issues and shared best practices for mitigating them.

For instance, a high-speed SPI design like this will likely never perform well on a 2-layer PCB. However, with a well-designed 4-layer PCB that incorporates a

proper microstrip line structure, achieving good EMC performance is much more feasible.

To optimize PDN design and minimize unexpected emissions, key factors to consider include:

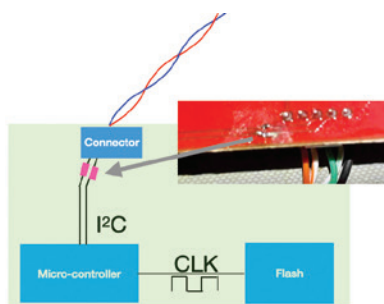
- *Distance from the IC pin to the first capacitor*—This should be within 1/20 of the wavelength of the driver's switching speed to prevent voltage depletion effects
- *Transmission line impedance*—It should be matched to the current requirements to ensure stable operation (i.e., making sure the "bucket" is big enough to handle the switching demand) and
- *Drive strength of clock signals*—Many manufacturers default to a very fast dv/dt , which is often unnecessary. Reducing the slew rate in software can significantly help.

I collaborated with the client to re-spin the PCB design, focusing on power distribution network improvements. The goal was to eliminate the ferrite beads altogether and instead use a simple resistor on the clock line for better impedance control.

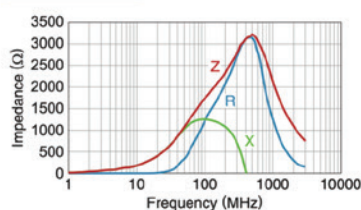
This case was an excellent reminder that unexpected emissions often originate from power integrity issues, not just high-speed signals. A well-thought-out PDN strategy can make or break EMC performance. 🛠️

ENDNOTES

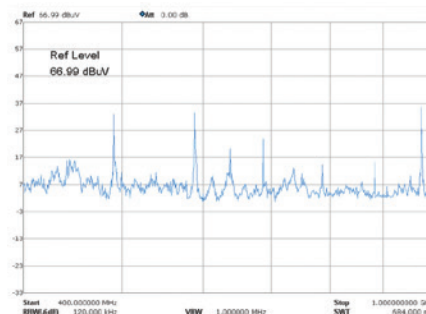
1. Todd Hubing, "Automotive circuit board and system design for EMC," <https://cecas.clemson.edu/cvel/workshop/pdf/AutoEMC-Workshop-Hubing.pdf>.
2. Dan Becker, "A Novel Approach to Power Distribution: Building a Solid Foundation."



(a) Using two ferrite beads on the I²C lines, close to the connector



(b) The ferrite bead has very low impedance below 10 MHz and reaches its maximum impedance around 500 MHz



(c) New measurement results using an RF current probe

Figure 3: New measurements with two ferrite beads on the I²C lines

ANSI Z535.7 – PRODUCT SAFETY INFORMATION IN ELECTRONIC MEDIA IN FOCUS

By Erin Earley

For those that follow our “On Your Mark” columns, you know the emphasis placed on the value of ANSI Z535 – the U.S. standards that create a guide for the design, application, and use of signs, colors, and symbols intended to identify and warn against hazards and for other accident prevention purposes. These standards, along with their international counterpart, ISO 3864-2, are effective starting points in helping you to develop adequate warnings. Recently, we had an exciting new development in this family of standards: the release of an all-new seventh standard. In this article, we’ll explore the new standard and how its principles can be used to create effective warnings that drive safety.

A NEW STANDARD ENTERS INTO THE ANSI Z535 FAMILY

The ANSI Z535 standards are commonly used by manufacturers and workplaces across the U.S. as a main guideline for following best practices and creating consistency in their safety warnings and instructions. The family of the ANSI standards (Z535.1 to Z535.6) were republished in 2022 and 2023. In late 2024, ANSI Z535.7 was released, a new ANSI Z535 standard focusing on product safety information in electronic media. Together, these standards – now a family of seven – contain the information needed to specify formats, colors, and symbols for safety signs used in environmental and facility applications, in product and product literature applications, in temporary safety tag and barricade tape applications, and in electronic media.

WHAT IS ANSI Z535.7?

ANSI Z535.7 addresses a topic that has not been covered before by ANSI but is one often faced with uncertainty for today’s machinery manufacturers: providing guidelines for the design of product safety information in electronic media.

Erin Earley, head of communications at Clarion Safety Systems, shares her company’s passion for safer products and workplaces. She’s written extensively about best practices for product safety labels and facility safety signs. Clarion is a member of the ANSI Z535 Committee for Safety Signs and Colors, the U.S. ANSI TAG to ISO/TC 145, and the U.S. ANSI TAG to ISO 45001. Erin can be reached at earley@clarionsafety.com.



The new standard aims to offer a comprehensive system for presenting safety information in a variety of digital formats. The standard’s focus on safety information in digital media includes a wide purview: electronic/digital manuals; electronic/digital user guides; e-instructions; digital maintenance or service manuals; visuals, animations, or videos; e-warnings in reference to phones, tablets, or computers. It provides a framework for the design, placement, and duration of safety messages within these electronic collateral materials.

ANSI Z535.7’S ORIGIN AND DEVELOPMENT

How did ANSI Z535.7 originate?

“The ANSI Z535 committee recognized the limitations of existing standards – which were created mainly with static, printed materials in mind – and the need to adapt to the dynamic, interactive nature of electronic media,” says Angela Lambert, an ANSI Z535 committee member and head of standards compliance at Clarion Safety Systems. Lambert is also a subcommittee member of ANSI Z535.7, part of a small group of experts that championed the standards’ development.

According to ANSI Z535.7’s introduction, “Historically, there has been a lack of widely available or generally applicable graphic systems for presenting safety information in electronic media.”

ANSI Z535.7 addresses a topic that has not been covered before by ANSI but is one often faced with uncertainty for today's machinery manufacturers: providing guidelines for the design of product safety information in electronic media.

The committee began the standard's development in 2021, approving and publishing the new standard in late 2024.

"ANSI Z535.7 was written intentionally to complement ANSI Z535.4, which focuses on safety labels for physical products, and ANSI Z535.6, which addresses safety communication in manuals. The new standard builds on the foundation of the .4 and .6 standards, to provide guidance for digital media, in line with an organization's comprehensive safety strategy," Lambert says.

PUTTING THE NEW STANDARD INTO PRACTICE

"If you're an engineer or manufacturer who's charged with product or machine safety, you've likely had electronic media on your mind. If that hasn't happened yet, it likely will soon. That's the direction our world is going in. Products and how we communicate safety information about them are constantly changing, especially in the past decade. Digital screens or electronic displays are now often used. In addition to that, users often expect dynamic safety instructions, whether in the form of videos, online manuals, or apps. Many manufacturers currently find themselves in the middle of a digital journey, walking a line between older, static formats and newer, digital ones. Finding a balance can be daunting."

That's where ANSI Z535.7 provides support. It details principles and guidelines specific to the design and maintenance of safety information provided through electronic media. The standard covers key areas such as the appropriateness of electronic media for safety communication, font size based on safe viewing distance, duration to display safety information within dynamic electronic media, and maintenance of access to electronic safety information.

ANSI Z535.7 recognizes that electronic media's nature is dynamic and has many variables when it comes to format. The standard needs to be able to address videos or animation, as well as content that is interactive, contains both visual and auditory components, may not be accessed in a linear or page by page format, and may be contained in multiple systems. While this type of fluidity is not simple to



Figure 1: The new ANSI Z535.7 standard introduces a unified communication system for electronic media, enhancing clarity and consistency in product safety information addressing device-specific variations to improve user experience.


standardize across every product and situation, the standard aims to provide a communication system that applies to a range of products and industries – a common direction for the use of ANSI Z535 elements that can be applied effectively across electronic media formats.

“While the standard doesn’t dictate the specific safety messages included in electronic media, it offers guidance on formatting them effectively. That means it can help engineers or manufacturers to figure out how to communicate safety information in the mediums they use. The guidelines closely follow the .6 standard and reference the .4 standard; there aren’t necessarily any surprises for those that already are knowledgeable on ANSI Z535 best practices, but there is clarity on how to warn effectively digitally, and how to present a cohesive safety message in print and electronic formats,” Lambert says.

As examples, ANSI Z535.7:

- Categorizes safety messages into four types based on risk levels, referencing ANSI Z535.6 for guidance.
- Covers key components of safety messages, including proper signal word use to indicate risk severity levels.
- Emphasizes clear design principles of safety messages to enhance a user’s understanding and ability to take actions to mitigate risk effectively.

The goal is to aid in the development of a unified design approach that prioritizes clarity, consistency, and effective communication of product safety information. Critical safety information needs to be consistently understood no matter what type of medium (on-product safety labels, print instruction manuals, videos, LCD screens, etc.) is used.

“What I can also tell manufacturers and engineers is that ANSI Z535 is committed to continuing to provide updated safety resources and guidelines that are responsive to our changing environment. In fact, revisions will begin soon on ANSI Z535.7. Technology changes fast, and the standard will be responsive to that so that the guidelines stay current and impactful,” Lambert says. 



Trust Matters!

Meeting Medical EMC
IEC 60601-1-2+
Pre-Compliance and Full-Compliance




Radiated Emissions Conducted Immunity



Conducted Emissions Magnetic Immunity

ABSOLUTE-EMC.com
(703) 774-7505
info@absolute-emc.com

**End-to-end radio
type approval
services.**



*free regulatory
news updates*



Approve-IT

**Trusted for
more than 30
years in over
250 countries
and territories.**

approve-it.net

PRODUCT showcase

**EXODUS
ADVANCED
COMMUNICATIONS**



**Amplifiers
CW & Pulse
Watts to KW**

**RF & Microwave
Amplifiers
10KHz-75GHz**

*Innovative Engineering,
Ultimate Solutions!*

**Power Your Success
with Top-Tier
RF Modules
and Amplifiers**



**EXODUS ADVANCED
COMMUNICATIONS**

www.exoduscomm.com
sales@exoduscomm.com

HAEFELY
Current and voltage – our passion

axos⁸



SURGE **EFT / BURST** **VOLTAGE DIPS**

MAGNETIC FIELD **RING WAVE** **TELECOM WAVE**

emc-sales@haefely.com

StaticStop
by SelectTech

The Static Control Flooring Experts

- Maintenance Products
- Most Effective Flooring Solutions
- Industry Leading Technical and Installation Support



www.staticstop.com
877-738-4537



**F2 LABS IS FIERCELY COMMITTED
TO SERVING MANUFACTURERS
THROUGH THE PRODUCT
COMPLIANCE PROCESS**

**Certification Services for
All Types of Electrical Products**

**Engineering, Testing, and
Technical Services**

FDA 510K, CE, UL, FCC, CSA, ISCED CANADA & MORE
F2 Labs is accredited by A2LA to ISO/IEC 17025

**Contact Sales@f2labs.com
or Call 877-405-1580
Today for a Quote**

www.f2labs.com



**High Voltage
Control, Test & Measurement**



**10V to 1,200,000V
MicroAmps to 1,700,000 Amps PK Pulse
DC to 10MHz**

We Specialize in Custom HV Design

**High Voltage
Electronic and Electromechanical Devices
we design, test, manufacture & calibrate:**

- HV Relays
- HV Probes
- HV Voltage Dividers
- HV AC & DC Hipots
- HV Power Class Voltmeters
- HV Switches
- HV Circuit Breakers
- HV Vacuum Contactors
- HV Calibration - A2LA Accredited
- Lab, Industrial & Military Applications

ROSS ENGINEERING CORPORATION
www.rossengineeringcorp.com
408-377-4621 | info@rossengineeringcorp.com

UEMC

**MRI / CT / X-Ray
POWER FILTER
SOLUTIONS**


**WE'RE HIRING
NOW** SALES DIRECTOR

Medical Filter

**MADE IN
USA**

SCIF Filter

EMI Filter



SALES@UEMC.TECH 346-312-9556
WWW.UEMCINC.COM

Upcoming Events

May 6

- ★ 2025 Chicago IEEE EMC Mini Symposium

May 8

- ★ EMC Fest 2025

May 12-16

2025 International ESD Workshop
(IEW-Europe)

May 13-15

- ★ 2025 IEEE International Symposium on
Product Compliance Engineering (ISPCE)

May 18-21

2025 International Applied Computational
Electromagnetics Society (ACES) Symposium

May 19-21

EMC & Compliance International Exhibition &
Workshops

May 19-22

2025 IEEE International Instrumentation and
Measurement Technology Conference

May 19-23

2025 Asia-Pacific International Symposium
and Exhibition on Electromagnetic
Compatibility (APEMC)

May 20

- ★ AMTA 2025 Regional Meeting

June 3-6

WPTCE 2025 IEEE Wireless Power Technology
Conference and Expo

June 15-20

- ★ IMS 2025 – IEEE International Microwave
Symposium

June 26

Cybersecurity Maturity Model Certification for
Federal Government Procurements

- ★ Visit In Compliance's booth at these events!

Advertiser Index

A.H. Systems, Inc. Cover 2

Absolute EMC 48

Approve-IT 48

AR RF/Microwave Instrumentation 3

Coilcraft 11

E. D. & D., Inc. 7

Element Materials Technology 23

ETS-Lindgren Cover 4

Exodus Advanced Communications 49

F2 Labs 49

Haefely AG 49

HV TECHNOLOGIES, Inc. 29

IEEE EMC+SIPI 2025 39

MFG Tray (Molded Fiber Glass) 31

Ophir RF Cover 3

Ross Engineering Corporation 49

SelecTech, Inc. 49

SGS North America Inc. 25

Suzhou 3ctest Electronic Co. Ltd. 17

UEMC Inc. 49

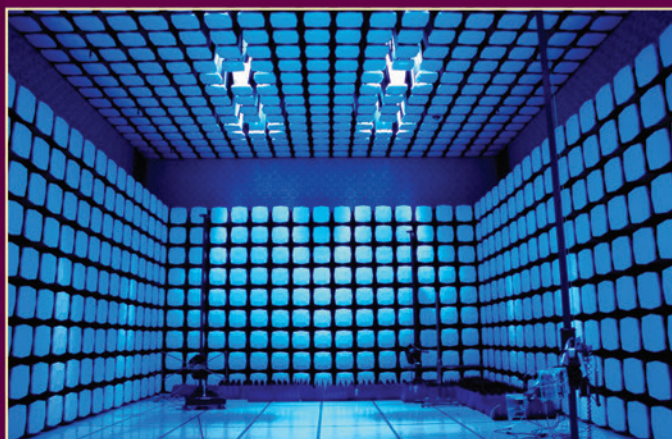
Is it time to renew your
subscription to *In Compliance*?
Never miss an issue, renew now.

Was this issue of *In Compliance*
forwarded to you?
Get your own free subscription.

Do you only want to receive the
In Compliance newsletters?
You can do that here.

OPHIR^{RF}

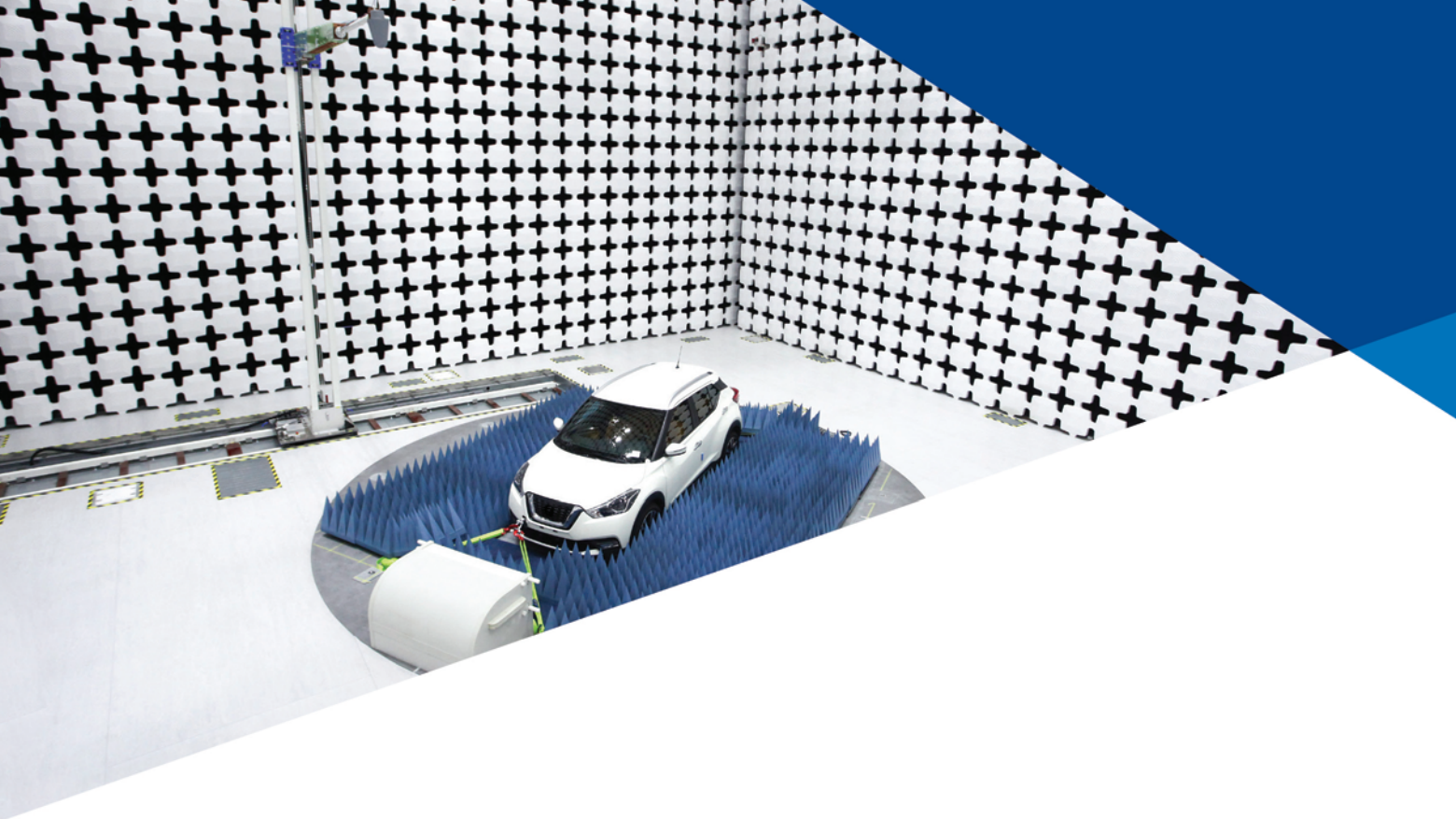
HIGH POWER RF SYSTEMS



LOS ANGELES

Since 1992

www.OphirRF.com



REDEFINING AUTOMOTIVE EMC TEST AND MEASUREMENT SOLUTIONS.

As automotive systems become more advanced, industry is paying greater attention to the design and testing of complex components and assemblies that form a vehicle's internal network. With today's trend toward greater levels of autonomy and safety aligned with the increasing popularity of electric vehicles, the need for additional and more sophisticated automotive EMC and antenna pattern measurement test scenarios has become more urgent.

At ETS-Lindgren, we understand the complexity of vehicle platforms, the importance of addressing different variations of electric propulsion, entertainment, and driver related automation, and the need for them to all function reliably – without affecting safety or the legacy communications infrastructure. With creative new EMC test solutions for full vehicle and component level testing, ETS-Lindgren's expertise in RF and related test systems helps manufacturers and labs verify that automotive designs perform as intended and are compliant with EMC, safety, wireless, and signal integrity requirements. Join us in taking Automotive EMC Test and Measurement to an entirely new level, while being *Committed to a Smarter, More Connected Future*.

For more information on our Automotive EMC Test and Measurement solutions, visit our website at www.ets-lindgren.com.

Connect with us at:



**COMMITTED TO A SMARTER,
MORE CONNECTED FUTURE**

 **ETS·LINDGREN**
An ESCO Technologies Company

Offices Worldwide | ets-lindgren.com

5/25 RR © 2025 ETS-Lindgren v1.0