JUNE 2022

IN COMPLIANCE™

THE COMPLIANCE INFORMATION RESOURCE FOR ELECTRICAL ENGINEERS

SCIF and Radio Frequency

Secured Facility Design

PLUS

Using Multiport Connectors in High-Frequency Military and Avionics Systems

Users Guide to Hipot Testing

High-Integrity Components in Electrical Equipment, Part II

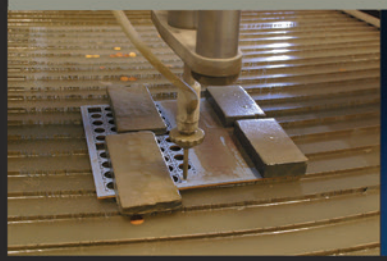
SPIRA

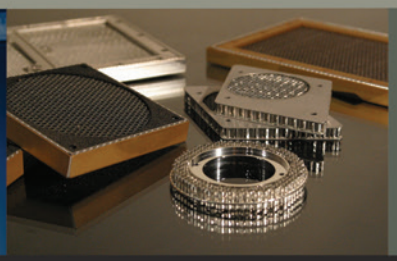
40 YEARS ANNIVERSARY

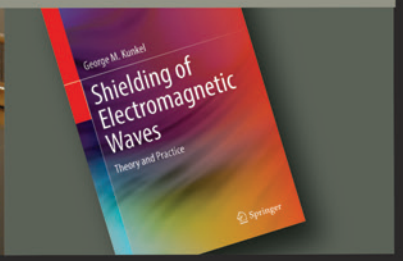
THE LEADER IN EMI GASKETS

Excellence by Design: Exceptional, Durable Shielding

When EMI protection is important, top manufacturers choose Spira EMI gaskets. Spira gaskets are well known for solving EMI shielding problems that no other gasket can solve, and are perfect for both military and commercial applications. Gaskets are designed to be highly reliable, and built to last the life of the system. Salt fog, high humidity and RoHS versions are available. Choose Spira gaskets to pass your shielding tests the first time.







EMI & Environmental Connector-Seal Gaskets. Superior EMI and environmental protection for flange-mounted connectors in front or back mount configurations.

Spira-Shield. All Spira gaskets utilize our unique patented spiral design which yields EMI shielding quality up to 165 dB with exceptionally long life.

Shielded Honeycomb Air-Vent and Fan Filters. High and reliable shielded filters at competitive prices providing over 80dB of shielding at 1GHz.

Groundbreaking new book on EMI Shielding Theory. A new, more accurate and efficient way for engineers to understand electromagnetic shielding theory and practice.

LEARN MORE & ORDER FREE SAMPLES – CONTACT US TODAY!

www.spira-emi.com • (818) 764-8222 • info@spira-emi.com

The EERC™

electrical engineering resource center

Visit **incompliancemag.com/EERC** to access your free resources today!

YOUR GUIDE TO IEC 60601-1, 3RD EDITION, AMENDMENT 2

guide provided by

CSA GROUP

DB OR NOT DB?

white paper provided by

ROHDE&SCHWARZ

MATHEMATICAL TOOLS OF THE TRADE POSTER

poster provided by

HOW TO ENSURE YOUR LED LIGHTING PRODUCTS MEET INDUSTRY STANDARDS

application note provided by

VITREK

EXPLORING THE NECESSITY OF THE HOT HIPOT TEST

white paper provided by

ASSOCIATED RESEARCH
AN IKONIX BRAND

FREQUENCY AND WAVELENGTH CALCULATION

calculator provided by

A.H. Systems, Inc.

THE ULTIMATE MIL-STD-461G TESTALK

video provided by

NTS

In Compliance Magazine
ISSN 1948-8254 (print)
ISSN 1948-8262 (online)
is published by

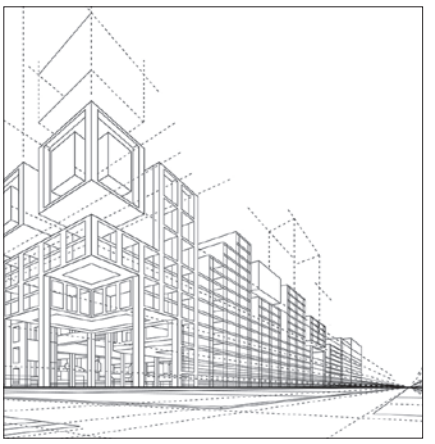
Same Page Publishing Inc.
451 King Street, #458
Littleton, MA 01460
tel: (978) 486-4684
fax: (978) 486-4691

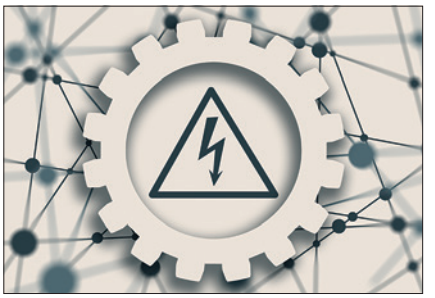
IN COMPLIANCE

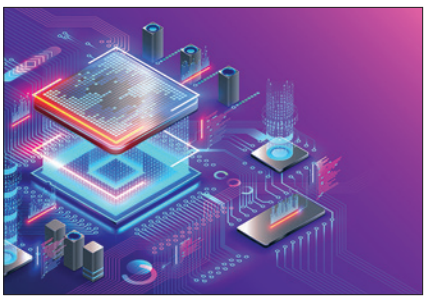
PRINTED WITH SOY INK

JUNE 2022
Volume 14 | Number 6

CONTENTS







FCC to Explore Options for Improving RF Receiver Performance

The U.S. Federal Communications Commission (FCC) is seeking public comments and suggestions for improving the performance of radio frequency (RF) receivers.

According to a Notice of Inquiry, the Commission believes that its efforts to improve efficiencies in spectrum management need to expand to include all aspects of wireless systems, including both transmitters and receivers. Although current regulations applicable to transmitters implicitly acknowledged receiver performance, the Commission says recent advances in receiver technology and the development of more interference-resistant receivers potentially offer additional opportunities to improve spectrum management efficiencies.

The Commission says that its Inquiry will investigate a range of options for fostering improved RF receiver performance, including industry-led voluntary measures, new policies and guidance from the Commission and, of course, updated or revised rules. The expectation is that a thorough evaluation of all of these options will clear the way for the introduction of new spectrum-based services in the same or nearby frequency bands, and help the U.S. maintain its global leadership in wireless technologies.

FDA Clarifies "Refuse to Accept" Policy for 510(k) Submissions

The U.S. Food and Drug Administration (FDA) has issued an updated guidance to explain its criteria for assessing whether a medical device premarket notification (510(k)) submission meets the agency's minimum requirements for substantive review.

Under the Medical Device User Fee and Modernization Act (MDUFA) and its successive amendments, the FDA must meet performance goals related to the agency's review of medical device submissions, based on the timeliness of those reviews. The FDA's Refuse to Accept (RTA) policy provides for an early review of all submissions in accordance with specific acceptance criteria and enables the agency to inform a submitting party whether its submission is "administratively complete" within 15 days of its filing.

The FDA says that the guidance, titled "Refuse to Accept Policy for 510(k)s," is intended to ensure consistency in acceptance decisions made by the agency and to help submitters better understand the types of information needed by the FDA to conduct its review.

The guidance includes several appendices that provide detailed "Acceptance Checklists" to be used by device manufacturers to verify that their submission for Traditional, Abbreviated, or Special 510(k) notification meets the FDA's requirements for review by the agency.

According to the FDA, the guidance will promote a more efficient approach to the review of medical devices by reducing review backlogs and clearing a path for the prompt review of safe and effective medical devices. But, like all guidances, the FDA's guidance on its RTA policy represents only the agency's current thinking on the topic and is not binding on either the FDA or the public.

FDA Updates List of Recognized Standards

The U.S. Food and Drug Administration (FDA) has updated its list of recognized international and national standards that can be used to demonstrate compliance with certain requirements for premarket review and authorization of medical devices.

In a Notice published in the *Federal Register*, the agency announced additions, withdrawals, and revisions to the list of FDA Recognized Consensus Standards. Notable among the more than 30 new standards added to the list is the addition of IEC 61326-1, which addresses general EMC requirements for medical electric equipment used for measurement, control, and laboratory use, and IEC 61326-2-6, which details EMC requirements specific to in vitro diagnostic devices.

Also newly added to the list of recognized standards is ANSI/AAMI 2700-1:2019, which covers essential safety requirements for medical devices and systems that incorporate software or other information technologies.

Smartphones with the Highest Levels of Electromagnetic Radiation

Recent research posted to a popular financial industry website shows that certain smartphone models may pose a higher potential safety risk due to the levels of electromagnetic radiation they produce.

Data from the German Federal Office for Radiation and posted to the Bankless Times website ranks ten popular smartphone models by the specific absorption rate (SAR) levels they emit. At the top of the list was the Motorola Edge smartphone model, which reportedly has a SAR level of 1.79 W/Kg, closely followed by the ZTE Axon 11 5G, with a SAR level of 1.59 W/Kg, and the OnePlus 6T model smartphone, with a SAR level of 1.55 W/Kg.

In the U.S., the Federal Communications Commission (FCC) mandates a maximum SAR for smartphones of 1.6 W/Kg.

The article ends by sharing the FDA's recommendations for minimizing exposure to cell phone radiation, including limiting the time you spend using your smartphone and using the available hands-free features.

FDA Updates Data on Breakthrough Device Program

The U.S. Food and Drug Administration (FDA) reports that it has granted more than 650 medical devices designations under its Breakthrough Devices Program.

The Breakthrough Devices Program, which replaced the FDA's earlier Expedited Access Pathway (EAP) program in 2019, is a voluntary program intended to provide patients and healthcare providers with more timely access to advance medical devices and device combination products. The Program offers device manufacturers a prioritized review of their submissions and direct access to FDA experts to address issues that develop during the premarket review phase.

To be eligible for designation under the Program, a device must meet two criteria, as follows:

1. The device provides for more effective treatment or diagnosis of life-threatening or irreversibly debilitating human diseases or conditions; and
2. One of the following:
   a. Represents a breakthrough technology;
   b. No approved or cleared alternatives exist;
   c. Offers significant advantages over existing approved or cleared alternatives; or
   d. Device availability is in the best interest of the patient.

According to the latest data available, the FDA has granted 657 Breakthrough Device designations as of March 31, 2022. This includes 147 designations in 2020, 216 in 2021, and 64 for the year to date. Cardiovascular and neurological devices dominate the types of breakthrough designations so far, with 158 and 114 designations respectively.

FDA Clarifies Cybersecurity Recommendations for Medical Devices

The U.S. Food and Drug Administration (FDA) has issued an updated draft guidance that contains recommendations for medical device manufacturers on ensuring the security of their devices from cyberattacks.

Published in the U.S. Federal Register, the updated draft guidance, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," provides recommendations on security measures that manufacturers should consider across a device's entire lifecycle. Some specific recommendations include:

- Adopting a secure product development framework to help reduce the number and potential impact of cybersecurity vulnerabilities during the useful life of a device;
- Developing a software bill of materials to track both manufacturer-developed and third-party device and device software components; and
- Ensuring that devices can be updated as necessary to protect against emerging threats.

The draft guidance also encourages device manufacturers to include documentation regarding cybersecurity protections as part of most FDA premarket submission applications, including 510(k) and PMA submissions.

Senate Introduces Medical Device Security Act

The U.S. Senate has introduced a bipartisan measure that would help to ensure the security and integrity of medical devices by implementing mandatory premarket cybersecurity requirements.

Introduced by Senators Bill Cassidy, M.D. (R-LA) and Tammy Baldwin (D-WI), the "Protecting and Transforming Cyber Health Care Act, otherwise known as the PATCH Act, would amend the Federal Food, Drug, and Cosmetic Act to "require…the inclusion in any premarket submission for a cyber device of information to demonstrate a reasonable assurance of safety and effectiveness throughout the lifecycle of the cyber device."

Companion legislation was previously introduced in the U.S. House of Representatives by Michael Burgess (R-TX) and Angie Craig (D-MN).

If approved by both Houses of Congress and signed by President Biden, the PATCH Act would authorize the FDA to require device manufacturers to demonstrate compliance with many of the recommendations contained in the agency's draft updated guidance on cybersecurity in medical devices.

ar rf/microwave instrumentation • ar modular rf • sunar • ar europe

We're with you all the way

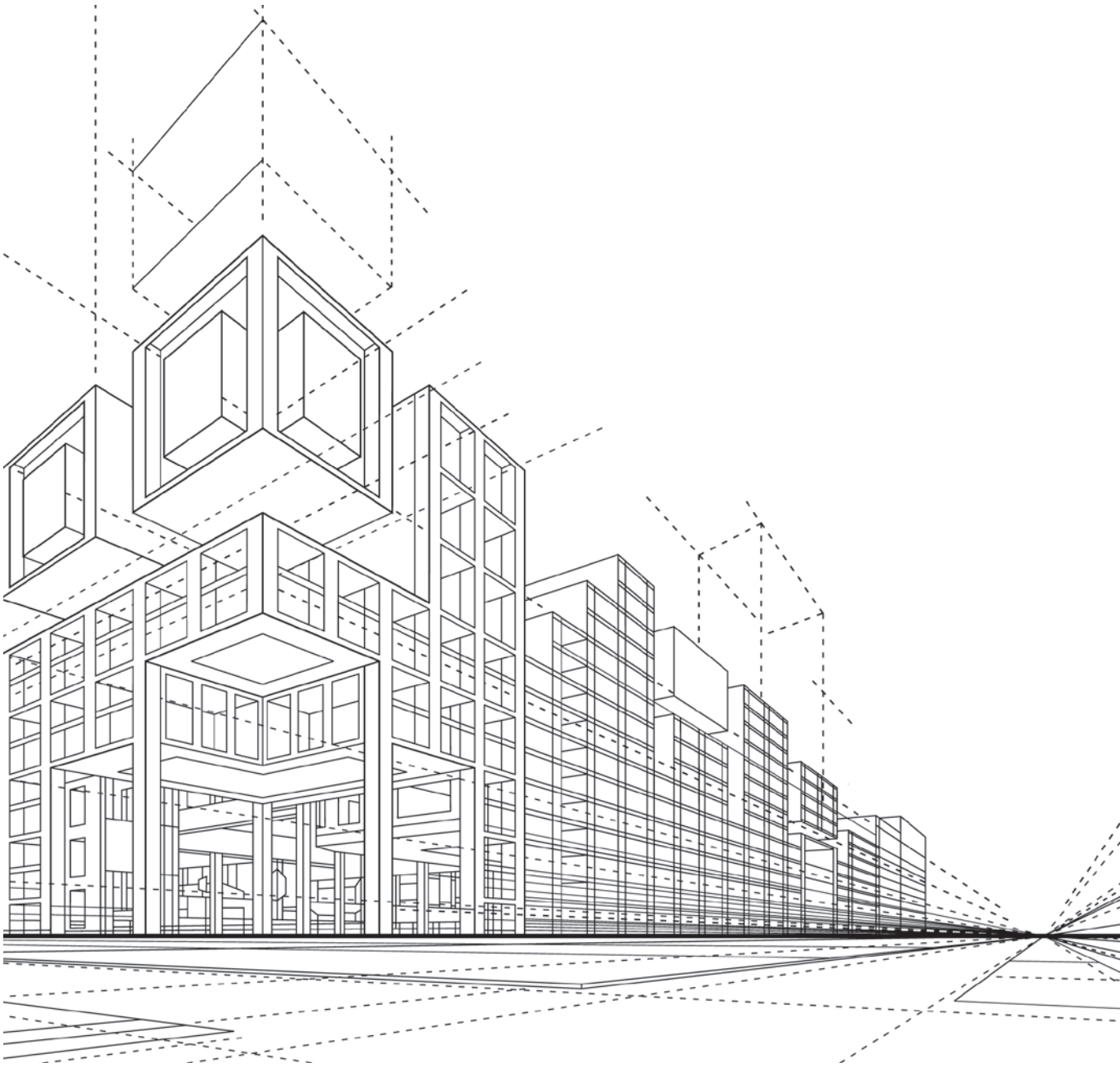
The **broadest bandwidth** with the **highest power.**

AR offers over **100 amplifiers** ranging from **10 Hz - 50 GHz** and with power levels of **1 W - 100 kW.**

For more information on AR Amplifiers, visit www.arworld.us
Or contact us at info@arworld.us & 215.723.8181

SCIF AND RADIO FREQUENCY SECURED FACILITY DESIGN, PART 2

An RF Shielding Performance Guide to ICS/ICD 705 and NSA 94-106 Design



Joel Kellogg is the Director of Business Development for Healthcare, Industry, and Government at ETS-Lindgren, and has more than 20 years of design, production, and management experience in healthcare, government, and industrial projects. He can be reached at joel.kellogg@ets-lindgren.com.

By Joel Kellogg

In recent years, we've noticed a growing confusion in the industry over design and performance requirements for sensitive compartmented information facilities (SCIF). Part 2 of this article is intended to highlight the significant difference in the performance of radiofrequency (RF) shielding between facilities designed per ICS/ICD-705[1] and those intended to meet NSA 94-106[2] performance requirements. We will also highlight some of the design and construction methodologies that lead to significant differences in performance.

INTRODUCTION TO SCIF SPECIFICATIONS

As noted in Part 1[3] of this article, there is a common misconception that a SCIF design utilizing ICS/ICD-705 construction recommendations will achieve the performance requirement set forth in NSA 94-106, the NSA standard for RF shielding performance and testing. Part 1 reviewed the typical construction recommendations identified in ICS/ICD-705, recommended materials, and typical installation methodologies used. The article further identified differences in typical construction between SCIF designs and facilities designed to meet the performance requirements identified in NSA 94-106 and provided explanations as to how those differences impact RF shielding effectiveness.

Part 2 of this article will highlight some of the methods utilized in ICS/ICD-705 that limit RF shielding performance and some alternate methods that could increase the RF shielding performance. Further, we will discuss other common deviations that often increase project costs without providing any enhanced RF performance. Finally, Part 2 will document the significant differences in potential RF performance utilizing measurement data collected from a facility built per ICS/ICD-705 construction methods and a facility designed to meet NSA 94-106 requirements.

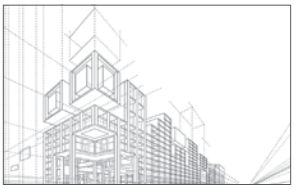
SCIF OVERVIEW

Ranging from physical barriers to facilities constructed using RF shielding with construction methods to reduce acoustic noise, SCIF requirements and construction specifications for a given project are based on a host of factors, including the purpose of the facility, surveillance risk, physical location, etc. The risk and vulnerability of the SCIF should be evaluated by the Accrediting Officer (AO) and Site Security Manager (SSM). That evaluation will help inform the selection of the technical measures required for each SCIF application. The project's Certified TEMPEST Technical Authority (CTTA) will assess the requirements for TEMPEST,[4] providing direction on RF shielding requirements and design.

Despite a clear process for design direction and general construction recommendations established in ICS/ICD-705, many project documents deviate from the typical ICS/ICD-705 direction. Those deviations can range from specifying alternate shielding materials to utilizing alternate construction methods to establishing RF performance requirements not supported by the project's design. These deviations often have a variety of adverse effects from increased project costs to designs that do not support the shielding requirements. This puts all involved, including the facility owners, facility designers, and general contractors, in the challenging position of having to work through the disconnects between design and specified performance, often during the construction phase of a project.

NSA 94-106 VERSUS ICD/ICS-705 PERFORMANCE

In Part 1 of this article, we noted that it is not uncommon for NSA 94-106 RF shielding performance requirements to be specified as part of a project's requirements for a SCIF using ICS/ICD-705



Based on their assessment, the CTTA may provide recommendations or require the shielding of floors and ceilings and request the inclusion of filters, treated penetrations, and RF doors.

wall types and construction methods. Further, many projects will reference what appears to be an arbitrary performance requirement. For example, a project's specifications may require 60 dB of performance from 1 GHz to 10 GHz, despite the fact that ICS/ICD-705 does not specify an RF shielding performance. Further, the general construction methods outlined in ICS/ICD-705 are not intended to achieve a specific RF shielding performance utilizing industry-standard methods for quantifying RF shielding performance as defined in test specifications such as IEEE 299[5] and NSA 94-106.

Previously, we noted several reasons why design recommendations in ICS/ICD-705 will not achieve NSA performance requirements. Some of these reasons include the manufacturer's data for the shielding foil material typically specified for SCIF applications clearly demonstrating that the material will not achieve NSA 94-106 shielding performance requirements. We also identified that the recommended construction for walls in ICS/ICD-705 results in substantial perforation of the shielding material, which will degrade performance. Other factors include the typical ICS/ICD-705 design recommendations that do not require shielding on the ceiling or floor and do not call for use of other elements critical to achieving high levels of RF shielding performance, including filters, waveguides for mechanicals, and RF shielded doors.

Based on their assessment, the CTTA may provide recommendations or require the shielding of floors and ceilings and request the inclusion of filters, treated penetrations, and RF doors. But this does not mean the design will meet NSA 94-106 performance without substantial changes to the general design recommendations provided in ICS/ICD-705.

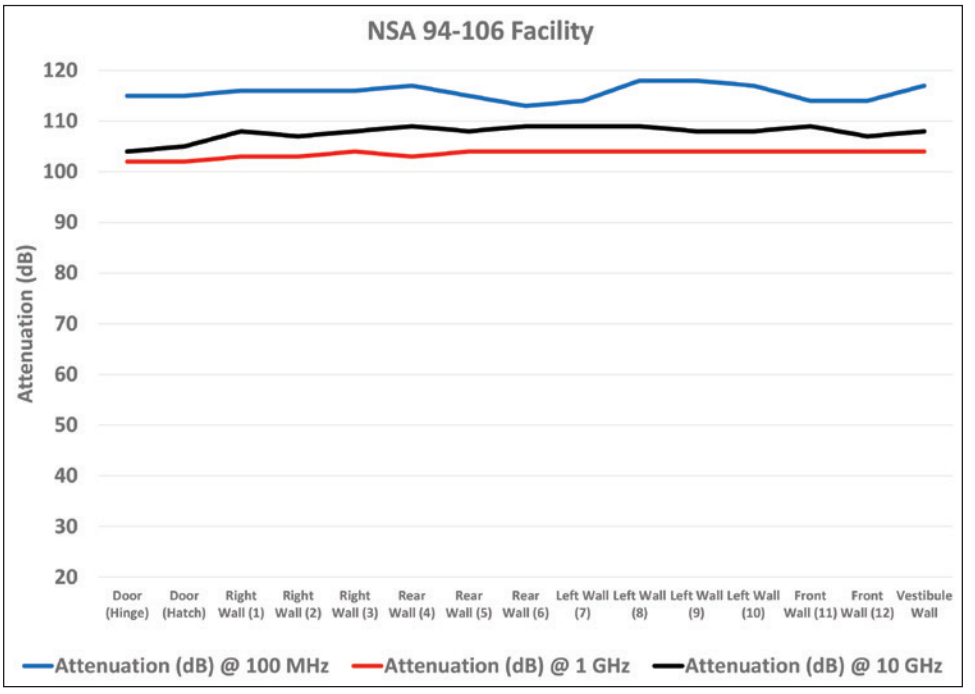


Figure 1: Facility design to meet NSA 94-106 requirements. Attenuation measured utilizing IEEE 299 test procedure.

To highlight this discrepancy, data is provided from two different SCIF facilities. The first facility, with performance data provided in Figure 1, was designed and constructed in strict accordance with NSA 94-106. Therefore, this facility was designed and constructed using shielding materials that meet all the magnetic field, electric field, plane wave, and microwave performance requirements identified in NSA 94-106, which include 100 dB of attenuation at 10 GHz. This requires a six-sided RF shielded enclosure with properly treated penetrations, electrical filters, and a high-performance shielded door.

The second facility design utilized the ICS/ICD-705 Wall A construction for interior walls and along exterior building perimeters. The facility design provided shielding enhancements beyond those identified in ICS/ICD-705, including RF doors, electrical filters for power and building management systems, HVAC RF waveguides, and RF waveguides for plumbing, which enhanced performance over the typical recommendations provided in ICS/ICD-705. Finally, the facility also included windows, which are typically discouraged under ICS/ICD-705 but are occasionally included in a SCIF design. This facility's project requirement identified custom RF shielding performance at 90 MHz, 900 MHz, and 6 GHz with attenuation requirements of 10 dB to 30 dB.

Since the SCIF facility performance requirements identified frequencies that did not coincide with NSA 94-106 test frequencies, only the 100 MHz, 1 GHz, and 10 GHz test frequencies of the facility designed to meet NSA 94-106 were provided to achieve as relevant a comparison as possible. There is clearly a significant difference in the performance, with average differences of 55 dB or more and peak differences of up to 80 dB. The ICS/ICD-705 Wall A calls for the shielding layer to be sandwiched between two layers of drywall, but the finish layer of drywall had not been installed at the

time that these measurements were recorded and the shielding performance would likely decrease further once the drywall is added.

DESIGN AND PRODUCT SELECTION CONTRIBUTORS TO LIMITED RF SHIELDING PERFORMANCE

RF performance will be significantly limited in cases where the SCIF design only calls for the ICS/ICD-705 wall construction without shielding on the ceiling and floor, and without RF doors, no treated penetrations, or filtered power. However, it is apparent from the data presented in Figure 2, the case in which many of these factors were eliminated, that there are still additional factors that limit performance.

In this specific application, the windows are one factor that limited performance. There are a few different types of protection for windows, including RF film, RF glass, and RF shielded windows, which incorporate an RF shielded screen. These technologies are typically limited to between 40 dB and 80 dB at 10 GHz, depending on the performance of a specific product, and vary in performance from 1 kHz to 10 GHz.

Another factor limiting the RF shielding performance is the primary recommended shielding material. An

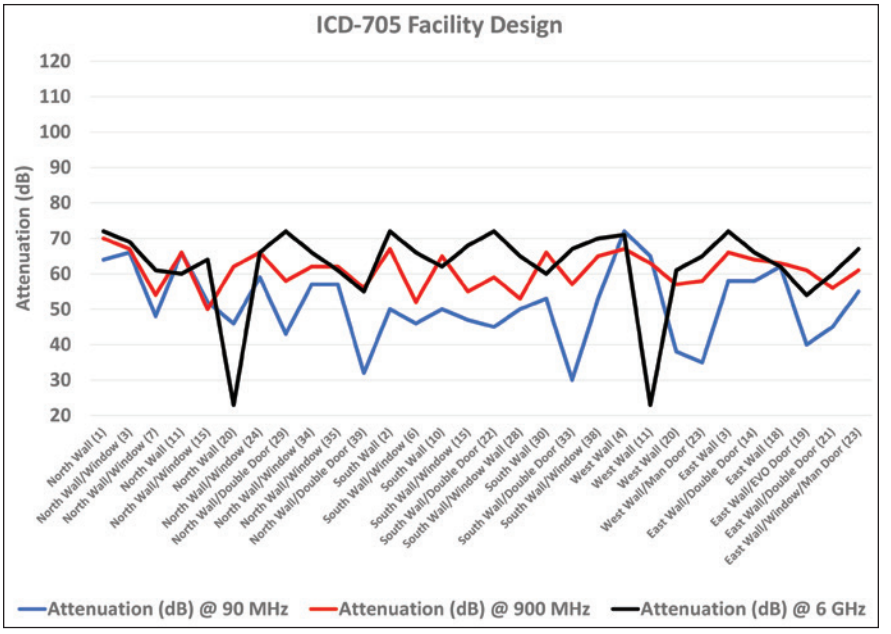


Figure 2: Facility design using ICD-705 Wall A with the addition of floor and ceilings, RF doors, filters, and treated penetrations. Attenuation measured utilizing IEEE 299 test procedure.

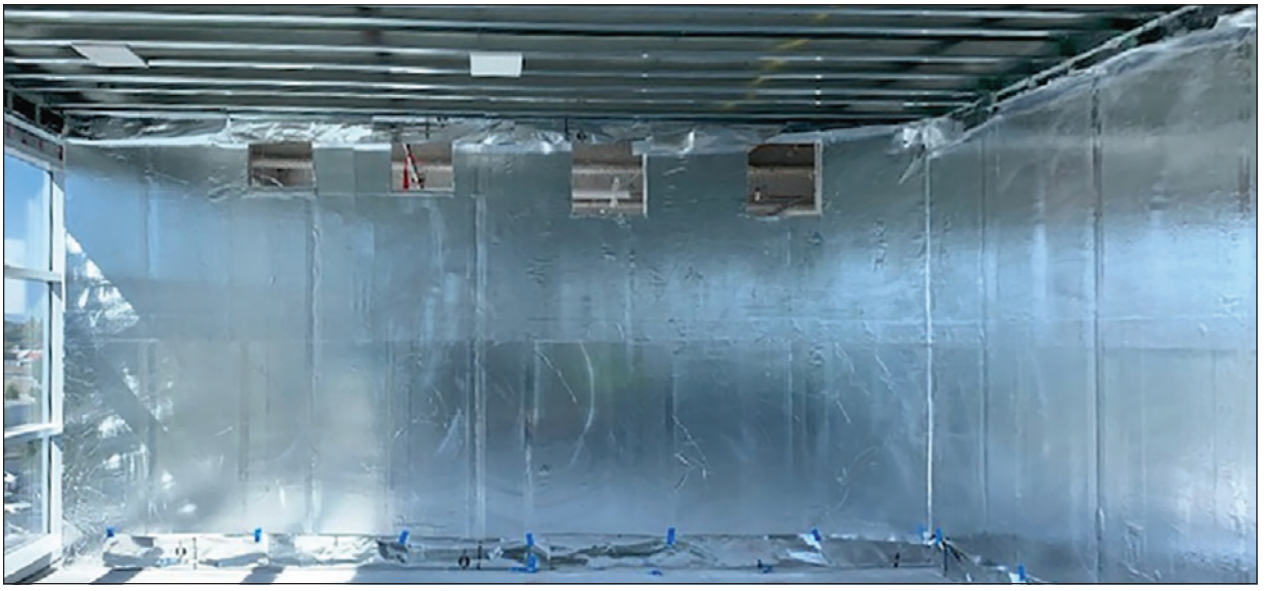


Figure 3: Example of ICS/ICD-705 RF shielding barrier installation

example of the material often used in SCIF designs is shown in Figure 3. The most frequently recommended shielding material does meet the RF shielding attenuation requirements of NSA 94-106, according to the manufacturer's data. But the manufacturer's data is based on a small sample under ideal test conditions, tested on an RF shielded enclosure, and performs optimally at greater than 100 dB from 100 MHz to approximately 1.5 GHz. Above 1.5 GHz, the performance rolls off according to the manufacturer's data. The performance below 100 MHz appears to roll off as well, and the attenuation will certainly decrease substantially for magnetic (H-field) fields as the frequency decreases.

To overcome the limited performance in some frequency ranges, some designs will specify thicker copper foil or aluminum sheets. But the specified materials may still not meet NSA 94-106 if identified as a performance requirement. Further, in the next section of this article, we will identify some construction challenges that will degrade RF shielding performance and limit the benefit of specifying a different material

It is also common to see many issues overlooked in designs that are critical to RF performance, resulting in incremental degradation of RF shielding performance. Common issues include not identifying all items that require filtering. Whether it is used for power, communication, data, or building management systems, a component than includes or uses conductive cables or wires needs to be filtered to maximize the RF performance of a shielding system.

There are multiple examples of a facility filtering all power sources but choosing not to filter all data lines because the data is entering through the floor, which is slab on grade. However, it does not matter the location from where that cable or wire is entering. If it is conductive, it has the ability to carry signals and radiate similar to an antenna. Similarly, critical or protected signals are at risk of coupling to those cables or wires and leaving the secured space. In some cases, this lack of protection may be a concern over costs associated with data filters or communication filters. However, a cost-effective solution may be to use fiber-optics in the secure space that can penetrate the shielding through an inexpensive RF waveguide or series of RF waveguides.

Other common design issues include allowing untreated mechanicals and plumbing not specific to the SCIF to penetrate and pass through the SCIF RF shielding. This simply creates additional points where RF signals can leak into or out of the SCIF. Again, if the purpose is to maximize RF shielding performance, then any penetration into or out of the shielded space must be properly treated. To avoid potential RF performance issues, it is recommended that only items being utilized in the RF shielded space of a SCIF pass through the RF barrier and that any other items supplying other areas of the facility be routed outside the shielded space. Of course, there are exceptions, but those should be evaluated individually based on an assortment of factors including the cost and the impact on RF performance.

CONSTRUCTION CHALLENGES CONTRIBUTORS TO LIMITED RF SHIELDING PERFORMANCE

The recommended wall detailed in ICS/ICD-705 shows the RF shielding material sandwiched between two layers of drywall or drywall and a substrate such as plywood (see Figure 4). The second layer of drywall must be secured to the wall, and this is typically achieved by mechanically fastening the drywall with screws. But this method penetrates the RF shielding, thus creating the potential for RF shielding leakage.

As mentioned in the previous sections, some designs will identify the use of an alternative shielding material. But this method of construction results in potential RF shielding leakage regardless of shielding material specified. Therefore, the installation of alternative shielding materials may not necessarily enhance RF shielding performance and result in additional project costs with no benefit to the RF shielding performance.

Other common construction challenges when building a SCIF include shielding at the ceiling, RF-shielded doors, and treatment of penetrations when specific RF performance requirements have been identified as part of the design requirements. Many SCIF designs may require that the wall foil turns onto and overlaps the ceiling around the perimeter of the SCIF when the ceiling is a metal pan deck. However, RF performance will be limited by the existing penetrations through the metal deck.

Additionally, projects may identify that a shielding material must be applied to a ceiling. In most cases, the ceiling is also used to support electrical and mechanical systems and components such as plumbing and HVAC. This is often accomplished using threaded rods or angles that are attached through the ceiling. An example is shown in Figure 5.

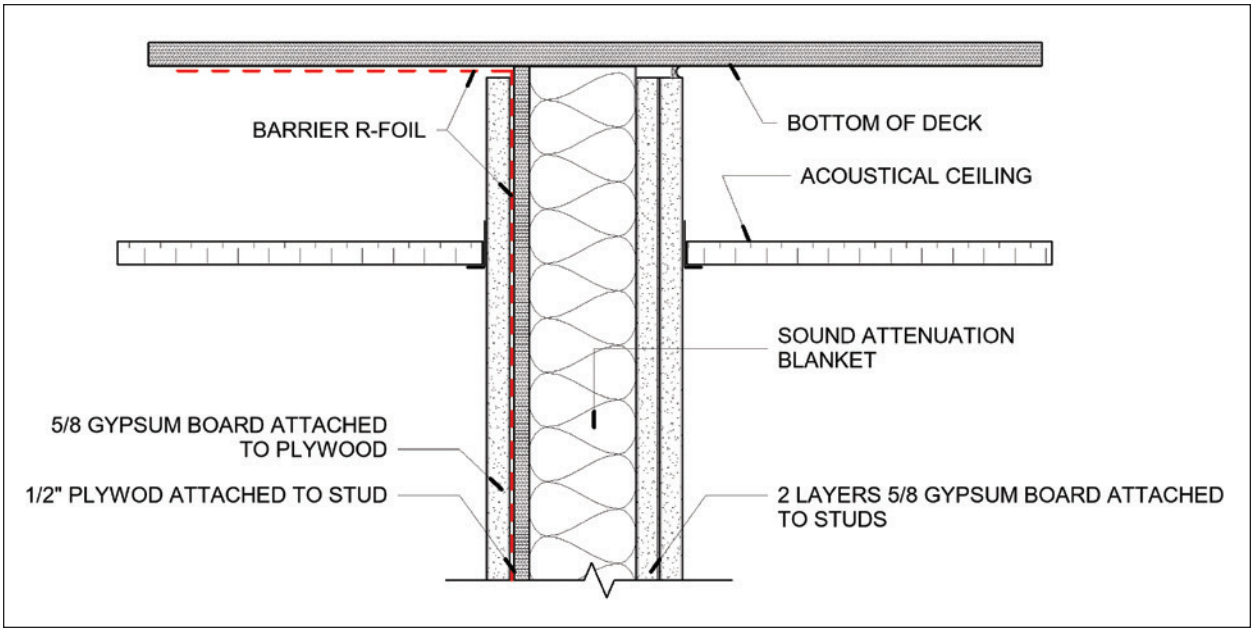
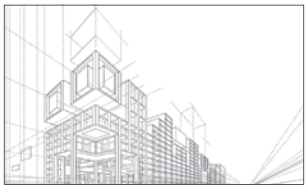


Figure 4: ICS/ICD-705 Wall C depicting an RF barrier between plywood substrate and finish drywall

Unfortunately, this technique may result in hundreds, if not thousands, of penetrations through the ceiling, creating the potential for RF leakage. RF shielding companies know how to treat these connections to maximize the RF shielding performance, but an HVAC contractor or plumber with no RF shielding experience is not likely to know how to manage the penetrations. Regardless, these additional penetrations of the shielding can have a negative impact on the overall RF shielding performance.

Figure 5: HVAC, electrical, and plumbing support angles with threaded rod penetrating copper fabric shielding material at the ceiling



Currently, there is no RF door available on the market that meets the typical acoustic requirements for a SCIF and the high levels of RF performance required under NSA 94-106.

There may also be untreated penetrations through the walls. If the penetrations are made of a conductive material, such as with conduit, plumbing, and HVAC ducts, it may be recommended that the shielding be bonded to the penetration in an effort to maximize the shielding performance. However, this recommendation does not represent a best practice for RF shielding and will likely reduce the overall shielding performance. Further, these penetrations may have construction debris or paint and may limit electrical conductivity if not cleaned properly. Lastly, the penetration may not be conductive, made of either PVC or some other nonconductive material. These penetrations represent additional areas that could significantly reduce the RF shielding performance. An example is shown in Figure 6.

ADDRESSING SECURITY REQUIREMENTS FOR RF SHIELDED DOORS

There is also a significant impact to doors when referencing NSA 94-106 or some other level of higher RF performance criteria for a SCIF application. Currently, there is no RF door available on the market that meets the typical acoustic requirements for a SCIF and the high levels of RF performance required under NSA 94-106. Additionally, specific high-security locks, including X10 locks, are required to meet security requirements. In order to maintain RF attenuation levels of 100 dB, locks typically need to be taken apart and modified to be integrated into an RF door. But this step voids the security rating of the lock.

Under NSA 94-106, these issues are addressed by either creating a vestibule or an enlarged door jamb to accommodate an acoustic door with the required security locks and a separate RF door to meet the RF performance requirements. Most SCIF designs do not include this type of design for doors, creating a significant and expensive construction issue when SCIF project documents identify NSA 94-106 or some other elevated level RF performance (>60 dB at 10 GHz).

CONCLUSION

As discussed in Part 1 of this article, referencing both ICD/ICS-705 and NSA 94-106 as part of a project can create much confusion in terms of project requirements. Part 2 of this article highlights the performance differences between the construction recommendations presented in ICD/ICS-705 and the requirements identified in NSA 94-106. Further, we highlighted that project-specific performance requirements may be difficult to achieve utilizing the construction recommendations provided in ICD/ICS-705. Placing specific RF attenuation requirements on a project utilizing ICD/ICS-705 can put a project at risk if the project's design is not carefully reviewed to ensure that RF performance requirements are met.

Figure 6: Untreated penetrations passing through shielding material representing a point where shielding performance may be significantly degraded

Finally, it is not uncommon to discover that a project's design will not meet the RF performance requirements. This puts the project team in the precarious position of having to determine where to compromise between design and project performance requirements while absorbing unexpected and potentially substantial additional costs.

To mitigate these issues, we recommend that SCIF design teams review the actual requirements with the CTTA before a project specification or request for quotation is finalized. It's also a good idea to include an RF shielding consultant on the design team to assist in coordinating the RF shielding design and to ensure that the finished structure meets the performance requirements.

REFERENCES

1. ICS/ICD-705, "Technical Specification for Construction and Management of Sensitive Compartmented Information Facilities." Available at https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf.
2. NSA 94-106 (not available for public reference).
3. "SCIF and Radio Frequency Secured Facility Design: An RF Shielding Design Guide to Navigating ICS/ICD 705 and NSA 94-106 Requirements," *In Compliance Magazine*, June 2021. Available at https://incompliancemag.com/article/scif-and-radio-frequency-secured-facility-design.
4. TEMPEST is a U.S. National Security Agency specification and a NATO certification used in reference to secure facilities.
5. IEEE 299, "IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures."

USING MULTIPORT CONNECTORS IN HIGH-FREQUENCY MILITARY AND AVIONICS SYSTEMS

Low Loss and High Security and Repeatability, with Reduced Size and Weight

Ted Prema began his career at Times Microwave Systems in 1979 as a program manager and has held multiple management and technical sales responsibilities in the company's commercial and mil-aero business segments over the years. He has a wealth of experience in applications engineering, RF Assembly design engineering, and program management. He earned his BSEE from Rensselaer Polytechnic Institute and MBA from the University of New Haven. Prema can be reached at techquestions@timesmicro.com.

By Ted Prema

Today, military and avionics electronic systems are being developed with increased frequency ranges to add bandwidth and functionality while also being designed to fit smaller spaces. Meeting reduced size, weight, and power (SWaP) system goals poses challenges for high-frequency RF/microwave cables and connectors that must meet complex electrical, mechanical, and environmental specifications but also enable access to subsystem modules for maintenance and troubleshooting. Fortunately, new multiport interconnector technologies exhibit low loss at RF/microwave frequencies with high security and repeatability. Their straightforward approach makes it easy to disconnect even in space-limited applications while maintaining the most demanding EMI/EMC requirements.

Civilian and military avionics systems such as radar altimeters and microwave landing systems (MLS) that once occupied DC to 12 GHz are now expanding into higher frequencies, typically to 18 GHz and often as high as 40 GHz. This expansion requires subsystem interconnects capable of providing the highest, most reliable performance while also fitting within limited airframe space.

In general, military electronic systems such as electronic warfare (EW), radar, and electronic countermeasures (ECM) systems are being designed for smaller spaces and higher efficiency via modular architectures. Such design approaches require fool-proof wideband interconnections that can be connected and disconnected within the tightest spaces while meeting all the electrical, mechanical, and environmental requirements of traditionally more-permanent 50-Ω interconnections, including waveguide and coaxial cables and connectors. The limited space also increases the need for very low EM radiated and leakage levels at all high-frequency interconnections to minimize interference between subsystem modules.

THE POTENTIAL OF MULTIPORT CONNECTORS

The miniaturization and functional density of modern military and avionics systems point to the need for multiport connectors that can be used to route many signals in small spaces. Multiport connectors make it possible to reduce the total amount of interconnection hardware for manned avionics systems as well as in unmanned aerial vehicles (UAVs) where a little less weight goes a long way in efforts to increase vehicle range.

Applications with growing numbers of interconnections at increasing RF/microwave frequencies can easily evolve into tangled masses of coaxial cables with difficult-to-trace interconnections and terminations when each cable has its own input and output connectors. The basic concept of a multiport interconnection is to locate interconnection points for as many of the cables as possible within a single harness so that different subsystem modules can be interconnected at one junction point and even color-coded or labeled to ease identification and accessibility during maintenance and inspection.

But among the challenges in creating such a multiport harness is enabling straightforward connector-to-connector attachments within the harness without adding the equivalent size and weight of the total separate interconnections while maintaining the electrical and mechanical performance requirements

Traditional coaxial connectors such as 50-Ω Threaded Neill–Concelman (TNC) connectors (Figure 1) have long joined military and avionics subsystem modules at frequencies through 18 GHz, terminating flexible and semi-rigid coaxial cables by crimp or solder attachments. The threaded mating of male and female TNC connectors forms a secure and reliable electrical and mechanical connection capable of withstanding the high shock and vibration levels to which those

systems are often subjected. A multiport connection must handle severe physical stress while reaching higher frequencies to support the wide bandwidths of modern systems. Since coaxial connectors are wavelength-dependent in terms of interface size, the interface dimensions must be much smaller than those of a traditional component such as a TNC connector to provide low-loss performance through 30 GHz or even 40 GHz.

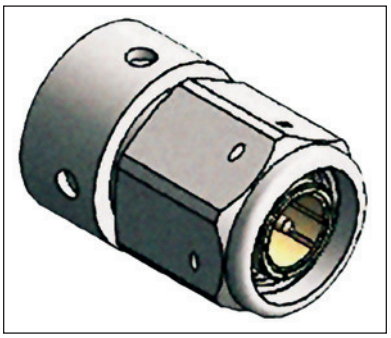


Figure 1: A traditional TNC connector

As military and avionics systems designers target denser solutions for tighter spaces, they impose changing requirements for coaxial connectors and interfaces, not just regarding their size and weight but also the need for greater control of the electromagnetic (EM) energy passing through connector interfaces at higher frequencies.

MULTIPORT CONNECTOR CHALLENGES

Traditional connector designs such as TNC connectors can require additional shielding (and weight) to limit electromagnetic interference (EMI) at microwave frequencies and to achieve the level of electromagnetic compatibility (EMC) required for the successful and reliable operation of high-frequency electronic systems with closely spaced coaxial interfaces. A connector interface that leaks EM energy and lacks proper shielding at the interface can result in a system failing EMC tests and suffering performance failures. A faulty connector interface with a lack of proper electrical bonding and shielding also exposes the conductor's signal to external influence. The interface specifications for traditional connectors such as TNC connectors are tightly controlled and detailed in published documentation such as MIL-STD-348 to avoid disparities in physical dimensions and tolerances.

A traditional military or avionic electronic system using multiple coaxial cable assemblies to link multiple subsystems and/or modules might have 50 or more individual connectors such as TNC connectors to join different subsystems to a main controller unit. Each connector occupies some amount of volume within the system equipment enclosure, the total volume of which can be reduced by an alternative connector interface such as a harness or shell with multiple ports that replace the comparable number of coaxial connectors that would normally be used for the interconnections.

The multiple-port interface is more complex than a single TNC interface but depending on the number of ports and the spacing between them, it can be made small enough to gain a significant advantage in size and weight compared to the same number of conventional coaxial cable assemblies. For military and avionics applications, such a multiport connector interface must meet or exceed the electrical, mechanical, and environmental specifications of the individual traditional coaxial connectors it is replacing.

MULTIPORT RF INTERFACE

Some general requirements for a multiport RF/microwave connector interface for modern military and avionics systems are based on the goal of saving size and weight without sacrificing the performance of traditional coaxial connector interfaces. For example, for radars and other systems that rely upon measurements of amplitude and phase for target positioning, sets of conventional coaxial cable assemblies are painstakingly amplitude- and phase-matched across wide frequency ranges to ensure that they do not contribute to errors in radar return signal measurements. Conventional coaxial cables and connectors can be assembled with the millimeter-wave dimensional precision required to manufacture sets of cables closely matched in amplitude and with the same phase lengths for connecting a radar's antennas to its transceiver or receiver and transmitter.

A smaller multiport connector solution to replace multiple cable assemblies in a radar system may be required to provide amplitude matching between ports that is typically within tenths of a dB and a phase balance that is typically within a few degrees. Specifications for coaxial cables and other transmission lines used in electronic systems are usually generated by an OEM, who details all of the

electrical and environmental requirements of their system and then works with an experienced RF assembly manufacturer who can design the optimized RF cable system. The ideal manufacturer is one who designs and manufactures the cable and connectors to create an optimized solution.

An effective multiport coaxial connector interface must also be designed to withstand the unique environmental conditions in which military and avionics systems are expected to operate, such as high shock and vibration, while maintaining electrically stable and secure interconnections. For systems that rely on signal amplitude and/or phase characteristics as part of a higher-order modulation scheme, effective multiport connector solutions must maintain continuous, undistorted electrical connections even under conditions of high shock, high vibration, and high humidity.

The deleterious effects of water absorption on a connector interface can be minimized by encasing the interface in a sealed enclosure. Cable assemblies for high-performance aircraft should be sealed to a level of not less than 1 x 10-5 cc/sec/ft of cable length. This lesson was learned in the 1970s when unsealed cable assemblies created reliability issues and resulted in the creation of Navy MIL-T-81490 and Air Force MIL-C-87104 specifications, which require 100% testing of vapor leakage, most often performed with a helium mass spectrometer.

Miniaturizing an RF/microwave connector interface requires tight spacing between multiple ports while still achieving sufficient isolation between ports to minimize EMI. For higher-power connector interfaces, port spacing can also play a role in the amount of heat that can be dissipated compared with conventional multiple coaxial cable assemblies. Conventional coaxial cable assemblies must tolerate wide operating temperature ranges as part of military and avionics systems without significant expansion or contraction of their conductive or dielectric materials. At higher RF/microwave frequencies, as signal wavelengths become smaller, the effects of physical changes in a material due to temperature are typically evidenced as variations in the amplitude and phase responses of signals carried by the channel's connector interface.

SAVED BY THE SHELL

A key part of a reliable multiport RF/microwave connector solution for military and avionics systems is the shell which houses the number of ports needed for the number of interconnections required by a system (see Figure 2). One shell can be machined to include as many as 50 ports or more, and additional ports or multiple shells can be constructed when more interconnections are needed within a system. Depending upon the application, such multiport shells can be machined from lightweight materials such as aluminum and manufactured with lead-free, REACH/RoHS-compliant processes tested to the

An electrically dense, multiport RF/microwave connector interface capable of replacing conventional (and trusted) coaxial cables and connectors in military and avionics systems must overcome a long list of engineering challenges.

most severe corrosion-resistance requirements. Such processes can help the multiport connector interfaces maintain excellent low-loss performance through mmWave frequencies even when exposed to fuel, salt spray, and corrosive chemicals.

The shell can also be sufficiently shielded to meet the most demanding EMI/EMC requirements for densely packed military and avionics systems. To ensure full contact force at the electronic contact points, the connection ports are spring-loaded with sufficient force to ensure continuous electrical connections under all conditions including high vibration. Mating a single multiport connector to multiple cables rather than employing multiple, entirely separate coaxial cable assemblies can help reduce system installation time, ease system maintenance and testing, and increase system reliability. By understanding the harsh environmental conditions of most military and avionics systems, the multiport connector shell can be constructed for the challenging combination of high vibration, shock, humidity, temperature, and chemical exposure that normally result in the electrical and mechanical deterioration of conventional coaxial cable assemblies.

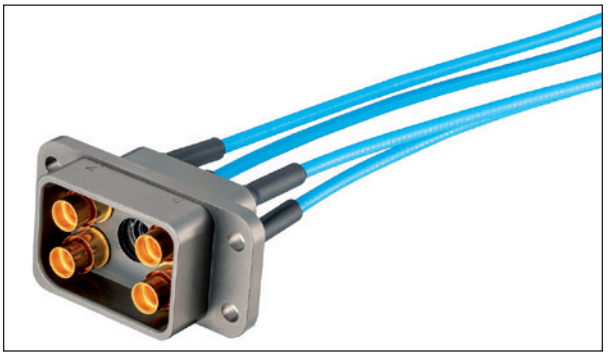


Figure 2: A machined shell is a key part of a multi-port RF/microwave connector solution

ENGINEERING CHALLENGES

An electrically dense, multiport RF/microwave connector interface capable of replacing conventional (and trusted) coaxial cables and connectors in military and avionics systems must overcome a long list of engineering challenges. These challenges include high reliability while operating under high shock and vibration, over wide temperature ranges, and in vacuum-like conditions that exist at high altitudes.

As previously noted, signals used in modern military and avionics systems, including intelligence, radar, collision avoidance, electronic guidance, navigation, EW, and communications, are using higher frequencies and covering wider bandwidths. Military and avionics systems that once operated at frequencies of 18 GHz are now extending into the millimeter-wave (mmWave) frequency range of 40 GHz. Further, to increase functionality, these systems are increasing electronic density, with more circuits and devices per square inch than ever. With more antennas and sensors, high-density systems require a greater number of interconnections, with smaller interconnection dimensions to fit in tight spaces.

Densification and miniaturization are partially driven by the rising demands for small SWaP military and avionics systems which depend on tighter interconnection spacing. An effective multiport RF/microwave connector interface solution should support multiple coaxial cable diameters, including 0.047-, 0.087-, and 0.141-in./diameter flexible and semi-rigid cable types for flexibility around the world in different applications and different frequency ranges.

A typical military or avionics system would connect its line replaceable unit (LRU) to the multiport RF/microwave connector interface. The LRU would connect with internal components and modules by means of small form factor connectors such as locking miniature push-on, locking miniature blind mate, or SMP-style, or directly to a printed circuit board (PCB). Connections with phase-critical

requirements can also be made with phase-stable or silicon dioxide (SiO_2) cables. Less critical connections most often utilize cables with Polytetrafluoroethylene (PTFE) (Teflon) dielectric such as small diameter flexible or semi-rigid RG-type cables or a flexible alternative to semi-rigid cables.

To accommodate densely packed, in-the-box applications, new high-performance, flexible cable assemblies are available for use that can be bent around tight corners and closely behind the connector to minimize footprint, save space, and simplify cable routing.

Depending on electrical and mechanical requirements, an extensive range of cables can also be used outside the LRU to connect to its end. Examples include military-grade, environmentally sealed cable assemblies most often used in airframe applications. These cables are available in a wide range of sizes, with armored options for use in applications where the cable will be subjected to a higher level of wear and tear and with lightweight options for applications where minimizing weight is critical. Selecting the best cable size will be based on the specific application's operating frequency, loss, and power requirements.

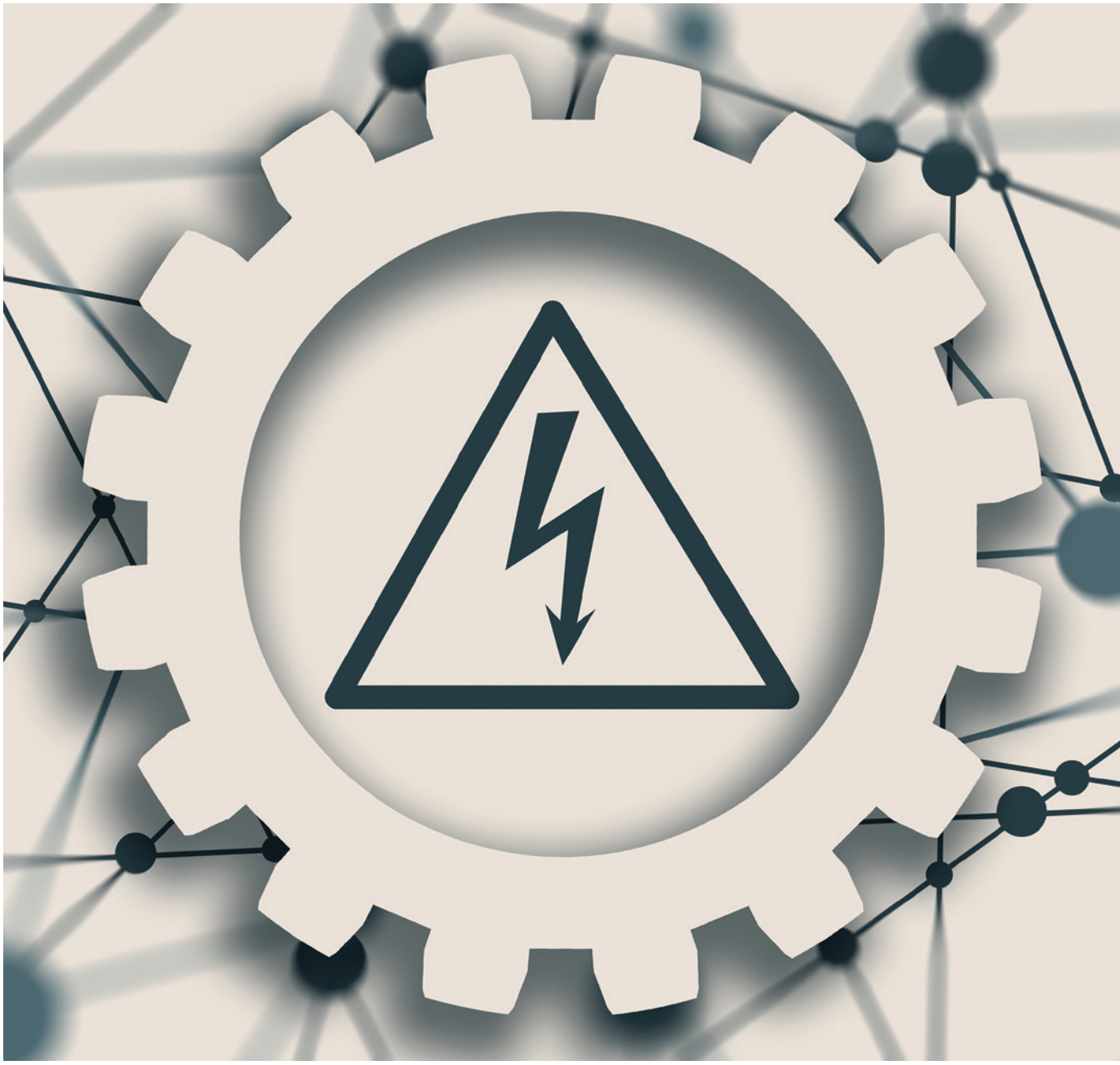
It is also not uncommon to use multiple cable types in a series run to address installation challenges or achieve a desired electrical result, such as a specific attenuation value that may need to be matched to a different part of the aircraft. Multiport contacts can also be keyed to prevent mismating with the keying plug inserted into one of the ports to avoid mating to one with a different key arrangement. Keying can also be done by using shells that have different radii.

CONCLUSION

Military and avionics systems are all customized by nature, with their own unique RF/microwave connector interface requirements. So the benefits of a multiport connector solution can be significant compared to the use of conventional RF/microwave cable assemblies. Specific requirements should be reviewed, such as frequency range, phase matching, EMI, etc., when considering a multiport connector interface. For densely packed systems in need of miniaturization, a multiport connector interface can provide an interconnection approach that speeds system assembly while meeting the EMC needs of the most densely packed electronic systems.

USERS GUIDE TO HIPOT TESTING

Production Safety Testing Ensures Compliance with Global Safety Standards



Chad Clark has been with Vitrek LLC since 2008. Over the years, Chad has had the opportunity to work directly with end-users to develop safe methods and procedures, enabling countless products to be NRTL safety listed. Chad holds a BE in Economics from California State University, Long Beach, and can be reached at chad@vitrek.com.

By Chad Clark

Because virtually all electronic devices and electrical apparatus require safety certification, manufacturers must submit samples of their products to compliance agencies and regulatory authorities to ensure they meet global standards.

This article gives an overview of the many safety standards required for certification and how advanced hipot testers have evolved to speed and simplify the compliance process. It also discusses the critical pre-testing setup and safety procedures required to ensure user safety. Finally, it describes the four types of essential hipot tests, dialectic withstand, insulation resistance, ground continuity, and ground bond testing, conducted during final production as well as the test results to look for.

UNDERSTANDING GLOBAL SAFETY STANDARDS

During the production phase of product development, products destined for sale in the U.S. market are typically sent to Nationally Recognized Testing Laboratories (NRTLs) for compliance testing. NRTLs provide services to certify compliance with the relevant standard(s) and regularly inspect the testing equipment and facilities.

The compliance evaluation conducted by an NRTL typically investigates two key areas of a product, as follows:

1. Construction—Mechanical construction, spacing, clearances, etc.; and
2. Safety—To assure safe operation, even under high-stress conditions.

The details of what constitutes an NRTL-certified product depend on the specific standard (or standards) applicable to that product. For products that will be sold and used in jurisdictions outside the U.S., the requirements of different standards may be applicable, potentially complicating the process of achieving global access.

In an effort to address this challenge, efforts are ongoing to harmonize standards internationally. An example is IEC 61800-5-1, a standard developed by the International Electrotechnical Commission (IEC) that addresses the safety aspects related to electrical, thermal, and energy in adjustable speed electrical power drive systems. In the U.S., the requirements of IEC 61800-5-1 have effectively replaced those of UL 508C, which has been withdrawn and superseded by UL 61800-5-1.

THE EVOLUTION OF HIPOT TESTING

Hipot testing has long been a standard procedure for various types of equipment. Hipot testers get their name from the "high potential" (high voltage) that they produce in order to perform dielectric withstand and insulation resistance tests. Many hipot testers also provide accurate, low-resistance measurements and low-resistance/high-current outputs to test ground resistance and ground bond integrity.

Figure 1: Modern hipot testers are designed to perform a range of electrical safety testing procedures.

The early commercial hipot tester was not much more than a step-up transformer used to adjust an applied voltage in stepped increases over prescribed time segments to test for leakage or component breakdown. However, this legacy method could easily lead to incorrect results when leakage current causes the voltage output from a high-impedance transformer source to drop.

In contrast, today's most advanced hipot testers utilize electronic source technology to assure compliance with IEC-61010, which explicitly requires that "the voltage test equipment shall be able to maintain the required voltage for the specified period of time."

HIPOT TESTING SETUP AND SAFETY PROCEDURES

By its very nature, electrical safety testing involves the use of high voltages and requires test operators to follow strict adherence to safety procedures. Operators should understand that high voltages are dangerous and that care must be taken to avoid contact with energized circuits. The importance of having trained personnel as the first step in ensuring a safe testing environment can't be overstated.

Station Setup

The next step is determining where the test station will be located. The test area should be isolated from the factory assembly area and located away from routine foot traffic to help ensure the safety of those who occasionally come near the test station. In addition, operator distractions should be kept to a minimum and the area should be conspicuously marked with internationally approved signage, such as "DANGER - HIGH VOLTAGE."

During testing, the hipot tester itself should have indicator lights to denote when high voltage is present. There should be ample and reliable power supplied to the test station. Verify that the power wiring meets electrical code requirements for polarization and grounding. Always use an outlet that has a properly connected protection ground and make sure this ground has been tested to ensure a low impedance path to the panel ground and earth bonded ground.

Figure 2a/2b illustrates two alternative approaches to the setup of a benchtop hipot test. In Figure 2a, the operator is wearing safety glasses, and the device under test (DUT) is placed on the test bench equipped with a combination of palm switches and a footswitch to prevent the operator from making direct contact with the DUT while testing is underway. As a practical matter, the use of palm switches is typically restricted to short-duration tests done on a repetitive basis with a series of DUTs. If this test setup is used for longer tests, operators often find a way to bypass the palm switches, thereby defeating their intended purpose of protecting the operator.

Figure 2b shows the DUT placed under a protective cover with an interlock to isolate the operator during the test. The use of an enclosure is a more reliable means of assuring operator safety, particularly when testing requires longer time periods. More elaborate test stations can include a hipot tester interlock as well.

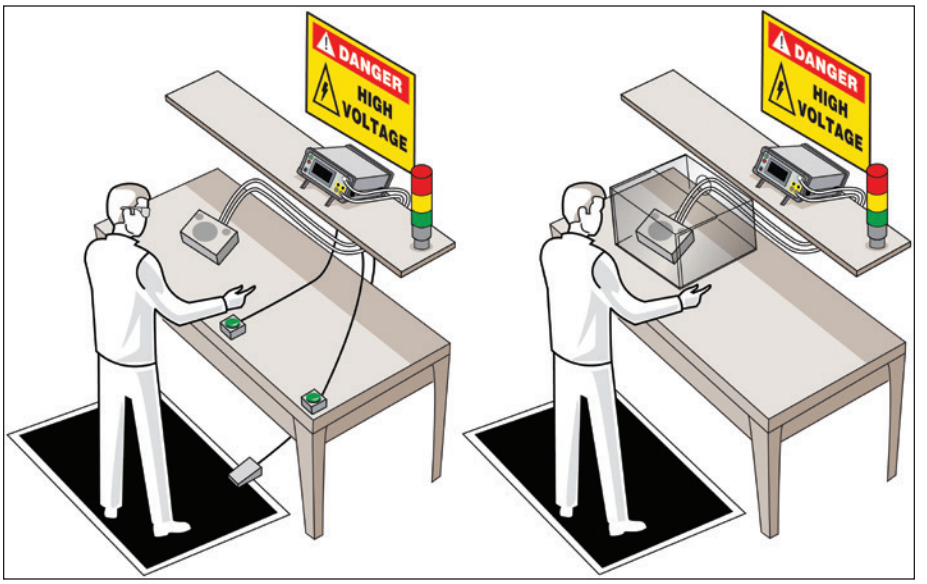


Figure 2a/2b: Two alternatives for benchtop hipot testing setup. 2a (left) employs palm and footswitches. In 2b, the DUT is placed under a protective cover.

NASA AWARD WINNER

A HIGHER STANDARD FOR SPACE TESTING

Trusted by NASA, NTS is the worldwide leader in space and aeronautics testing. Call (800) 270-2516—and discover what it means to test to a higher standard.

NTS | A HIGHER STANDARD
TESTING | INSPECTION | CERTIFICATION

www.nts.com

One safety method that utilizes the interlock is a light curtain, which is an infrared light beam that opens the interlock if anyone interrupts any part of the beam. The output of the light curtain is connected to the interlock terminal on the hipot tester. If the interlock is open, high voltage is immediately terminated. The light curtain is placed in between the hipot tester or the DUT and the operator. For the operator to touch the high voltage, they would have to pass through the light curtain, triggering the opening of the interlock and terminating the high voltage.

If the hipot is placed behind a light curtain, a method must be available to initiate the test, and a footswitch is an easy solution. But keep in mind that the test space must be designed to prevent anyone from reaching the high voltage by going around the light curtain.

Operator injury may result if the hipot tester is not properly connected to an earth ground. The work area and bench surface should consist of non-metallic materials, which means that metalwork surfaces should be avoided, and metal objects should not be placed between the operator and the DUT. All other metal objects should either be grounded or placed outside of the test area altogether. An ESD mat is not a recommended platform for a test station, as it may cause erroneous readings for leakage and is unnecessary in this application.

The test equipment should also provide for immediate and safe removal of the output voltage using internal discharge circuity, either at the conclusion of the test or if the test is interrupted. Never remove power for the hipot tester. If there is a power interruption, use extreme care in any contact with the DUT. The safest approach is to leave the DUT connected to the hipot tester until power is restored and the tester can conduct its discharge function.

The test station should have sufficient space for the tester and the DUT without the operator having to reach over the DUT to access the tester. The tester should be at least three inches away from the wall to provide proper airflow for the unit. Ideally, the DUT should be isolated from the operator and the tester. For larger DUTs, which are wheeled to the test station, the cart should be non-conductive and have locking wheels. (This also applies if the tester needs to be wheeled to the DUT.) Keep the area clean and neat, and arrange the equipment so that it is easy and safe for the operator to use.

There are many safety features that can be added to the test station to prevent the operator from encountering high voltage, such as guards or enclosures. When placed around a DUT, guards or enclosures should be non-conducting and be equipped with safety interlocks that interrupt all high voltages when open. Interlocks should be arranged so that operators are never exposed to high voltages under any conditions.

In addition, it is easy to implement circuit palm switches that prevent the operator from encountering high voltage during testing. The basic operation of a palm switch requires the operator to use both hands to initiate a test with, potentially, a footswitch to activate the test. If one or both hands are removed from the switches while testing, the test is immediately stopped. The switches are placed directly in front of the operator and spaced shoulder-width apart. Spacing the switches in this way prevents an operator from trying to press both buttons down with one hand or object.

No high voltage can be applied to the output terminals and DUT until both switches are pressed simultaneously. The operator cannot touch the DUT or test leads if both hands are on the palm switches. The palm switches are connected to the digital I/O on the hipot tester. Only when the switches are in the down position is the start function enabled. Once one switch goes up, the safety interlock is enabled, terminating the output voltage of the hipot test. This method is safe, quick, and effective.

On a regular basis, typically at the start of every shift, the tester itself should be checked by connecting the tester to both PASS and FAIL samples. These samples should be designed to confirm the proper operation of the tester based on the type(s) of tests to be conducted (hipot, insulation resistance, ground resistance, or ground bond). Once all of the connections are made, and the prescribed test procedure is selected, the operator should confirm that all test parameters specified in the testing documentation are displayed on the tester screen. Operation of the test can then be conducted, keeping in mind the safety considerations described previously.

HIPOT TESTING DURING PRODUCTION

Hipot testing during production is performed to:

- Assure compliance with safety agency labeling requirements;
- Detect defective components or assembly flaws; and
- Reduce the incidence of latent field failures and the attendant warranty costs.

Once in production, products must be 100% tested to confirm compliance with the related agency certifications and safety standards. Production tests are less stringent than initial certification testing but will generally include basic dielectric withstand and shock hazard (leakage) tests.

Plug-connected devices will also be subjected to ground resistance and ground bond tests if required by the applicable standard. Electrical motors, transformers, and other such devices will likely include insulation resistance tests.

Periodic inspection and calibration of test equipment is a standard requirement to maintain NRTL certification for the product being produced. This inspection will include a check of hipot instrument calibration certification. This "cal cert" is typically required to be renewed on an annual basis. (NRTLs require compliance certification with ISO 17025.) Another common requirement prescribed by most NRTLs is a daily functional test of the hipot equipment.

Test 1: Dielectric Withstand

The basic hipot test applies a high voltage from the conductors to the chassis of the DUT. This test is often referred to as dielectric test or voltage withstand test. Its purpose is to confirm that the insulation and isolation of the non-conducting surfaces from

the operating voltage are sufficient to avoid a shock hazard. The typical specification for this test is 1000V + 2x normal operating voltage.

Both AC and DC hipot tests are possible and, in general, the test should use the same type of voltage as would be used during normal operation. However, if a DC hipot test is used on an AC circuit, the hipot voltage should be two times the peak, that is (2 x 1.4 x RMS) + 1000V (see Figure 3).

Depending on the applicable standard, units will pass this test if either:

- The leakage current measured is less than the maximum allowable current; or
- No breakdown occurs, i.e., there is no sudden and uncontrolled flow of current.

In the case of double-insulated products, higher voltages are often specified in the test standard. In addition, this class of device typically requires special fixturing to connect the non-conductive outer shell to a conductive element.

Defects that are often detected with the hipot test include contamination (e.g., dirt, debris, etc.) and lack of proper spacing (creepage and clearance) of components. Creepage is measured across surfaces, while clearance is the air gap between components. Contamination would likely cause an unacceptable level of leakage current. Clearance problems can result in a breakdown.

Desirable hipot tester features for dielectric withstand testing include:

- Adjustable maximum output voltage:
  - 5KV is adequate for many applications
  - Higher voltages (up to 30KV) may be required
  - AC and DC outputs
  - Excellent regulation – both line and load
  - Controllable ramp rates, dwell times, and discharge features
  - Phase angle measurement of leakage current – capacitive coupling detection
  - Some standards allow for in-phase and quadrature currents to be measured separately. Leakage current due to capacitive coupling may not be a safety concern
- Min/max pass/fail current limits:
  - Separate limits during ramp
- Programmable multichannel testing

Test 2: Insulation Resistance

Insulation resistance testing is likely to be required in motor winding, transformer winding, and other applications involving cabling or insulated wire. Insulation resistance testing typically involves confirming that the resistance exceeds a defined high resistance value.

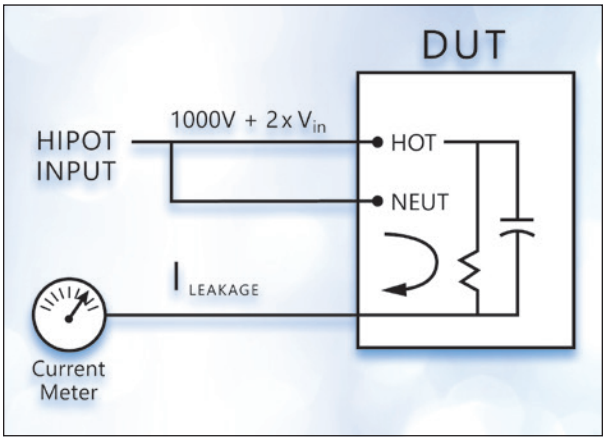


Figure 3: Hipot is applied to both conductors and leakage is measured in the return circuit through the ground connection.

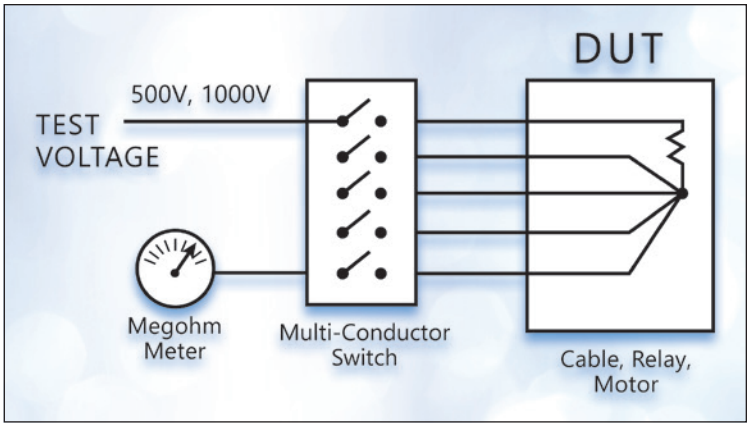


Figure 4: Voltage is applied to one conductor at a time while adjacent conductors are bundled. Resistance is calculated based on leakage current.

In many instances, insulation resistance needs to be measured between several conductors. Examples include cable/connector assemblies, multiconductor cables, and relays. To make this measurement, all the conductors except one are shorted together, and the test voltage is applied from the remaining conductor across the bundled ones. Each wire is then tested in this fashion (see Figure 4.)

Desirable hipot tester features for insulation resistance testing include:

- Wide range of selectable test voltages
- Accurate/repeatable high-resistance measurement
- Programmable high voltage switching accessory
- Multichannel programmable testing
- Pass on steady and increasing voltage

Test 3: Ground Continuity

Ground continuity testing is performed to confirm that the conductive chassis of a device is safely connected to the earth ground pin on the power plug. This assures protection against shock hazards even if the equipment suffers an internal short to the chassis. The current would be shunted via the ground wire and would likely trip the breaker or blow the fuse.

Ground continuity is performed by applying a low current (e.g., 50 mA) and calculating the resistance from the ground pin on the power plug to selected locations on the exposed surfaces of the DUT.

Desirable hipot tester features for ground continuity testing include:

- Accurate, repeatable low resistance meter
- Plug adaptor accessory to speed testing

Figure 5: An example of an advanced hipot tester with ground bond testing capabilities

Test 4: Ground Bond

Whereas ground continuity measures the resistance of the safety ground connection, the ground bond test assures the integrity of the connection. Using the same test setup, a high current is passed through the circuit. If the ground bond is solid, the current passes without a change in resistance.

Desirable hipot tester features for ground bond testing include:

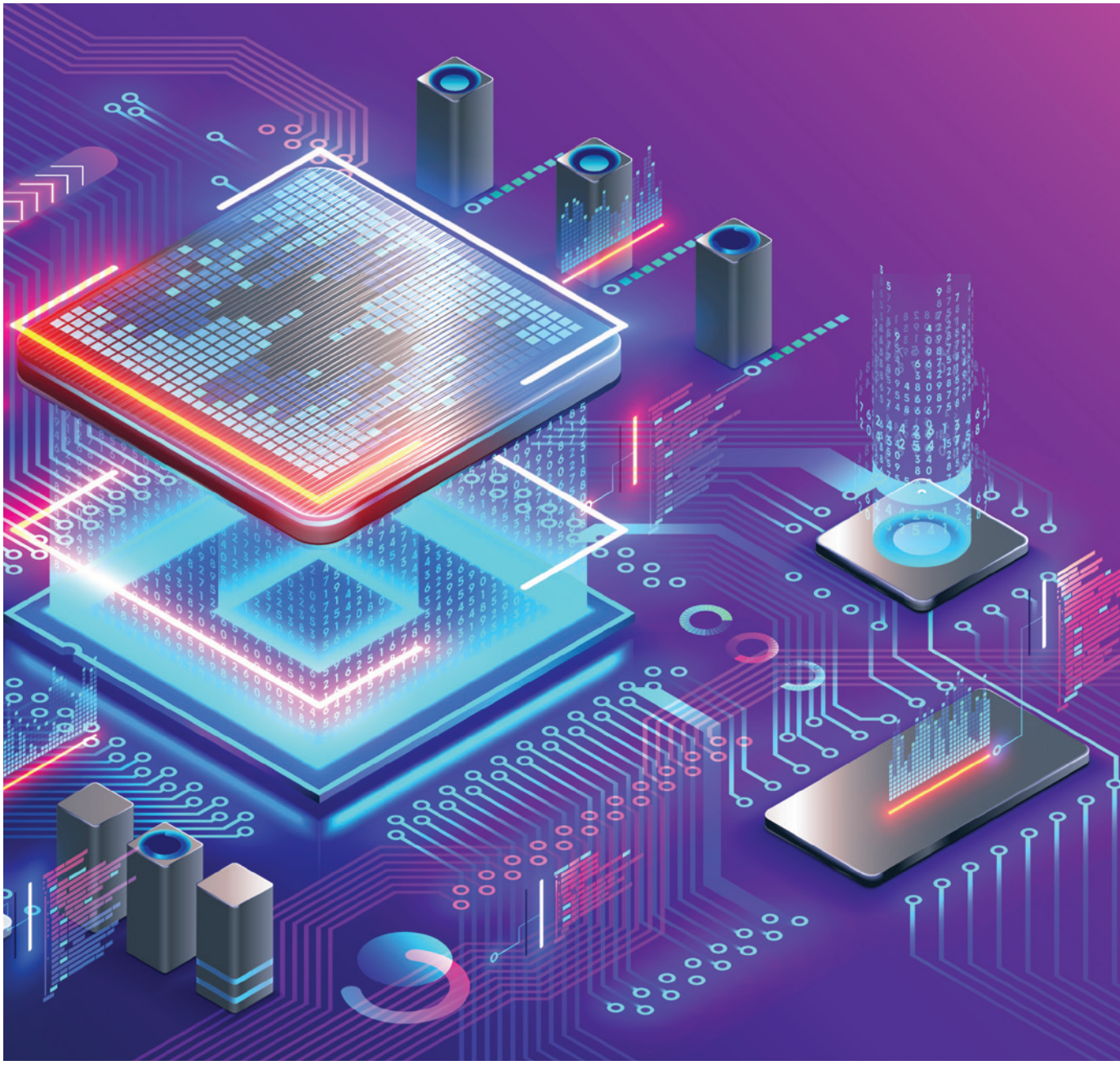
- Accurate high-current source
- Programmable test currents and test times
- Plug adaptor accessory to speed testing
- 4-wire milliohm meter - providing a Kelvin connection for highly accurate low resistance measurement

CONCLUSION

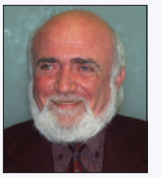
Hipot testing is an important final step in the production process for most electrical and electronic equipment. With programmable features and advanced functionality, today's hipot testers simplify electrical safety testing. But before commencing testing, manufacturers should be aware of the many updated safety certification standards and their requirements. And test operators must ensure upfront that they have set up a safe testing environment and fully understand the applicable testing protocols.

HIGH-INTEGRITY COMPONENTS IN ELECTRICAL EQUIPMENT, PART II

How to Deal with High-Integrity Components



Steli Loznen has over 40 years of experience in compliance issues associated with electrical equipment and participates in the IEC standardization as WG Convener and Project Leader. In 2017, he received the IEC's "1906 Award" in recognition of his efforts to advance the work of the IEC. Loznen is also a member of the Experts Evaluation Team of the European Commission, a member of the Board of Governors of the IEEE-PSES, and a vice-president for IEEE-PSES technical activities. Loznen is co-author of "Electrical Product Compliance and Safety Engineering" – vol.1-2017; vol 2-2021 published by Artech House. He can be reached at sloznen@ieee.org.



By Steli Loznen

Part I of this article focused on the distinction between safety-critical components and high-integrity components. In this second part, we discuss the main aspects related to high-integrity components.

SAFETY STRATEGY FOR HIGH-INTEGRITY COMPONENTS

In general, good high-integrity component (HIC) design is based on having several physical barriers between a hazard and any entity for whom that hazard may pose a danger. The greater the potential consequences of the risk presented by the hazard, the greater the importance of undertaking whatever mitigation measures or efforts are required to reduce the likelihood of the risk being realized. For some components, especially those used in primary circuits, achieving adequate levels of safety can require meeting very demanding requirements.

An effective HIC safety strategy views hazard identification and hazard analysis and control as a continuous, iterative process applied throughout HIC development and use. Once hazards have been identified, they are addressed either by eliminating them from the HIC design if possible or, if not, by preventing or minimizing their likelihood of occurrence, controlling the risks that do occur, and minimizing their potential damage. Safety must be built into an HIC from the beginning; it cannot be added to a completed design or tested into an equipment.

Qualitative rather than quantitative approaches need to be emphasized in any HIC, as quantitative procedures must necessarily omit important but unmeasurable factors and, therefore, may be misleading.

Supporting a claim of high integrity for a component requires a lot of work. The technical literature explicitly states that it is hard to build a safety case for an HIC. In broad terms, a safety case represents the full suite of documentary justification used to support the safe operation of an HIC. This includes claims being made regarding the safety of the HIC, the arguments that allow such claims to be made, and the necessary evidence to substantiate them. Each element (e.g., design, manufacture, failure analysis, a forewarning of failure, etc.) of a safety case should be robust and stand on its own, with individual elements as independent of one another as possible so that a deficiency in one element does not undermine the arguments presented in the other elements.

Routine verification tests are recommended for high-integrity diode safety barriers, as well as tests of current-carrying capacity of printed circuit board connections on which HICs are mounted.

In addition, qualified non-destructive testing (NDT) during HIC manufacturing is used to ensure the absence of structurally significant defects. Derived from defect tolerance assessment, this type of testing will reliably detect defects early in the product life cycle with a suitable margin. These tests, together with other relevant routine production line tests, are the basis for building confidence for achieving full manufacture inspection qualification. The general approach is to determine the size of a limiting defect at the end of a product's life and then applying a margin of at least two times. This number is then combined with the predicted failure rate throughout a product's life to determine a defect size that must be rejected at the start of life.

Defect tolerance assessment methodology covers the approach and key input parameters, including selection of limiting locations, material property determination (lower bound materials toughness properties), classification of loadings and stresses, defect characterization, analysis type, failure assessment curves, materials aging, and the determination of limiting and safety-significant defects.

In this context, it is important that an HIC be designed for inspectability. The main elements of this methodology are to develop an inspection specification to define defect types and performance requirements, develop inspection techniques to meet the requirements of that specification, and then qualifying inspection procedures and personnel through a combination of technical justifications and practical trials.

The following examples illustrate the parameters of concern that need to be addressed for several typical components to qualify as an HIC [1]:

a. A safety shunt can enter in a failure mode only by short circuit, and at least two shunts in parallel shall be used as an HIC;
b. A mains transformer becomes an HIC when it has an attached fuse in the primary circuit and a current limiting resistor in the secondary output. In addition, the wire sizes and segregation must be inspected and must pass routine testing;
c. A current limiting resistor HIC needs to be constructed from vitreous-enameled wires and may fail only by opening. A carbon resistor cannot be an HIC;
d. Capacitor (e.g., Y1 capacitors) HICs need to have high reliability, and at least two capacitors shall be mounted in series. Electrolytic and tantalum capacitors cannot be an HIC;
e. A pressure sensor transmitter is an HIC if it is designed to meet safety integrity level 3 (SIL 3), per IEC 61508, the industrial functional safety standard, and has high availability (i.e., continues to work in the presence of failure).

The SIL mentioned above has four categories, from 1 to 4. It is defined by the end-user through a risk analysis of the process. SIL is related to the fulfillment of the tolerance risk. This means that the SIL level results from the combination of two factors:

- Frequency of failure occurrence, and
- Consideration of the consequences of failure (dangerous failure or safe failure).

In accordance with established engineering practices, improving the safety and reliability of the equipment's expected function should be implemented by adding elements of redundancy and diversity. Redundancy is targeted at meeting the single failure criteria, whereby the failure of just one part of an HIC must not result in the failure of the overall HIC. Diversity aims to provide protection against common cause failure; redundant electrical power and communications are recommended to be utilized.

HIGH-INTEGRITY PROTECTION SYSTEMS (HIPS)

An interesting application of the HIC is represented by the high-integrity protection system (HIPS), a part of a safety instrumented system (SIS) and regarded as the last line of defense. A HIPS is an independently instrumented system, the function of which is to protect an installation from over-pressure, overheating, or overflow hazards, and differs from traditional safety systems such as relief devices. A HIPS system consists of multiple barriers, including a process shutdown system (PSD) and an emergency shutdown system (ESD). It also includes processes to isolate the concerned equipment from the source of danger and mitigating the risk of harm before the design conditions are exceeded.

A typical HIPS will include 2 or 3 output elements (solenoid valves and actuators) in series and is often required to shut down within 2-3 seconds for gas and 6-8 seconds for liquids, depending on the pipeline pressure, flow rate, and the diameter and class of the pipeline. The initiator of the shutdown sequence (peak pressure surge, flow, or temperature) is detected by an input element, such as sensing transmitters for pressure, flow, or temperature. In this case, three sensors are connected to the logic solver (solid-state or programmable logic controller (PLC)), which is configured to vote with a 2oo3 logic (2 out of 3). If the predefined parameters for pressure, flow, or temperature are exceeded, the logic solver will shut down the output elements and the process. The 2oo3 configuration is usually preferred for HIPS, as it provides availability as well as reliability for the system [2].

Each HIPS component needs to be documented with the following information:

- Quality plan and manufacturing control plan
- Component certificates
- Component specifications
- Component reliability report
- Tests procedures

- Tests reports
- Dimensional drawings

The minimum SIL level required for a HIPS is SIL 3. This safety integrity level is to be justified by evidence of compliance with the following requirements [3]:

- Common cause failure (or CCF, the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system and leading to system failure) is to be considered;
- Safe failure (a failure that does not have the potential to put the HIPS system in a hazardous or fail-to-function state) of the process is to be defined;
- Proof-test (a periodic test performed to detect failures in a HIPS system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition) intervals are to be defined and applied;
- The response time requirements for the HIPS system are to be clearly defined;
- A description of the process measurements and trip points is to be provided;
- A description of SIS process output actions and the criteria for successful operation is to be defined;
- A trip is to be ordered when the system de-energizes;
- HIPS system is to be reset after shutdown;
- Procedures for starting up and restarting the HIPS system are to be clearly defined;
- All interfaces between the HIPS system and the other systems are to be carefully analyzed;
- The software is to be compliant with SIL 3 level; and
- The meantime to repair in which it is feasible for the HIPS system to be compliant with SIL 3 level.

Looking at the components available on the market today, it is not difficult to source the different specifications needed for an HIC. The challenge is more in the validation and verification of the end-use equipment to ensure that it fully meets the requirements outlined in the safety requirements specification (SRS) and that the SIL level is maintained throughout the safety lifetime of the equipment.

The traditional approach to producing software is to determine the requirements, implement them, and then try to ensure that there are no errors in either.

SOFTWARE AS A HIGH-INTEGRITY COMPONENT

The traditional approach to producing software is to determine the requirements, implement them, and then try to ensure that there are no errors in either. The problems with this approach from a safety standpoint are that correct implementation of the requirements does not guarantee safety, and it is impossible to ensure that software is "perfect." In fact, perfect (error-free) software does not exist. Software as a component requires special attention and needs to be treated as a high-integrity component.

It is possible that the origins of the concept of HIC can be found in software, in which the architecture focuses on the decomposition of the design into individual functional or logical components that represent well-defined communication interfaces containing methods, events, and properties. When high-integrity components are defined as those with a low likelihood of failure, it is difficult to apply this definition to software components. Some regulations consider the probability of failure of software as 100% based on the presumption that if a defect exists in the software (e.g., error in the algorithm), and the algorithm is executed, the error will happen in any case. In other words, the software cannot be a high integrity software.

In reality, this is not totally correct. Using adequate tools (i.e., architectural risk control measures, aspect-oriented, logical and physical design, etc.), software components can be of high integrity, becoming fault-tolerant and reducing the opportunities for software failures that can cause an unacceptable risk of harm [3].

When designing high-integrity software, it is important to keep fault tolerance and security issues at the forefront of considerations. The three main objectives of high-integrity software are:

1. Confidentiality (sometimes termed privacy) by protecting against unauthorized and/or accidental disclosure of information caused by system failures or user errors;
2. Integrity by protecting against unauthorized and/or unintentional modification of information caused by system failures or user errors; and
3. Availability by protecting against unauthorized withholding of information and/or failures of resources.

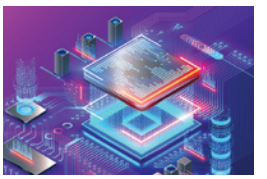
For example, software in safety-critical equipment requires encryption, authentication, and access control to protect against unauthorized modification. When the information from such equipment passes over an untrusted communication link, additional mechanisms must be incorporated to deal with any lost, spurious, or corrupted communications.

Following is a short list of safety features incorporated in a high-integrity software:

- Dual watchdogs, such as independent watchdog and system window watchdog
- Backup clock circuitry with clock security system
- Supply monitoring
- I/O function locking
- Critical register protections with write-once registers
- Memory protection unit with enough regions to ensure data integrity from invalid behavior
- Dual stack pointer
- Fault exceptions and debug module

The control system for an HIC software module utilizes fiber optics for communication and incorporates multiple fault-tolerant redundancies and highly reliable SIL-rated, field-proven components.

Choosing the right path in selecting components that meet specific qualification standards gives increased confidence in the component robustness for an equipment where safety integrity is required.



The HIC software design should provide the capability for full system testing as required to maintain its SIL rating over the life of the HIC software module.

To guide the development of high-integrity software, some international safety standards can be used, as follows:

- Industrial functionality: IEC 61508 series, using SIL 3
- Safety-instrumented systems for the process industry sector: IEC61511 and ANSI/ISA S84.01
- Machinery equipment: ISO 13849 series and IEC 62061
- Industrial cybersecurity: IEC 62443, using Security Level (S-L) 4
- Programmable controllers: IEC 61131 series
- Automotive industry: ISO 26262 series, using ASIL D
- Medical application: IEC 62304, using Class C
- Railway: EN 50128 and EN 50657, using SIL 4
- User-programmable integrated circuits (i.e., FPGA and CPLD): EN 50129

The above standards provide processes and techniques to help make a claim of achieving an acceptable level of integrity and hence risk. Note also that some of these processes and techniques also help to reduce random hardware failure.

CONCLUSION

There are many different challenges in analyzing, designing, building, and testing an HIC. One of the main challenges is the lack of standards outlining design parameters, resulting in a high level of interaction between end-users, engineering, and contractors during the analysis and design phase.

In our opinion, safety-critical components and high-integrity components are examples that provide a better understanding of safety significance and complexity. Choosing the right path in selecting components that meet specific qualification standards gives increased confidence in the component robustness for an equipment where safety integrity is required. The designer needs to assess the characteristics of these components and the failure trigger stress factors (electrical, thermal, shock and vibration, aging, electrical noise, etc.) to reduce the likelihood of component failure.

The assessment of the mechanisms of failure (both permanent and transient), the mechanisms for detection of these failures, and the capability to respond to a failure by a clear understanding of the propagation limits of failure are tools that increase the probability that the harmful states cannot be reached or, if they are reached, are detected and handled safely before losses occur.

Despite the paramount importance of safety issues in electrical equipment, purchasers and vendors of electrical equipment often have a limited understanding of safety issues and the hazards of such equipment. The result of this limited understanding is a lack of effective means to manage these issues. This is an important social, ethical, and regulatory issue that will need to be addressed constructively in order to ensure that these principles are correctly applied to electrical equipment.

REFERENCES

1. *Independent High Integrity Safety System,* ABB, 2017.
2. IEC Standard 61508-1: 2010, Ed.2.0, "*Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 1: General requirements.*"
3. *Software System Safety Handbook,* Joint Services Computer Resources Management Group, U.S. Navy, U.S. Army, and the U.S. Air Force, 1999.

EVALUATION OF PCB DESIGN OPTIONS ON ANALOG SIGNAL RF IMMUNITY USING A MULTILAYER PCB

Part 2: Radiated Immunity Testing

By Bogdan Adamczyk, Scott Mee, and Bilguun Baatar

This is the second of three articles devoted to the design, test, and EMC immunity evaluation of multilayer PCBs containing analog circuitry. The first article presented a top-level block diagram description of the design problem under research [1,2]. This article is devoted to the RF immunity testing according to the ISO11452-11 Radiated Immunity Reverberation Method standard from 400MHz – 1GHz, up to 100V/m. As a reminder, two analog measurements are present on the PCB. The first analog measurement captures analog temperature values from a Negative Temperature Coefficient (NTC) thermocouple at the end of a short harness. The second analog measurement captures the analog voltage of 12 volts connected at the banana jack terminals of the PCB. Both sets of values are processed by the microcontroller and reported to the test engineer outside the chamber via Universal Asynchronous Receiver Transmitter (UART) and fiber optic communications for isolation. However, for this article, only analog temperature measurements are presented and discussed.

Dr. Bogdan Adamczyk is professor and director of the EMC Center at Grand Valley State University (http://www.gvsu.edu/emccenter) where he regularly teaches EMC certificate courses for industry. He is an iNARTE certified EMC Master Design Engineer. Prof. Adamczyk is the author of the textbook "Foundations of Electromagnetic Compatibility with Practical Applications" (Wiley, 2017) and the upcoming textbook "Principles of Electromagnetic Compatibility with Laboratory Exercises" (Wiley 2022). He can be reached at adamczyb@gvsu.edu.

Scott Mee is a co-founder and owner at E3 Compliance which specializes in EMC & SIPI design, simulation, pre-compliance testing and diagnostics. He has published and presented numerous articles and papers on EMC. He is an iNARTE certified EMC Engineer and Master EMC Design Engineer. Scott participates in the industrial collaboration with GVSU at the EMC Center. He can be reached at scott@e3compliance.com.

Bilguun Baatar is an electrical engineer specializing in EMC design and testing. He graduated from Grand Valley State University with a BSE in Electrical Engineering and his focus is on EMC pre-compliance testing and expanding the understanding of EMC concepts/procedures. He can be reached at bilguun.baatar@e3compliance.com.

1. PCB VARIANTS AND TESTS CONFIGURATIONS

In this study, there are seven design variants that all contain a similar schematic but implement different PCB layout techniques (see [1] for the details). The design variants are described in Table 1.

Variant	Analog Trace Routing Style	Analog Trace Routing Layer	Grounding Method	Ground Split Geometry	Ground Split Layers
1	Differential	Microstrip on top layer	Single Ground Reference (GND)	N/A	N/A
2	Single Ended				
3	Differential	Embedded on layer 3			
4	Single Ended				
5	Single Ended	Microstrip on top layer	Split Ground Reference (AGND and GND)	AGND under analog circuitry, adjacent to GND*	All layers
6				AGND under analog traces, surrounded by GND*	Layer 2 only
7		1-3-1-3-1-3-1-3-1			

Table 1: Design variants

Table 2 shows the test configurations used during the testing of the selected variants.

The details of the measurement setup are shown in Figure 1.

All tests were run in continuous wave (CW) transmission (e.g. no modulations utilized).

2. IMMUNITY TESTING RESULTS – CONFIGURATION A

Variant 1 and Variant 2 test results are shown in Figure 2.

Observations: Variant 1 tested in Configuration A exhibited anomalies (with the exception of 600 to 680MHz) with the analog temperature readings. Variant 2 tested in Configuration A exhibited anomalies (with the exception of 640 to 650MHz and 700 to 720MHz) with the analog temperature readings. Compared to Variant 1, Variant 2 performed slightly better, especially below 600MHz. This demonstrated that differential routing did not provide any significant benefit.

Next, Variant 3 was tested, and the results were compared to those of Variant 1. The comparison is shown in Figure 3 on page 42.

Observations: Compared to Variant 1, Variant 3 performed slightly worse throughout the whole range. This demonstrated that burying differentially routed traces did not provide a noticeable benefit.

Next, Variant 4 was tested, and the results were compared to those of Variant 2. The comparison is shown in Figure 4 on page 42.

Observations: Variant 4 performed very similarly to Variant 2, with no significant differences. This demonstrated that burying the traces in a single-ended mode did not provide any noticeable benefit.

Configuration A	Configuration B	Configuration C
• Non-conductive enclosure • No filters on analog signal traces • All 7 variants	• Conductive enclosure • 4 non-conductive standoffs • Non-conductive ground ring gaskets (top & bottom) • No filters on analog signal traces • 3 worst performing variants, (1,5,6)	• Conductive enclosure • 4 conductive standoffs • Conductive ground ring gaskets (top & bottom) • Selective filtering on analog signal traces • Worst performing variant (1)

Table 2: Description of test configurations

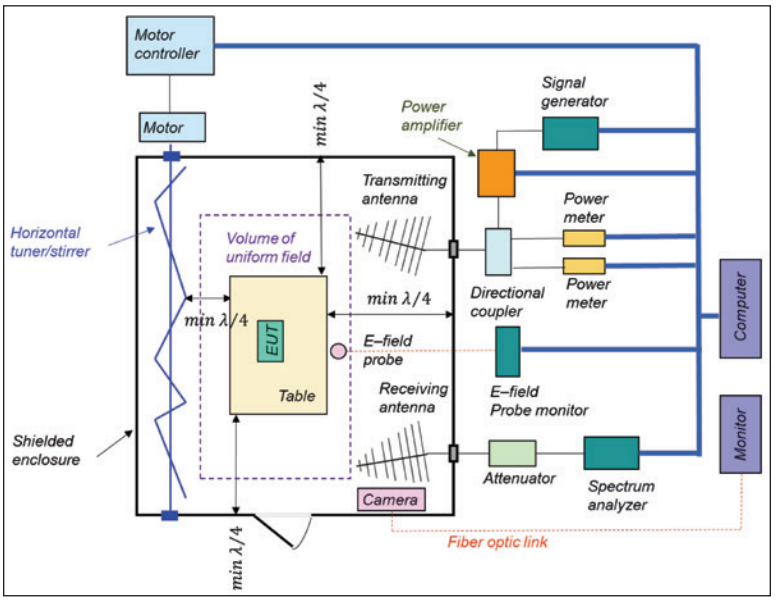


Figure 1: ISO11452-11 measurement setup

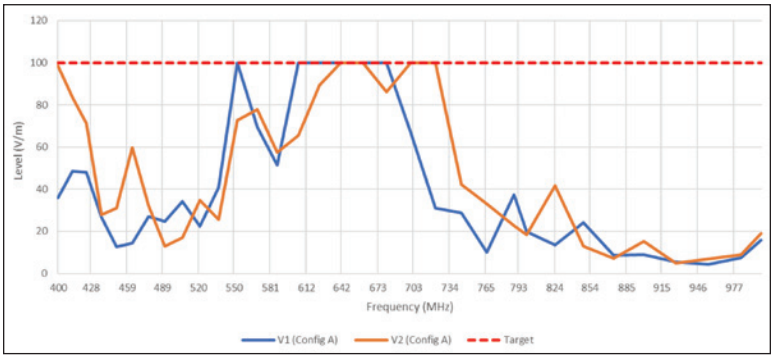


Figure 2: Configuration A: Variant 1 vs. Variant 2

Next, Variant 5 was tested, and the results were compared to those of Variant 2. The comparison is shown in Figure 5.

Observations: Variant 5 showed slightly worse performance than Variant 2 across the entire spectrum. This demonstrated that splitting the grounds, ground (GND) and analog ground (AGND), has a negative impact on the performance.

Next, Variant 6 was tested, and the results were compared to those of Variant 5. The comparison is shown in Figure 6.

Observations: Variant 6 performed slightly better than Variant 5 except for the region around 460MHz. This could indicate that having AGND isolated on Layer 3 has a positive impact on the performance in a split ground topology.

Next, Variant 7 was tested, and the results were compared to those of Variant 6. The comparison is shown in Figure 7.

Observations: Jumping the analog traces from Layer 1 to 3 (Variant 7) introduces regions where one variant outperforms the other. Variant 7 shows better immunity in the lower frequency range, while Variant 6 is better in the mid-frequency range. Our experience has shown that jumping layers should be avoided as it introduces anomalies in an unpredictable frequency range.

3. IMMUNITY TESTING RESULTS – CONFIGURATION B

The three variants which exhibited the weakest RF immunity performance in Configuration A were re-tested in the same frequency range. The weakest RF immunity was exhibited by Variants 1, 5, and 6.

Figure 8 on page 44 compares the test results for Variant 1, Configuration A vs. B.

Observations: Variant 1 in Configuration A generally outperforms Configuration B up to 700MHz. Between 700MHz and 800MHz, Configuration B shows a benefit. Beyond 800MHz,

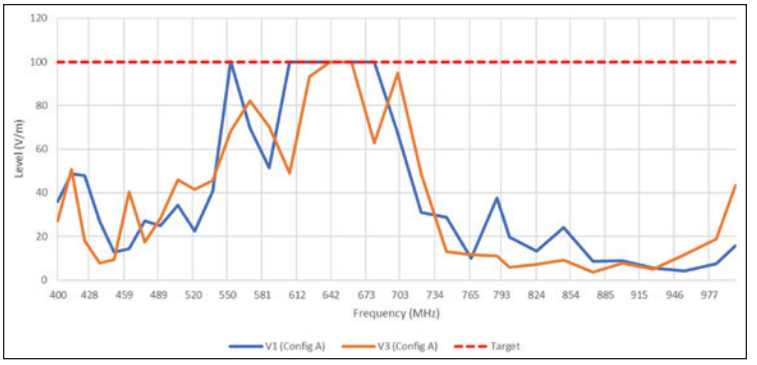


Figure 3: Configuration A: Variant 1 vs. Variant 3

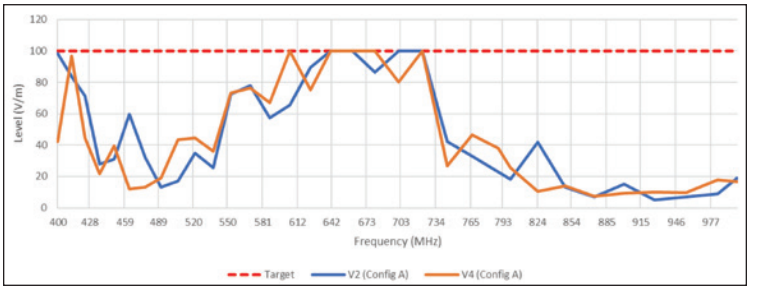


Figure 4: Configuration A: Variant 2 vs. Variant 4

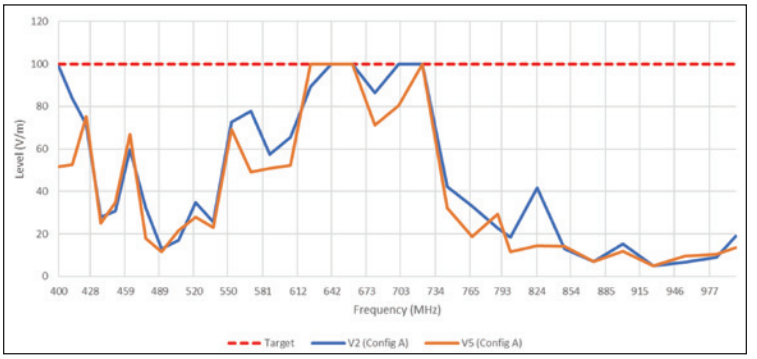


Figure 5: Configuration A: Variant 2 vs. Variant 5

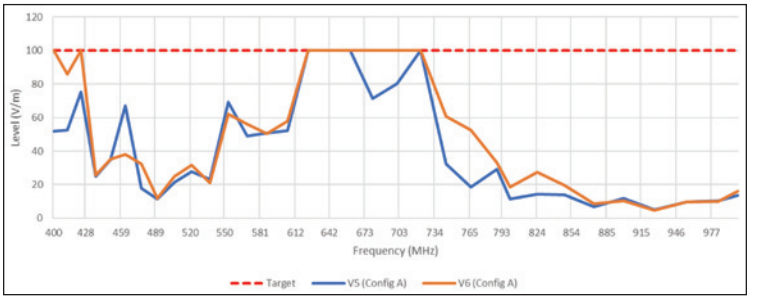


Figure 6: Configuration A: Variant 5 vs. Variant 6

there is no noticeable difference in performance. Based on the data, an ungrounded shielded enclosure provides benefits in a limited frequency range.

Figure 9 on page 44 compares the test results for Variant 5, Configuration A vs. B.

Observations: Variant 5 in Configuration B performed similarly to Configuration A with the exception of 400MHz and 740MHz – 880MHz range. There are inconsistent benefits of Configuration B most likely due to the split ground strategy that doesn't provide complete shielding from the enclosure.

Figure 10 on page 44 compares the test results for Variant 6, Configuration A vs. B.

Observations: Variant 6 in Configuration B performed similarly to Configuration A with the exception of frequencies around 420MHz and 620MHz – 720MHz range. There are inconsistent benefits of introducing an ungrounded conductive enclosure (Configuration B). In Variant 6, the analog

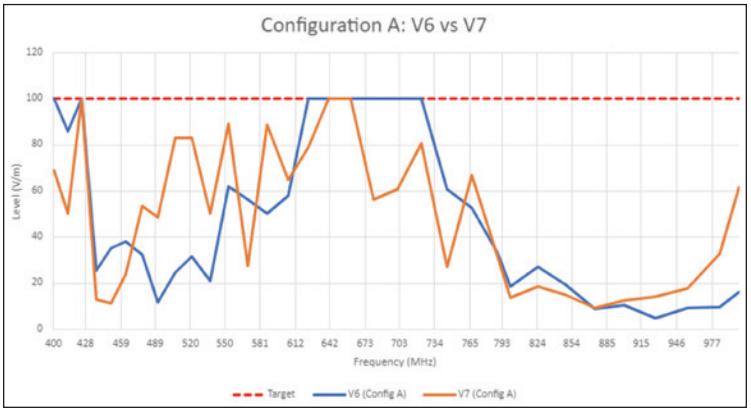


Figure 7: Configuration A: Variant 6 vs. Variant 7

traces are routed on the top layer with PCB GND surround and a separate Analog GND beneath on Layer 2. All other layers are PCB GND. These layout design features make the ungrounded shielded enclosure have less impact on the immunity performance.

4. IMMUNITY TESTING RESULTS – CONFIGURATION C

Finally, the worst-performing variant from Configuration B (Variant 1) was re-tested in the same frequency range. Figure 11 compares the test results for Variant 1, Configuration A vs. C.

Observations: Variant 1 in Configuration C performed dramatically better than Configuration A over a wide band of frequencies from 400MHz to 1000MHz. Improvements were made due to the shielded enclosure, conductive standoffs, conductive gaskets, and selective filtering components on the analog lines. Since Configuration B (shielded enclosure, non-conductive standoffs) didn't provide as much benefit as Configuration C, the added conductive gaskets, conductive standoffs, and component filtering likely provided the most benefit.

5. FUTURE WORK

The next article will discuss the results of the RF conducted immunity testing.

REFERENCES

1. Baatar, B., Costantino, C., Morey, R., Muldowney, C., *EMC PCB Design Study,* GVSU senior project sponsored by E3 Compliance, LLC.
2. Adamczyk, B., Mee, S., Baatar, B., "Evaluation of PCB Design Options using a Multilayer PCB – Part 1: Top-Level Description of the Design Problem," *In Compliance Magazine*, May 2022.

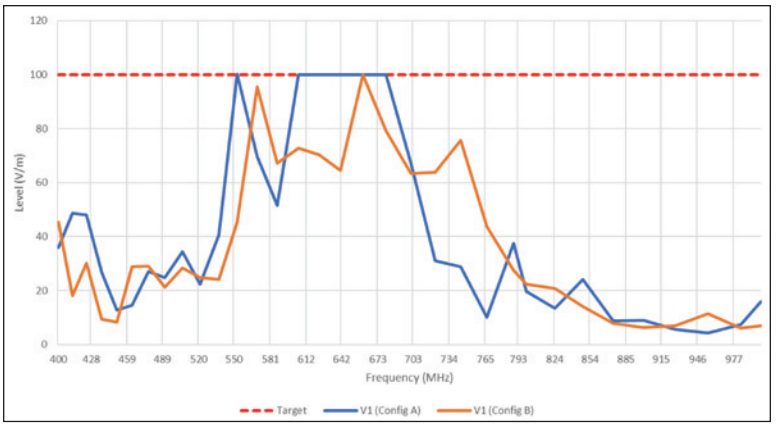


Figure 8: Variant 1 – Configuration A vs. B

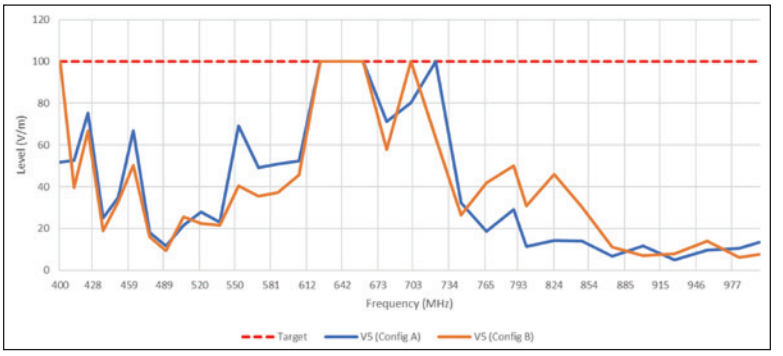


Figure 9: Variant 5 – Configuration A vs. B

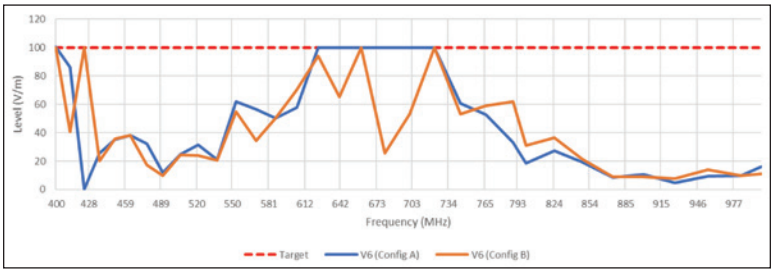


Figure 10: Variant 6 – Configuration A vs. B

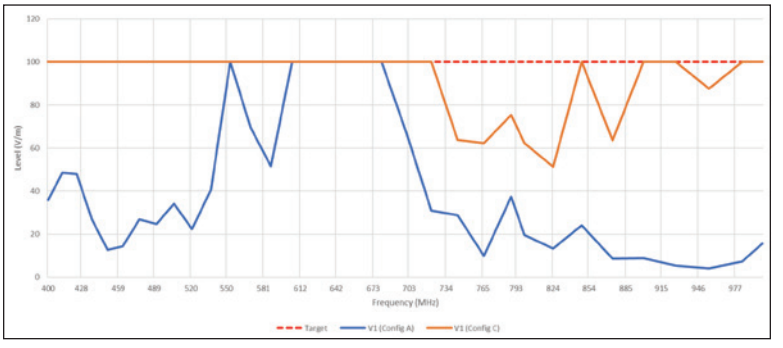


Figure 11: Variant 1 – Configuration A vs. C

PRODUCT Showcase

ESD IN JOE'S GARAGE

By Jeremy Smallwood and David E. Swenson for EOS/ESD Association, Inc.

When handling ESD-sensitive components, we must protect them from ESD damage. ANSI/ESD S20.20 tells us its purpose is "to provide administrative and technical requirements for establishing, implementing and maintaining an ESD Control Program," and it "applies to organizations that manufacture, process, assemble, install, package…. or otherwise handle…parts, assemblies, and equipment susceptible to ESD damage…" It all sounds very "big company."

What if you have three people trying to run a repair shop or make a few products? Or a single servicing engineer visiting customers? Even larger companies sometimes have single workstation electrostatic protected areas (EPA) or activities that do not seem to fit the standard. Not to mention the R&D guys with a single workstation prototyping area… It just does not seem practical to have ESD control according to IEC 61340-5-1 and ANSI/ESD S20.20, and why would they bother?

Let us deal with the last bit first. As an R&D guy, I would not want to waste my time trying to debug a prototype that I had unknowingly damaged through ESD. I would want this even less if my project was a one-off product going to a customer or if I was fitting memory or boards into a client's equipment. Yes, it does happen.

Joe has a small company and wants a workstation to produce prototypes, one-off, and small quantity products next to his desk in his converted garage. This is otherwise fitted out as an ordinary office which he shares with a couple of sales and admin colleagues. His main customer wants him to comply with S20.20. If all goes well, he might need to hire another electronics guy to work with soon. Fortunately, Joe went on an ESD training course when with his last employer, so he knows what to do.

Joe fits his workstation surface to an ESD control specification and grounds it via a common point ground buss bonded to the electric protective earth. He makes sure he eliminates all unnecessary insulators from this workstation. He wants to sit at the workstation as he works and roll to and from his office desk. He uses a grounded floor mat and a wheeled chair. He wears a wrist strap bonded to the common point ground while working there. Joe

Dr. Jeremy Smallwood is an independent consultant, trainer, and researcher specializing in electrostatics and electrostatic discharge (ESD) protection and control. Jeremy is the author of "The ESD Control Program Handbook" published by Wiley in 2020.

David E. Swenson has been a member of the ESD Association since 1984 and has served in several key Association leadership positions over his long career. He has received numerous Association and industry awards for his work.

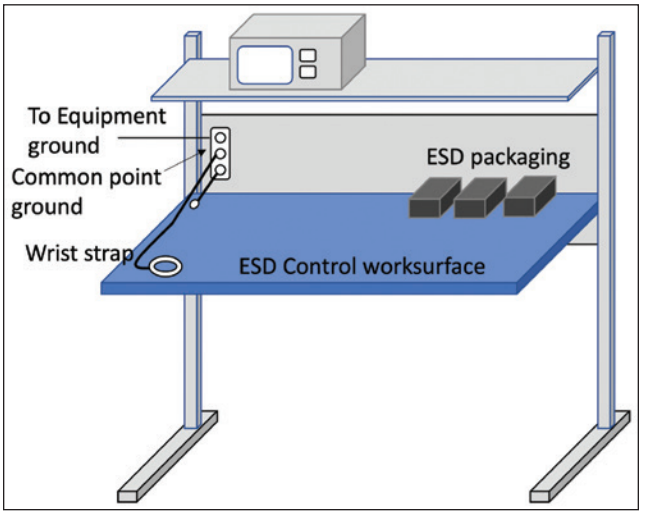


Figure 1: Joe's ESD Protected Area (EPA) workstation

decides the ESD risk from electrostatic fields arising from using his office chair is negligible. After all, he will always be sitting in it and grounded when working at the workstation. So, he does not need a grounded floor mat as there is nothing to ground with it. This will reduce his cash outlay and can be added as a refinement later. When he does, he will also be able to use ESD footwear to ground himself through the mat when standing, which will be useful for mobility.

Joe's Garage Compliance Verification Plan			
Item	**Test**	**Pass criteria**	**Test frequency**
Work surface	Resistance from surface to ground	1 MΩ to 1 GΩ	monthly
Wrist strap ground point	Resistance from connector to ground	1 Ω ± 10%	monthly
Wrist strap as worn	Resistance from hand to groundable point (lead end)	0.7 to 35 MΩ	daily
Packaging surface	Point to point resistance	10 kΩ to 100 GΩ	Monthly sampling and spot checks

Table 1: Sample Compliance Verification Plan

Joe has a lot of test equipment, some of which has insulating and potentially charging enclosures. He puts this equipment on a shelf over 30 cm above the workstation. So, the shelf does not have to be restricted to ESD control equipment or materials, provided he keeps the ESD susceptible items (ESDS) on the work surface and does not move items between workstation and shelf. The ESD risk from fields is minimized by keeping the 30 cm distance. Components go in ESD control specification bins or other packaging, at the back of the workstation. Joe decides that the boundary of the EPA is the boundary of the workstation and floor mat and puts up an EPA sign.

The key requirements of S20.20 are documentation – the ESD Control Plan, ESD Training, Compliance Verification (CV), and Product Qualification Plans. So, Joe writes a one-page ESD Plan that adequately specifies his workstation ESD controls. He specifies the use of protective earth as ESD earth in the Plan. Referring to the standard (which is available complimentary), he makes a short checklist of all the other things that must be covered in his documentation.

Joe's ESD Training Plan notes that his colleagues need to know there is an ESD risk, can identify the EPA boundary, and they must not enter his EPA or touch anything in it – unless, of course, they have had appropriate ESD Training. He adds some notes on what that training would need to include. For the moment, Joe is testing the EPA equipment himself, but in the future, he will probably get his recruit to do it, so he adds that training on ESD measurements is needed for the person who does the ESD testing.

Joe combines his CV Plan in a simple table that also specifies the measurable ESD control equipment performance requirements, reference to the test procedure, and frequency of testing. He also writes a small test procedure with photographs for each of the test methods and equipment. For a wrist strap test, he will use a small off-the-shelf tester, so he notes the pass/fail limits in his CV plan.

The Product Qualification Plan must give criteria by which Joe knows the ESD control items will work in the EPA. For this, he simply specifies the datasheet values needed to give installed ESD control items within the range specified in his CV Plan. He also specifies that correct performance must be verified on installation using the CV Plan methods.

Joe's full final ESD control documents end up as a few pages, will be compliant with S20.20, and if correctly implemented and maintained, should satisfy his customer. Lastly, he adds a note that he must update the Plan if the ESD Control specification of his EPA is updated!

Some interesting situations come up in small electronics facilities, which can, at first sight, cause a challenge to the ESD control practitioner. An attendee at an ESD control course was setting up a mobile servicing EPA in the back of his van. How, he asked, should he ground it? Must he take a metal rod that can be pushed into the ground somewhere convenient outside? The answer was remarkably simple. Connecting the EPA equipment to a common ground point could be a good ground just by equipotential bonding. If there is no voltage difference between conductors, there can be no ESD – this is recognized as accepted grounding practice under S20.20. Knowledge and understanding are keys to implementing simple and effective ESD control. ESD control does not have to be complicated. It just needs

to be well thought out and control the ESD risks.

Suppose I want to take an ESDS memory device out of its ESD protective package and put it into a computer in an uncontrolled area. The ESDS is safe until I take it out of its package. So, I leave it in there until I am safe to insert it into the computer. The main ESD risks will be if the voltage is different between the ungrounded computer and my body. I can control this by connecting myself with a wrist strap to a suitable part of the computer, e.g., chassis or a 0 V rail (equipotential bonding again). A secondary risk is that charged insulators nearby could cause induced voltages on the ESDS, which might give ESD when it touches the computer. I reduce this by removing insulators to over 30 cm from the working area. It can help suppress fields to have an earthed static dissipative mat to place over desk surfaces. Once I have everything grounded (or equipotential bonded), I can take the ESDS from its package and insert it into the computer. Portable service kit solutions are available that provide the wrist strap and cord, as well as a grounding cord and connector for when that can be used. A flexible dissipative mat is often provided that acts as a roll-up container for the kit between work areas.

The IEC 61340-5-1 and ANSI/ESD S20.20 standards allow a great deal of flexibility in how an effective ESD control program can be achieved. They do require that the control program, training, compliance verification, and ESD control product qualification practices are adequately documented. Part of the art is to ensure that this is done in a concise and clear manner that is easily understood by the users, customers, and auditors who will want to understand the controls and check their compliance.

Banana Skins

383 Walkie-talkies interfere with electronic door locks on aircraft cockpits

Here's another good reason why the use of mobile phones on planes should remain banned: your call could lock the crew in the cockpit. The problem was first reported in December 2003, when a Northwest Airlines mechanic scrambled the electronic locks on the security doors of an Airbus A330 by using his walkie-talkie in the vicinity of the flight deck.

By June 2004, Boeing had discovered that similar problems affected 1,700 of its aircraft. The solution has been a two-year, top-secret repair schedule. Boeing reports that all its jets were fixed by the end of September, while Airbus says it still has doors to mend. The faulty system has now been augmented by a technical innovation described as "a manually operated sliding bolt".

(Taken from 'News' in the 'Travel' section of the Sunday Times, *October 16 2005, page 19, http://www.sunday-times.co.uk.)*

384 Interference and the European Rail Traffic Management System (ETRMS)

Emissions: Until relatively recently the only limits on emissions from electrical equipment on rail vehicles operating in the UK were those related to signalling interference. Problems of incompatibility between equipment within the train were dealt with on an ad-hoc basis. As a result most electronic equipment on older vehicles is relatively "hard" and does not suffer problems due to interference from adjacent electronic equipment.

However, some older electronic equipment has been found unexpectedly sensitive to emissions. Examples of this are the brake units fitted to HST power cars which were found to be affected by mobile telephones and NRN radios. One type of CSR radio unit which is often affected by conducted emissions from conventional control equipment has been found to be non-compliant with EN 50121 immunity requirements.

The conclusion from this is that compliance with the current standard set out in EN 50121-3-2, tables 4 to 6 will avoid introducing unreliability into existing train borne systems in the majority of cases. To cater for the small percentage of vehicles where problems will be encountered it is recommended that, when ERTMS systems are fitted to vehicles that have electronic systems without proven immunity, tests are carried out on such systems to ensure compatibility.

Immunity: For similar reasons to those stated above with regard to emissions, the situation with regard to immunity requirements for new electronic equipment is perhaps even less certain. There is a large amount of highly inductive electrical equipment on most rail vehicles and on older vehicles this has never

been subject to any formal assessment of electromagnetic emissions.

The author is personally aware of electrical fields in the passenger saloon of a 25kV electric multiple unit that were so strong whenever the main vacuum circuit breaker was operated that a 12mm arc would be generated between two 1m long conductors held in free air. This phenomenon was accentuated by a faulty connection to the main transformer secondary output but similar effects were also observed on other units.

The arc would be alarming to passengers but apparently had no effect on the electronic traction control equipment. Historically the most troublesome sources of interference have been less spectacular and associated with control gear at battery voltage. The required immunity limits in this area are well documented in RIA 12, EN 50121 and EN 50155.

It has been suspected that older vehicles may generate interference levels outside these limits. In an attempt to provide some quantifiable measure of the typical conducted EMC environment, measurements were taken on a small sample of vehicles. These consisted of a diesel locomotive, an electric locomotive, a DMU and an EMU. The results of these tests are contained in report 02/T087/ENGE/014/TRT - ERTMS Engineering Interfaces – Supplies and EMI Tests.

The test results suggest that the conducted electromagnetic interference on older rail vehicles is broadly in line with the present test limits in EN 50155 and EN 50121-3-2. Some electrical disturbances outside the limits were measured as follows:

- Repetitive high frequency waveforms were noted in several cases. The amplitude of these gave no cause for concern but the frequency was above the test limits in EN 50121 and RIA 12 and could corrupt data signals.
- Significant voltage differentials were found between negative and the vehicle frame in some cases. This may cause problems if care is not taken with equipotential bonding of ERTMS components.
- On some vehicles there was a high level of ac ripple superimposed on the dc supply. This need be nothing more than an irritation to the designers provided it is considered at an early stage in the design.

It is expected that more extreme electrical disturbances will be found in service due to random combinations of circumstances that occur from time to time. It is recommended that the ERTMS specification should call up full compliance with EN 50155 (*despite the evidence in this report that this will not be sufficient in some cases – Editor*).

Power supplies – Voltages: The tests carried out on Class 155 DMUs indicated that, even under ideal conditions, the voltage would dip below the lower limits for several seconds during engine starting. Anecdotal evidence indicates that a 110V dc diesel locomotive battery voltage can dip to below 15 V dc during cold weather starting. It is recommended that this be brought to the attention of prospective suppliers of equipment via a requirements specification. It is essential that during such dips, the equipment continues to function within specification or shuts down to a safe condition.

There may be significant ripple on supplies on certain vehicles under different charging conditions. The current requirement according to EN 50155 is for a maximum or 15% ripple on the nominal dc voltage. In previous years, the limit according to RIA 13 was 30%. Tests carried out on vehicles indicate that even this expanded limit is sometimes exceeded (*actually up to 50% - Editor*).

It will be noted that there is a significant difference between the measured ripple for Class 43 at 0.4% and the worst case on Class 508 at about 50%. It is assumed that the difference is due to the characteristics of the load because the basic dc supply system is the same in all cases, comprising an ac source and simple rectifier. The conclusion that must be drawn is that significant ripple can occur in many types of vehicle when certain conditions exist. It is recommended that this possibility be drawn to the attention of prospective suppliers so they can take appropriate precautions.

(Extracted from the Rail Safety & Standards Board Report 02/T087/ENGE/002/TRT, Issue 3 08/03, sections 11.1, 11.2 and 11.3 on pages 16, 17 and 18. The report is available from http://www.rssb.co.uk, but easier to find with a Google search for 02/T087/ENGE/002/TRT.)

The regular "Banana Skins" column was published in the EMC Journal, starting in January 1998. Alan E. Hutley, a prominent member of the electronics community, distinguished publisher of the EMC Journal, founder of the EMCIA EMC Industry Association and the EMCUK Exhibition & Conference, has graciously given his permission for In Compliance to republish this reader-favorite column. The Banana Skin columns were compiled by Keith Armstrong, of Cherry Clough Consultants Ltd, from items he found in various publications, and anecdotes and links sent in by the many fans of the column. All of the EMC Journal columns are available at: https://www.emcstandards.co.uk/emi-stories, indexed both by application and type of EM disturbance, and new ones have recently begun being added. Keith has also given his permission for these stories to be shared through In Compliance as a service to the worldwide EMC community. We are proud to carry on the tradition of sharing Banana Skins for the purpose of promoting education for EMI/EMC engineers.

Advertiser Index

Upcoming Events

June 13-16
MIL-STD-810 Training

June 19-24
International Microwave Symposium

June 27-29
Sensors Expo & Conference

July 12-14
EMV 2022

August 1-5
IEEE EMC+SIPI 2022

September 5-8
EMC Curope 2022

September 13-15
The Battery Show

September 13-15
Fundamentals of Random Vibration and Shock Testing Training

September 13-16
Lab Techniques, Robust Design, and Troubleshooting

September 18-23
44th Annual EOS/ESD Symposium

September 20-22
IEEE ISPCE 2022

September 29
2022 Minnesotae EMC Event

Due to COVID-19 concerns, events may be postponed. Please check the event website for current information.

CW & Pulse

Watts-to-KW

10KHz-51GHz

is your

Key to Success

AMP2033LC, 6.0–18.0GHz, 100 Watts
another outstanding TWT replacement

... we are redefining

Ingenuity!

EXODUS a world apart!

EXODUS ADVANCED COMMUNICATIONS

3674 E. Sunset Road, Suite 100
Las Vegas, Nevada 89120
Tel: 702-534-6564

Web: www.exoduscomm.com

Email: sales@exoduscomm.com

A leading manufacturer in Shielded Enclosures & Anechoic Chambers

We design, engineer, and build quality turnkey anechoic solutions to meet your requirements and specifications.

See how Raymond EMC can take your projects to the next level with our **cutting-edge custom products** and **outstanding client service**. Learn more and request pricing at **raymondemc.com**.

Scan to Download

Download a complimentary copy of our whitepaper, **EMC Chamber Installation Best Practices: What Everyone Needs to Know to Ensure a Successful Chamber Installation**: https://hubs.ly/HOZyY_MO

Raymond EMC provides clients with:

- Anechoic and Reverb Chambers
- RF Shielded Enclosures, including Deployable Solutions
- Upgrades, repairs, maintenance, relocation, testing
- Responsive service by our seasoned team of experts

Serving clients in **North America** & **Internationally**

sales@raymondemc.com
raymondemc.com
siepel.com

1-800-EMC-1495
Follow us on

RAYMONDEMC

Siepel