

JUNE 2025
TM

IN COMPLIANCE

THE COMPLIANCE INFORMATION RESOURCE FOR ELECTRICAL ENGINEERS

The Evolution of **EMI Receivers**

INCLUDING

Cybersecurity Developments in
Wireless and Communications
Technologies

Preparing for the EU's New
RED Cybersecurity Requirements

Expert Insights

EMC Concepts Explained

Hot Topics in ESD

Does your antenna supplier do **all** this?



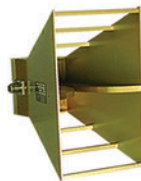
	Your Supplier	A.H. Systems
Design / build their own?		✓
99% in stock now?		✓
Next day delivery?		✓
Over a hundred items to choose from?		✓
Portable antenna kits?		✓
Still working after 10 years?		✓
Over 80 years of experience?		✓
Personal technical support?		✓
Personal Customer Service?		✓
Global support network?		✓

A.H. Systems does **all** of this, **all** of the time because we are the EMI test Antenna Specialists. We do not build "boxes". We do not build "Systems". We do design and build the highest quality, most accurate EMI test antennas (20 Hz - 40 GHz)

It may be more convenient to buy everything from one supplier, but remember "Your test system is only as good as the antenna you put in front of it!"



Log Periodics
80 MHz - 7 GHz
13 Models



DRG Horns
170 MHz - 40 GHz
6 Models



All in one small package
20 Hz - 40 GHz



Biconicals
20 MHz - 18 GHz
7 Models

The Antenna Specialists



Innovation

Quality

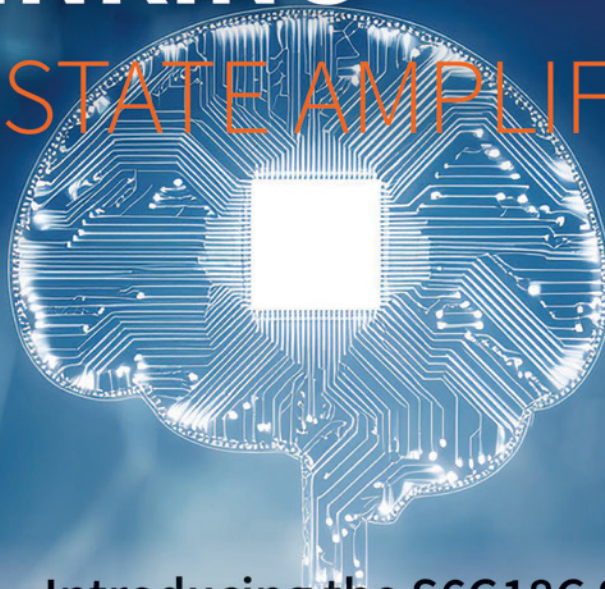
Performance

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

A.H. Systems



RETHINKING SOLID-STATE AMPLIFIERS



Introducing the S6G18C Series with Higher Power Options



THINK UNMATCHED PERFORMANCE AND FLEXIBILITY!

The enhanced S6G18C Series from AR, now featuring higher power variants at 125-watt, 250-watt, and 450-watt levels. With scalability to 1000 watts and beyond, the S6G18C Series ensures unmatched performance and flexibility.

- **Superior Linear Performance** for precision output.
- **Improved Harmonic Performance** with up to -20 dBc (compared to -3 dBc in TWT systems).
- **Enhanced Reliability** thanks to solid-state technology with no critical failure points.
- **Swift Maintenance** enabled by modular construction.
- **Lower Cost of Ownership** through reduced downtime and the elimination of backup unit expenses.

With intuitive touch-screen interfaces and multiple remote-control options, these amplifiers are as user-friendly as they are powerful.



*To learn more about the S6G18C Series
and what sets it apart from other
amplifiers, Download the Brochure Now.*

THE POWER OF
emtest / TSEQ / ar

3

IN COMPLIANCE

ELECTRONIC DESIGN, TESTING & STANDARDS

AT WORK.
AT HOME.
ON THE GO.

**In Compliance
is here for you.**

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

The EERC™

Electrical Engineering
Resource Center

white paper

RF Signal Generation Primer

Siglent's RF signal generation capabilities extend into complex IQ signals with wide bandwidth and fast symbol rates. Learn more about the capabilities and functions of RF signal generators, including the newest SSG6082A-V 8 GHz Vector Signal Generator.

offered by
 SIGLENT®

white paper

Reverberation Chambers

A technical overview of reverberation chamber design for EMC radiated immunity testing. Covers mode density, tuner efficiency, chamber Q, and validation methods in accordance with IEC, MIL-STD, and RTCA guidelines.

offered by



white paper

Mastering High Voltage: The Importance of Accurate Test Equipment

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

offered by



application note

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

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

offered by



<https://incompliancemag.com/EERC>

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

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

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

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

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

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

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

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

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

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

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

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

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

Please contact our
circulation department at
circulation@
incompliancemag.com

FEATURE ARTICLES

18 The Evolution of EMI Receivers

By William Koerner

28 Cybersecurity Developments in Wireless and Communications Technologies

By Michael F. Violette, P.E.

36 Preparing for the EU's New RED Cybersecurity Requirements

By Corey L. Sweeney, Jack Black, and
Marilyn Sweeney

COLUMNS

44 EMC Concepts Explained

By Bogdan Adamczyk

48 Hot Topics in ESD

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

DEPARTMENTS

6 Compliance
News

9 Expert
Insights

43 Product
Showcase

50 Upcoming
Events

50 Advertiser
Index



NIST Updates Privacy Framework for Cybersecurity

The U.S. National Institute of Standards and Technology (NIST) has released an updated version of its Privacy Framework (PF) in an effort to better align it with its Cybersecurity Guidelines.

According to a press release, version 1.1 of the NIST Privacy Framework includes changes to the original version's content and structure. Specifically, the update includes:

- Changes to the Framework's original content related to the Governing and Protection functions, as well as changes based on stakeholder feedback since the release of the original Framework five years ago
- A new section on AI and privacy risk management, and details on how the Framework applies to this rapidly emerging technology
- Posting of the Framework's use guidelines to the internet as an interactive "frequently asked questions" (FAQs) page, to make it more accessible for users and easier to update as needed.

FCC Issues Notice of Harmful Interference

Continuing the agency's strong enforcement efforts to protect essential radio transmissions, the U.S. Federal Communications Commission (FCC) has ordered the owners of a Texas ranch to immediately cease operation of a transmitting device that is interfering with licensed public

safety communications systems in the area.

According to a "Notification of Harmful Interference" issued in mid-April, agents from the Dallas office of the FCC's Enforcement Bureau responded to an interference complaint by the City of McKinney, Texas. Using direction-finding

techniques, their investigation identified a signal booster located at Luxia Craig Ranch that created emissions that were interfering with the City's public safety communications system.

The interference ceased when a Luxia representative disconnected power to the booster.

FDA to Phase Out Animal Testing Requirements for Drugs

The U.S. Food and Drug Administration (FDA) reports that it is taking action to reduce or eliminate animal testing in the development of certain categories of drugs and other medications.

In a press release, the agency announced it plans to "reduce, refine, or potentially replace" animal testing in the development and testing of monoclonal antibody therapies and other drugs. Instead, the FDA says it will favor more effective, human-relevant methods, including AI-based computational models of toxicity and cell lines, and organoid toxicity testing.

The FDA has prepared a "Roadmap to Reducing Animal Testing in Preclinical Safety Studies," detailing some of these alternative testing methods. The agency says that the expanded use of these "new approach methodologies" (NAMs) will improve drug safety and accelerate the evaluation process, while also reducing animal experimentation.

While the FDA's current efforts are limited to drug testing, it may be a first step in the long-term efforts to reduce or eliminate the use of animal testing in clinical trials for a broader range of healthcare-related products, including medical devices.

Thank you to our Premium Digital Partners

ARRL Files Comments in Response to U.S. FCC's Deregulation Plans

The National Association for Amateur Radio (the ARRL) has filed comments with the U.S. Federal Communications Commission (FCC) in response to its request for input on reducing or eliminating unnecessary regulatory requirements.

In a letter submitted to the Commission, the ARRL details nine separate recommendations that it says “would promote and protect the art, science, and enjoyment of amateur radio, and enhance the development of the next generation of radio amateurs.”

Here's a brief summary of the regulatory changes proposed by the ARRL in its letter:

- Delete the LF and VHF/UHF symbol (baud) rate and bandwidth limitations
- Modernized 80/75-meter sub-band divisions
- Delete amplifier drive limitations
- Delete and replace obsolete digital code limitations

- Implement changes to third-party rules adopted internationally at WRC-03
- Update and modernize entry-level technician class license privileges
- Remove non-current personal information in amateur ULS records
- Delete obsolete identification requirements for special call signs
- Delete obsolete paper license replacement provisions

The ARRL's filing was in response to a Public Notice issued by the FCC, titled “In Re: Delete, Delete, Delete,” seeking public input on FCC rules that pose an unnecessary regulatory burden on affected parties. In its Public Notice, the FCC says that its current efforts align with the Trump Administration's Executive Orders to “unleash prosperity through deregulation.”

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

ED&D

PRODUCT SAFETY SOLUTIONS

www.ProductSafeT.com

IEC/ISO 17025
Accredited Calibrations



Equipment Calibrated in **SCOPE!**

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



Call Us Today!
USA/Canada Toll Free:
800.806.6236
International:
+1.919.469.9434
Website:

www.ProductSafeT.com

Research Triangle Park • North Carolina • USA

Impact Hammers



JET-01 & JET-02 Jet Nozzles



WTR01 Water Tank & Pump System

CE

UL

SP

EN

FC

ADNS
NORDIC COUNTRIES

IC DOC

TÜV GS

MET

S

+

S

DE

VS

Force Gauges

Finger Probes

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



Efforts Underway to Save Marconi Radio Towers in Canada

Efforts are reportedly underway to preserve some of the defining infrastructure of modern radio technology.

The ARRL reports that the National Trust for Canada has launched a “Next Great Save” project to restore some of the original radio towers designed and developed by Guglielmo Marconi,

who pioneered the creation of radio wave-based telegraphy in the late 1800s. Built in 1904, the Battle Harbour Marconi Towers are reportedly experiencing structural failure after more than a century of exposure to storms and extreme climate conditions on the Labrador Coast of Canada, and are in dire need of restoration.

The Battle Harbour Marconi Towers were reportedly used to facilitate the transmission of news and announcements from Admiral Robert Peary during his 1909 North Pole expedition. Today, the Marconi Towers are thought to be the last of their kind still standing in North America.



FCC Issues Limited Delay in TCPA Implementation

The U.S. Federal Communications Commission (FCC) has temporarily delayed the implementation of a key aspect of its robocall consent requirements to give affected parties more time to modify their existing communications systems.

According to an Order, the FCC will extend by one year the effective date of rules that require organizations that receive a request to revoke a consent by a consumer about one type of message to apply that revocation request to all future robocalls and robotexts from that individual. The original effective date of April 11, 2025, has now been extended to April 11, 2026.

The delay in the implementation of the revocation provisions, which fall under the scope of the Telephone Consumer Protection Act (TCPA), was prompted by requests from several associations and groups of banks and financial institutions. The requesting parties noted that making modifications to their existing communications systems to comply with the requirements is far more complex and presents multiple challenges not applicable to smaller institutions and that more time is needed to bring their communications systems into compliance with the new requirements.

EU Sets Plan to Become Global Leader in AI Technology

As the world actively explores the potential benefits of the application and uses of artificial intelligence (AI), the European Union (EU) is taking action to position itself as the leading global AI player.

The EU Commission has announced the launch of its AI Continent Action Plan, a comprehensive initiative intended to tap into Europe's strong industrial base to foster the future development of AI-based

technologies. According to a press release issued by the Commission in early April, the Commission's Action Plan consists of five key pillars, as follows:

1. Build a large-scale AI data and computing infrastructure
2. Increase access to large and high-quality data
3. Develop algorithms and foster AI adoption in strategic EU sectors

4. Strengthen AI skills and talents
5. Simplify regulation

The EU's efforts on AI build on an effort by the Commission in early 2024 to support EU start-ups and small companies in the development of reliable and safe AI technologies. The EU has also recently announced a €200 billion investment in AI across Europe through its InvestAI initiative.

EMC BENCH NOTES

Pre-Compliance Testing for Radiated Emissions

Part 1: Equipment Needs

By Kenneth Wyatt

In past articles, we've discussed troubleshooting techniques for dealing with radiated emissions. Let's turn our attention towards performing our own radiated emissions pre-compliance testing in-house.

The purpose of pre-compliance testing is an attempt to duplicate the test setup as used by your third-party test lab (Figure 1). Because these test chambers are fully shielded and lined with expensive ferrite and carbon-loaded RF absorber material to reduce reflections, they can cost several million dollars to construct.

Most companies will not want to invest this amount, so rely on third-party test labs. In order to get a more accurate measurement of radiated emissions without the cost, we'll show you how to set up your own pre-compliance test in-house. I've used these methods successfully for many of my clients.

Ideally, you should procure a copy of the appropriate EMC test standard used, depending on the product type. For example, for military testing, you'll need a copy of MIL-STD-461. For commercial, industrial, or medical products, you'd use one of the IEC standards, such as IEC/EN 61326, IEC/EN 60601, or the generic IEC/EN 61000-6-3, which will refer back to CISPR 11 or CISPR 32. For automotive modules, you'll need a copy of CISPR 25. These will describe the equipment and setups and test limits required.

EQUIPMENT REQUIRED

Let's start off with the basic equipment you'll need. This will include a good spectrum analyzer or EMI receiver, a calibrated EMI antenna, a tripod and test bench or table for the equipment under test (EUT) and a large enough space in which to test.

I've listed many choices of analyzers and antennas in volume 1 and standards and test setups in volume 2 of my EMC Troubleshooting Trilogy (Reference 1). Figure 2 shows a popular example of an affordable bench top spectrum analyzer.

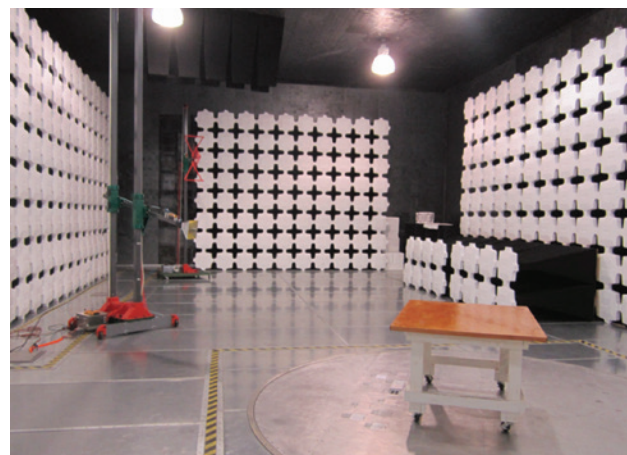


Figure 1: A typical commercial 10m semi-anechoic chamber

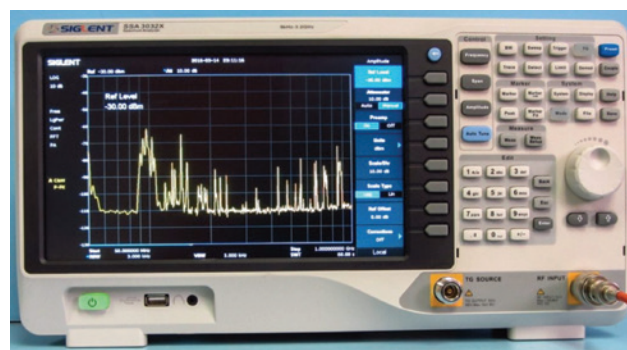


Figure 2: An example of an affordable spectrum analyzer usable for pre-compliance testing of radiated emissions.

Figures 3, 4 and 5 show example antennas.

You'll want to specify an analyzer with the required test frequency range as specified in the appropriate standards your product requires. Most tests will go up to at least 6 GHz. Military tests go as high as 18 GHz, but depending on the product type, they can go higher. If you plan to use the analyzer for conducted emissions, the lower frequency will need to be 9 kHz.



Figure 3: A typical full-sized calibrated EMI antenna. These can be 1m or more in size.

You'll find the larger EMI antennas to be more sensitive in the frequencies below 300 MHz. This is helpful, because we'll often see emissions in the 50 to 300 MHz frequency band.

Some of the physically smaller antennas (Figure 4), may work at a 1 or 3m test distance, but probably not at 10m due to lack of sensitivity.

If you've no room to store one of the larger full-sized EMI antennas, then you might consider a broadband active antenna in Figure 5. A built-in RF preamplifier brings the sensitivity up to about the same as a full-sized EMI antenna. I'm currently using this antenna because it packs up nicely in a small transit case. I've compared the performance of these three antennas in Reference 2.

Often, you'll also require a 20-dB broadband RF preamplifier in order to boost the signals to a useable level. Some analyzers may have this capability built-in, though.

One last item you'll need is a sturdy antenna tripod. Several companies make these and I describe several in volume 1 (Reference 1). For the larger antennas, see examples of heavy-duty tripods in Figure 6. Lighter antennas can use a lighter tripod. Check volume 1 of my trilogy for many more choices.

EXAMPLE TEST SETUPS

Where to test? Because the measurement assumes a reflective surface, most of the time, we'll just use the earth or floor and assume we'll get some fraction of the reflecting wave. Commercial labs will raise and lower the antenna at the dominant harmonic frequencies in order to maximize both the direct and reflected wave. Some companies use



Figure 4: A physically small calibrated antenna that could work well at a 1m or 3m test distance. Because of the small dimensions, it would not be suitable at 10m.



Figure 5: For a reduced-size calibrated antenna, I like an active antenna with built-in broadband RF preamplifier. This helps reduce the noise floor to compensate for the very short antenna elements.



Figure 6: Examples of heavy-duty tripods. This style is best for full-sized EMI antennas.

their parking lot away from other vehicles or metal reflective objects. I've also used office cubicles or conference rooms. Figure 7 shows the basic test setup.

Military and automotive module testing uses a fixed table with antennas spaced at a 1m test distance. Commercial, industrial, and medical products are tested on a rotating table at either a 3m or 10m test distance.

I've found conference rooms work pretty well. They are out of the weather, resources are usually close at hand, and it's easier to clear out an area to test. Figure 8 shows one of my early setups while testing an industrial alarm system at the client's facility. Notice the client constructed a wooden turntable, which allowed rotation of the product under test to find the maximum emission.

Figure 9 is a similar 3m setup in an office cubicle. The back end of the antenna had to stick out halfway into the hallway, though, attracting some attention. I used the opportunity to discuss the basics of radiated emission pre-compliance testing with a few interested employees.

SUMMARY

If you already have the equipment for benchtop troubleshooting, then all you'll need to add would be a calibrated antenna, tripod, connecting coax cables and possibly a low-noise broadband RF preamplifier. An optional, but highly recommended addition would include a 6-dB attenuator placed at the antenna port, which will help stabilize a 50 Ω load impedance across the test frequency band.

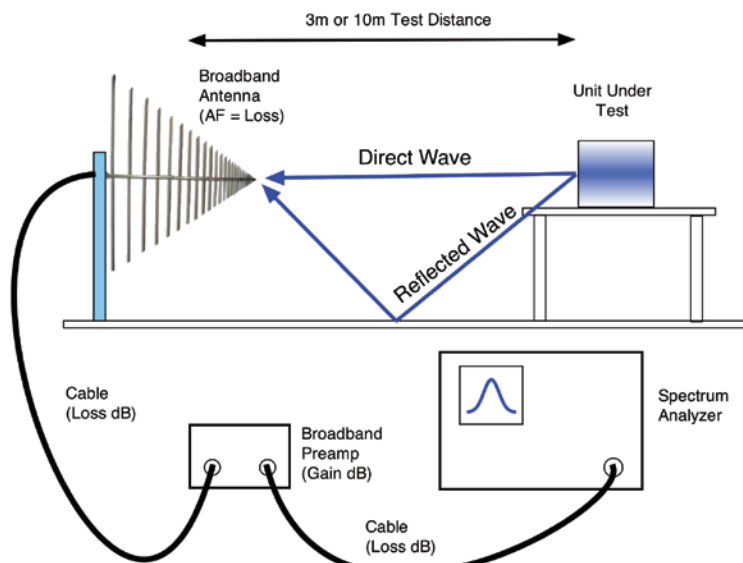



Figure 7: Block diagram of a typical radiated emissions test setup. The 3m or 10m test distance is measured from the front of the product under test and a reference point on a broadband log-periodic (usually about the mid-point along the boom) or center support of a broadband dipole.

Next time, we'll discuss the details of making the measurement and add some additional examples of successful test locations and setups. 

REFERENCES

1. Wyatt, *EMC Troubleshooting Trilogy*.
2. Wyatt, "Evaluating Reduced-Size EMI Antennas - Part 1," *EDN*.



Figure 8: An example 3m test setup in a conference room.



Figure 9: Another example of a 3m test setup in an office cubicle.

PRACTICAL ENGINEERING

Material Group Selection and How It Affects Spacings

By Don MacArthur

Often overlooked during the development of appropriate spacings (creepage distances) for safety-certified products is the failure to account accurately for the material group of the components involved. This oversight can have significant implications. Let us briefly explore this issue to raise awareness among readers.

MATERIAL GROUP REVIEW

One of the items from which creepage distance is determined is the Comparative Tracking Index (CTI) rating of the insulating material of the component. Table 1 is a list of the material group number and its associated CTI value obtained in accordance with IEC 60112.

Material Group	CTI Rating
I	600 ≤ CTI
II	400 ≤ CTI < 600
IIIa	175 ≤ CTI < 400
IIIb	100 ≤ CTI < 175

Table 1

As Table 1 indicates, Material Group I has the highest CTI rating, while Material Group IIIb ranks as the least favorable.

Pro Tip: Components with Material Group I CTI ratings are the preferred choice for highly reliable applications.

Pro Tip: Before finalizing the use of a component, consult the manufacturer’s datasheet to ascertain the specified material group. If this information is unavailable, consider contacting the supplier for clarification or exploring alternative parts from different suppliers.

Bonus: For glass, ceramics, or other inorganic insulating materials that do not track, maintaining creepage distances is not required.

BASE TEST CASE

To best see the effects that material group selection has on creepage distances, let us use a best test case using a working voltage (root-mean-square or direct current) of 300 V, a pollution degree 2 environment, an insulation location of “other insulating materials” and a location where reinforced or double insulation is required. Spacings are derived from UL 61010-1 Third Edition.

RESULTS FOR MATERIAL GROUP III

Starting from worst to best, here are the results for the case where the component selected has a CTI failing under the Material Group III category:

In Figure 1, that light green denotes input to the spacings calculator, and pinkish reflects the required creepage distance in millimeters (mm).

RESULTS FOR MATERIAL GROUP II

See Figure 2.

RESULTS FOR MATERIAL GROUP I

See Figure 3.

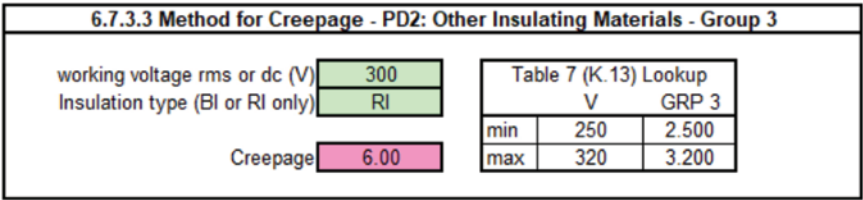
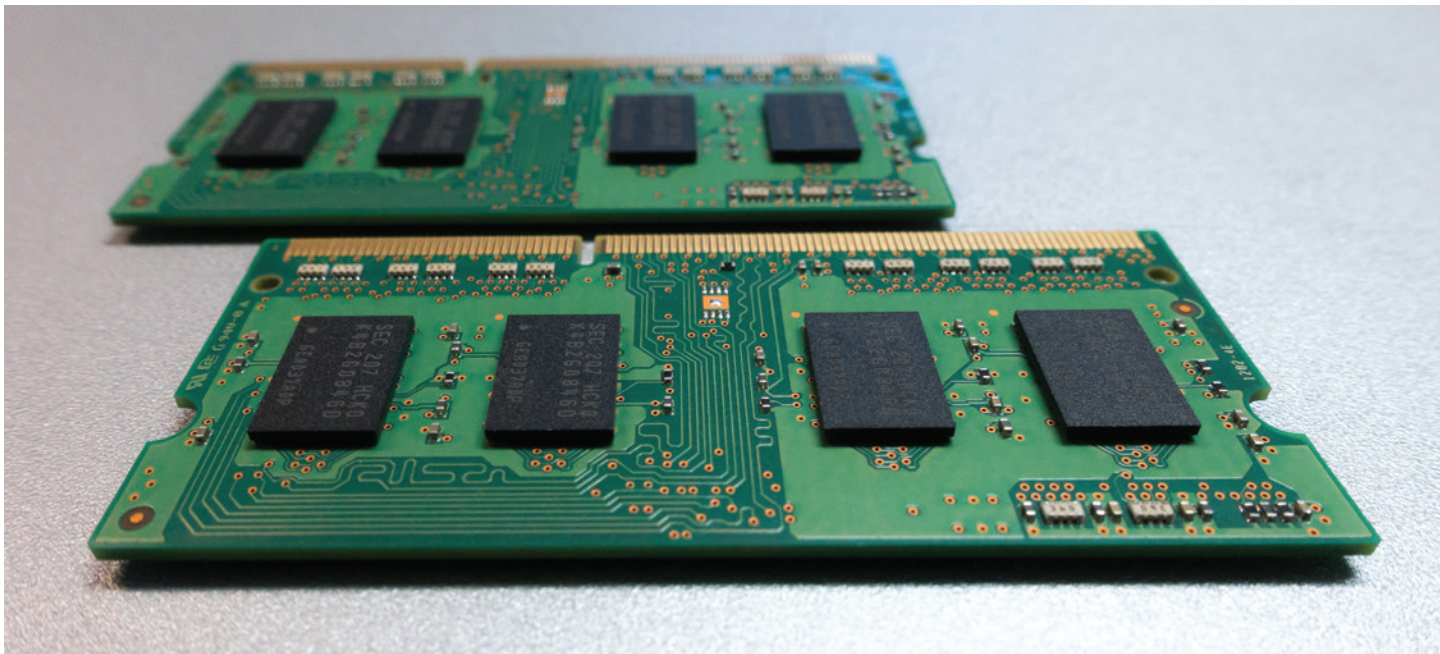


Figure 1




SUMMARY OF RESULTS

See Table 2.

Material Group	Required Creepage Distance (mm)
I	3.0
II	4.17
III	6.00

Table 2

CONCLUSION

As demonstrated above, the required creepage distance for a component with a Material Group III CTI rating is twice that of a component with a Material Group I rating! This result may be acceptable or problematic depending on the specific application and whether your design accommodates these doubled spacings. Carefully considering the material group of components well in advance of your design layout is crucial. Imagine being locked into using a particular part, only to discover later that it has a Material Group II or III CTI rating, while your available space only allows for a Material Group I part. 

6.7.3.3 Method for Creepage - PD2: Other Insulating Materials - Group 2			
working voltage rms or dc (V)	300	Table 7 (K.13) Lookup V GRP 2	
Insulation type (BI or RI only)	RI		
Creepage	4.17	min	250 1.800
		max	320 2.200

Figure 2

6.7.3.3 Method for Creepage - PD2: Other Insulating Materials - Group 1			
working voltage rms or dc (V)	300	Table 7 (K.13) Lookup V GRP 1	
Insulation type (BI or RI only)	RI		
Creepage	3.00	min	250 1.250
		max	320 1.600

Figure 3

MILITARY AND AEROSPACE EMC

The Currents of EMI

By Patrick André

“Follow the currents.” That statement was made by Dr. Bruce Archambeault, who says that current flow is the most important concept of EMC. I have to agree with him because if we know how currents are being generated and how they move through our circuits and chassis, we can understand our sources of emissions and coupling mechanisms of susceptibility in greater ways.

In EMC engineering, we try to classify currents into two categories: Common Mode (CM) currents and Differential Mode (DM) currents. Differential mode currents are easier to understand. A unit demands power from a power line, e.g., a 28 VDC power bus. The current then flows back on the return line. This is the differential mode current.

However, in the operation of the equipment, some current may be inductively or capacitively coupled to the chassis, to other circuits, or used by the system and routed to other lines. This can result in an imbalance in the power line currents. In this case, 1.001 amps may flow in the power line, but only 1.000 amps flow in the return line. The result is that we have 1.000 amps of differential mode current and 0.001 amp of common mode current, which has a remote return path.

Note these currents are due to inductive or capacitive coupling; thus, I am assuming they are high frequency currents since DC is coupled neither inductively nor capacitively. To be high frequency, some function must occur, such as being chopped by a switching power supply or used in digital circuits. Considering power supplies, FETs and transformers used in switch mode power supplies create fields by their

operation. A FET turning on and off will have high frequency transients from the sudden starting and stopping of the current flow.

Looking at this FET as the noise source - the voltage will spike when the FET transitions from a conducting to a non-conducting mode. This FET voltage spike will be with respect to the reference plane or the chassis. High frequency, short duration voltages between two conductors will induce a current between them. However, once generated, currents must find a path back to the source (currents flow in loops). The trouble comes when that return current path is either unknown or uncontrolled. Our last Military and Aerospace EMC article stated that radiated emissions can be over limit with as little as 10 μ A of uncontrolled common mode current.


Common mode inductors, ferrites, and the like are often employed to control the flow of these currents out of the equipment. However, the addition of impedance in series is most successful when there is a local return path for the currents to flow. This means the use of capacitors from the reference plane or chassis back to the line connected to the FET in this case. In doing so, a closed loop for the current is provided, and it will be a preferred path when that common mode inductance is placed on the outboard side of the capacitance.

Realize that loop areas produced by these current paths are also receiver antennas as much as they are transmitting antennas. They can receive and then inject interference-like energy into the circuit, which may disrupt the operation of sensors, digital circuits, and the like, which may be

connected to the same current path. Thus, the control of current loops has two beneficial effects: the reduction of emissions and greater immunity to outside signals.

When differential noise is an issue, the solution will be to use capacitance from line to line, and linear inductance, preferably in both the power lead and the return. When a switching circuit demands current, providing a local source for this current in the form of capacitance can reduce or soften the demand from the power line. Series inductance should not be common mode inductance but linear inductors designed to handle peak current demand without saturation. Using ferrites as the core material for linear inductors can be problematic. When used on an AC line and run to saturation, ferrites have been found to create more noise than when they are not in circuit. Proceed with caution when using inductors.

Finally, single-ended signals are not truly single-ended. Current will not flow from here to there and will not have a return path. So, returns tend to be other than adjacent lines. If this is a pure DC line, there is no issue. The problem is that radio frequency energy is easily coupled and can appear on these lines. With a remote return, the loop sizes increase, and so do emission and susceptibility problems. Thus, single-ended lines are not a cure for EMI problems, and they can have their own set of issues.

Ultimately, if we follow the currents and know how they are generated and where they travel, we can understand a great deal more about how to return the currents locally and avoid them from leaving the equipment in the first place. 

STANDARDS PRACTICE

Opt for Reverb Chamber Testing

By Karen Burnham

There are plenty of ways of testing units for radiated immunity (or radiated susceptibility, for the aerospace/defense world). As of MIL-STD-461 Rev E, that document allows RS103 to be tested in a reverb chamber as an alternative to the more traditional absorber-lined semi-anechoic chamber (ALSE) test setup. In the automotive industry, ISO 11452-11 describes a reverb test method for components, and this has flowed down to some OEM-specific requirements, like Ford's RI114. If you're worried that testing to the 3 V/m or 10 V/m immunity levels of IEC 61000-4-3 is still missing some real-world vulnerabilities of your hardware, you may want to consider testing per IEC 61000-4-21.


There are significant advantages to testing in a reverb chamber. One major advantage is that instead of illuminating specific faces of the unit under test (UUT), due to the chamber reflections, a UUT is being hit from multiple directions. This is much more representative of real-world conditions, where you rarely know exactly where a threat radiator might be relative to your unit. RS103 only tests in one orientation (and even though testers are supposed to establish the "worst case" orientation, "worst case" at one frequency might not be the worst at all frequencies). The automotive industry generally tests three different orientations. But even with that extra testing (and the additional test time it requires), things can be missed. I've seen cases where a unit passed traditional ALSE immunity testing then failed during vehicle level (ISO 11451) immunity. When that unit was re-tested in a reverb chamber, it replicated the failure seen on the vehicle. Given that the goal of module

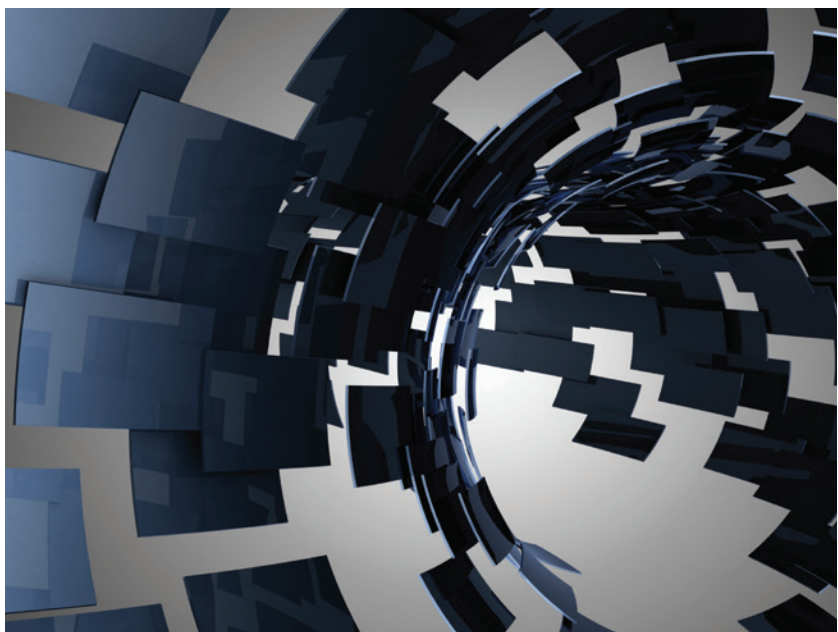
testing is to catch issues early instead of finding them late in the program, much of the automotive industry has been strongly encouraging units to do immunity testing in reverb chambers.

For the automotive industry in particular, reverb testing saves a lot of time (and time in a test chamber = money). It's well known that radiated immunity can be one of the most time-consuming tests, triply so for ISO 11452 testing, where three separate orientations are required. Reverb testing cuts down that test time by needing only one UUT orientation, roughly a third of what it would take in an ALSE. However, even for aerospace/defense RS103 testing, the time savings are significant: you don't need to test in two polarizations, and you don't need multiple antenna locations to cover a large test area at high frequencies.

Of course, nothing is an unqualified good. You generally don't want to test units with sensitive RF

components in a reverb chamber since they're harder to protect and the field strengths can get very high. You must also consider each chamber's Lowest Usable Frequency (LUF). Below that frequency, it can't maintain a volume of field uniformity (see Figure A.5 of IEC 61000-4-21 for a good illustration)). The LUF is largely determined by the physical size of the chamber, where reaching lower frequencies requires a bigger chamber.

If you can access a reverb chamber and do your testing there, IEC 61000-4-21 can be an invaluable resource. It goes through the mathematical details of setting up and calibrating a chamber for either emissions or immunity (or shielding effectiveness) testing. The math can look intimidating and requires a significant amount of statistics, but wading through it should be trivial compared to the cost of longer testing in an ALSE—or missing problems that you must then troubleshoot right before product launch. 



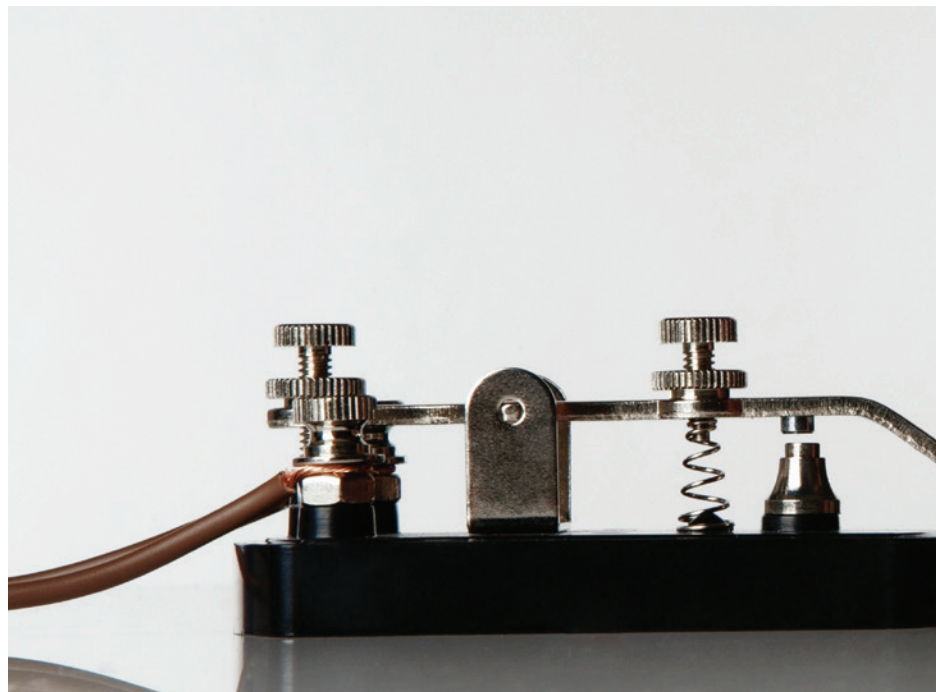
Morse Code? Really?

The mention of “Morse code” often results in a circle of silence, and people back away from what they may perceive as someone who may be seriously demented, be a radical from the “Flat Earth Society,” or have an incurable disease. Occasionally, there will be the question, “Does anyone really use that anymore?” (Of course, you already know the answer to that question, or there would be no reason for me to be writing this!)

Notice that the three letters SMS are “run together” without the space between letters which is the normal configuration of letters when sent in Morse code. When this is done, the result is termed a “pro sign” or “procedural sign.”

(Side note: A few months ago, I had occasion to drive a family member to the local hospital Emergency room and, as I was walking back to the hospital entrance after parking the car, I heard an automobile horn bleeping out “■■■ ■■■■■■■■ ■■■” (S O S) slowly, over and over again. I called this to the attention of the hospital guard and suggested there might be someone in trouble calling for

Aircraft radio homing beacons guide planes from point to point and signal on their assigned radio frequencies with a three-letter code sent in Morse. The code identifies the beacon and is printed on aviation navigation charts along with the radio frequency for that beacon, which most often corresponds to the same three-letter code for the airport. Aircraft pilots still carry



current navigation charts as backup when a solar corona mass emission (CME) from the sun disrupts the satellite GPS signals.

Merchant Marine and Navy ships began moving away from the use of Morse code for radio communication at sea around 1999. Naval ships still retain the capability to use signal flags and flashing lamps using Morse code in close ship-to-ship messaging. The flashing lamps are being “upgraded” to “encode” Morse signals by computer to send messages and decode systems on the receiving ship capture the signals and display the received text in plain language.

Yet, the U.S. Navy still teaches some sailors to read, send, and receive Morse code. The Navy’s Information Warfare community uses Morse code as part of the cryptologic technician (CTR) skill set. The Basic Manual Morse Trainer (BMMT) course teaches sailors how to intercept Morse communications, copy and send Morse code, and more. The course also includes the latest Manual Morse software used by the Department of Defense.

Morse code is still taught to radio intercept troops. Believe it or not, there are still countries that use Morse code for military communication. It is still preferred for long distance communication.

The giant intercept antennas built by the U.S. armed services (Air Force and Navy), known as “elephant cages” because of their large size, were being shut down and

dismantled. Originally used to read the Morse code used by other nations to maintain contact with their pilots and alert our U.S. pilots of developing situations, new Pentagon management had decided they were no longer needed.

Later, I learned that some sites might have been saved from destruction and taken over by “different management” and that “new” government personnel were being trained in the use of Morse code in order to maintain a watch on other countries that still use the code for “intelligence” purposes. Any guesses as to the three-letter code that might identify that management group?

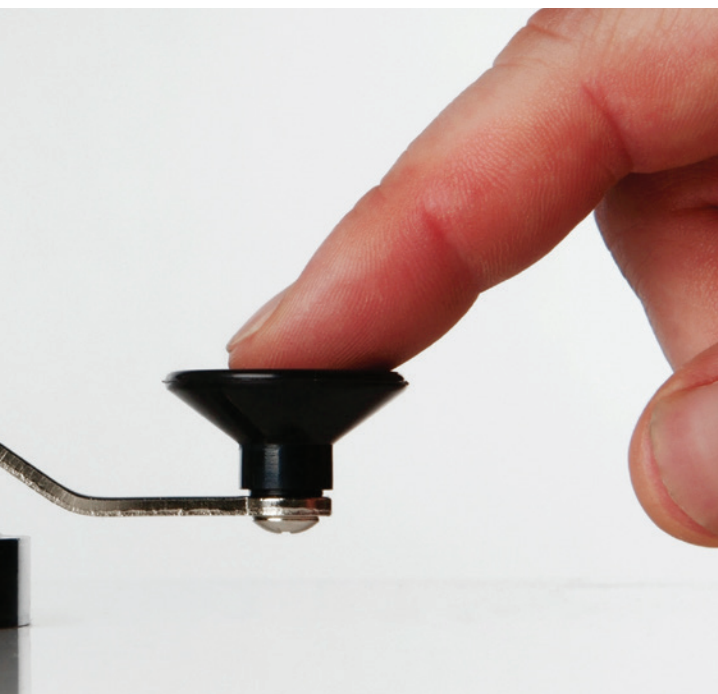
By far the largest group of Morse code users is the Amateur Radio community, and that community usage is growing constantly. Part of that growth results from the improvement in long distance propagation as the Sun pumps more ionized particles into the ionosphere during the current rise of sunspots in this 25th Solar cycle. The total population of Amateur Radio Operators worldwide is currently estimated to be in excess of 3,000,000, and the number in the U.S. is known to be more than 747,000.

A significant growth in Amateur use of Morse code has been noted since the pandemic, encouraged by several organizations promoting the use of CW. (CW == continuous wave, and is another name for Morse code on the air typified by single frequency signals interrupted by switching on and off... i.e., Morse code.)

One of the more successful examples of this is the Long Island CW (LICW) Club which uses virtual classes to teach sending and receiving Morse code. The LICW Club began operation just before the start of the pandemic and has grown to over 5300 members in 50 states and 59 countries. Its cadre of instructors teaches 138 classes each week for students of all levels.

Many of the LICW Club students have gone on to become net control stations and net traffic managers for the Morse code National Traffic System, which handles emergency communications in the U.S. when a disaster strikes and wipes out all the normal power and communications systems. Amateur Radio operators are usually the first “call for help” from a disaster area. When government help arrives and establishes its own emergency communications systems, Amateur Radio then handles health and welfare-related messages between the thousands of citizens in the affected area and their concerned relatives and extended family members in the rest of the country. Most of those messages are handled using Morse code.

So, the long answer to the original question “Does anyone use Morse code anymore?” is yes, and its use is not fading away but growing as more Amateur Radio operators use “Radio’s first language.” 📻



THE EVOLUTION OF EMI RECEIVERS

Reducing Time to Market and Visits to Testing Labs for New Products



William (Bill) Koerner is a Senior Application Engineer with Keysight Technologies, where he focuses on supporting the company's microwave compliance testing solutions, including wireless regulatory (Wi-Fi, Bluetooth®, Zigbee), EMI receivers, and co-existence testing for medical devices. Koerner is also Keysight's representative to the FCC's Telecommunications Certification Body (TCB), the ETSI Broadband Radio Access Networks (BRAN) working committee, and several Wi-Fi Alliance TG working groups. Koerner got his start at the original Hewlett-Packard as a Microwave Systems Engineer in the mid-1980s. He can be reached at bill.koerner@keysight.com.



By William Koerner

Since the first observations of interference from unknown events with AM radios in the early 1920s, the field of electromagnetic interference (EMI) has continued to evolve and involve more than AM radios. Today, any product with a power cord or that is battery-operated can and will generate electromagnetic fields. Electromagnetic compatibility (EMC) testing is required for any product that has electrical, digital, and/or radio components.

With the growth of the variety and volume of those products, the time to complete EMC testing typically takes longer, due to competition for lab time, and for surprises in tracking down short-burst or impulse-type emissions. The automotive industry, for example, requires exacting methodologies to measure all emissions accurately. Long test times impact test facility availability and potentially reduce the number of devices that are certified. It's also easy to miss intermittent disturbance signals with conventional scans since an extended dwell time must occur at each frequency.

With the implementation of time domain functionality in EMI receivers and short-time FFT (STFFT) engines, EMI receivers now enable independent compliance test laboratories and in-house certification labs to shorten their overall test time, and for device manufacturers to quickly troubleshoot intermittent and impulse signals during design validation and pre-compliance testing.

This article will provide a short history of radiated EMI testing, a discussion on the evolution of EMI receiver designs, and a look at the newer time domain scan and FFT capabilities to meet EMI measurement requirements. We'll also discuss EMC standards such as CISPR 16-1-1 and MIL-STD-461 and highlight how you can easily reduce receiver scan and test time from multiple hours to seconds. Finally, we'll identify

those areas where this makes the biggest difference, and when you may not need to consider adapting the newer technology.

HISTORY OF RADIATED EMISSIONS TESTING

How It All Began

In preparing to write this article, I wanted to do a little research on how the use of electromagnetic waves came about, and how it was discovered that it created some unintentional issues. In reading the "Empire Of the Air" by Tom Lewis,¹ it was interesting to discover that, besides the well-known inventors and scientists like Marconi and Tesla, others such as Henry de Forrest, David Sarnoff, and Edwin Armstrong played major roles in the growth of the use of electromagnetic waves for wireless transmission in the late 1800s. Perhaps the first documented case of electromagnetic interference occurred in September 1901 when the competing wireless telegraphs of de Forrest and Marconi jammed each other during the International Yacht Races,² resulting in neither inventor being able to report the results of the race.

Their work aligns with the discovery of solar activity creating "phantom telegraph operators," in which radiated emissions are picked up by the long parallel transmission wires that generate telegraph output without telegraph input,³ as well as the growth of broadcasting and the use of electronic equipment in commercial and military applications. As a result of these developments, some sort of rules or regulations would become necessary to prevent radio interference or equipment malfunctions.

Beginning of Regulatory Oversight

In 1892, the German "Law of Telegraph" became the first law in the world that dealt with electromagnetic interference.⁴ Similar actions followed and the Comité International Spécial des Perturbations

Early studies of interference tended to be called “noise,” primarily because their presence was identified as audio noise. Many attempts were made to quantify and measure this noise so that measurement techniques and limits could be established.

Radioélectriques (CISPR) was founded in 1934 as part of the International Electrotechnical Commission (IEC).⁵ That same year, the U.S. Communications Act was passed, establishing the Federal Communications Commission (FCC) in the United States, which took over the radio regulation functions of the previous Federal Radio Commission.⁶ One of its stated purposes was “for the purpose of promoting safety of life and property through the use of wire and radio communications.”

Early studies of interference tended to be called “noise,” primarily because their presence was identified as audio noise. Many attempts were made to quantify and measure this noise so that measurement techniques and limits could be established. But getting agreement with different measurements proved difficult, in part due to the concern being limited to an “annoyance factor,” that is, how the noise or interference “annoyed” the intended transmission or product use. The consensus was that high-repetition noise was more annoying than low-repetition noise. This ultimately led to the development of radio noise, objective sound meters, and quasi-peak detectors.⁷

DEVELOPMENT OF EMI RECEIVERS

The First Tuned Receivers

The initial EMI receivers had the ability to tune and measure interference versus frequency. However, these receivers required manual tuning and also required the operator to read an analog meter for the amplitude and the frequency dial for the frequency. Due to the early technology, several instruments were typically needed to cover the complete frequency range required.

In addition, the amplitude response of the receivers did not have a flat frequency response, so some sort of substitution technique was required for calibrated measurements.

Invention of the Superheterodyne Receiver

Manual tuning and inaccurate amplitude measurements made initial interference measurements tedious and time-consuming. That changed with the invention of the superheterodyne receiver by Edwin Armstrong in 1918 (his prototype is shown in Figure 1). His receiver allowed for tuning and receiving signals at even higher frequencies than before and has served as the foundation for receiver designs even today.

With the invention of the superheterodyne receiver, wireless telegraphy was suddenly not just the only opportunity. In 1919, the Radio Corporation of America (more commonly known as RCA) was incorporated, combining the patents of Marconi, de Forrest, Armstrong, and General Electric to focus on the business of radio, or voice broadcasting. The big breakthrough for RCA was the broadcast of the heavyweight fight between Jack Dempsey and Georges Carpentier. In a first of its kind, the fight was broadcast to over 300,000 people across the U.S. That created the demand for “radio” for personal use, and a whole new industry was born.⁸

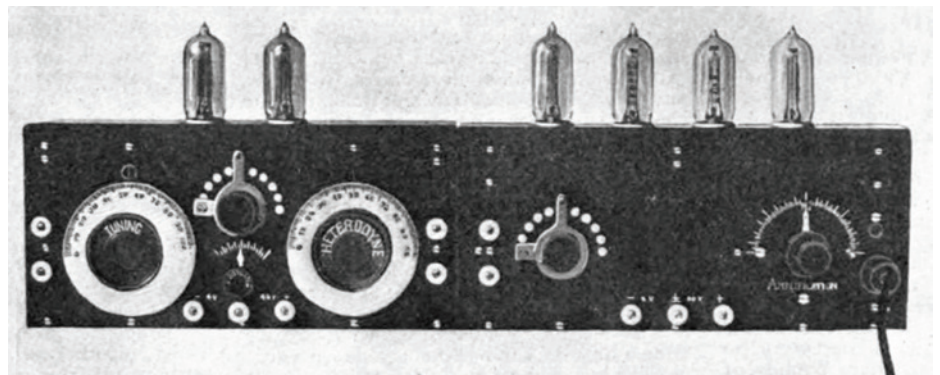


Figure 1: Prototype superheterodyne receiver built at Armstrong's Signal Corp laboratory in Paris, 1918¹²

Have you seen the industry's lowest-profile wirewound chip inductor?



Hopefully the arrows help.

With a maximum height of just 0.28 mm, our new 0201HT Series is the industry's lowest-profile wirewound chip inductor, also featuring a tiny 0.58 x 0.46 mm footprint.

It offers up to 70 % higher Q and lower DCR than similarly-sized thin-film chip inductors and is optimized for high frequency impedance matching in applications such as cell phones, wearable devices,

WiFi, Bluetooth, GPS and LTE/5G IoT networks.

The 0201HT provides SRF as high as 36 GHz and is available in 14 inductance values from 0.5 to 13 nH.

Find out why this tiny part stands so tall. Download the datasheet and order your free samples today at www.coilcraft.com.



WWW.COILCRAFT.COM

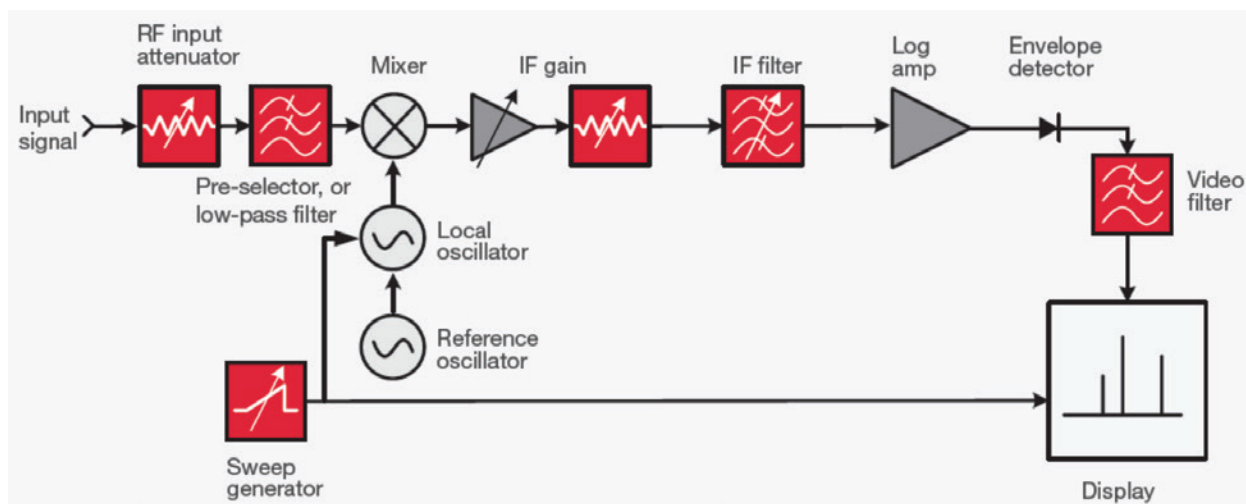


Figure 2: Traditional swept spectrum analyzer architecture

EMI Receiver or Spectrum Analyzer?

With the initial issue of dealing with radio “noise,” the development of broadcast radio, and the introduction of radar during World War II, the need to analyze high-frequency signals for either content or noise was imperative to ensure the systems worked as expected and, even more importantly, met the emission standards established by the FCC and CISPR. This drove the need for not just a noise receiver or EMI receiver, but also a spectrum analyzer.

Figure 2 shows the typical architecture for a traditional swept spectrum analyzer. Developments of stable local oscillators that could be swept allowed for fast, continuous tuning and measurements across the defined frequency range. Note that there is typically a pre-selector or low-pass filter before the first mixer. This allows for a lower noise floor for the measurement and prevents broadband signals from overdriving the mixer.

The EMI receiver has evolved with a very similar architecture, but there are subtle differences due to the nature of the signals to be analyzed. Figure 3 shows the RF front end for a typical EMI receiver.

One major difference between the spectrum analyzer and EMI receiver is the dual signal paths. The low band path

in Figure 3 is for the lower frequencies (< 3.6 GHz in this example), which has unique pre-selectors that are a combination of bandpass filters for the lower frequencies. This allows for wider bandwidth than that available in the high band path, but also prevents broadband impulsive noise from overloading the first mixer. It also allows for less input attenuation to provide the dynamic range to measure the CISPR pulse and meets CISPR 16 requirements.

The high band path has a Yttrium Iron Garnet (YIG) swept preselector to protect the first mixer and resembles the traditional swept spectrum analyzer architecture. The bandwidth of the YIG preselector is much narrower than the RF preselector in the low band path, which ensures the dynamic range required at the higher frequencies.

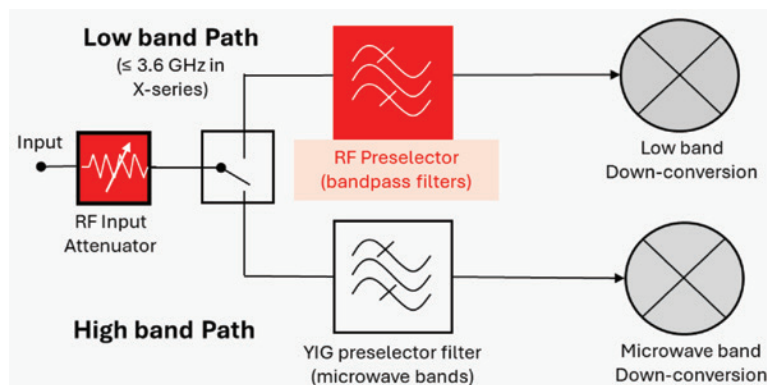


Figure 3: Traditional EMI receiver front end

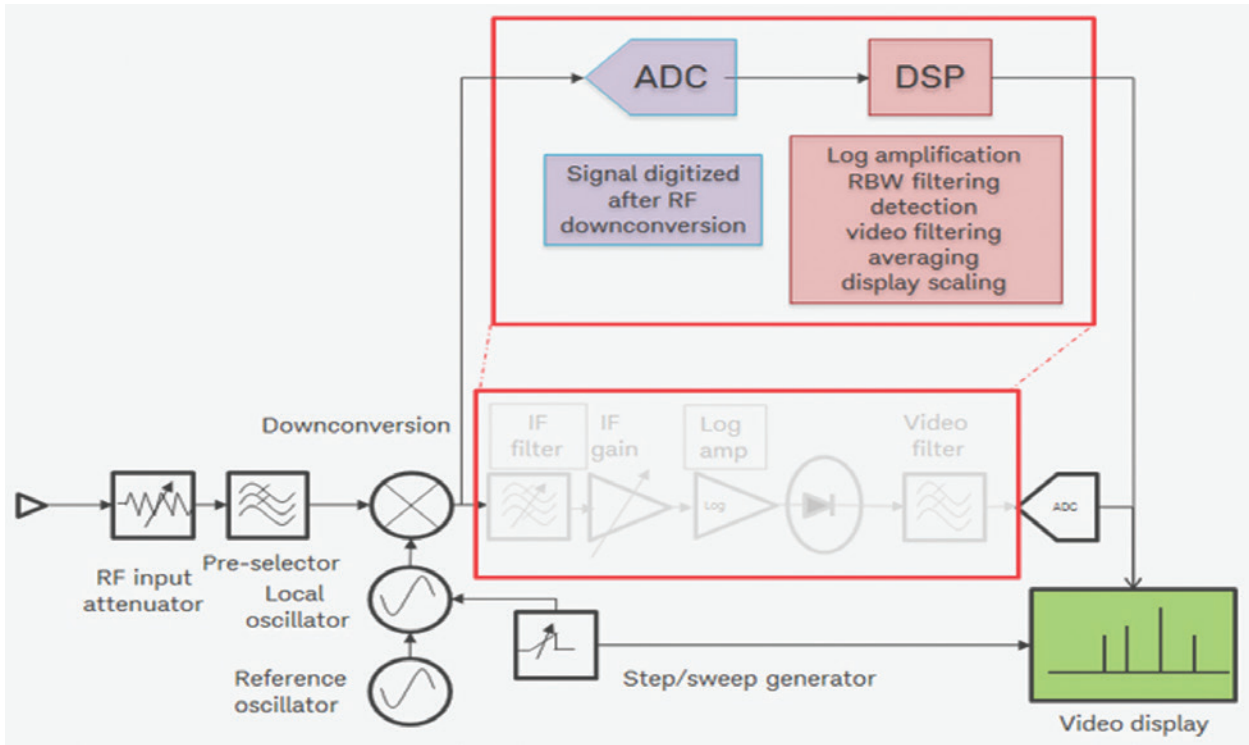


Figure 4: Digital IF section architecture

ANALOG VS DIGITAL IF SECTIONS

Figure 2 shows the traditional analog IF section in a spectrum analyzer and is very similar to what was in EMI receivers as well. Perhaps the biggest change in either the spectrum analyzer or the EMI receiver was the introduction of digital IF sections. I remember in the 1980s that analog-to-digital converters (ADCs) were becoming prominent, with the idea of getting the signal of interest to digital as close to the input as possible. This has a great impact on measurement speed, accuracy, and the ability to measure complex signals using advanced digital signal processing (DSP) techniques.

Figure 4 shows the analog IF section replaced with a digital section. After the down conversion, the signal is converted to a digital value, which is a digital amplitude value. The term “digital IF” describes the digital processing that replaces analog IF processing found in traditional receivers and spectrum analyzers.⁹

At this stage, any additional processing is done with DSPs and mathematical functions, mainly some version of fast Fourier transform (FFT). Resolution

bandwidths (RBWs), video filtering, averaging, and detection are all done with the desired mathematical function. Digitally implemented RBWs offer both improvements and improved filter performance, as well as tighter filter shape factors. Most noticeably, digital RBWs allow for much faster sweep times, as there is no charge time for the filter. Digital IF gain can provide extremely accurate reference levels. Digital logarithmic correction factors reduce measurement uncertainty associated with analog log amplifiers.

Table 1 shows a typical comparison of the differences in amplitude uncertainties between digital and analog IF sections. The data represented here was collected by surveying receiver and spectrum analyzer specification guides.¹⁰

Amplitude uncertainty	Digital IF	Analog IF
Reference level switching	0 dB	$\leq \pm 1$ dB
RBW switching	± 0.05 dB	$\leq \pm 0.5$ dB
Display scale fidelity	± 0.15 dB	$\leq \pm 0.85$ dB

Table 1: Comparison of amplitude uncertainties with digital and analog IF architectures

To resolve the issue between frequency range and resolution, the use of short-time fast Fourier transform (STFFT) engines can be used. This involves overlapping the FFTs by overlapping the captured time domain signal in the different FFT frames.

FFT IMPLEMENTATIONS

With the implementation of ADCs in the IF section and careful selection of RF preselection in the front-end, it is possible to measure broadband signals instantaneously. Current ADCs support multi-GHz sample rates and at least 14 bits, making for dynamic ranges of >80 dB. Combined with the RF preselection, instantaneous bandwidths of hundreds of MHz, possibly even 1 GHz, are possible.

ADC with FFT

While having an ADC with a fast sampling rate is required to capture a broadband signal, it comes with a trade-off between the frequency range of the captured signal and the frequency resolution of the acquired signal. In order to support the RBW requirements for CISPR standards, the number of samples is very large and may not be commercially feasible to implement.

Overlapping FFTs

To resolve the issue between frequency range and resolution, the use of short-time fast Fourier transform (STFFT) engines can be used. This involves overlapping the FFTs by overlapping the captured time domain signal in the different FFT frames. For example, if the frame length is set to 2048 points, the time samples 1-2048 are collected in the first frame, time samples 1024-3072 are collected in the second frame, etc. This example shows an overlap of 50%.

Figure 5 shows an example of measuring an impulse signal with 50% overlap. In this scenario, the second FFT frame (bottom row) gives a full response because the impulsive envelope occurred at the time of maximum weighting.¹¹ With 90% overlap, the worst-case error from the windowing occurs when the envelope peak is displaced from the weighting peak by 5% of the FFT duration.

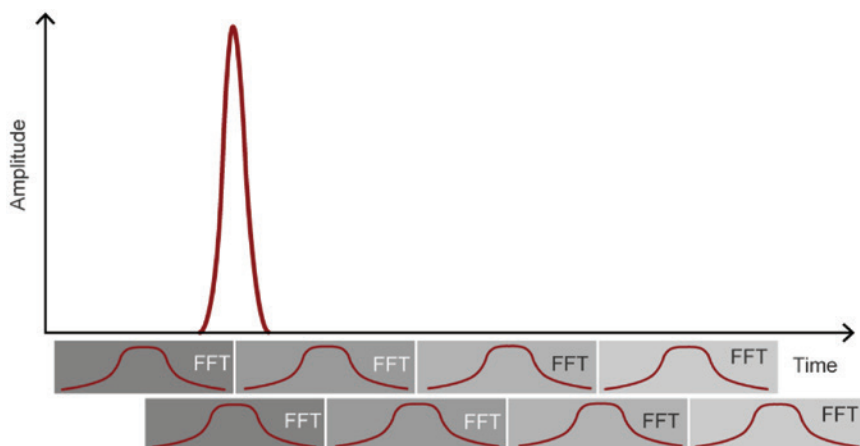


Figure 5: Measurements made with FFTs at 50% overlap in the time domain

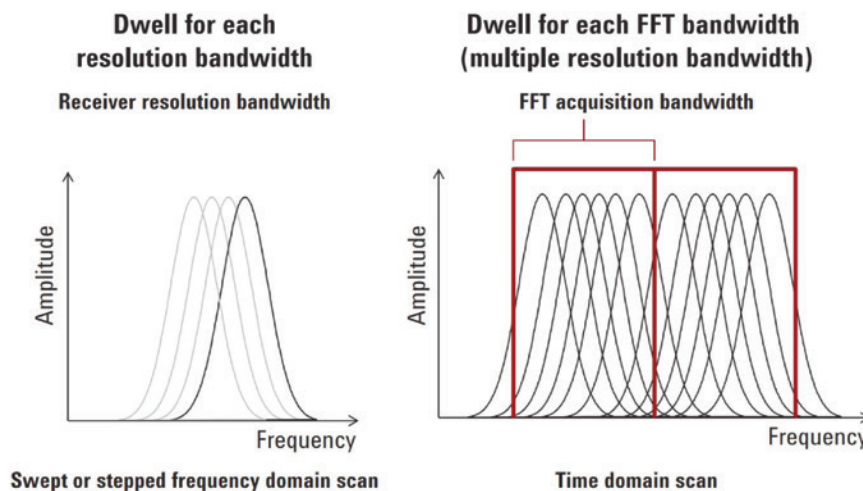


Figure 6: Comparison of resolution bandwidth and FFT acquisition bandwidths

An additional advantage is that the overlapping FFTs allow you to capture all data in the acquisition bandwidth in one dwell time, compared to having to stop at each frequency point for the dwell time for the traditional swept or stepped frequency domain scan.

SHOULD YOU USE OVERLAPPING FFTS?

While overlapping FFTs allows you to analyze broadband data instantaneously, it does come with a higher cost than traditional swept frequency receivers. Given that, here are several scenarios where the use of overlapping FFTs is beneficial:

1. *Faster measurement times:* Because the overlapping FFTs allow you to capture broadband signals in one dwell time, the measurement time is much faster than the traditional swept frequency receivers. Table 2 shows the dramatic difference in measurement times for a typical automated broadband noise test.

2. *Impulsive noise detection:* If your equipment under test (EUT) has impulse noise contributors, or if you need to investigate if it has those characteristics, then the FFT capability may be the only way to capture that phenomenon.

CISPR Band C/D	Stepped Scan	Wideband FFT
30 MHz – 1 GHz Quasi Peak detector 1 second dwell time RBW = 120kHz	~9 hour	< 6 sec
4 Antenna positions left side right side vertical orientation horizontal orientation	~36 hour	< 24 sec

Table 2: Measurement time comparisons between stepped scan and wideband FFT EMI receivers



UNRIVALLED WIRELESS TESTING CAPABILITY REDUCE RISK AND TIME TO MARKET



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



FFT implementations in EMI receivers offer many benefits, namely much faster measurement times and the ability to capture intermittent/impulsive emissions. Their use for design validation and pre-compliance testing is very useful in identifying unique and intermittent emissions that may be missed using conventional EMI receivers.


Figure 7 shows an example on the left of an impulsive signal (in this case, a pulsed comb generator) where the traditional stepped scan is only able to capture one of the frequencies, vs. the overlapped FFT on the right, where all frequencies are captured on one acquisition.

3. *Unique EUT characteristics:* If your EUT has unique characteristics (for example, it is not able to be left in a powered on condition for a complete test, or it has motors or switches that operate normally during the use of the product such as pumps or motor drives in a washing machine), then you would benefit from FFTs being able to capture the emissions when the EUT is exhibiting one of those emissions.
4. *Exhaustive pre-compliance validation:* If you wish to exhaustively test your EUT for pre-compliance for any impulsive surprises, then the overlapping FFTs will allow you to detect those before you send it to the test lab for final compliance tests.

SUMMARY

FFT implementations in EMI receivers offer many benefits, namely much faster measurement times and the ability to capture intermittent/impulsive

emissions. Their use for design validation and pre-compliance testing is very useful in identifying unique and intermittent emissions that may be missed using conventional EMI receivers. Their applicability for CISPR compliance testing, while defined in CISPR 16-1-1:2010-06 edition, may not mean you can use them for full compliance testing. Because of the limitations on sampling rates and memory depth, the ability to measure low PRF impulses is a challenge.

Some CISPR standards for specific device types may not allow for the use of FFTs for compliance measurements. You will need to review the CISPR standard applicable to your EUT to determine if that edition is referenced in your standard to decide whether FFT measurements are allowed for full compliance testing. 

ENDNOTES

1. Thomas S. W. Lewis, *Empire of the Air*, 1991, Harper Collins Publishers.
2. Ibid., page 40.
3. Gubisch, R., Holz, B., “The Engineer’s Guide to Global EMC Requirements: 2007 Edition,” pp. 2, Intertek, 2007.

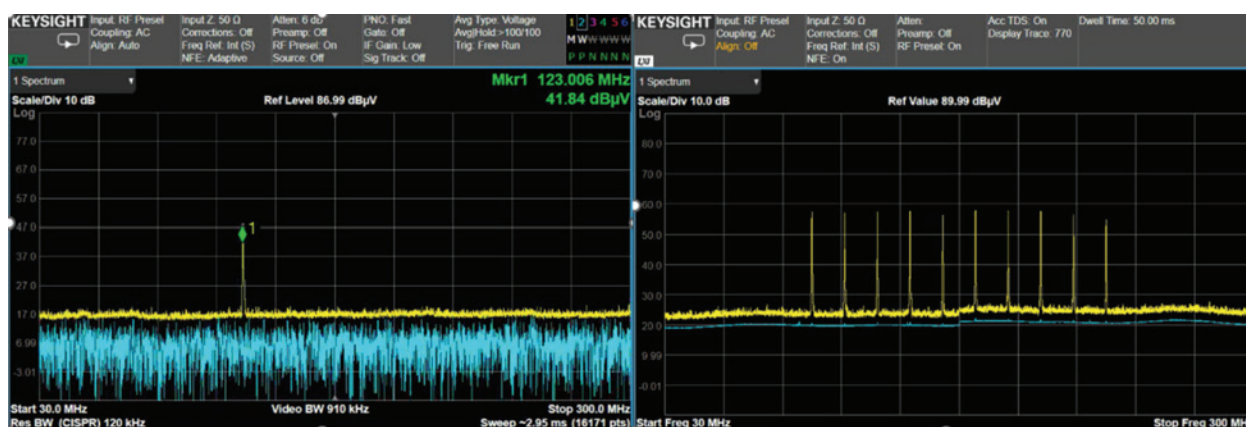


Figure 7: Stepped scan vs FFT scan for impulse signal

4. Mohd Fahmi, Abdul Rahim, Agilent Technologies, Inc., "Evolution and Trends of EMI Receiver," 2013 IEEE International RF and Microwave Conference, Penang, Malaysia.
5. CISPR, Wikipedia, <https://en.wikipedia.org/wiki/CISPR>.
6. Federal Communications Commission, Wikipedia, https://en.wikipedia.org/wiki/Federal_Communications_Commission.
7. Burrill, C.M., "Progress in the Development of Instruments for Measuring Radio Noise", Proceedings of the IRE, vol. 29, issue 8 pp. 433-442, August 1941.
8. Houck, H. W., "The Armstrong Super-Autodyne Amplifier, part 1," *Radio Amateur News*, Experimenter Publishing Co., New York, vol. 1, no. 8, February 1920, p. 403.
9. Thomas S. W. Lewis, *Empire of the Air*, 1991, Harper Collins Publishers, Chapter 6.
10. Keysight Technologies, "Enhance EMC Testing with Digital IF – Application Note," June 18, 2015.
11. Ibid.
12. Keysight Technologies, "Boost EMC Test Throughput with Accelerated Time Domain Scan," July 14, 2023.

CYBER-SECURITY

A Coming Wave

Powering Resilience in
IT, Wireless & Beyond.

- ✓ Cyber Testing
- ✓ System Assurance
- ✓ Compliance with Industry Standards



Washington Laboratories, Ltd.
301-216-1500 | WWW.WLL.COM | info@wll.com

Hot Topic:
CRA Compliance



Webinar Access Here

CYBERSECURITY DEVELOPMENTS IN WIRELESS AND COMMUNICATIONS TECHNOLOGIES

Managing Cyber Vulnerabilities Across International Boundaries



Michael Violette is the founder and president of Washington Laboratories and the director of American Certification Body. He can be reached at mikev@wll.com.



By Michael F. Violette, P.E.

The advent of several regulatory initiatives in 2025 will make their impact on the wireless and communications industry. It is well-known and well-publicized that hacking and subversion of the communications infrastructure by bad actors continues to rise. The effect is experienced every day by consumers, public safety and services, defense, and by every sector of our modern society. The growing implementation of “connectivity everywhere, all-the-time” means that necessary measures must be taken to address security issues related to the design and testing of devices and their integration into networks. The actions by bad actors (for whatever gains they hope to achieve, monetary, civic instability, pilfering of design, etc.) mean that security precautions are now more necessary than ever.

There are many reported instances of cybersecurity weaknesses, and the industry and regulators are taking back the management of this space. In the U.S., the National Institute of Standards and Technologies (NIST) has been at the forefront of leading cybersecurity infrastructure protections. The NIST Cybersecurity Framework (CSF 2.0) is designed to support industry, government, and other organizations. CSF 2.0 is becoming well-organized and accepted. I liken the current efforts to the early 1990s when the goals and objectives of telecom mutual recognition agreements (MRAs) were worked out and are still working well today.

This article outlines recent and near-term cybersecurity protections that are being enacted in the U.S., Canada, the European Union (EU), and other jurisdictions. At the core, achieving a balance between effective cyber protection and free trade can present multiple challenges when it comes to finding common ground.

CURRENT CYBERSECURITY INITIATIVES

Current cybersecurity-focused efforts include:

- ***EU Cybersecurity Act***: Introduces an EU-wide certification framework for ICT products, services, and processes.¹
- ***U.S. Federal Information Security Modernization Act (FISMA)***: Provides a framework to protect government information operations against cybersecurity threats.²
- ***Health Infrastructure Security and Accountability Act***: Sets stringent minimum cybersecurity standards and requires annual audits for compliance.³

These are broad mandates driven by regulators but supported by many industries and industry sectors that recognize the real risks of penetration of networks and devices for ill gains. NIST in particular is taking strong positions on education and frameworks under the drive to provide cyber protection.

NIST’s CSF 2.0 is a set of voluntary guidelines designed to help organizations assess and improve their ability to prevent, detect, and respond to cybersecurity risks. The CSF framework was initially published in 2014 for critical infrastructure sectors but has since been widely adopted globally across various industries, including government and private enterprises. The framework integrates existing standards, guidelines, and best practices to provide a structured approach to cybersecurity risk management.

So far, adopting the NIST CSF framework is voluntary, but it is increasingly being seen as a mandatory requirement in many organizations. Especially within federal government agencies, compliance with the NIST CSF is deemed mandatory

Covered Equipment or Services	Date of Inclusion on Covered List
Telecommunications equipment produced by Huawei Technologies Company, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced by ZTE Corporation, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by Hytera Communications Corporation, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by Hangzhou Hikvision Digital Technology Company, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by Dahua Technology Company, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by China Mobile International USA Inc. subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by China Telecom (Americas) Corp. subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by Pacific Networks Corp and its wholly-owned subsidiary ComNet (USA) LLC subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by China Unicom (Americas) Operations Limited subject to section 214 of the Communications Act of 1934.	September 20, 2022
Cybersecurity and anti-virus software produced or provided by Kaspersky Lab, Inc. or any of its successors and assignees, including equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software.	July 23, 2024

Table 1: The FCC's Covered List of equipment or services

for those vendors who wish to partner with those agencies. But more and more private enterprises are taking a strong stance to protect their operations against cyber exposure, balancing access with appropriate protections. Entities must continuously be vigilant against nominal hacking and vicious attacks and take appropriate measures to ensure immunity.

THE U.S. FCC'S "COVERED LIST"

There are broad and narrow protections that the U.S. federal government has taken at both the enterprise (business) level and at the device (consumer/user) level. Some of those protections include outright exclusion of certain entities from accessing the communications infrastructure in the U.S. And increasing threats from some of our largest international trading partners have forced the U.S. to take certain actions. Some of these efforts may seem draconian, but are deemed necessary to protect the security and integrity of communications and supply chain networks.

Toward that end, the U.S. Federal Communications Commission (FCC) has published a "Covered List" of such entities whose systems and devices pose a potential security threat to U.S. organizations. Published in August 2024, FCC document KDB 986446 D01 Covered Equipment Guidance v03, "Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program," details the names of entities that are deemed a "national security threat." Almost all of these listed entities are based in the People's Republic of China (PRC).

The FCC's Covered List is regularly updated to include additional entities and communications service providers who are banned from connecting their equipment to the U.S. communications network. A current list of these companies and their restricted equipment and services is found in Table 1, with a short description of their infraction and the date they were placed on the Covered List. The most recent addition is Kaspersky Lab, Inc., a Russian-owned entity based in Moscow.

THE FCC'S CYBER TRUST MARK PROGRAM

Further, the FCC has recently implemented a Cyber Trust Mark program that mandates that certain equipment show protection against attacks that compromise data, penetration protections, and

In Compliant with
IEC 61000-4-2: 2025



Electrostatic Discharge (ESD) Simulator

EDS MAX20



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

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

EDS MAX30



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

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

SUZHOU 3CTEST ELECTRONIC CO., LTD.

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



SUBSCRIBE: 3CTEST

monetary losses. This particular action is mostly for the protection of consumers, but may be (and probably will be) broadened to include all systems and devices that must be reviewed and approved under the FCC's Equipment Authorization program. That Program is a system that requires companies that have wireless equipment to have their devices "certified" by a testing laboratory authorized under the FCC's Telecommunications Certification Body (TCB) program, which is tasked to test, review, and certify devices under the purview of the FCC's Office of Engineering and Technology (OET).

The purpose of the Cyber Trust Mark is, again, to protect against compromising equipment that is exposed to the Internet. The program is still evolving, in real ways, but will ultimately lead to protections for the U.S. communications infrastructure.⁴

For the moment, the Cyber Trust Mark program is also voluntary but expect that to change as well. In my opinion, it won't be long until this voluntary program becomes mandatory for device approvals. This is in step with the coming EU requirements for radio equipment under its Radio Equipment Directive (RED) and Cybersecurity Act, discussed in the next section.

What this means for device compliance is profound and must be considered for Internet of Things (IoT)-related devices that may be vulnerable (which is, to say, everything, from video systems to baby monitors to electric razors).

The FCC's Cyber Trust Mark is shown in Figure 1.

As stated on the FCC's information page on this topic, the FCC is still "standing up" to this comprehensive program. The rollout of this program is likely to be in the next year or two or by 2026. A structure is still being worked out under which U.S.-based firms (and, at this time, only U.S.-based firms) can issue the Cyber Trust Mark.



U.S. CYBER TRUST MARK

Figure 1: U.S. Cyber Trust Mark

EUROPEAN UNION CYBER-SECURITY ACTIVITY

For context, the EU's Radio Equipment Directive (2014/53/EU) has been a very successful program within the EU that provides a comprehensive route to protect the radio spectrum. Industry, regulators, and society (although only a small percentage of the population knows this) rely on standard approaches to control interference, improve communications performance, and ensure that the device in your hand will work across various networks.

These networks include, among others, cellular systems, local Wi-Fi, and something called LoRa (long-distance radio), which extends, in a sense, the connectivity of the Internet of Things (IoT) and other devices. In essence, the LoRa frequency ranges propagate farther than the Wi-Fi and cellular frequencies. This is handy for sensors and other communications implementations. The long-distance record for LoRa data transmission is now 1336 km or 830 miles!⁵

However, I digress. One can simply note that cyber protections address a sometimes-dizzying array of devices and technologies.

In addition to the EU's RED, the European Union Agency for Cybersecurity (ENISA) has taken steps to integrate cybersecurity protections into RED requirements, most notably its efforts to integrate supplemental measures related to cybersecurity.

Commission Delegated Regulation (EU) 2022/30 adds key changes to the requirements contained in Article 3.3 d/e/f of the RED, and serves as the basis for the EU's Cybersecurity Act.

An August 1, 2025 deadline approaches for the updated RED requirements related to cybersecurity to come into force. There is a strong movement to comply, and opportunities await for multinational players to help

the industry maintain their market access, which is difficult enough in the practical realities of global product approvals.

EXODUS

ADVANCED COMMUNICATIONS

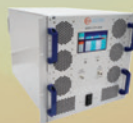
Model Number	Frequency Range	Rated Power Watts	Gain dB
10KHz-250MHz, Low Frequency Amplifiers			
AMP20094	10 kHz-250 MHz	150	52
AMP20093	10 kHz-250 MHz	300	55
AMP20095	10 kHz-250 MHz	600	58
AMP20168	10 kHz-250 MHz	1250	62
AMP20162	10 kHz-250 MHz	2500	64
80-1000MHz, VHF, UHF Range Amplifiers			
AMP20032	80-1000 MHz	300	55
AMP20081	80-1000 MHz	500	57
AMP20083	80-1000 MHz	750	60
AMP20130	80-1000 MHz	1300	61
AMP20139	80-1000 MHz	2000	63
700MHz-6.0GHz, Broadband Amplifiers			
AMP20079	0.7-6.0 GHz	100	50
AMP20078	1.0-6.0 GHz	150	52
AMP20080	1.0-6.0 GHz	200	53
AMP20043	1.0-6.0 GHz	300	55
AMP20160	1.0-6.0 GHz	750	59
2.0-8.0GHz, SC Band Amplifiers			
AMP20098	2.0-8.0 GHz	120	51
AMP20100	2.0-8.0 GHz	200	53
AMP20102	2.0-8.0 GHz	400	56
6.0-18.0GHz, High Frequency Amplifiers			
AMP20118	6.0-18.0 GHz	40	46
AMP20111	6.0-18.0 GHz	50	47
AMP20045	6.0-18.0 GHz	100	50
AMP20071	6.0-18.0 GHz	200	53
AMP20072	6.0-18.0 GHz	300	55
AMP20154	6.0-18.0 GHz	700	58
18-26.5GHz, K-Band, Millimeter Amplifiers			
AMP40013	18.0-26.5 GHz	10	40
AMP40033	18.0-26.5 GHz	20	43
AMP40031	18.0-26.5 GHz	50	47
AMP40029	18.0-26.5 GHz	80	49
AMP40028	18.0-26.5 GHz	150	52
26.5-40.0GHz, Ka-Band, Millimeter Amplifiers			
AMP40044	26.5-40.0 GHz	10	40
AMP40038	26.5-40.0 GHz	20	43
AMP40037	26.5-40.0 GHz	40	46
AMP40034	26.5-40.0 GHz	80	49
AMP40035	26.5-40.0 GHz	120	52
18.0-40.0GHz, Millimeter Amplifiers			
AMP40018	18.0-40.0 GHz	10	40
AMP20005	18.0-40.0 GHz	25	44
AMP20167	18.0-40.0 GHz	60	48
40.0-50.0GHz, Q-Band, Millimeter Amplifiers			
AMP40049	40.0-50.0 GHz	1	30
AMP40045	40.0-50.0 GHz	5	37
400MHz-12.0GHz, Pulse AMPs, RADAR & HIRF			
AMP20141	0.4-1.0 GHz	4 KW	66
AMP20057	1.0-2.0 GHz	4 KW	66
AMP20144	2.0-4.0 GHz	4 KW	66
AMP20101	2.0-8.0 GHz	2 KW	63
AMP20097	4.0-8.0 GHz	2 KW	63
AMP40053	8.0-12.0 GHz	2 KW	63



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

**Amplifiers
CW & Pulse**

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



0.4-1.0GHz
4KW Pulse



1.0-2.5GHz
8KW Pulse



10kHz-250MHz
3000Watts



800MHz-6.0GHz
1000Watts



2.0-8.0GHz
500Watts

Evaluations of equipment and systems must include physical, data and protocols for “disaster recovery” which typically include some kind of risk assessment to ensure that procedures are in place to limit damage, physical or otherwise.

Article 3.3 d/e/f of the RED deals with network security, protection of personal data, and prevention of fraud. Article 3.3 d focuses primarily on devices to minimize the quasi-physical threats of compromising a device.

Article 3.3 e is self-explanatory but not always easy to follow. For example, how does a service provider or device manufacturer demonstrate that personal data is not subject to “spoofing.” In a practical way, this means solid fire walls and the education of operators and users so that they are not fooled by poaching attacks. And this is also tightly coupled with Article 3.3 f, which can occur if the proper protections are not imbued in the device design or the operation of the device.

Nonetheless, humans are subject to being “fooled,” and the best a device manufacturer or operator can do is to limit damage in some cases or have backups or built-in protections.

Evaluations of equipment and systems must include physical, data and protocols for “disaster recovery” which typically include some kind of risk assessment to ensure that procedures are in place to limit damage, physical or otherwise, from pernicious effects of the intent of “bad actors,” which can be domestic or foreign agents intent on disrupting or stealing from any manner of devices connected to the Internet, either directly or indirectly.

Eventually, these changes to the RED will affect broad areas of industry and nearly any internet device (connected directly or indirectly). This act affects large swaths of the industry and will be mandatory for information and communication technology (ICT) devices, which include just about everything.

INDUSTRY ACTIONS

Regardless of the regulatory environment, industry is taking on its own sets of protections, requiring

that vendors demonstrate that suppliers have cyber protections in place. This requires a set of internal and external measures that protect design and data integrity, especially when dealing with personal information. Increasingly, vendors must build the operational infrastructure to manage internal affairs. Sometimes, these might just be “checklists” or the stuff of audits and more scrutiny by third parties. It all depends on a few things, each one of which adds a twist to staying in compliance, including:

1. Oversight by government or regulators
2. Internal policies
3. Industry trends

In our compliance world, accreditation bodies (ABs) may perform a role in having a third-party, independent assessment. This activity often involves a mix of remote or on-site reviews of documentation, procedures, training, or other proof of competence. A certification body (CB), notably under the FCC’s Equipment Authorization Program, has to comply with ISO 17065 and, potentially, ISO 17025 for testing laboratories. ABs may also follow ISO 17011 and Personnel Certification according to ISO 17024. Many of the same principles apply to the various ISO 170XX standards, but at the core is the demonstration of confidence.

This is extending into cyberspace, with its particular focus on the protection of networks, people, and personal information. The framework of the assessment is the same with the particular focus depending on the intent and content of the standard that is being assessed.

Many companies are taking matters into their own hands by requiring compliance with these ideals as a condition for working with them. It simply is what it is, and it is for a good cause. In any event, it becomes a business decision: if a company wishes to work in this increasingly complex space of interconnectedness, they

must go through the actions, and it is not capricious. It involves a management-level decision to move the organization in that direction. The implementation of procedures affects all levels of an operation, from design to communication to inventory to supply chain verification.

This last point may be a little tricky because a vulnerability exists at the chip level. This is why suppliers on the FCC's Covered List are suspect because it is conceivable, if not already happening, that malicious code can be embedded in the firmware of a microprocessor or other critical data part that can listen and report out activities of the user(s). For the integrator, there is practically no way to know this, and that is the difficult part for manufacturers who have wider goals and implementations of the technologies.

This goes right to the heart of the protection of IoT devices: "Someone might be listening..."

INTERNATIONAL COOPERATION

The ISO documents referenced previously are International Standard Organization (ISO) documents, which implies that there are many organizations at the table. For the narrow purpose of the importance of U.S./EU trade, ISO documents are key. It is not uncommon for individual countries to adopt the ISO requirements to suit their own National Standards structure. However, in the majority of cases, the text(s) are the same.

A success story: the EU and North America (at least for now) have mutual recognition agreements (MRAs) which allow for a free flow of goods across the borders. The MRAs include EMC and radio regulations that have worked very well for U.S. and Canadian manufacturers.

Yet this structure does not only affect U.S./CN/EU trade, but the approvals are often used for market access for other countries wherein the regulatory structure is not in place, or the regulatory structures have not matured and (depending on the size of the economy) may not be warranted. That is, these countries don't need a full-blown regulatory structure and often rely on "CE Marking" or "FCC Certification" for placing products on the market.

These MRAs have been in place for EMC and radio equipment for a few decades, allowing access to markets under a combined mix of international and domestic regulations.

It remains to be seen whether the MRAs will include some of these new cyber provisions. For the moment, the FCC is requiring any entity that issues a Cyber Trust Mark approval to be located in the U.S. Reciprocally, but perhaps malleable is the EU, which is currently not recognizing Notified Bodies for cyber approvals outside of the EU. In effect, each country/economy is becoming more focused on protecting its own industries.

Perhaps this will change. But with the current political climate in flux at the time this article was written, it is hard to predict what the picture will look like in the near future or in the next few years. But as happens with most regulatory actions (and practically so), they are unlikely to be rolled back.

Whatever the final outcomes (and they are not static, mind you!) these frameworks are here to stay. 🇺🇸

ENDNOTES

1. "The EU Cybersecurity Act," the European Commission's webpage for the EU's Cybersecurity Act, available at <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act> (as of 4 May 2025).
2. "S. 2251, Cybersecurity Act of 2023," the U.S. Congressional Budget Office webpage for the U.S. Federal Information Security Modernization Act (FISMA), available at <https://www.cbo.gov/publication/59481> (as of 4 May 2025).
3. "Health Infrastructure Security and Accountability Act: A New Era for Healthcare Cybersecurity," an article posted to the website of law firm JD Supra, available at <https://www.jdsupra.com/legalnews/health-infrastructure-security-and-1139975> (as of 4 May 2025).
4. Additional details about the FCC's Cyber Trust Mark program are available at <https://www.fcc.gov/CyberTrustMark>.
5. A comprehensive overview regarding the parameters of LoRa can be found at <https://www.thethingsnetwork.org/docs/lorawan/regional-parameters>.

PREPARING FOR THE EU'S NEW RED CYBERSECURITY REQUIREMENTS

Steps to Take Now to Ensure Compliance



Corey Sweeney is the President of D.L.S. Electronic Systems, Inc., a compliance testing laboratory located in Wheeling, IL. Sweeney can be reached at cs@dlsemc.com.

Jack Black is the business development manager for D.L.S. and has over 30 years of experience in the field of compliance testing and standards development. Black can be reached at jblack@dlsemc.com.

Marilyn Sweeney is CEO and one of the founding members of D.L.S. Sweeney can be reached at msweeney@dlsemc.com.

By Corey L. Sweeney, Jack Black, and Marilyn Sweeney

Editor's Note: As we go to press, relevant cybersecurity requirements are still being developed, so the information presented here may change.

The European Union's (EU's) 2024 Cyber Resilience Act makes complying with the cybersecurity standards in the Radio Equipment Directive (RED) mandatory. If your product has Bluetooth, Wi-Fi, or other wireless connectivity in it, and you intend to sell in Europe, it is likely that you will need to comply with Chapter 1, Article 3, Item 3(d), 3(e), and 3(f) of the RED before August 1, 2025. Your firmware developers may need a significant amount of time to implement the provisions, so if you have not already started securing your product to the new regulation, you need to do so now.

Since the new regulation is extremely vague, the European Telecommunications Standards Institute (ETSI) came up with a set of related standards to clarify the requirements that include:

- ETSI EN 303 645 for the manufacturers to follow; and
- ETSI TS 103 701 for test labs to follow.

The new ETSI Cybersecurity standards state that the following products must comply:

- Devices capable of communicating over the Internet (either directly themselves or through another device, like a smartphone);
- Toys and childcare equipment; and
- Wearables (smartwatches, etc.).

There are exemptions for specific products that fall under the scope of their own medical, avionics, or automotive directives, as it will be up to those directives to add their own cybersecurity standards.

THE RED, THE CYBERSECURITY ACT, AND THE CYBER RESILIENCE ACT

The EU tends to create directives/regulations that modify previous directives/regulations. As you can see below, this means that there is a tendency to end up with a chain of directives instead of a cohesive document. Here's a brief overview of the relevant directives and regulations summarized above.

The Radio Equipment Directive (RED) (Directive 2014/53/EU)

In Article 3, Item 3, this directive includes provisions so that:

- (d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- (e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; and
- (f) radio equipment supports certain features ensuring protection from fraud.

However (d), (e), and (f) were "inactive" until 2022. It looks like there were no cybersecurity certification methods to accomplish this at the time, which might be what is meant by "inactive."

The EU Cybersecurity Act (Regulation (EU) 2019/881)

This regulation created a framework for cybersecurity certification "schemes" in Europe. A scheme is the requirements for cybersecurity certification for one particular group of products/services.

Cyber Resilience Act Directive (EU) 2020/1828

This directive supplements Article 3 of the RED and sets out the essential requirements with which radio

equipment placed on the EU market shall comply, in relation to:

- Article 3(1)(a) health and safety;
- Article 3(1)(b) electromagnetic compatibility;
- Article 3(2) the effective and efficient use of radio spectrum; and
- Article 3(3) those categories or classes of radio equipment specified in related Commission delegated acts.

The RED empowers the EU Commission to adopt delegated acts in order to render applicable any of the essential requirements set out in Article 3(3) by specifying each of those requirements that shall concern categories or classes of radio equipment. Three points of the second subparagraph of Article 3(3) are relevant to this initiative:

- 3(3)(d) to ensure network protection;
- 3(3)(e) to ensure safeguards for the protection of personal data and privacy; and
- 3(3)(f) to ensure protection from fraud.

2022 Supplement to the Radio Equipment Directive 2014/53/EU - COMMISSION DELEGATED REGULATION (EU) 2022/30

This regulation activates (d), (e), and (f) in RED and defines the products to which they apply to as:

- Devices capable of communicating over the Internet;
- Toys and childcare equipment; and
- Wearables (smartwatches, etc.).

The August 1, 2024 deadline was later changed to August 1, 2025.

On August 5, 2022, the EU Commission issued a standardization request to CEN and CENELEC to develop harmonized standards in support of Delegated Regulation 2022/30. In response, ETSI came up with:

- The “baseline” standards with which manufacturers need to comply (ETSI EN 303 645);
- The procedures the test lab uses to assess a manufacturer’s compliance (ETSI TS 103 701);
- “Vertical standards” - ETSI EN 303 645 interpreted for specific devices like smart locks, etc.; and

- If a product does not have a “vertical standard,” then the baseline standards apply.

Delegated Regulation C(2023)4823

This regulation changed the date of the deadline from August 1, 2024, to August 1, 2025.

Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847)

This regulation adds requirements for manufacturers such as:

- Cybersecurity is considered throughout the product’s lifecycle (i.e. in the planning, design, development, production, delivery, and maintenance phases).
- All cybersecurity risks must be documented.
- Manufacturers will have to report actively exploited vulnerabilities and incidents.
- Once sold, manufacturers are responsible for ensuring that, for the expected product lifetime or for a period of five years (whichever is shorter), vulnerabilities are handled effectively.
- Clear and understandable instructions for the use of products with digital elements are available.
- Security updates are made available for at least five years.

WHY CYBERSECURITY RULES ARE NECESSARY

Improve Network Resilience

Most manufacturers of IoT devices have ignored cybersecurity issues while making products that are extremely vulnerable. You may remember when, on October 21, 2016, roughly ten percent of the websites on the internet became unreachable, including amazon.com, cnn.com, github.com, and many other popular sites, which broke additional sites that required those services to be functioning. Dyn, then the third largest DNS service provider, was taken down by a distributed denial of service attack (DDoS). At the time, Dyn was thought to be too large a DNS provider for a DDoS to work against them.

What had changed was that botnets, which were usually limited by the number of computers people had, started compromising vulnerable IoT devices which had far outnumbered the computers. With so many more devices under its control, the botnet was able to easily take down Dyn.

Improving network resilience means protecting the internet/phone network itself by making sure the network is protected from your product. But it goes beyond just IoT.

Improving network resilience means protecting the internet/phone network itself by making sure the network is protected from your product. But it goes beyond just IoT. For example, see “Hackers Remotely Kill a Jeep on the Highway – with me in it.” This video shows a person trying to drive down the highway while attackers start continuously spraying his windshield-wiper fluid, blurring his vision. It also shows a driver being unable to control his jeep when attackers remotely drive it into a ditch.

Consumer Privacy Issues

You have probably heard stories of people getting death threats through their Ring-connected doorbells/security

cameras. Amazon had to pay out more than \$5 million (USD), as summarized in “FTC Sends Refunds to Ring Customers Stemming from 2023 Settlement over Charges the Company Failed to Block Employees and Hackers from Accessing Consumer Videos.”

Reduce the Risk of Monetary Fraud

Under the EU's RED, Article 3.3(f) focuses on monetary fraud prevention measures. It requires manufacturers to incorporate features in internet-connected devices that actively prevent fraudulent electronic payments and monetary transfers, particularly in devices handling financial transactions.



EMC IMMUNITY TESTING SOLUTIONS

Optimized for <6 GHz



T&M Instrument Amplifier

- ▼ Solid-state GaN PAs
- ▼ Broadband design: 0.5 GHz to 6 GHz ~
- ▼ Output power: up to 500 W
(custom options available in the kW range)
- ▼ Integrated coupler & protection circuitry
- ▼ Remote control operation



Couplers, Cable Assemblies & Power Sensors

- ▼ StabilityPlus™ Phase Stable Cable Assemblies
ensure accurate transmission in high-frequency EMC test environments.
- ▼ RTP Real-Time Peak Power Sensors to 18 GHz
measure, monitor, and verify power levels to maintain high-integrity testing.
- ▼ Low-Loss, High-Power Bidirectional Airline Couplers
provide high directivity and low insertion loss for maximum performance high-integrity testing.

ETSI EN 303 645 is a list of over 60 provisions (the precise number depends on the exact version). While the rules themselves can be worded to try to cover all edge cases, this discussion will be about the rules in terms of what they mean for most people.

Key points include:

- Focus on payment-related devices;
- User authentication controls;
- Secure communication protocols; and
- Compliance with industry standards.

Manufacturers are required to conduct thorough risk assessments to identify potential vulnerabilities within their devices that could be exploited for fraudulent activities. Ongoing updates and patches need to be provided to address emerging vulnerabilities and maintain security levels against evolving fraud tactics.

HOW THE NEW STANDARD ADDRESSES THESE ISSUES

ETSI EN 303 645 is a list of over 60 provisions (the precise number depends on the exact version). Following are some examples. While the rules themselves can be worded to try to cover all edge cases, this discussion will be about the rules in terms of what they mean for most people.

No Universal Default Passwords

Manufacturers were hard coding default login/password parameters (often times the login and password were both “admin”) without requiring the user to change the passwords. Since most users do not explicitly change the default admin password on their own, this allows an obvious compromise route for anyone who downloaded the user manual and looked up the password. So, this is about making the passwords non-obvious.

Securely Store Sensitive Security Parameters

Manufacturers must implement robust measures to protect sensitive data stored on connected devices, ensuring that this data is securely handled throughout the product’s lifecycle, as mandated by the CRA’s cybersecurity standards within the broader framework of RED compliance for wireless devices.

Key points include:

- Data protection;
- Secure storage mechanisms;
- Lifecycle security; and
- RED compliance.

Example scenarios:

- A smart home device storing user login credentials must encrypt the data using a strong encryption algorithm.
- A wearable fitness tracker collecting health data should use secure protocols to transmit that data to the cloud.
- Manufacturers need to implement regular software updates to address vulnerabilities that could compromise sensitive data storage.

Use Best Practice Cryptography in Communications

Basically, for most people, this will mean things like:

- Communicate over either TLS (formerly called SSL) or SSH; and
- Use a key size that is large enough so that the keys will still be considered secure when you end support for that product.

The Manufacturer Shall Publish the Defined Support Period

The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period. Basically, this means management needs to decide on how long a period they are willing to commit to providing security updates for the product’s software/firmware (it must be at least 5 years). And, then to comply, they need to add the period that they commit to in the product specifications on the official website for the product.

Although most products will need to comply with ETSI EN 303 645, there will also be a special ETSI TS standard applicable to your product if it is covered in one of the “vertical standards.”

Implement a Means to Manage Reports of Vulnerabilities

Once your product is on the market, most of your new security vulnerabilities will probably be found in your vendors’ libraries. You will need to set a policy and implement it for how people should send you vulnerability reports when they find one in your product. If you do not already have a Vulnerability Disclosure Policy, you will need to create one once your product is on the market. People need to be able to assess their risk by reading your Coordinated Accepting Vulnerability Reports when vulnerabilities are discovered in your product.

HOW TO COMPLY

Determine Which Standard Applies to Your Product

Although most products will need to comply with ETSI EN 303 645, there will also be a special ETSI TS standard applicable to your product if it is covered in one of the “vertical standards.” For example, if your product is a home gateway, then your standard will be ETSI TS 103 928.

Download the Standard

As of March 10, 2025, the current version of ETSI EN 303 645 is v3.1.3; however, this may change between now and the time you read this article. You can download the current version of ETSI EN 303 645 on the ETSI website.¹

Determining Provisions

Determine which provisions listed in Annex B with which you intend to comply and decide on your intention for each provision. Choose from the following:

- Mandatory provision (marked with an “M” in the status column)
 - You intend to implement this provision;

- Your product does not meet the condition marked on the provision, i.e. not applicable; or
- Your product does not have the feature marked on the provision, i.e. not applicable.
- Recommended provision
 - You intend to implement this provision; or
 - You do not intend to implement this provision. You are required to mark the reason why you are not implementing it.

Attempt to Secure Your Product

Implement the provisions into your product.

Document Your Results in the Implementation Conformance Statement (ICS) Form

The Implementation Conformance Statement (ICS) form is generally found within the standard that applies to your product. When you finish implementing everything needed in your product, you must fill out the ICS Form to self-declare your conformity to the standard. This self-declaration states

EMC PARTNER
MIL-MG3

The new standard in defence testing

Portable multifunction impulse test generator with plug-ins for MIL-STD and DO-160 applications.

- ⊕ Test MIL-STD-461: CS106/115/116/118
- ⊕ CS117 testing available
- ⊕ DO-160 sections 17 and 19
- ⊕ Modular & easy upgradable

www.emc-partner.com

HVA
Your contact for North America
www.hvtechnologies.com

Mail emcsales@hvtechnologies.com
Phone 703-365-2330

that you comply with all aspects of the regulation that apply to your product and that you are taking full responsibility for securing your product to the new requirements. It shows which requirements your product complies with, which requirements do not apply to your product, and why you did not implement the optional requirements.

You then have the option of sending your product, along with your ICS form and an IXIT form, to a third-party test lab for guidance, direction, and reassurance that no aspect of the new requirements has been missed. They will answer your questions and validate that the information in the form describes a complying product and that the product is consistent with what was filled out in the form.

IXIT Form


The test lab will send you an IXIT form. As a manufacturer, you must fill out this form, describing the details of the product and the process you went through to comply with each aspect of the standard that is applicable to your product. For example, it asks:

- What kind of authentication your network connection uses (e.g., TLS connections with public/private ECDSA keys);

- Your company's policies for how quickly they will respond to vulnerabilities found in the device;
- Where the user can find your statement on what personal data is used and how it is used;
- How the device will get updates to get security patches whenever they come out; and

The test lab also validates that the product is consistent with what was filled out in the form and that it is a compliant product.

IS THE CYBERSECURITY REQUIREMENT ONLY FOR SELLING IN EUROPE?

Other regions and other industries will also be making similar requirements. In the U.S., the Federal Communications Commission (FCC) is creating the "U.S. Cyber Trust Mark" to be implemented for IoT. Canada is also creating the "CyberSecure Canada Mark." Cybersecurity requirements for the EU Machinery Directive will be going into effect in 2027. 

ENDNOTE

1. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf



PRODUCT showcase

ABSOLUTE EMC

Trust Matters!



Unlock Superior EMC Performance with Our All-In-One Product Line!

HAEFELY
Current and voltage – our passion

montena

YIC TECHNOLOGIES

evalzer

BOLAB SYSTEMS GMBH

EMC Instruments Co., Ltd.

THE COMPLIANCE ASSESSMENT BUSINESS COMPLIANCE DELIVERED

LUMILOOP **messtechnik** **SCHWARZBECK**

Your Trusted Partner for Support, Service, and Sales!

ABSOLUTE-EMC.com



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

Certification Services for All Types of Electrical Products
Engineering, Testing, and Technical Services

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

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

F2 LABS

www.f2labs.com

HAEFELY
Current and voltage – our passion

axos⁸



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

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

emc-sales@haefely.com



IN COMPLIANCE

The Premium Digital Edition

Whether you read In Compliance Magazine in print or online, we are committed to providing you with the best reading experience possible.


Our digital edition presents a responsive, interactive, and user-friendly version of the magazine on any device.

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

StaticStop
by SelectTech

The Static Control Flooring Experts

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



www.staticstop.com
877-738-4537

UEMC

MRI / CT / X-Ray
POWER FILTER SOLUTIONS

WE'RE HIRING NOW
SALES DIRECTOR

Medical Filter **MADE IN USA** **SCIF Filter** **EMI Filter**



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

SHIELDING TO PREVENT RADIATION

Part 1: Uniform Plane Wave Reflection and Transmission at a Normal Boundary

By Bogdan Adamczyk

This is the first of seven articles devoted to the topic of shielding to prevent electromagnetic wave radiation. The shielding theory is based on the accepted theory originally presented in [1] and embraced by many EMC experts [2,3,4]. The results presented here are valid under the assumption of a uniform plane wave with normal (perpendicular) incidence on a boundary between two media.

FUNDAMENTAL FRAMEWORK

Shielding theory is based on three fundamental concepts:

- reflection and transmission of electromagnetic waves at the boundaries of two media
- radiated fields of the electric and magnetic dipole antennas
- wave impedance of an electromagnetic wave

The first concept leads to the analytical formulas for the far-field shielding effectiveness of a metallic shield. When combined with the concepts of the fundamental dipole antennas and wave impedance, the far-field formulas lead to the expressions for the near-field shielding effectiveness.

UNIFORM PLANE WAVE

We will begin our shielding discussion with the concept of a uniform plane wave. This concept was presented in [5] and is briefly reviewed here. Since the uniform plane wave is an electromagnetic wave, it must satisfy Maxwell's curl equations, which for the source-free media in the time domain are given by

$$\nabla \times \mathbf{E} = -\mu \frac{\partial \mathbf{H}}{\partial t} \quad (1a)$$

Dr. Bogdan Adamczyk is professor and director of the EMC Center at Grand Valley State University (<http://www.gvsu.edu/emccenter>) where he performs EMC educational research and regularly teaches EM/EMC courses and EMC certificate courses for industry. He is an iNARTE-certified EMC Master Design Engineer. He is the author of two textbooks, "Foundations of Electromagnetic Compatibility with Practical Applications" (Wiley, 2017) and "Principles of Electromagnetic Compatibility: Laboratory Exercises and Lectures" (Wiley, 2024). He has been writing "EMC Concepts Explained" monthly since January 2017. He can be reached at adamczyk@gvsu.edu.



$$\nabla \times \mathbf{H} = \sigma \mathbf{E} + \epsilon \frac{\partial \mathbf{E}}{\partial t} \quad (1b)$$

When solving these equations, it is customary to have the \mathbf{E} field point in the positive x direction, as shown in Figure 1.

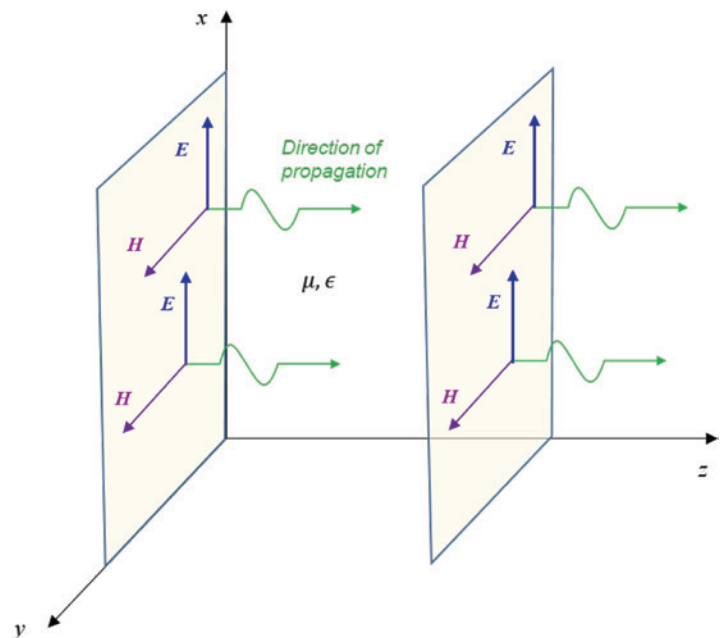


Figure 1: Uniform plane wave propagating in the +z direction

In a sinusoidal-steady state, the solution of Equations (1a) and (1b) is [6],

$$\hat{E}_x = \hat{E}_m^+ e^{-\hat{\gamma}z} + \hat{E}_m^- e^{\hat{\gamma}z} = \hat{E}_m^+ e^{-\alpha z} e^{-j\beta z} + \hat{E}_m^- e^{\alpha z} e^{j\beta z} \quad (2a)$$

$$\hat{H}_y = \frac{\hat{E}_m^+}{\eta} e^{-\hat{\gamma}z} - \frac{\hat{E}_m^-}{\eta} e^{\hat{\gamma}z} = \frac{\hat{E}_m^+}{\eta} e^{-\alpha z} e^{-j\beta z} e^{-j\theta_\eta} - \frac{\hat{E}_m^-}{\eta} e^{\alpha z} e^{j\beta z} e^{-j\theta_\eta} \quad (2b)$$

where

$$\hat{\gamma} = \sqrt{j\omega\mu(\sigma + j\omega\epsilon)} = \alpha + j\beta \quad (3)$$

is the *propagation constant* and

$$\hat{\eta} = \sqrt{\frac{j\omega\mu}{\sigma + j\omega\epsilon}} = \eta e^{j\theta_\eta} \quad (4)$$

is the complex *intrinsic impedance of the medium*.

The solution in Equations (2a) and (2b) consists of the superposition of the forward and backward propagating waves.

REFLECTION AND TRANSMISSION AT A NORMAL BOUNDARY

In the next article, we will discuss the electromagnetic wave shielding in the far field. To derive the equations describing this phenomenon, we need to understand the reflection and transmission of electromagnetic waves at the boundaries of two media. We will consider a normal incidence of a uniform plane wave on the boundary between two media, as shown in Figure 2.

When the wave encounters the boundary between two media, a reflected and transmitted wave is created [2,7]. The *incident wave* is described by

$$\hat{E}_i = \hat{E}_i e^{-\hat{\gamma}_1 z} \mathbf{a}_x = \hat{E}_i e^{-\alpha_1 z} e^{-j\beta_1 z} \mathbf{a}_x \quad (5a)$$

$$\hat{H}_i = \frac{\hat{E}_i}{\hat{\eta}_1} e^{-\hat{\gamma}_1 z} \mathbf{a}_y = \frac{\hat{E}_i}{\eta_1} e^{-\alpha_1 z} e^{-j\beta_1 z} e^{-j\theta_{\eta_1}} \mathbf{a}_y \quad (5b)$$

while the *reflected wave* is expressed as

$$\hat{E}_r = \hat{E}_r e^{\hat{\gamma}_1 z} \mathbf{a}_x = \hat{E}_r e^{\alpha_1 z} e^{j\beta_1 z} \mathbf{a}_x \quad (6a)$$

$$\hat{H}_r = -\frac{\hat{E}_r}{\hat{\eta}_1} e^{\hat{\gamma}_1 z} \mathbf{a}_y = -\frac{\hat{E}_r}{\eta_1} e^{\alpha_1 z} e^{j\beta_1 z} e^{-j\theta_{\eta_1}} \mathbf{a}_y \quad (6b)$$

where the propagation constant and the intrinsic impedance in medium 1 are given by

$$\hat{\gamma}_1 = \sqrt{j\omega\mu_1(\sigma_1 + j\omega\epsilon_1)} = \alpha_1 + j\beta_1 \quad (7)$$

$$\hat{\eta}_1 = \sqrt{\frac{j\omega\mu_1}{\sigma_1 + j\omega\epsilon_1}} = \eta_1 e^{j\theta_{\eta_1}} \quad (8)$$

The *transmitted wave* is represented as

$$\hat{E}_t = \hat{E}_t e^{-\hat{\gamma}_2 z} \mathbf{a}_x = \hat{E}_t e^{-\alpha_2 z} e^{-j\beta_2 z} \mathbf{a}_x \quad (9a)$$

$$\hat{H}_t = \frac{\hat{E}_t}{\hat{\eta}_2} e^{-\hat{\gamma}_2 z} \mathbf{a}_y = \frac{\hat{E}_t}{\eta_2} e^{-\alpha_2 z} e^{-j\beta_2 z} e^{-j\theta_{\eta_2}} \mathbf{a}_y \quad (9b)$$

where the propagation constant and the intrinsic impedance in medium two are given by

$$\hat{\gamma}_2 = \sqrt{j\omega\mu_2(\sigma_2 + j\omega\epsilon_2)} = \alpha_2 + j\beta_2 \quad (10)$$

$$\hat{\eta}_2 = \sqrt{\frac{j\omega\mu_2}{\sigma_2 + j\omega\epsilon_2}} = \eta_2 e^{j\theta_{\eta_2}} \quad (11)$$

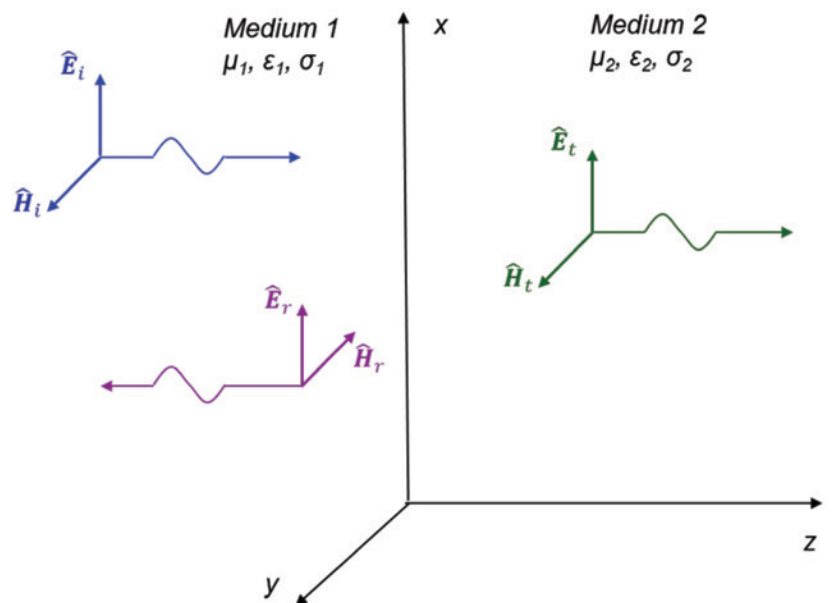


Figure 2: Reflection and transmission of a uniform wave at the boundary between two media

At the boundary of the two media, the tangential component of the electric field intensity is continuous [6]. Thus,

$$\hat{E}_i + \hat{E}_r = \hat{E}_t \quad z = 0 \quad (12)$$

or

$$\hat{E}_i e^{-\hat{\gamma}_1 z} + \hat{E}_r e^{\hat{\gamma}_1 z} = \hat{E}_t e^{-\hat{\gamma}_2 z} \quad z = 0 \quad (13)$$

leading to

$$\hat{E}_i + \hat{E}_r = \hat{E}_t \quad (14)$$

The boundary condition imposed on the magnetic field (when the boundary is free of current density) requires that the tangential component of the magnetic field intensity must be continuous. Thus,

$$\hat{H}_i + \hat{H}_r = \hat{H}_t \quad z = 0 \quad (15)$$

or

$$\frac{\hat{E}_i}{\hat{\eta}_1} e^{-\hat{\gamma}_1 z} - \frac{\hat{E}_r}{\hat{\eta}_1} e^{\hat{\gamma}_1 z} = \frac{\hat{E}_t}{\hat{\eta}_2} e^{-\hat{\gamma}_2 z} \quad z = 0 \quad (16)$$

leading to

$$\frac{\hat{E}_i}{\hat{\eta}_1} - \frac{\hat{E}_r}{\hat{\eta}_1} = \frac{\hat{E}_t}{\hat{\eta}_2} \quad (17)$$

Substituting Eq. (14) into Eq. (17) results in

$$\frac{\hat{E}_i}{\hat{\eta}_1} - \frac{\hat{E}_r}{\hat{\eta}_1} = \frac{\hat{E}_i + \hat{E}_r}{\hat{\eta}_2} \quad (18)$$

or

$$\frac{\hat{E}_i}{\hat{\eta}_1} - \frac{\hat{E}_r}{\hat{\eta}_1} = \frac{\hat{E}_i}{\hat{\eta}_2} + \frac{\hat{E}_r}{\hat{\eta}_2} \quad (19)$$

or

$$\frac{\hat{E}_i}{\hat{\eta}_1} - \frac{\hat{E}_i}{\hat{\eta}_2} = \frac{\hat{E}_r}{\hat{\eta}_1} + \frac{\hat{E}_r}{\hat{\eta}_2} \quad (20)$$

or

$$\hat{E}_i \left(\frac{1}{\hat{\eta}_1} - \frac{1}{\hat{\eta}_2} \right) = \hat{E}_r \left(\frac{1}{\hat{\eta}_1} + \frac{1}{\hat{\eta}_2} \right) \quad (21)$$

or

$$\hat{E}_i \left(\frac{\hat{\eta}_2 - \hat{\eta}_1}{\hat{\eta}_1 \hat{\eta}_2} \right) = \hat{E}_r \left(\frac{\hat{\eta}_2 + \hat{\eta}_1}{\hat{\eta}_1 \hat{\eta}_2} \right) \quad (22)$$

Leading to the definition of the *reflection coefficient* at the boundary as

$$\hat{\Gamma} = \Gamma \angle \theta_{\Gamma} = \frac{\hat{E}_r}{\hat{E}_i} = \frac{\hat{\eta}_2 - \hat{\eta}_1}{\hat{\eta}_2 + \hat{\eta}_1} \quad (23)$$

Thus the reflected wave is related to the incident wave by

$$\hat{E}_r = \hat{\Gamma} \hat{E}_i \quad (24)$$

From Eq. (14) we get

$$\hat{E}_r = \hat{E}_t - \hat{E}_i \quad (25)$$

Substituting Eq. (25) into Eq. (17) results in

$$\frac{\hat{E}_i}{\hat{\eta}_1} - \frac{\hat{E}_t - \hat{E}_i}{\hat{\eta}_1} = \frac{\hat{E}_t}{\hat{\eta}_2} \quad (26)$$

or

$$\frac{\hat{E}_i}{\hat{\eta}_1} - \frac{\hat{E}_t}{\hat{\eta}_1} + \frac{\hat{E}_i}{\hat{\eta}_1} = \frac{\hat{E}_t}{\hat{\eta}_2} \quad (27)$$

or

$$\frac{\hat{E}_i}{\hat{\eta}_1} + \frac{\hat{E}_i}{\hat{\eta}_1} = \frac{\hat{E}_t}{\hat{\eta}_2} + \frac{\hat{E}_t}{\hat{\eta}_1} \quad (28)$$

or

$$\hat{E}_i \left(\frac{1}{\hat{\eta}_1} + \frac{1}{\hat{\eta}_1} \right) = \hat{E}_t \left(\frac{1}{\hat{\eta}_2} + \frac{1}{\hat{\eta}_1} \right) \quad (29)$$

or


$$\hat{E}_i \left(\frac{2}{\hat{\eta}_1} \right) = \hat{E}_t \left(\frac{\hat{\eta}_1 + \hat{\eta}_2}{\hat{\eta}_1 \hat{\eta}_2} \right) \quad (30)$$

Leading to the definition of the *transmission coefficient* at the boundary as

$$\hat{T} = T \angle \theta_T = \frac{\hat{E}_t}{\hat{E}_i} = \frac{2\hat{\eta}_2}{\hat{\eta}_2 + \hat{\eta}_1} \quad (31)$$

Thus the transmitted wave is related to the incident wave by

$$\hat{E}_r = \hat{T} \hat{E}_i \quad (32)$$

The next article in the series will use the results presented here to discuss the uniform plane wave incidence on a solid conducting shield in the far field. 

REFERENCES

1. Sergei Alexander Schelkunoff, *Electromagnetic Waves*, D. van Nostrand Company Inc., 1943
2. Clayton R. Paul, *Introduction to Electromagnetic Compatibility*, Wiley, 2006.
3. Henry W. Ott, *Electromagnetic Compatibility Engineering*, Wiley, 2009.
4. Todd H. Hubing, et al., *Analysis and Comparison of Plane Wave Shielding Effectiveness Decompositions*, IEEE Transactions on Electromagnetic Compatibility, Vol. 56, No. 6, December 2014.
5. Bogdan Adamczyk, "Skin Depth in Good Conductors," *In Compliance Magazine*, February 2020.
6. Bogdan Adamczyk, *Foundations of Electromagnetic Compatibility with Practical Applications*, Wiley, 2017.
7. Bogdan Adamczyk, *Principles of Electromagnetic Compatibility – Laboratory Exercises and Lectures*, Wiley, 2023.



**2025 IEEE INTERNATIONAL SYMPOSIUM
ON ELECTROMAGNETIC COMPATIBILITY,
SIGNAL & POWER INTEGRITY**



REGISTER BY JULY 18 FOR EARLY DISCOUNTS!

PARTICIPATE IN 200+ TECHNICAL SESSIONS,
Workshops & Tutorials, Hands on Experiments & Demonstrations, and Special Sessions with the world's leading engineers in EMC and SIPI.

PARTICIPATE IN LIVE DEMONSTRATIONS
presented by industry experts to learn how to solve real-world problems.

LEARN ABOUT THE LATEST GLOBAL STANDARDS
in EMC and SIPI, hear updates, ask questions, and attend Working Group Meetings as part of the "Standards Week" special track.

ATTEND THE "ASK THE EXPERTS" PANELS
Bring your questions or simply listen and learn from the experts!

ENHANCE YOUR KNOWLEDGE OF EMC AND SIPI
during the educational courses for Clayton R. Paul Global University and Global SIPI University

BRING THE FAMILY
and Experience Raleigh, North Carolina in the beautiful, "City of Oaks". Companions are invited to join the Social Events and fun area tours.

NETWORK WITH FRIENDS AND COLLEAGUES
during the Welcome Reception, the Gala Dinner, Young Professionals, and Women in Engineering events.







#IEEE_ESP25





IEEE



EMC SOCIETY

www.emc2025.org

WHY ESD ELECTRONIC DESIGN AUTOMATION CHECKS ARE SO CRITICAL: PART 2

On behalf of EOS/ESDA Association, Inc.

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

A new version of Technical Report TR18.0-01-25 (TR18) on ESD Electronic Design Automation (EDA) Checks by the ESD Association's Working Group 18 is about to be released. This article, divided into Part 1 and Part 2, provides guidelines for the EDA industry and the ESD design community for establishing a comprehensive ESD verification flow to address the ESD design challenges of modern ICs. Part 1 covered the concept of ESD checks throughout the IC Design Flow, including Schematic-based and Layout-based ESD checks. Part 2 covers Package-level and System-level checks, ESD Circuit simulation, and ESD TCAD simulation, completing the coverage of all ESD EDA checks described in the Technical Report.

PACKAGE-LEVEL ESD CHECKS

The increasing complexity of IC packaging, especially with advanced process nodes and multi-die (chiplet) System-in-Package (SiP) configurations, necessitates comprehensive ESD verification at the package level. The physical and electrical properties of an IC package significantly influence the ESD protection network's response. This complexity is further amplified in 2.5D and 3D IC flows, where multiple dies are integrated into a single package, each with unique ESD risks and target levels.

To ensure that the designed protection levels are maintained across all package options, the current state of package-level ESD verification involves several critical steps: extracting metadata of die pads and package pins, setting up EDA tools, defining ESD targets for each signal IO and supply pin, applying appropriate ESD rules on design, and verifying the integrity of the overall ESD protection network considering the additional RLC paths introduced by the package.

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



Advanced packaging technologies, such as 2.5D and 3D integrations, introduce additional challenges like differentiation between internal (die-to-die) and external IOs, the huge number of die-to-die IOs to check, integration of chiplets from different process technologies/foundries, use of SI-interposers and TSVs, and ESD risk associated with the final assembled package and the assembly process itself.

SYSTEM-LEVEL ESD CHECKS

System-level checks are an important component of the full spectrum of ESD checks. These checks can be done with SPICE-like simulators via SEED (System Efficient ESD Design), full-wave analysis software, or near-field analysis techniques.

If a failure occurs during a PCB-level ESD qualification, the following analysis methods can be used to diagnose the root cause: perform SEED analysis of the PCB path containing the failed IC component, perform scanning analysis by applying near-field electromagnetic interference pulses to failing areas of the PCB topology, or execute a full wave analysis on the failing PCB to identify the failing topology.

ESD CIRCUIT SIMULATION (SPICE)

Circuit simulation is invaluable for the design of ESD protection networks, prediction of ESD robustness, and debugging of ESD failures. Circuit simulation requires proper configuration of the ESD source, ESD protection device, and ESD path as the simulation test bench.

An HBM ESD source is typically modeled as an equivalent lumped circuit to produce the exponentially decaying current pulse (Figure 1a). A CDM ESD source can be similarly represented, or by an array of capacitors attached to the IC in a distributed manner to model the field coupling from the CDM tester (Figure 1b). A behavioral approach is also applicable, such as using a damped sinusoidal wave to simulate CDM current pulse.


An ESD event is most comprehensively simulated through whole-chip transient simulation with nonlinear ESD device models. However, such simulation is traditionally resource-intensive and time-consuming. Simplifications can be made to improve simulation efficiency, with trade-offs in accuracy.

ESD TCAD SIMULATION

Technology Computer-Aided Design (TCAD) represents a holistic approach that comprehends physical device structure, fabrication process simulation, and semiconductor physics models. TCAD can predict parameters of ESD devices, simulate device behavior within ESD protection circuits, and develop rules for automatic design checkers.

TCAD applications are effective at the technology and ESD IP development stages. One of the most important representations of a TCAD approach for EDA is mixed-mode simulation, which extends transient simulations' capabilities from a single device structure to several devices within small circuits (Figure 2).

CONCLUSIONS

ESD EDA verification is a complex task. IC companies use different ESD protection approaches, design flows, and verification tools. The Technical Report introduces several generic rules that can be used as the basis for a typical ESD EDA verification flow. As more ESD EDA tools become more mature and commercially available, there will be further opportunities for standardizing ESD EDA verification approaches and specific ESD checks. 

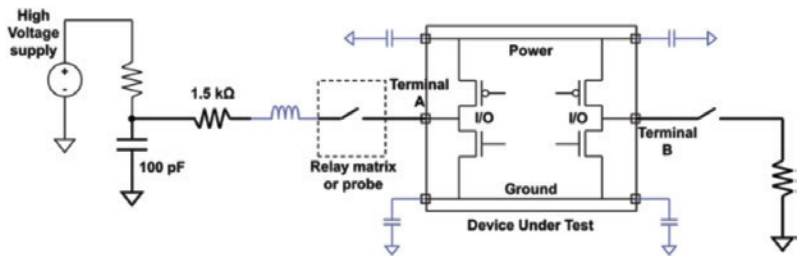


Figure 1a: HBM ESD simulation test-bench

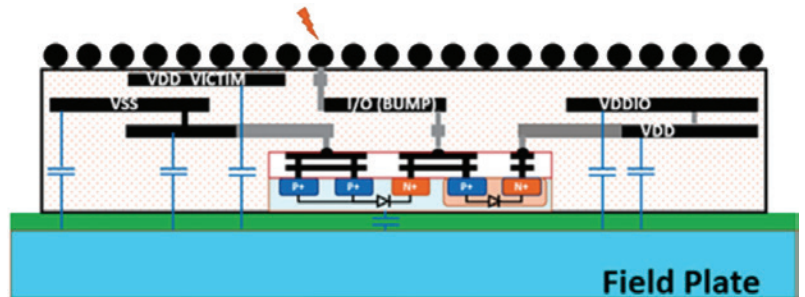


Figure 1b: CDM ESD simulation test-bench

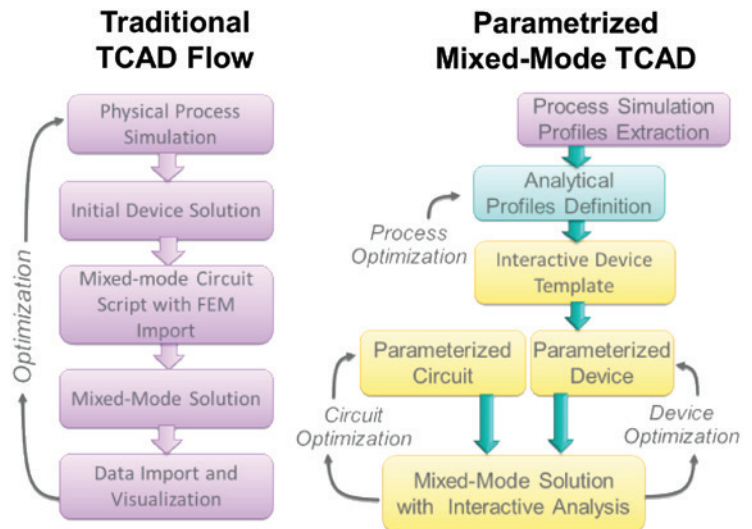


Figure 2: Comparison of conventional and parameterized mixed-mode simulation flows.

Upcoming Events

June 3-6

WPTCE 2025 IEEE Wireless Power
Technology Conference and Expo

June 15-20

- ★ IMS 2025 – IEEE International Microwave Symposium

June 26

Cybersecurity Maturity Model Certification
for Federal Government Procurements

July 13-18

2025 IEEE International Symposium on
Antennas and Propagation & ITNC-USNC-
URSI Radio Science Meeting

July 31

Internet of Things: Testing and Protections
for Devices and Systems

August 18-22

- ★ 2025 IEEE International Symposium on
Electromagnetic Compatibility, Signal &
Power Integrity (EMC + SIPI)

August 28

Radio Regulations for Module Integrators

September 1-5

EMC Europe

September 13-18

- ★ 47th Annual Electrical Overstress/
Electrostatic Discharge Symposium

September 21-26

European Microwave Week 2025

September 25

- ★ 2025 Minnesota EMC Event

★ Visit In Compliance's booth at these events!

Advertiser Index

A.H. Systems, Inc. Cover 2

Absolute EMC 43

AR/RF Microwave Instrumentation 3

Coilcraft 21

E. D. & D., Inc. 7

Element Materials Technology 25

ETS-Lindgren Cover 4

Exodus Advanced Communications 33

F2 Labs 43

Haefely AG 43

HV TECHNOLOGIES, Inc. 41

IEEE EMC+SIPI 2025 47

Maury Microwave 39

Ophir RF Cover 3

SelecTech, Inc. 43

Suzhou 3ctest Electronic Co. Ltd. 31

UEMC Inc. 43

Washington Laboratories, Ltd. 27

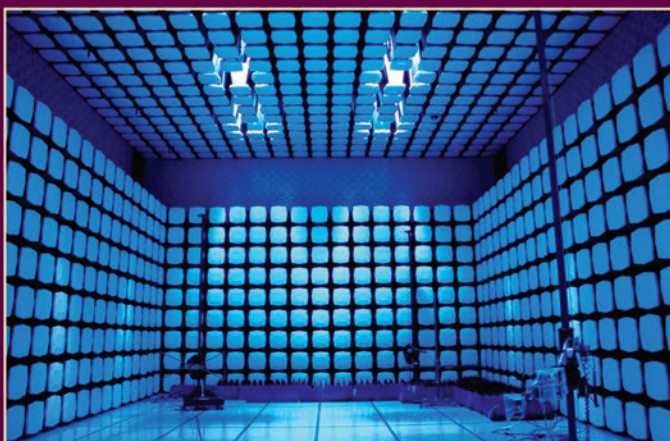
Is it time to renew your
subscription to *In Compliance*?
Never miss an issue, renew now.

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

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

OPHIR^{RF}

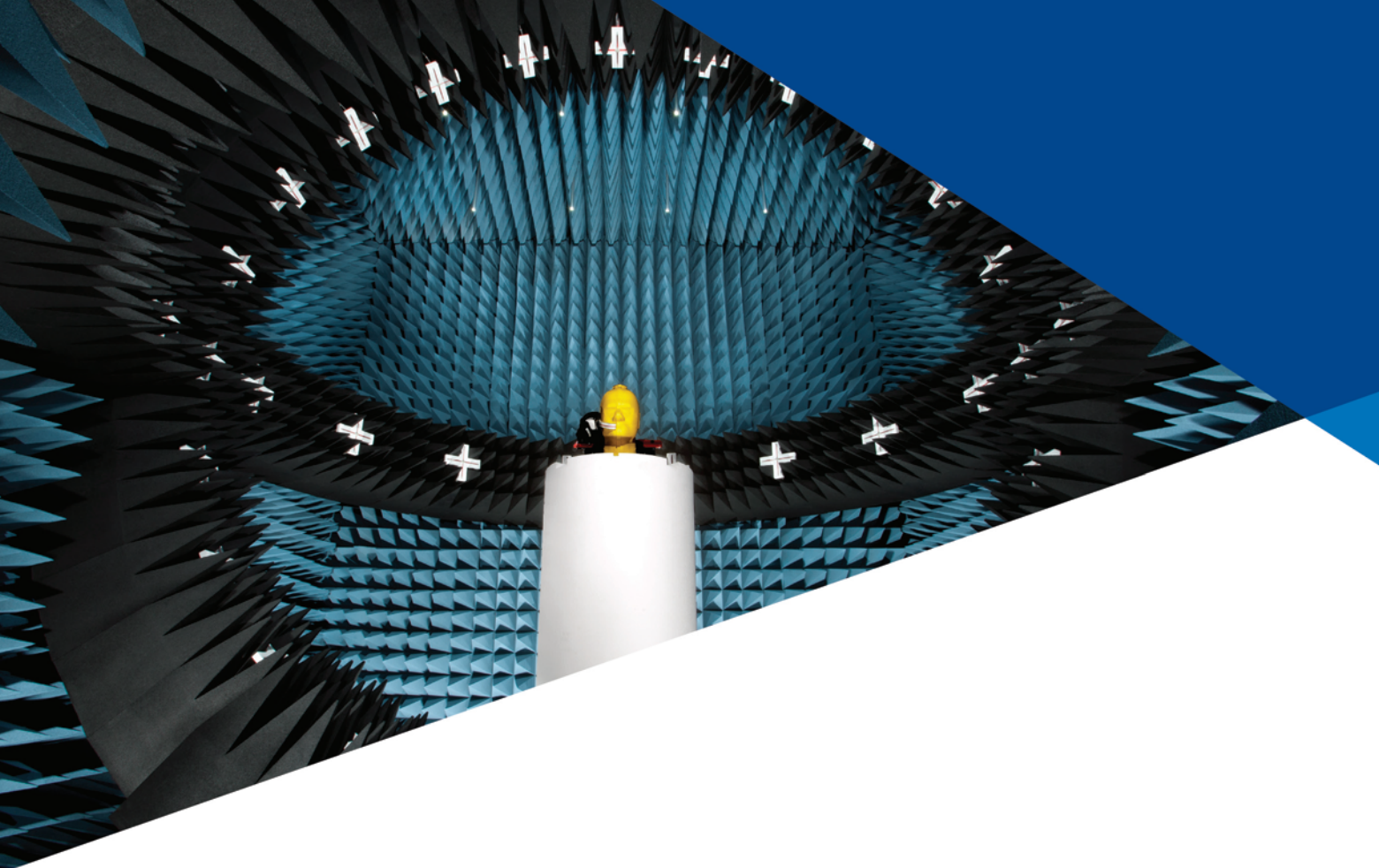
HIGH POWER RF SYSTEMS



LOS ANGELES

Since 1992

www.OphirRF.com



MEET WIRELESS TESTING CHALLENGES WITH CONFIDENCE.

Wireless technologies are here and this reality has challenged EMC test systems to push the limits of measurements up to 200 and 300 GHz. ETS-Lindgren, an expert in both the EMC and Wireless testing methodologies, understands the new demands of Wireless technologies and how the traditional EMC test methods and procedures are breaking down as the measurements push into the mmWave spectrum and beyond.

ETS-Lindgren is the global leader in Wireless and OTA measurement solutions, trusted for over 50,000 test and measurement projects worldwide. As the builder of the world's largest anechoic chamber and the provider for 80% of CTIA Authorized Test Labs (CATLs), ETS-Lindgren offers unmatched expertise in addressing the challenges of modern Wireless technologies — including WiFi 7. We remain *Committed to a Smarter, More Connected Future*.

For more information on our Wireless Solutions or to register for one of our on-demand Wireless webinars, visit our website at www.ets-lindgren.com or contact your local ETS-Lindgren office or representative.

Connect with us at:



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

ETS·LINDGREN[®]
An ESCO Technologies Company

Offices Worldwide | ets-lindgren.com

6/25 RR © 2025 ETS-Lindgren v1.0