

FEBRUARY 2024

IN COMPLIANCE™

THE COMPLIANCE INFORMATION RESOURCE FOR ELECTRICAL ENGINEERS

Electronic Warfare and

Cyber Defense of Satellites

PLUS

Energy-Related Products
and Resource Efficiency
Requirements

Electric Shock Stimulation
for Complex Leakage Current
Waveforms

Creating an Effective and
Defensible Product Recall

All you need in one small package

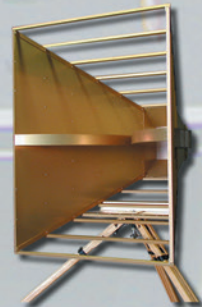


Antennas | Probes | Accessories | Preamplifiers | Low-Loss Cables | Recalibration Services



Travel Made Easy

with Next-Day,
On-Time
Delivery



Don't Leave home without it. A.H. Systems provides many models of Portable Antenna Kits, each containing all the necessary Antennas, Current Probes, and Cables to satisfy numerous customer requirements. Excellent performance, portability (compact size and lightweight), along with ease of setup make all of the Antenna Kits your choice for indoor or field testing. Loss and breakage are virtually eliminated as each component has a specific storage compartment within the case. All Antenna Kits are accompanied with a Tripod and Azimuth & Elevation Head, both contained in a

ANTENNAS... Tripod Carrying Case...and dont forget your keys! **and KITS TOO...**



Innovation

Quality

Performance

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

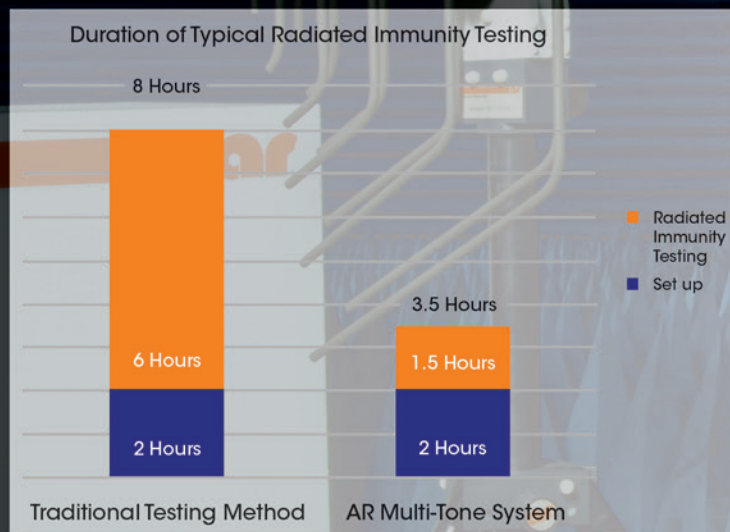
A.H. Systems



This is How You Reduce Testing Time by **More Than 50%**

With regulatory adoption of multiple signal radiated immunity test methods (IEC-61000-4-3:2020, 4th edition), AR's Multi-Tone System enables you to vastly reduce your test times in accordance with automotive, commercial, and aviation EMC RI standards. Included is AR's proprietary emcware® software, offering users numerous test and calibration routines utilizing multiple signal methodology, to meet these standards.

For example, AR's Multi-Tone System can reduce the typical time to run traditional tests such as IEC 61000-4-3, ISO 11451, and ISO 11452, by over 50%. In the event of an EUT failure, margin investigation and traditional single tone testing is easily performed through AR's emcware® software.



Multiple full sweeps are often required during mitigation efforts, which is where the multiple signal approach will pay dividends.

This is a creative way to help your company be more profitable by using your assets more efficiently.

Visit us at www.arworld.us or call 215-723-8181. Talk to an applications engineer at 800.933.8181.



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

**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** Bruce Archambeault
bruce@brucearch.com
Ken Javor
ken.javor@emcompliance.com

Keith Armstrong
keith.armstrong@cherryclough.com
Ken Ross
kenrossesq@gmail.com

Leonard Eisner
Leo@EisnerSafety.com
Werner Schaefer
wernerschaefer@comcast.net

Daryl Gerke
dgerke@emiguru.com

**columns
contributors** EMC Concepts Explained
Bogdan Adamczyk
adamczyk@gvsu.edu
Hot Topics in ESD
EOS/ESD Association, Inc
info@esda.org

On Your Mark
Erin Earley
earley@clarionsafety.com
Troubleshooting EMI Like a Pro
Min Zhang
info@mach1desgin.co.uk

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 \$129 for 12 issues. The digital edition is free. Please contact our circulation department at circulation@incompliancemag.com



WHY CAPACITANCE? BENEFITS & APPLICATIONS OF DIGITAL CAPACITIVE SOLUTIONS

application note provided by

VITREK



MAGNETIC FIELD CONVERSIONS

conversion chart provided by



SHIELDING SOLUTIONS FOR eSIMs IN DIGITAL FORENSICS

white paper provided by



A DASH OF MAXWELL'S: A MAXWELL'S EQUATIONS PRIMER PART ONE

primer provided by

IN COMPLIANCE



A DASH OF MAXWELL'S: A MAXWELL'S EQUATIONS PRIMER PART TWO

primer provided by

IN COMPLIANCE

8 ELECTRONIC WARFARE AND CYBER DEFENSE OF SATELLITES

By Jeff Viel

With the increasing sophistication of electronic warfare and cyberattacks, it is critical to develop and implement effective cyber defense strategies to ensure the integrity and effectiveness of satellite systems. This article will explore the various test methods and techniques that will be used to protect satellites from electronic warfare and cyberattacks.



18 Energy-Related Products and Resource Efficiency Requirements

By Alex Martin

This article reflects on the recent drafting of a European circular product standard, the publication of EN4555X material efficiency standards, and some specific international and national standards. This standardization activity is spearheading thinking on resource efficiency, and the requirements of these standards could soon find their way into future EU ecodesign laws.



24 Electric Shock Stimulation for Complex Leakage Current Waveforms

By Hai Jiang and Paul Brazis

Leakage or touch current tests for electrical shock protection is mandated by safety standards in the process of issuing a safety certification for various electrical products. In this article, electrical shock sensation experiments were conducted for a complex waveform composed of a combination of 60 Hz and a higher frequency sinusoidal signal.



32 Creating an Effective and Defensible Product Recall

By Kenneth Ross

Recalls can create huge problems for manufacturers and product sellers. They can generate new product liability lawsuits that are harder to defend, involve a significant financial cost to implement, and create reputational problems with consumers and retailers. Manufacturers must carefully design a recall or other corrective action that is as effective as possible and adequate under the circumstances. Various government entities are issuing new requirements that can help with these efforts.



6 Compliance News

42 Hot Topics in ESD

50 Advertiser Index

38 EMC Concepts Explained

46 Troubleshooting EMI Like A Pro

50 Upcoming Events

41 Product Showcase

48 Banana Skins

FCC Proposes That All Mobile Phones Be Hearing-Aid Compatible

The U.S. Federal Communications Commission (FCC) has taken another step forward to ensure access to vital communications technology and services for those with hearing impairments or hearing loss.

In a Notice of Proposed Rulemaking (NPRM), the FCC has proposed that 100% of all wireless handsets, including mobile phones and smartphones, be fully hearing-aid compatible (HAC) by mid-2027. Under the NPRM, handset manufacturers would have a 24-month transition period to achieve this goal. Nationwide service providers would have 30 months

to reach 100% HAC, while non-nationwide service providers would have 42 months.

To help facilitate efforts to achieve this goal, the Commission is also seeking comments on broadening the scope of HAC-enabling technologies to include the use of Bluetooth connectivity options.

The FCC says that its proposed rulemaking is based on recommendations from its Hearing Aid Compatibility Task Force, which consists of regulators, accessibility advocates, device manufacturers, and wireless service providers.

FCC Proposes \$1.2 Million Fine for Marketing of Noncompliant Radio Devices

In another example of its stepped-up enforcement efforts, the U.S. Federal Communications Commission (FCC) has cited a New York City-based technology retailer for marketing unapproved radio frequency (RF) devices.

According to a Notice of Apparent Liability for Forfeiture issued by the Commission, Sound Around, an online seller

of audio and video electronics and accessories, marketed 33 unauthorized, non-compliant radio frequency devices through its website. The company also reportedly failed to comply with repeated requests from the FCC's Enforcement Bureau to cease its marketing of the non-compliant devices, dating as far back as 2011, and provided incomplete responses

to multiple inquiries from the Bureau, thereby obstructing its investigation into the violations.

Accordingly, the FCC has proposed a financial penalty of \$1,202,454 against Sound Around, an amount which the FCC says reflects the company's willful and ongoing disregard of FCC rules.

EU Commission Proposes "One Substance, One Assessment" Strategy for Chemical Assessments

The Commission of the European Union (EU) has recently adopted three separate legislative proposals in an effort to streamline the assessment of chemicals to be marketed or sold in the EU.

According to a press release, the Commission's "one substance, one assessment" package includes the following legislative proposals:

- A proposal for a Regulation establishing a common data platform on chemicals;
- A proposal for a Regulation on the reattribution of scientific and technical tasks and improving cooperation among Union agencies in the area of chemicals; and

- A proposal for a Directive on the reattribution of scientific and technical tasks to the European Chemical Agency (ECHA).

The Commission believes that adopting this "one substance, one assessment" approach will streamline the assessment of chemicals across the EU, strengthen the knowledge base of chemicals, and ensure early detection and action on emerging chemical risks.

The Commission's proposals will now undergo the standard EU legislative procedure in which both the EU Parliament and Council discuss the proposals and jointly agree on a common text before final adoption.

Is it time to renew your subscription?
Don't miss an issue!
Renew today.



Did you borrow this issue of *In Compliance*?
Get your own free subscription!



FCC Issues Annual Report on Robocalls

The U.S. Federal Communications Commission (FCC) has released its annual report to Congress detailing consumer complaints and enforcement action in connection with illegal robocalls.

The report offers insight into trends related to informal consumer complaints regarding robocalls that were received by the Commission over five full calendar years, from 2018-2022, as well as complaint data and information about enforcement actions through November 2023.

Over the nearly six-year period covered in this report, the FCC received a total of 1,341,635 informal consumer complaints under four different provisions of the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act). The largest number of complaints filed (312,225, or 42%) were for violations of the FCC's restrictions on sales calls made to residential telephone numbers (section 227(c)), while an additional 289,061 (21.5%) were filed for

providing misleading or inaccurate caller identification information (section 227(e)).

The report also indicates that the FCC's stepped-up enforcement efforts over the past several years are having a positive impact in reducing the number of informal consumer complaints. After a record 333,146 informal complaints filed in 2018, annual informal complaint numbers have generally seen marked declines, with just 169,465 informal complaints filed in 2022, and only 125,586 complaints filed in 2023 through the end of November.

As evidence of those stepped-up enforcement efforts, the FCC's report provides details on three separate Notices of Apparent Liability for Forfeiture issued in 2022, with total proposed fines of over \$461 million. Two of those cases resulted in Forfeiture Orders issued by the Commission in 2023, amounting to more than \$416 million in penalties.

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



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

Call Us Today!
 USA/Canada Toll Free:
800.806.6236
 International:
+1.919.469.9434
 Website:
www.ProductSafeT.com
 Research Triangle Park • North Carolina • USA



Force Gauges

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

Finger Probes



Impact Hammers



JET-01 & JET-02
Jet Nozzles



WTR01 Water Tank & Pump System



ELECTRONIC WARFARE AND CYBER DEFENSE OF SATELLITES

Strategies and Test Methods for Protecting Satellites From Cyberattacks



Jeffrey Viel is the Chief Engineer of Electromagnetic Environmental Effects (E3) for NTS Technical Systems, with over 30 years of EMI/EMC/E3 test, analysis, and design experience in the aerospace, defense, and telecommunications industries. He can be reached at jeffrey.viel@nts.com.



By Jeff Viel

In today's world, satellites play a critical role in providing communication, navigation, and surveillance services to the defense and aerospace industries. However, with the increasing sophistication of electronic warfare and cyberattacks, these satellites have become vulnerable to a wide range of threats. Therefore, to ensure the integrity and effectiveness of satellite systems, it is essential to develop and implement effective electronic warfare and cyber defense strategies.

This article explores the various test methods and techniques used to protect satellites from electronic warfare and cyberattacks. We will discuss the types of threats that satellites face and the challenges associated with testing for electronic warfare and cyber defense. We will also provide case studies of successful testing and protection of satellites against such attacks. Finally, we will explore future developments and research directions in this field.

With this article, we intend to provide a comprehensive analysis of the present circumstances of electronic warfare and cyber defense testing for satellites. Our goal is to help those in the defense and aerospace industries better understand the risks associated with satellite systems and the best practices for protecting them from electronic warfare and cyberattacks.

THE IMPORTANCE OF PROTECTING SATELLITES FROM ELECTRONIC WARFARE AND CYBERATTACKS

Satellites play a vital role in the functioning of our modern world. They facilitate communication, navigation, and reconnaissance services to the defense and aerospace industries. However, with the increasing threat of electronic warfare and cyberattacks, these satellites have become vulnerable to various types of risks.

Electronic warfare threats can be classified as electromagnetic, cyber, or physical attacks that exploit vulnerabilities in satellite systems. These threats can interfere with satellite signals, disrupt communication links, and even cause permanent damage to the satellite. Similarly, cyber threats can exploit vulnerabilities in satellite software and control systems, causing information loss, system malfunction, or unauthorized access.

The consequences of a successful attack on a satellite system can be disastrous, not only for the defense and aerospace industries but also for society as a whole. Therefore, protecting satellites from electronic warfare and cyberattacks is critical. Testing and analysis are necessary to identify vulnerabilities and develop effective countermeasures.

The protection of satellites from electronic warfare and cyberattacks is essential for maintaining the integrity and reliability of satellite systems. As threats continue to evolve and become more sophisticated, it is vital to implement robust and effective protection strategies.

ELECTRONIC WARFARE THREATS TO SATELLITES: AN OVERVIEW OF THE VARIOUS ATTACK TYPES

Electronic warfare (EW) threats can pose a significant risk to satellites. Here's an overview of the different types of attacks:

- *Electromagnetic (EM) attacks*: EM attacks involve the use of high-powered radio waves to disrupt or disable satellite communication links. The attacker can use various methods, such as jamming or spoofing, to interfere with the satellite's signals and cause communication disruption.
- *Direct energy weapons (DEWs)*: DEWs are high-powered energy beams that can damage or destroy a satellite's physical components. The attacker can use



It's essential to identify and understand these different types of electronic warfare attacks to develop effective countermeasures and protection strategies for satellites.

a variety of energy sources, including lasers, particle beams, or high-powered microwaves, to cause damage to the satellite.

- *Kinetic energy weapons (KEWs):* KEWs involve the use of physical objects, such as missiles or projectiles, to destroy or disable a satellite. The attacker can use this method to create debris or destroy the satellite altogether.
- *Cyberattacks:* Cyberattacks can target the satellite's software or control systems, causing system malfunction, information loss, or unauthorized access. The attacker can exploit vulnerabilities in the software or the control systems to gain access and manipulate the satellite's functions.

It's essential to identify and understand these different types of EW attacks to develop effective countermeasures and protection strategies for satellites. Testing and analysis are necessary to simulate these threats and evaluate the resilience of satellite systems against such attacks.

CYBER THREATS TO SATELLITES: AN OVERVIEW OF DIVERSE ATTACK TYPES

Cyber threats are a significant risk to satellite systems. Here's an overview of several cyberattack methods:

- *Malware attacks:* Malware attacks involve the injection of malicious code into the satellite's software or control systems, causing system malfunction, information loss, or unauthorized access. The attacker can use a variety of methods to deliver the malware, including phishing emails, infected software updates, or direct access to the satellite's control systems.
- *Denial of service (DoS) attacks:* DoS attacks involve overwhelming the satellite's communication links with fake requests or traffic, causing communication disruption. The attacker can use various methods, such as DDoS (distributed denial of service) attacks, to flood the satellite's communication channels with requests.

- *Man-in-the-middle (MitM) attacks:* MitM attacks include monitoring and controlling the satellite's communication lines allowing the attacker to eavesdrop on communication or inject malicious code. The attacker can use various methods, such as spoofing or interception, to carry out the MitM attack.
- *Physical access attacks:* Physical access attacks involve gaining unauthorized access to the satellite's hardware components, such as memory chips or processors, to steal information or manipulate the satellite's functions. The attacker can use various methods, such as side-channel attacks or hardware trojans, to gain access to the satellite's hardware.

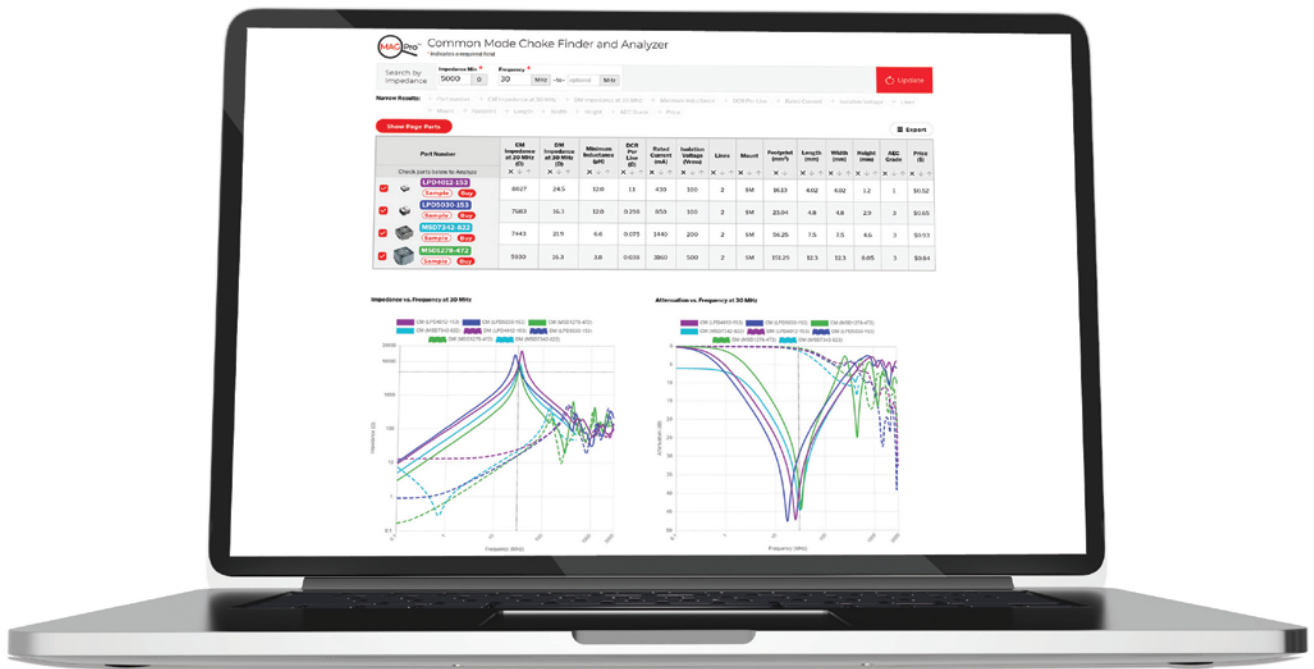
It's crucial to recognize and comprehend these various cyberattacks to create efficient defenses and protection plans for satellite systems. To model these dangers and assess the resistance of satellite systems to such attacks, testing and analysis are required.

TEST METHODS FOR ELECTRONIC WARFARE PROTECTION: AN OVERVIEW OF TESTING APPROACHES AND TECHNIQUES

Testing and analysis are necessary to ensure that satellite systems are resilient against electronic warfare (EW) attacks. Here's an overview of testing approaches and techniques for EW protection:

- *Vulnerability assessment:* Vulnerability assessment involves identifying potential vulnerabilities in satellite systems and evaluating their susceptibility to different types of EW attacks. Several techniques, including software analysis, reverse engineering, or hardware testing, can be used to conduct the assessment.
- *Simulation testing:* Simulation testing involves creating an environment that simulates various types of EW attacks to evaluate the resilience of satellite systems. The simulation can be carried out using various techniques, such as signal injection, radio frequency (RF) jamming, or spoofing.

Have you tried our **MAGPro**TM Common Mode Choke Finder?



There's nothing common about it!

Find the optimal off-the-shelf common mode chokes for your emi/rfi filter parameters.

Step 1: Search parts by your desired Impedance, Attenuation or Inductance at your operating frequency.

Step 2: View results in a sortable table with complete performance specifications. Then select parts for further analysis.

Step 3: Quickly compare impedance and attenuation vs. frequency graphs for up to six part numbers.

Step 4: Request free samples of the most interesting parts for evaluation and testing.



It's that Simple!

Try it at coilcraft.com/CMCfinder.

WWW.COILCRAFT.COM



It's essential to use a combination of testing approaches and techniques to ensure that satellite systems are resilient against electronic warfare attacks.

- *Range testing:* Range testing involves carrying out EW testing on a physical range to evaluate the effectiveness of different types of countermeasures. Several techniques can be used to conduct range testing, such as high-power RF emitters, controlled electromagnetic environments, or hardware-in-the-loop simulations.
- *Field testing:* Field testing involves carrying out EW testing on a real-world satellite system to evaluate the effectiveness of different types of countermeasures in a real-world environment. Field testing can be accomplished via an array of techniques, such as flight testing, ground testing, or environmental testing.
- *Compliance testing:* Compliance testing involves assessing the satellite's adherence to cybersecurity norms and rules, such as the NIST (National Institute of Standards and Technology) Cybersecurity Framework or the European Union's General Data Protection Regulation (GDPR). Compliance testing could be executed using a variety of techniques, such as self-assessment, independent verification, or certification audits.
- *Software testing:* Software testing involves evaluating the satellite's software code and control systems to identify vulnerabilities and weaknesses that could be exploited by cyber attackers. Software testing can be done in several ways, such as static code analysis, dynamic analysis, or fuzz testing.

It's essential to use a combination of these testing approaches and techniques to ensure that satellite systems are resilient against EW attacks. Testing and analysis can identify vulnerabilities and weaknesses in satellite systems and help develop effective countermeasures to protect against EW threats.

TEST METHODS FOR CYBER DEFENSE OF SATELLITES: AN OVERVIEW OF TESTING APPROACHES AND TECHNIQUES

Testing and analysis are necessary to ensure that satellite systems are resilient against cyber threats. Here's an overview of testing approaches and techniques for cyber defense:

- *Penetration testing:* Penetration testing includes mimicking a cyberattack to evaluate the effectiveness of the satellite's cyber defense mechanisms. The penetration test can be accomplished by a variety of means, such as vulnerability scanning, social engineering, or penetration testing tools.
- *Red teaming:* Red teaming involves creating a simulated attack scenario to evaluate the effectiveness of the satellite's cyber defense mechanisms in a real-world environment. The red teaming exercise can be executed in a variety of ways, such as scenario-based testing, cyber range simulations, or tabletop exercises.

To help ensure that satellite systems are resistant to cyberattacks, a mix of these testing methodologies and procedures must be used. Developing effective defenses against cyberattacks can be aided by testing and analysis, which can assist in pinpointing satellite systems' flaws and vulnerabilities.

CHALLENGES AND LIMITATIONS OF TESTING FOR ELECTRONIC WARFARE AND CYBER DEFENSE OF SATELLITES

Testing and analysis are essential for evaluating the resilience of satellite systems against electronic warfare (EW) and cyber threats. However, there are various challenges and limitations associated with this testing. Here's a list of some of those challenges and limitations:

- *Complexity:* Satellite systems are complex and can have multiple subsystems and components, making it challenging to test all aspects of the system. Additionally, satellite systems operate in harsh environments, such as space or high-altitude regions, making it difficult to replicate real-world conditions in a testing environment.
- *Cost:* Testing satellite systems can be expensive, especially for field testing or range testing. Additionally, it can be challenging to replicate

real-world scenarios in a testing environment, making it challenging to justify the cost of testing.

- *Security:* Testing satellite systems for EW and cyber defense can expose vulnerabilities and weaknesses in the system, making it a potential target for attackers. Therefore, testing must be carried out in a secure and controlled environment to prevent the compromise of sensitive information.
- *Limited data:* Testing satellite systems for EW and cyber defense is a relatively new field, and there is limited data available on the effectiveness of different countermeasures. Additionally, the rapid pace of technological advancements means that testing methods and countermeasures may become obsolete quickly.
- *Regulatory compliance:* Satellite systems are subject to various regulations and compliance requirements, such as export control regulations

or the International Traffic in Arms Regulations (ITAR). Testing and analysis must comply with these regulations and ensure that sensitive information is protected.

It's essential to consider these challenges and limitations when testing satellite systems for EW and cyber defense. Testing and analysis must be carried out in a secure, cost-effective, and compliant manner and must be continuously updated to keep pace with technological advancements and new threats.

FUTURE DEVELOPMENTS AND RESEARCH DIRECTIONS: INNOVATIONS IN TESTING AND PROTECTION OF SATELLITES AGAINST ELECTRONIC WARFARE AND CYBERATTACKS

As threats continue to evolve and become more sophisticated, the protection of satellites against EW threats and cyberattacks will require ongoing



Ultra-Compact AC/DC Programmable Power Supply

- Ultra Compact AC/DC Power Supply
- Up to 36 kVA in a single unit
- Mix-and-match parallel operation allows up to 144kVA.
- "R" models feature 100% Regenerative Power Capability
- Power line disturbance simulation features
- Sequence function for advanced simulation

Ultra-Compact AC/DC Programmable Power Supply

PCR-WEA/WEA2 series



The continued testing and protection of satellites against electronic warfare threats and cyberattacks are critical for maintaining the integrity and reliability of satellite systems.

innovation and research. Here are some potential future developments and research directions:

- *Artificial intelligence (AI)*: AI can help identify and respond to threats more quickly and effectively than traditional methods. AI can be used to analyze large data sets, identify patterns and anomalies, and develop predictive models for identifying potential threats.
- *Quantum key distribution (QKD)*: QKD is a technique for secure communication that uses quantum properties to transmit encryption keys. QKD could provide a more secure means of communication for satellite systems, making them less vulnerable to cyberattacks.
- *Hardware security*: Hardware security can provide a more secure means of protecting satellite systems against cyberattacks. Hardware security can involve designing hardware components that are resistant to tampering or developing techniques for detecting tampering or manipulation.
- *Threat intelligence sharing*: Threat intelligence sharing can help identify potential threats and develop effective countermeasures more quickly. Sharing threat intelligence among different organizations and agencies can help identify patterns and trends in cyberattacks and identify potential vulnerabilities in satellite systems.
- *Standardization*: Standardization can help ensure that satellite systems are designed and tested according to a common set of standards and best practices. Standardization can help identify potential vulnerabilities and develop effective countermeasures more quickly.

Thus, ongoing research and development will be essential to protecting satellite systems against EW and cyberattacks. Innovation in areas such as AI, QKD, hardware security, threat intelligence sharing, and standardization will be crucial for developing effective countermeasures against evolving threats.

THE IMPORTANCE OF CONTINUED TESTING AND PROTECTION OF SATELLITES AGAINST ELECTRONIC WARFARE AND CYBERATTACKS

The continued testing and protection of satellites against EW threats and cyberattacks are critical for maintaining the integrity and reliability of satellite systems. Here's why:

- *Protecting critical infrastructure*: Satellite systems are critical infrastructures that provide communication, navigation, and surveillance services to the defense and aerospace industries. A successful attack on satellite systems could have significant consequences for national security and public safety.
- *Evolving threats*: EW and cyber threats are evolving rapidly, with attackers developing new methods and techniques to exploit vulnerabilities in satellite systems. Continued testing and protection are necessary to keep pace with these evolving threats and to develop effective countermeasures.
- *Regulatory compliance*: Satellite systems are subject to various regulations and compliance requirements, such as export control regulations or ITAR regulations. Testing and protection must comply with these regulations and ensure that sensitive information is protected.
- *Cost-effectiveness*: Testing and protection can help identify vulnerabilities and weaknesses in satellite systems, allowing for more targeted investments in protection and countermeasures. This can result in cost savings in the long run by preventing the need for costly repairs or replacements.
- *Assurance*: Continued testing and protection can provide assurance to stakeholders, including customers, investors, and the public, that satellite systems are secure and reliable. This assurance can help maintain trust and confidence in satellite systems and the organizations that operate them.

Hence, the importance of continued testing and protection of satellite systems against EW threats and

cyberattacks cannot be overstated. Ongoing testing and protection are necessary to identify vulnerabilities, develop effective countermeasures, and maintain the integrity and reliability of satellite systems in the face of evolving threats.

ADDRESSING SATELLITE VULNERABILITIES THROUGH THE COMBINATION OF CYBER AND EW TEST METHODS

Satellite technology has revolutionized modern communication, navigation, and surveillance. However, as satellite technology continues to advance, so do the threats to their security. The growing concern about satellite vulnerabilities has been a major focus for the U.S. Department of Defense (DoD) and the broader security community.

One of the primary threats to satellite security is cyberattacks. Hackers can infiltrate satellite systems and cause disruptions or even take control of the satellite. The use of EW is also a growing concern, as adversaries can use jamming or spoofing techniques to disrupt satellite communications or navigation systems.

To mitigate the risk of satellite vulnerabilities, the DoD has recognized the need to combine cyber and EW test methods. This approach involves testing the security of satellite systems by simulating cyber and EW attacks to identify weaknesses and vulnerabilities in the system.

By combining these test methods, the DoD can gain a more comprehensive understanding of the satellite's security posture and develop countermeasures to mitigate the risk of attacks.

This approach has several benefits, including identifying potential security gaps that could be exploited by adversaries, reducing the likelihood of successful attacks, and minimizing the impact of attacks that do occur.

Furthermore, by testing systems in a controlled environment, the DoD can develop effective response strategies that will allow for faster and more effective recovery in the event of an attack.

However, there are also challenges associated with combining cyber and EW test methods. For



RTCA - DO - 160G Airborne Equipment Environmental Adaptability Test System

- S17 Voltage Spike Test System TPS-160S17
- S19 Induced Spike / Induced Signal Susceptibility Test System ISS 160S19 / ISS 1800
- S22 Indirect Lightning Induced Transient Susceptibility Test System LSS 160SM6, ETS 160MB
- S23 Lightning Direct Effect Test System
---LCG 464C High Current Physical Damage Test System
---LVG 3000 High Voltage Attachment Test System

Standard in compliant with: RTCA DO-160 Section 17/19 /22/23, MIL-STD-461G (CS117), SAE ARP5412, AECP 250/500



MIL - STD - 461 Military Test Systems

- CS106 Power Leads Spike Signal Conducted Susceptibility Test System TPS-CS106
- CS114 Bulk Cable Injection Conducted Susceptibility Test System CST-CS114
- CS115 Bulk Cable Injection Impulse Excitation Conducted Susceptibility Test System TPS-CS115
- CS116 Cables and Power Leads Damped Sinusoidal Transients Conducted Susceptibility DOS-CS116
- CS118 Personal Borne Electrostatic Discharge Test Equipment EDS 30T

Standard in compliant with: MIL-STD-461 CS106, CS114, CS115, CS116, CS118

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



0411200071-2000001
0-01112000022000

SUBSCRIBE: 3CTEST



The DoD has been working to combine cyber and electronic warfare testing methods with the goal of providing a more realistic picture of how these capabilities will perform in a real-world environment.

example, it can be difficult to accurately simulate real-world cyber and EW attacks, which can limit the effectiveness of testing. Additionally, the complexity of satellite systems can make it challenging to identify and address all potential vulnerabilities.

Despite these challenges, the need for combining cyber and EW test methods remains crucial to ensure the security of satellite technology.

As such, the DoD and other security agencies will continue to finance research and development to improve the effectiveness of these testing methods and stay ahead of evolving threats.

SATELLITE WEAKNESSES THAT CAN BE REVEALED THROUGH CYBER AND EW TEST METHODS

Examples of satellite weaknesses that can be revealed through cyber and EW test methods include:

- Vulnerabilities in the encryption of satellite communication systems can be exploited by cyber attackers to intercept or disrupt communication signals;
- Weaknesses in the satellite's hardware, such as outdated or unpatched software that hackers might take advantage of to access the satellite's system without authorization;
- The susceptibility of satellite systems to jamming or spoofing attacks can cause significant disruption or even loss of control of the satellite;
- Inadequate or insufficient security measures to protect satellite ground stations, which attackers can target to gain access to sensitive data or manipulate satellite operations; and
- The potential for interference or disruption caused by electromagnetic radiation from other sources can degrade the performance of the satellite and compromise its mission.

By using cyber and EW test methods, the DoD can simulate various types of attacks and identify weaknesses in satellite systems. This allows for the development of effective countermeasures and the implementation of security enhancements to strengthen satellite defenses and protect against potential threats.

THE DOD'S EFFORTS TO COMBINE CYBER AND ELECTRONIC WARFARE TESTING METHODS

The DoD is continually adapting to new threats and technologies to ensure that the military remains effective on the battlefield. One area of increasing importance is the integration of cyber and EW capabilities.

In recent years, the DoD has been working to combine cyber and EW testing methods with the goal of providing a more realistic picture of how these capabilities will perform in a real-world environment.

Efforts to Combine Cyber and EW Testing Methods

As modern warfare increasingly relies on electronic systems, the DoD has recognized the need to combine cyber and EW capabilities.

- The Joint Cyber/Electromagnetic Activities (JCEMA) test and evaluation framework was developed to evaluate the joint performance of cyber and EW capabilities;
- The JCEMA framework involves developing new testing procedures that can simulate the complex interactions between cyber and EW systems; and
- By testing cyber and EW systems together, the military can better understand how these systems will perform in a real-world environment and identify any weaknesses that need to be addressed.

Results of These Efforts

- The integration of cyber and EW testing methods is still a work in progress, but the DoD has made significant strides in this area;

- The JCEMA framework has been successfully used in a number of tests, providing valuable insights into the joint performance of cyber and EW capabilities;
- By testing cyber and EW systems together, the military has been able to identify areas where these capabilities can be further integrated and improved; and
- The DoD's efforts in this area have helped ensure that the military remains at the forefront of cyber and EW capabilities and can address the challenges of modern warfare.

Hence, the DoD's efforts to combine cyber and EW testing methods are an important step towards ensuring that the military can effectively operate on a modern battlefield. By testing these capabilities together, the military can better understand how they will perform in a real-world environment and identify any weaknesses that need to be addressed.

The Journal of Civil Engineering and Materials Application (JCEMA) framework and other testing procedures developed by the DoD will help to ensure that the military remains at the forefront of cyber and EW capabilities and can continue to protect national security in an increasingly complex technological landscape.

CONCLUSION

In conclusion, protecting satellite systems against EW threats and cyberattacks is critical for maintaining the integrity and reliability of satellite systems. EW and cyber threats are evolving rapidly, with attackers developing new methods and techniques to exploit vulnerabilities in satellite systems.

To keep pace with these evolving threats, continued testing and protection are necessary. The U.S. DoD has recognized the need to combine cyber and EW testing methods with the goal of providing a more realistic picture of how these capabilities will perform in a real-world environment. But ongoing research and development are necessary to innovate and develop new protection methods and techniques, such as AI, QKD, hardware security, threat intelligence sharing, and standardization. Further, testing and analysis must be carried out in a secure, cost-effective, and compliant manner.

Vulnerabilities must be identified and evaluated to develop effective countermeasures that protect satellite systems from EW and cyberattacks. The DoD and other agencies have invested in a range of technologies and strategies to enhance satellite security, including encryption, jam-resistant capabilities, and increased redundancy. The protection of satellite systems against EW and cyberattacks is also essential for maintaining critical infrastructure, complying with regulatory requirements, ensuring cost effectiveness, and providing assurance to stakeholders.

By exploring new technologies and strategies and investing in research and development, the DoD can help secure the future of satellite-based military capabilities and protect national security in an increasingly complex and uncertain world. Ultimately, the continued testing and protection of satellite systems against EW and cyberattacks will help maintain trust and confidence in satellite systems and the organizations that operate them. By working together, the military, government agencies, and industry partners can ensure the protection of satellite systems against evolving threats and maintain the operational effectiveness of critical military capabilities. ©



ENERGY-RELATED PRODUCTS AND RESOURCE EFFICIENCY REQUIREMENTS

A Look at Key Standards That Could Influence Future EU Legislative Proposals



Dr. Alex Martin is Principal Regulatory Consultant at RINA. Alex provides advice and compliance support on various regulations affecting electro-technical products, from EMCD, LVD, and RED through to environmental laws like RoHS, REACH, and WEEE. Alex can be reached at alex.martin@rina.org.



By Alex Martin

Among the 44 recitals in the EU's Ecodesign Framework Directive [1] is an assertion that the consideration of the environmental impact of an energy-related product [2] throughout its whole life cycle "has a high potential to facilitate improved environmental performance in a cost-effective way, including in terms of resource and material efficiency."

However, the Framework Directive does not define what it means by "resource and material efficiency," nor is this discussed in the European Commission's *Frequently Asked Questions (FAQ) on the Ecodesign Directive and its Implementing Regulations*. [3]

Nevertheless, resource efficiency requirements are now getting written into EU codesign implementing measures. [4] For instance, the 2019 Refrigerating Appliance Ecodesign Regulation [5] specifies several resource efficiency requirements. Among these requirements are provisions for refrigerating appliance manufacturers, their authorized representatives, or importers to ensure the availability of spare parts as well as to offer access to repair and maintenance information.

Meanwhile, the European Commission has driven the creation of European material efficiency standards through a request made to the European Standardization Organizations (i.e., CEN, CENELEC, and ETSI). International, European, and national standard setters also appear to have been giving attention to resource efficiency – and product circularity more generally – in their respective work programs.

This article discusses the recent drafting of a European circular product standard, the publication of EN4555X material efficiency standards, and some specific international and national standards. This

standardization activity is spearheading thinking on resource efficiency, and it could be that the requirements of these standards find their way into EU codesign implementing measures in the years ahead.

CIRCULAR PRODUCT DRAFT STANDARD – CD 45560

CEN and CENELEC's Joint Committee 10 has drafted a standard with the title of "Method to achieve circular designs of products." The Committee's intention is to produce a standard that will present a method to help achieve "circular-ready" product designs. This standard is poised to:

- Specify requirements and guidance for integrating circularity into the design and development process of products developed by an organization (e.g., the manufacturer of one or more energy-related products);
- Support organizations in developing product design rules to fulfill their chosen circular categories (e.g., the circular business models chosen by the organization, the legislative requirements);
- Focus on material efficiency; and
- Provide guidance on how to reduce environmental impacts.

EUROPEAN MATERIAL EFFICIENCY STANDARDS – EN4555X SERIES STANDARDS

Several generic material efficiency standards have been adopted as European Standards. The list that follows identifies these standards and summarizes what they address:

- **EN 45552:2020, *General Method for the Assessment of the Durability of Energy-related Products***
As energy-related products often cannot be completely recycled, each product disposed of as waste incurs losses in energy and materials.

Increasing the durability of energy-related products could therefore contribute to a reduction in the quantity of raw materials used, as well as the energy required for the production/disposal of such products. In turn, reductions in adverse environmental impacts become possible.

When considering durability, the trade-off between longer lifetimes (reducing impacts related to the manufacturing and disposal of the energy-related product) and reduced environmental impacts of new products (compared to worse/decreasing energy efficiency of older products) needs to be considered. In addition, consumer behavior and advances in technology have to be taken into account.

EN 45552:2020 specifies a general method for the assessment of the reliability and durability of energy-related products. In the standard, it is noted that durability can be expressed in different units (e.g., elapsed time, the number of operating cycles, distance, etc.). Meanwhile, reliability can be expressed as a particular unit combined with a probability. EN 45552:2020 describes a general assessment method that is intended to be adapted for application, at a product or product-group level, in order to assess the reliability/the durability of energy-related products.

- **EN 45553:2020, *General Method for the Assessment of the Ability to Remanufacture Energy-related Products***

This standard provides a general method for assessing the ability of an energy-related product to be remanufactured. Remanufacturing is identified as an industrial process where at least one change is applied that influences the safety, original performance, purpose, or type of the energy-related product.

- **EN 45554:2020, *General Methods for the Assessment of the Ability to Repair, Reuse and Upgrade Energy-related Products***

In this standard, common elements allowing an energy-related product to be repaired, reused, or upgraded are addressed at both the component and product levels. For instance, the standard details how to evaluate the ability of certain parts for disassembly.

- **EN 45555:2019, *General Methods for Assessing the Recyclability and Recoverability of Energy-related Products***

EN 45555:2019 notes that recovering materials and energy can reduce environmental impacts over the product life cycle, including through reduced extraction of natural resources and associated emissions of primary material production.

While recycling of energy-related products aims to close a circular economy loop, trade-offs might arise between different material efficiency-related topics. For instance, the mass of an energy-related product, as well as its durability, repairability, reusability, and energy efficiency, need to be balanced to improve the environmental benefit.

Once an energy-related product has reached the end of its life and is deemed waste, the product can either be prepared for reuse or recycled/recovered. EN 45555:2019 elaborates on the product characteristics that are relevant for the recyclability and recoverability of an entire energy-related product. The focus is, therefore, on the recyclability/recoverability of the product itself rather than the recycling or recovery processes. The general method presented in EN 45555:2019 considers the availability and efficiency of state-of-the-art recycling and recovery processes to determine the recyclability/recoverability rate of an energy-related product.

- **EN 45556:2019, *General Method for Assessing the Proportion of Reused Components in Energy-related Products***

EN 45556:2019 provides general methods for assessing the proportion of reused components in an energy-related product. The standard presents four calculation methods based on the mass of reused components and the number of reused components.

- **EN 45557:2020, *General Method for Assessing the Proportion of Recycled Material Content in Energy-related Products***

This standard facilitates the provision of substantiated claims concerning the recycled material content of energy-related products. Of particular importance is the tracing of recycled materials from different sources.

The recycled material content of a new product is a characteristic of the product and its parts. This contributes to material efficiency, in addition to the potential for reusability, recyclability, and recoverability.

With a focus on the efficient and effective use of natural resources, primary materials are often able to be substituted with recycled materials, reducing the demand for primary materials with related potential environmental, social, and economic implications. These could include reduced mining and consumption of natural resources, reduced landfills, reduced emissions, and energy savings. The overall environmental impact will depend on the difference in the impacts of making materials from primary sources (e.g., oil, ore, etc.) versus reprocessing waste into secondary materials, which would directly substitute primary materials.

The benefit of increasing recycled material content in products is, in many cases, the incentivization of recycling end-of-life waste material through the stimulation of demand for recycled materials. In other cases, where there is already a high demand for recycled materials compared to the available supply, the link between the specification of material with a higher amount of recycled content and the incentivization of recycling is weaker. Overall, the rationale for specifying recycled material content needs to be considered for each material individually, depending on the specific supply/demand situation. EN45557:2020 provides for such considerations.

- **EN 45558:2019, *General Method to Declare the Use of Critical Raw Materials in Energy-related Products***
Critical raw materials (CRMs) are economically important materials that exhibit high supply risks.



www.raymondemc.com

QUIET MATTERS.

Whatever your project needs to shield, we can create it.

We design, engineer, build, and install quality turnkey, shielded enclosures and anechoic solutions to meet your project's requirements and specifications.

EMC Chambers | Deployable Chambers | Anechoic Chambers | Shielded Enclosures | Shielded Doors | Shielded Cabinets | Shielded Bags and Tents | Chamber Accessories | Consulting Services | Installations Services | Chamber Relocation Services | Maintenance/Repairs/Upgrades

sales@raymondemc.com

1-800-EMC-1495

The European Commission (and certain national governments) have identified and listed CRMs. The availability of information on the use of CRMs in energy-related products is intended to improve the exchange of information.

As information on the use of CRMs in energy-related products is fairly limited at present, determining usage is important. The objective of EN 45558:2019 is to provide a general methodology for the declaration of the use of CRMs in energy-related products in support of EU ecodesign implementing measures.

EN 45558:2019 specifies a method for the declaration of CRMs, based on IEC 62474, *Material Declaration for Products of and for the Electrotechnical Industry*. The standard seeks to support efforts by energy-related product manufacturers to obtain information and report on the use of certain CRMs.

- **EN 45559:2019, *Methods for Providing Information Relating to Material Efficiency Aspects of Energy-related Products***

This standard describes a general method for the communication of material efficiency aspects of energy-related products. It is intended to be used when developing a communication strategy in horizontal, generic, product-specific, or product-group publications. The standard relates to EN 45552 to 45558.

However, none of these standards have been adopted as harmonized standards under EU ecodesign legislation. As general methods, the standards provide a starting point for energy-related product manufacturers to begin assessing their products. But they are not necessarily going to capture every nuance and provide the reasoning that would justify trade-offs and substantiate the “best” material efficiency options. Nevertheless, the standards put European-level material efficiency thinking in a larger context.

NOTABLE INTERNATIONAL AND NATIONAL STANDARDS

In addition to the adoption of EN 4555x series standards, certain international and national standards are worth noting. Among these are:

- **ISO 11469, *Plastics – Generic Identification and Marking of Plastics Products***

This international standard specifies a system of uniform marking of products that have been fabricated from plastics. The marking system is intended to help identify plastic products for subsequent decisions concerning handling, waste recovery, and/or disposal. Generic identification of the plastics is provided by the symbols and abbreviated terms given in ISO 1043, Parts 1 to 4.

The standard includes requirements on the marking system and the method of marking. The marking system is subdivided into marking of products, marking of single-constituent products, marking of polymer blends or alloys, and marking of compositions with special additives (fillers or reinforcing agents, plasticizers, flame retardants, and products with two or more components that are difficult to separate).

- **BS 8887, *Design for Manufacture, Assembly, Disassembly and End-of-Life Processing (“MADE”)***

The UK national standards body, the British Standards Institution (BSI), developed and published a series of standards dedicated to design for manufacture. The series consists of:

- BS 8887-1, *Design for Manufacture, Assembly, Disassembly and End-of-Life Processing (MADE) – Part 1: General concepts, process and requirements;*
- BS 8887-2, *Design for Manufacture, Assembly, Disassembly and End-of-Life Processing (MADE) – Part 2: Terms and definitions;*
- BS 8887-220, *Design for Manufacture, Assembly, Disassembly and End-of-Life Processing (MADE) – Part 220: The process of remanufacture – specification.* This outlines the steps required to change a used product into an “as-new” product, with at least equivalent performance and warranty of a comparable new replacement product; and
- BS 8887-240, *Design for Manufacture, Assembly, Disassembly and End-of-Life Processing (MADE) – Part 240: Reconditioning.*

The international standard BS ISO 8887-1, *Design for Manufacture, Assembly, Disassembly and End-of-Life Processing (MADE) Part 1: General concepts, process and requirements*, is currently under development by the BSI committee TDW/4 “Technical Product Realization.”

- **British PAS 141 reuse standard**

Publicly Available Specification (PAS) 141 was developed to increase the reuse of electrical and electronic equipment and to ensure that these items are tested and repaired to a minimum level. In the UK, the Waste and Resources Action Programme (WRAP) has developed a set of protocols based on industry experience highlighting tests and procedures to be carried out. The product protocols form a baseline for electrical product assessment and repair for reuse and can be used as a guideline for product assessment and testing.

- **Austrian standard ONR 192102:2014 on durable, repair-friendly designed electrical and electronic appliances**

This standard describes a label for repair-friendly designed appliances. Energy-related product manufacturers, their authorized representatives, or importers who intend to label their products must test their products according to the requirements of ONR 192102, verifying compliance with a test report. The standard outlines a labeling system with three levels of achievement (good, very good, excellent). This is mostly based on reparability criteria. The standard includes around 40 criteria for white goods and 53 criteria for small electronics (brown goods). The aim is to consider reparability to ensure energy-related products are not discarded sooner than is necessary as a result of a fault or an inability to repair a fault.

The criteria include accessibility of components, ease of disassembly, use of standard components, achievable service life (e.g., at least ten years for white goods), availability of spare parts (at least ten years after the last production batch), facilitation of regular maintenance, and further service information. No specific testing procedures or methods are detailed, though.

CONCLUDING THOUGHTS

It will be interesting to see what now becomes of the standards outlined – and standardization activities mentioned – with respect to EU ecodesign implementing measures.

For EU legislators, significant gains could be achieved by drawing upon the published standards

to identify and determine new requirements for inclusion in proposals for new or amended laws. For instance, requirements for CRM listings and product durability assessments could be incorporated into proposed revisions of EU ecodesign laws for domestic ovens, hobs and range hoods, as well as water pumps. This is possible, as is the drafting of product-specific European material efficiency standards to help give effect to these requirements for applicable energy-related products.

Upon adoption, such product-specific European material efficiency standards would likely get published in the EU *Official Journal* as harmonized standards under relevant ecodesign laws. This is, for instance, already the case for many product-specific performance standards. As is always the way with these things, future European Commission proposals for new or amended ecodesign laws will likely prove very telling. 

ENDNOTES

1. EU Directive 2009/125/EC.
2. These are any goods or systems “with an impact on energy consumption during use which is placed on the market or put into service, including parts with an impact on energy consumption during use which are placed on the market or put into service for customers and that are intended to be incorporated into products.”
3. See https://commission.europa.eu/system/files/2023-01/EC_FAQ_ED%20-%20JAN%202023.pdf
4. As defined in the Ecodesign Framework Directive, implementing measures are “measures adopted pursuant to this Directive laying down ecodesign requirements for defined products or for environmental aspects thereof”. Implementing measures include ecodesign regulations (e.g., the Refrigerating Appliance Ecodesign Regulation) and self-regulatory initiatives (e.g., the Games Consoles Ecodesign Voluntary Agreement).
5. This is Regulation (EU) 2019/2019.

ELECTRIC SHOCK STIMULATION FOR COMPLEX LEAKAGE CURRENT WAVEFORMS




by Hai Jiang and Paul Brazis

Editor's Note: *The paper on which this article is based was originally presented at the 2023 IEEE International Symposium on Product Compliance Engineering (ISPCE), held in Dallas, TX in May 2023. It is reprinted here with the gracious permission of the IEEE. Copyright 2024, IEEE.*

INTRODUCTION

Electrical shock protection is one of the key elements evaluated to ensure product compliance for public safety. As studied and reported by Dalziel [1], the human body physiological effects due to electric shock are determined by how much electrical current passes through the body. Leakage current test requirements provided in UL 101 [2] evaluate the potential body current for utilization equipment and maximizes electrical shock safety. IEC 60990 [3] specifies similar requirements using the same concept but uses a different term, “touch current”. One of the major differences between UL 101 and IEC 60990 is that UL 101 defines the limit and testing procedure measuring the Root-Mean-Square (RMS) value of the leakage current; IEC 60990, on the other hand, defines the limit and testing procedure on the measured peak value of the touch current. The peak limit in IEC 60990 is defined as the RMS limit multiplied by 1.414, which is the standard crest factor for a pure sinusoidal single-frequency waveform. Such criteria agree with each other when the product employs only linear electronic circuits and the measured leakage or touch current is a pure sinusoidal waveform. In the past sinusoidal waveforms were the most common signals encountered but not anymore. Modern technology regularly utilizes nonlinear electronic circuits for many applications such as household appliances, LED lighting, etc., to help improve electrical performance and operating efficiency. Waveforms of the leakage or touch current are, therefore, rarely found to be purely sinusoidal but

are typically more complex. Waveforms encountered in modern electric products are more commonly composed of mixed frequency signals and high-peak pulses superimposed on a 60 Hz baseline signal. In these cases, the crest factor between the peak and RMS values is no longer 1.414 but higher and with its value changing based on the waveshape of the leakage current waveform. Therefore, the peak limit and RMS limit are no longer interchangeable in products that use nonlinear electronic circuits. Depending on the specific waveshape, a product could meet the RMS limit but fail to the peak limit. For example, the authors have observed the waveform from a LED tube light was measured at 0.94 MIU in RMS but 7.86 MIU was measured in peak. As the limit in this case (UL 1993 was specified to be 5 MIU RMS (equivalent to 7.07 MIU peak), RMS and peak would give different certification testing results. MIU is a mathematical unit for leakage current measurement using the frequency-sensitive network about which more details can be found in [2] and [4].

The question has been asked for many years: which parameter does the human body respond to: peak or RMS? More experimental research needs to be done to study the comparative effect of peak and RMS values on the human body. In the 1940s, Charles Dalziel conducted human body experiments to study the physiological effects of “the inability to let-go” [1] (or “let-go”) and “perception” [5], and he concluded that the electrical shock physiological effects are controlled by the peak value, not the RMS for 60 Hz sinusoidal waveforms. Dalziel conducted extensive experimental research on the effects of current on the human body and is still cited as an authoritative source for electric shock data; that said, his research has some limitations in scope. For example, most of his experiments were conducted using single-frequency sinusoidal signals when determining the “let-go” current limit for human volunteers [1]. Dalziel did

study the effects of other types of waveforms, but these were limited to triangle, square, half-rectified and full-rectified waveforms with a fundamental frequency of 60 Hz. Dalziel also conducted experiments combining a 60 Hz sinusoidal waveform with its third harmonic (180 Hz) set equal to 37.5% of the fundamental when he found peak current as the critical factor in stimulating the human body [6]. In the discussion section of Dalziel's paper [6], J.A. Dickinson and F.B. Silsbee from the National Bureau of Standards (now the National Institute of Standards and Technology, NIST) questioned the validity of concluding that human body stimulation was controlled by peak current based on a single frequency or combined signals with third harmonics only. Therefore, these foundational tests by Dalziel are not easily relatable to waveforms commonly encountered today and still leave an open question on whether peak or RMS is the more appropriate parameter to assess shock hazards for non-sinusoidal waveforms.

In 1985 Hart reported experimental results comparing the electrical shock sensation of the peak and RMS for mixed-frequency signals [7]. The mixed signals explored by Hart were composed of a 60 Hz fundamental and secondary signal with frequencies between 30 to 100 kHz. Hart conducted testing on "several" people and six different secondary frequency signals and came to a similar conclusion as Dalziel that the peak is the determining factor for physiological effects rather than RMS.

Based on Dalziel and Hart's experimental results, Perkins demonstrated the complicated leakage/touch current waveforms for various products, including switch mode power supplies, variable speed drives (VSDs), network servers, etc.[8] In his paper, Perkins also demonstrated a method of measuring the peak leakage/touch current value using an oscilloscope and the traditional leakage current measurement network provided in both UL 101 and IEC 60990. In 1997, subsequent work led by Hart and Perkins reported experimental results with human volunteers comparing average,

peak, and RMS values of various waveforms with an equivalent 60 Hz sinusoidal (equivalent with respect to perception). The result of this work was included within the American National Standards Institute (ANSI) Standard C101 (now UL 101). In that study, different types of waveforms were considered but only for a single frequency of 60 Hz, which is not a true representation of the practical waveform exhibited by the products nowadays.

EXPERIMENTAL SETUP

For this UL Solutions study, a signal mixer/amplifier was used for the experimental work described herein, which had the capability of mixing two higher frequency signals with or without a 60 Hz signal. Using this setup, the reaction frequency factor was measured for each of the two male volunteers and compared with the reaction network factor given in UL 101 and IEC 60990. The customized frequency factor for the particular individual was then used to calculate the equivalent 60 Hz RMS and peak current signals for the mixed frequency signals. The results of this work were then compared with the results obtained using the method by Hart in [7].

Figure 1 shows the experimental setup for the complex waveform study. The power amplifier can mix three individual frequency signals plus a 60 Hz sinusoidal (integrated within the amplifier). The power

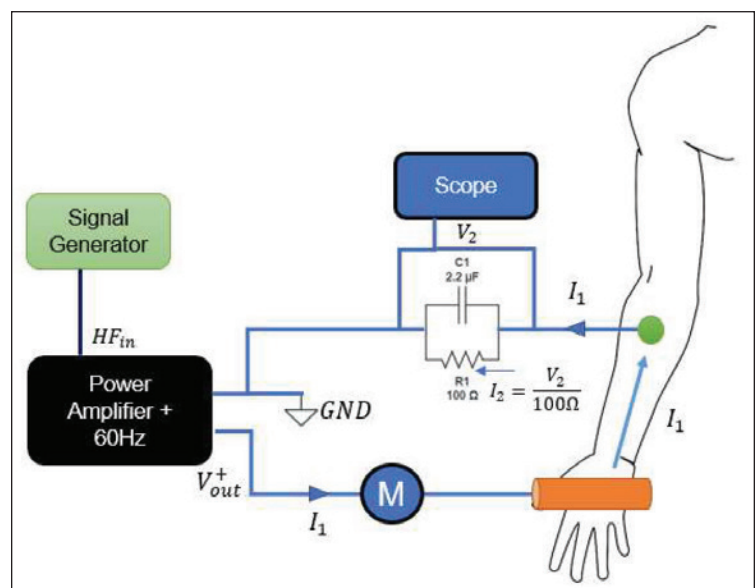


Figure 1: Complicated waveform electrical shock experimental setup

amplifier has a bandwidth of 100 kHz (-3 dB @ 100 kHz), and the output current is hardware limited to 35 mA for all frequencies for safety considerations. The maximum output voltage was also limited to $120 V_{\text{rms}}$ for safety. The current pathway was set from the lower arm to the hand (as shown) to mitigate the potential of current passing through the heart. The electrode on the arm consisted of an electronic pad manufactured by TENS for electrotherapy, as shown in Figure 1. The other electrode consisted of a copper cylinder, similar to that used by Dalziel [1] and for work previously published by the authors [9].

Reaction Frequency Factor

In [4], Dalziel conducted human body experiments and measured the threshold of perception for 143 men and 4 women for sinusoidal frequencies from 10 Hz to 200 kHz. The current pathway was from the upper arm (near shoulder) to the hand, which

was like that used in this paper (Figure 1). Three different contacts were examined in his investigation: hand hold, finger contact, and finger tap; thresholds of perception were reported for each contact, and statistical results for perception at 5%, 50%, and 95% population were provided.

The leakage current measurement circuit in both UL 101 [2] and IEC 60990 requires the reaction threshold network. It is noted that reaction is a different physiological effect than perception. Perception is an initial sensation of starting to feel the flow of electricity through the body. Reaction is what occurs when the electrical current is high enough for a person to “react” from the energized source. Perception will not likely lead to harmful injury, but reaction can lead to a secondary injury, e.g., falling from a ladder. Like perception, the reaction network is a low-pass filter compensating for the decrease of

EMC & COMPLIANCE INTERNATIONAL
TRAINING
CONFERENCE
EXHIBITION

EMC AND COMPLIANCE INTERNATIONAL 2024



May 22–23, 2024
9:00 AM – 6:00 PM



Newbury Racecourse, Newbury,
United Kingdom

- Cutting-Edge Industry Technology
- Exclusive Exhibition Spaces
- Expert Training with Live Q&A Sessions
- Unrestricted Remote Participation
- Expand Your Network in the Community



**FOR MORE INFORMATION,
REACH OUT TO US**



www.emcandci.com



info@emcandci.com

shock sensation for a given current magnitude as the frequency increases and is based on experimental measurements of perception/reaction as a function of frequency (for example, from Dalziel’s work). It is noted that Dalziel measured the perception threshold, which is a less intense physiological effect than the reaction; therefore, the absolute body current of Dalziel’s results is expected to be lower than the reaction current. This study focused on the reaction effects instead of perception because the reaction current can lead to harmful injuries and the reaction limit is the requirement of both the UL 101 and IEC 60990 standards.

Reaction is here defined as an uncomfortable sensation during which the volunteer reacts to the test current while holding the energized electrode. Several preliminary tests were conducted to familiarize the two test subjects with the sensation of the current at different frequencies. The experiment started with 60 Hz at 1 mA, which is above the perception threshold but lower than the reaction limit which is up to 2 mA. For the first few seconds, the touch current continued to increase due to transient/reactive effects at and near the skin interface. Once the current stabilized at 1 mA, the current was then increased to the reaction sensation of the subject. The subject was asked to memorize this sensation and attempts were made to adjust the current levels throughout this study to recreate the same sensation for all further experiments.

Alternate approaches were considered, such as use of a motion sensor to establish values where reaction was based on a sudden movement of the hand. The motion sensor was not used since the subject knew when the electrode would be energized, and were prepared for that shock sensation, and may still subjectively choose to either react (give up) early or attempt to endure the sensation for longer. Randomly energized plates were also considered but then rejected, as the

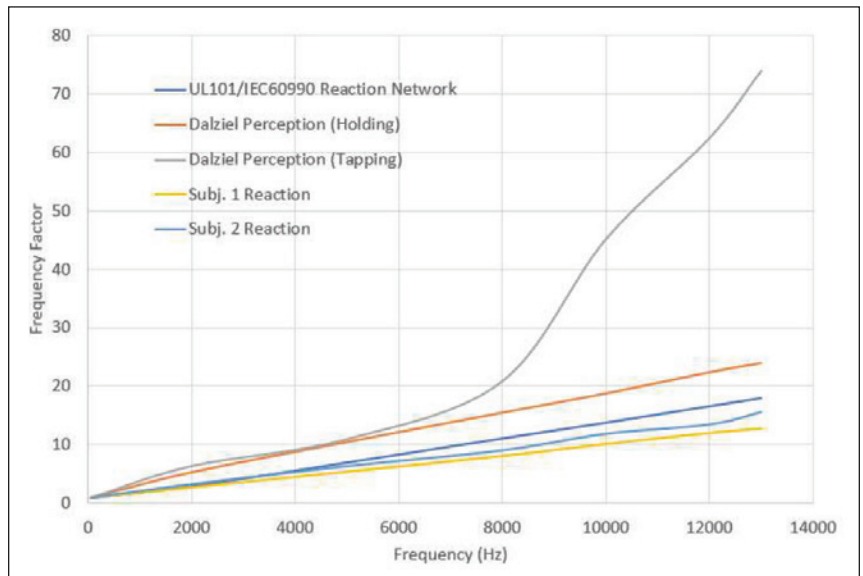


Figure 2: Frequency factor comparisons

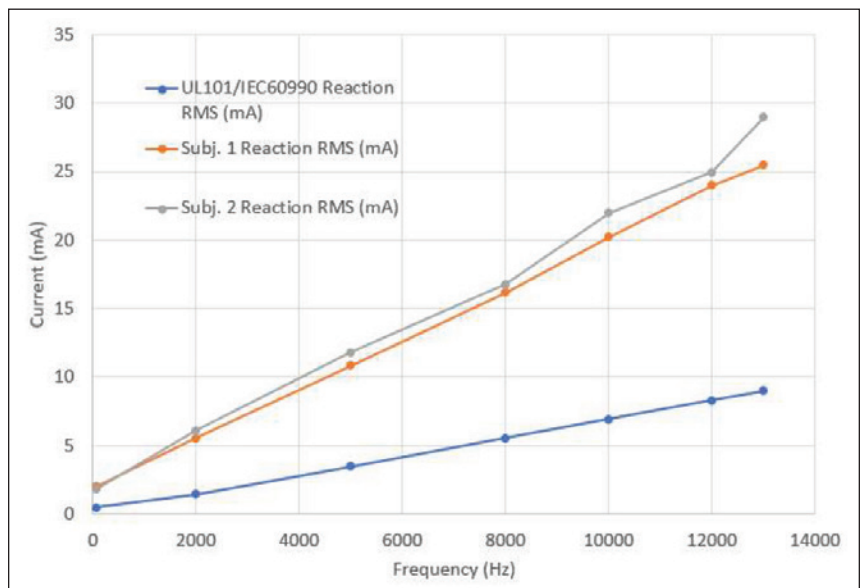


Figure 3: Measured reaction current over frequency compared with reaction limit given in UL 101

number of test iterations would need to be high and would be subject to bias and discomfort for the test subjects as there would be anticipation that plates may be energized. Therefore, having the test subject establish a threshold limit and in control of the stimuli was expected to minimize discomfort and maximize consistency in acquiring data, considering that the reaction intensity can be subjective and perceived differently.

Reaction thresholds were measured for two volunteers in the range of frequencies from 60 Hz to 15 kHz. Current thresholds at higher frequencies were not measured due to the maximum output current limitation of the power amplifier and its safety limits. Similar trends were expected based on Dalziel's results, though measurement of a "personal" reaction curve for each test subject was expected to improve accuracy since results depend on each individual's perceived sensation while the Dalziel curve is based on a statistical average from a larger population of test subjects.

Figure 2 shows the comparison of frequency factor curves from different sources. Dalziel's tapping result starts to deviate from the rest above 8 kHz, but the rest of the data follows a similar trend. The frequency factor is calculated using the following equation:

$$\text{Freq. Factor} = \frac{\text{Current at } x \text{ Hz}}{\text{Current at 60 Hz}}$$

The frequency factor normalizes the reaction for a given frequency relative to the touch current at 60 Hz. Figure 3 shows the measured reaction current for the two test subjects compared with the reaction limit in UL 101, calculated based on the frequency factor. In UL 101, the general reaction current limit is 0.5 MIU. It is noted that MIU is a mathematical unit for leakage current measurement using the frequency sensitive network [2].

As shown in Figure 3, the personal reaction currents were quite close for the two test subjects but higher than the UL 101 threshold limits. This can be understandable since the standard limit is intended to protect 95% of the population from reaction and therefore would typically be more conservative than curves from individuals. The two subjects are both male, between 40 to 50 years old.

Peak vs. RMS

The study described here starts with the same approach taken by Hart in [7]. As referred to in Figure 1, the following steps were taken as the experimental data was collected:

- Adjust the 60 Hz voltage supply to 1 mA through the subject's arm without a higher frequency component.
- Add the higher frequency component until the current I_2 reached 1.414 mA or a fixed current (in [7], Hart used 1.414 mA). Current is reduced relative to Hart in this study since the test subjects found the 1.414 level difficult to tolerate.
- Record I_1 and I_2 RMS and peak value.
- Reduce the high-frequency component to zero.
- Increase the 60 Hz current until the test subject reported the same feeling of intensity as the mixed-signal current; record I_1 and I_2 RMS and peak value.

RESULTS AND DISCUSSION

In these measurements, I_1 is the actual body current going through the arm in mA; I_2 is the theoretical current passing the resistor R_1 in MIU, which can be expressed by:

$$I_2 = \frac{I_1}{\text{Freq. Factor}} \text{ MIU}$$

The parallel RC circuit implements Dalziel's frequency factor as a low-pass filter. For 60 Hz signals, I_2 equals I_1 . At a higher frequency above 60 Hz, I_{2_Mixed} shall be equal to the current I_2 with only the 60 Hz signal if the reaction network can translate the shock sensation perfectly. Nevertheless, a deviation exists between the current I_2 of the mixed signal and the equivalent 60 Hz current with the same shock sensation for either RMS or peak. The deviation percentage is introduced to differentiate the effectiveness of the measurement to evaluate the shock sensation using a 60 Hz current limit. This deviation percentage quantifies the difference between the 60 Hz signal set by the test subject at the same perceived intensity level as the mixed signal and the actual level of the mixed signal to determine which parameter better predicts the shock intensity. The deviation percentage for either RMS or peak is calculated as:

$$\text{Deviation\%} = \frac{|\text{60Hz Only} - \text{Mixed } I_2|}{\text{60Hz Only}} \times 100\%$$

AT WORK.
AT HOME.
ON THE GO.

**In Compliance
is here for you.**

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

Therefore, the deviation percentage quantifies the difference between the perception of the test subject with the predicted perception level based on the frequency factor filter network. A smaller deviation implies that the frequency factor more accurately predicts 60 Hz equivalency for mixed frequencies.

Table 1 shows a sample result of an experiment for Subject 1. Current I_1 is the actual touch current of the high-frequency component required for current I_2 to reach 1.414 mA. Current I_2 is the total current after the Dalziel frequency network (low pass filter; therefore, this value gives a signal magnitude normalized to 60 Hz equivalent). The current I_2 is not the true current passing through a human body but is normalized by the reaction filter network to scale to 60 Hz equivalent. Therefore, if the Dalziel reaction network predicted the shock sensation perfectly, current I_2 shall equal to the 60 Hz only current (column 5) with the same shock sensation, and the deviation percentage would be zero. The RMS and peak of the equivalent 60 Hz-only current are shown with the same shock sensation of the mixed signal. Table 1 shows measured values and calculated deviation percentages for a single set of experiments for Subject 1.

Table 2 presents the comparison of RMS and peak results, using Dalziel and personal reaction curves for the two subjects. Overall, the peak showed a lower deviation than RMS values. For Subject 2, using the personal reaction curves significantly improves results, as the Dalziel curve gives inconsistent results across the frequency range. For Subject 1, personal and Dalziel reaction curves do not exhibit a significant change in the results. The use of personal reaction curves improves the RMS results for both test subjects, but the values are higher than the corresponding peak values. Though these initial results support the hypothesis that peak better characterizes perception/reaction levels across multiple frequencies, additional data is needed on a larger sample set of test subjects, as well as using additional complex waveforms (including those with more than two sinusoidal components as well as waveforms found in modern appliances) before making a conclusion whether peak or RMS values better characterize perception and reaction levels across multiple frequencies. ©

HF	60 Hz	HF/1 RMS (mA)	Mixed/2 RMS (mA)	1/2 Peak (mA)	60 Hz Measured Perception, RMS (mA)	60 Hz Measured Perception, Peak (mA)	Deviation Percentage, RMS	Deviation Percentage, Peak
2 kHz	1 mA	2.7	1.41	3	1.70	2.75	17.06%	9.09%
5 kHz	1 mA	6.7	1.41	3	1.82	2.935	22.53%	2.21%
8 kHz	1 mA	11	1.41	3	1.90	3.06	25.79%	1.96%
10 kHz	1 mA	13.7	1.41	3	2.00	3.2	29.50%	6.25%
12 kHz	1 mA	16.7	1.41	3	2.00	3.2	29.50%	6.25%

Table 1: Results examples for Subject 1 via Dalziel Reaction Network

HF	Subject 1				Subject 2			
	Personal Reaction Curve		Dalziel Reaction Curve		Personal Reaction Curve		Dalziel Reaction Curve	
	RMS	Peak	RMS	Peak	RMS	Peak	RMS	Peak
2 kHz	17.65%	1.82%	17.06%	9.09%	18.06%	2.69%	9.03%	16.73%
5 kHz	9.34%	11.28%	22.53%	2.21%	15.66%	2.75%	15.06%	10.09%
8 kHz	12.11%	7.84%	25.79%	1.96%	14.37%	4.21%	18.97%	5.26%
10 kHz	15.00%	4.69%	29.50%	6.25%	12.43%	5.36%	16.57%	7.14%
12 kHz	13.00%	6.56%	29.50%	6.25%	15.17%	2.03%	20.79%	1.69%
Mean	13.42%	6.44%	24.88%	5.15%	15.14%	3.41%	16.08%	8.18%
Median	13.00%	6.56%	25.79%	6.25%	15.17%	2.75%	16.57%	7.14%
Std Dev	0.0312	0.0353	0.0525	0.0303	0.0205	0.0135	0.0451	0.0567

Table 2: Comparison of personal and Dalziel filter

REFERENCES

1. C. Dalziel, E. Ogden, and C. Abbott, "Effect of Frequency On Let-go Currents," *AIEE Transactions in Electrical Engineering*, vol. 62, pp. 745-750, December 1943.
2. UL 101, "UL Standard for Safety for Leakage Current For Utilization Equipment," 6th Ed., 2019.
3. IEC 60990, "Methods of Measurement of Touch Current and Protective Conductor Current," 3rd Ed., May 2016.
4. Hai Jiang, "Study of High-Frequency Spectrum for 120 V Household Appliances," UL White Paper, April 2023.
5. C. Dalziel, and T. H. Mansfield, "Effect of Frequency On Perception Currents," *AIEE Transactions in Electrical Engineering*, vol. 69, Issue 2, pp. 1162-1168, January 1950.
6. C. Dalziel, J. Lagen, and J. Thurston, "Electric Shock," *AIEE Transactions in Electrical Engineering*, vol. 60, pp. 1073-1079, December 1941.
7. W.F. Hart, "A Five-Part Resistor-Capacitor Network for Measurement of Voltage and Current Levels Related To Electric Shock and Burns," *Electrical Shock Safety Criteria, Proceedings of the First International Symposium on Electrical Shock Safety Criteria*, pp. 183-192, 1985.
8. P. Perkins, "What does your touch current look like? Making proper touch current measurements," IEEE Symposium on Product Compliance Engineering (ISPCE) Measurements, May 2014.
9. H. Jiang and P. Brazis, "Experiments of DC human body resistance I: Equipment, setup, and contact materials," IEEE Symposium on Product Compliance Engineering (ISPCE), May 2018.

CREATING AN EFFECTIVE AND DEFENSIBLE PRODUCT RECALL

Recent Requirements Can Be Helpful



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



by Kenneth Ross

The recent news is replete with stories about product recalls being undertaken because of safety issues. In addition, there have been a number of recent jury verdicts based on injuries or deaths caused by a product that has been recalled, should have been recalled, or is in the process of being recalled. Needless to say, recalls can have a significant adverse effect on a manufacturer's or product seller's reputation, financial condition, relationship with retailers, and the ability to successfully defend a product liability case.

The law makes it easy for an injured party to claim that a recall was inadequate and that this inadequacy contributed to their injury. In addition, government entities in the U.S. and Europe are beginning to demand that companies do more things that should make their recalls more effective.

This article will discuss the law concerning recalls and recent government efforts to improve the effectiveness of such actions.

THE LAW

Court-made law ("common law") that has been adopted by most states in the U.S. is generically referred to as the "post-sale duty to warn." It states that a manufacturer may have a duty to warn consumers about hazards revealed after sale if consumers were not initially warned when the product was first sold. In addition, some state legislatures have enacted statutory laws that create a post-sale duty for products sold in that state.

This duty is based on negligence, which occurs after the product has been sold. Negligence is usually decided by a jury and is based on an allegation that the manufacturer failed to exercise reasonable care and that this failure resulted in injury, damage, or loss.

In other words, could the manufacturer have done more after sale to initiate the recall or corrective action earlier or done something to make it more effective, thus preventing the injury from occurring? Unless you are completely successful in your recall, you can always do more. However, since each jury gets to decide what is negligent, there really is no guidance for the manufacturer as to what "reasonable care" is and how effective the recall must be.

The common law and state statutory laws generally refer to "a duty to warn" and do not establish "a duty to recall." The law that pertains to the U.S. Consumer Product Safety Commission (CPSC) also does not require that the manufacturer always recall its product. The CPSC says that if the product has a defect that could create a substantial product hazard, the manufacturer must offer one of three remedies – replacement, repair, or refund of the subject product's purchase price.

In addition to the duty to warn, the common law also says that if a manufacturer voluntarily recalls its product, it can be held liable for injury or damage if the recall was done negligently. Virtually all recalls done under the supervision of a government agency are voluntary, and none are 100% effective. Therefore, the question is how to implement a recall that will not be considered negligent.

Another consideration when designing the recall or corrective action is whether you are providing a sufficient remedy to the consumer from a safety and economic standpoint. For example, if you are repairing the product, are you doing it for free? Or are you repairing the part or product but should be replacing it?

One new series of lawsuits that have recently been filed involve class actions alleging that the recall remedies are inadequate and, therefore, the consumer has suffered

some economic loss. These lawsuits can be filed even though there have been no incidents resulting in injury or damage. Most of the class-action lawsuits filed for an “inadequate remedy” have been against automobile manufacturers who have recalled their products, but most of these lawsuits have been dismissed by the court. However, there have also been cases filed against consumer product manufacturers that are still pending.

One recent case was brought against a bicycle parts manufacturer.¹ The complaint states:

“Even though Shimano has finally acknowledged the widespread issue, it is working hard to limit the cost of fixing the issue at the expense of consumers. Rather than offering to issue refunds or replacements for all of the Defective Cranksets, Shimano has taken the unconscionable position that only ‘(c)onsumers whose cranksets show signs of bonding separation or delamination during (an) inspection will be provided a free replacement crankset . . . that the dealer will professionally install.’”

The plaintiffs go on to allege:

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

The plaintiffs conclude by alleging that:

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

Plaintiffs are asking for reimbursement of all of the expenses that consumers could be subjected to as a result of this recall which would include a refund for the purchase price of the defective crankshaft.

Manufacturers should think about designing the remedy so that there is little risk that consumers will file a class action alleging that they suffered economic loss.

PRE-SALE PREPARATION

Below are some actions that companies can take to have a more effective and defensible recall or other post-sale corrective action.

Various entities in the supply chain should try to establish procedures before the product is designed and sold so that after the sale, each organization can easily and efficiently obtain and analyze information, make decisions about any appropriate post-sale remedial programs, and implement any necessary programs.

Some of the most significant elements to build into a product’s design, manufacturing, and distribution processes are traceability and marking procedures that are used before and during the manufacturing process and during distribution. To the extent possible, products, and especially safety-critical components, should be marked or coded so that in the event of a recall, the part can be traced to a specific product or part and can be easily replaced or repaired.

This traceability allows the manufacturer of the finished product or component part to narrow the affected population and clearly identify the population to the government, retailers, and customers.

One of the most important and difficult tasks for the manufacturer is setting up a communications network before the sale so that appropriate safety information is received if there is an issue after sale.

A manufacturer has many readily available sources of information anywhere its product is sold. Personnel at the component supplier, the dealer, and the OEM should be trained to ensure that sufficient information is gathered concerning warranty claims, injury or damage claims, accidents, near misses, and customer inquiries or complaints so that actual or potential problems can be identified.

Personnel should be trained to identify and clarify the information received so that it is accurate, substantiated, and properly documented. The manufacturer does not want to gather and maintain inaccurate and overstated complaints and claims that incorrectly make it appear that a problem exists.

In addition, the company must decide which claims to follow up on and how to do so. Do they need to see

and analyze the product? Do they need to interview the product user or claimant? Do they need to see the location of the incident?

POST-SALE PREPARATION AND IMPLEMENTATION

As a manufacturer obtains and analyzes post-sale information, it must determine whether any post-sale action is necessary at any point in time. This includes reporting to the CPSC and possibly undertaking some form of recall, repair, or replacement.

Analyzing the information and deciding what it means is the most critical phase of this process. It is recommended that manufacturers conduct a risk assessment prior to selling their products. This process identifies the risk, the probability of the risk occurring, the potential consequences if it occurs, and methods to minimize the risk.

Before sale, the manufacturer should make a best guess on the probability of the risk occurring. Of course, it is difficult to estimate the probability of an event occurring when it has never happened before. After sale, when events occur, a new risk assessment should be conducted by both the manufacturer and any applicable component supplier. This is easier since you are now aware of safety-related incidents and potential vulnerabilities.

Once you decide to undertake a recall or other corrective action, the process should be designed so it is as effective as possible given the information that has been obtained or could be obtained by the manufacturers, component part suppliers, or product sellers. For an earlier discussion of governmental guidances and British codes of practice on effective recalls, see my article entitled “*Preparing for and Implementing Product Recalls in 2022*,” from the May 2022 issue of *In Compliance Magazine*.²

CPSC RECALL ENHANCEMENT EFFORTS

The CPSC has been talking about efforts to make recalls more effective for at least 20 years. One of their first efforts was to retain an outside consultant to study the literature on recall effectiveness and suggest ways for manufacturers and product sellers to do better.³ Then there were recall effectiveness workshops presented by the CPSC in 2017⁴ and a report issued in 2020 by the U.S. Government Accountability

Office (GAO) with recommendations on actions that could be undertaken by the CPSC to improve recall effectiveness.⁵

Then, in February 2023, the CPSC made a presentation at the International Consumer Product Safety and Health Organization (ICPHSO) Conference that discussed “Corrective Action Plan Enhancements.” These enhancements have been incorporated into corrective action plan (“CAP”) agreements negotiated by the CPSC and manufacturers or product sellers. The main enhancements from the CPSC this year deal mainly with the internet and social media as these are much more likely to be accessed by potential customers than in the past.

When manufacturers and product sellers file a “non-Fast Track” report with the CPSC and agree to undertake a corrective action, they most likely will receive a proposed CAP agreement that could include some or all of the following enhancements to earlier corrective action agreements:

- In addition to the issuance of a press release, the company will publicize the CAP through all social media and mobile platforms. If the company does not have a social media presence, the CPSC may demand that they establish such a presence.
- Provide at least two CPSC staff-approved direct notices to all known consumers via mail, e-mail, phone, or text messages.
- The CPSC will specify how often the company must post on Facebook, Twitter (now “X”), and Instagram and require that these posts be available for a minimum of 10 years.
- The CPSC might request that the company initiate paid social media advertising on all of its most-followed social media platforms.
- The CPSC might request the company take out search engine advertisements and display ads on their retailer’s websites.
- The CPSC might also request that internet platforms that sold the recalled product provide two rounds of direct notice to customers who purchased the product on their internet platform.
- The CPSC may require confirmation within 30 days of the press release as to which platforms and retailers sent out CPSC staff-approved direct notice of a hazard to all known purchasers.

In addition, the CAP agreement might include a requirement for a compliance program which states as follows:

“The company will create and maintain a Compliance Program designed to ensure compliance with the CPSA and all other Acts and regulations administered by the CPSC. The company will identify a Safety Officer or Safety Committee responsible for the Firm’s compliance. The company agrees to provide documentation of the program and the specific modifications to its existing Compliance Program, if any, to address any material deficiencies, within 90 days of the acceptance of this CAP.”

CPSC trial attorneys are the compliance officers for these non-Fast Track filings. In December 2023, a CPSC trial attorney made a video presentation about what actions the CPSC views as contributing to an effective recall.⁶ It should be noted that the “requests” in the non-Fast Track CAP agreements go well beyond what has been required over the years for a Fast Track filing.

CPSC FY 2024 OPERATING PLAN

The CPSC Commissioners recently agreed to their 2024 operating plan. This plan has several goals that relate to recall effectiveness. The CPSC is seeking a response rate for all recalls of 33%. Most response rates in the past have been much lower. And the CPSC is trying to get 70% of all filing companies to agree to use social media to communicate a recall.

In addition, the CPSC identified the following priority activities for FY 2024:

- Examine mechanisms to improve recall effectiveness by exploring measures of consumer awareness of recall information either by direct contact or secondary means.
- Encourage commitments from recalling firms to communicate recall information to consumers in Spanish and additional languages commonly spoken in the United States.
- Conduct a study on consumer behavior in response to product recalls and implement the study’s recommendations.
- Work with firms to maximize communications about recalls through multiple communication channels and the use of technology.
- Prioritize resources to improve its recall monitoring process and conduct follow-up activities with firms, as appropriate.
- Work with a variety of stakeholders to be able to better understand consumer behavior in the recall context and to increase recall response rates.
- Seek mandatory recalls where firms will not take corrective actions voluntarily.
- Expand the recall monitoring program to identify recalling firms that are appropriate targets for an expanded recall announcement, a renewed investigation, or enforcement action.

EUROPEAN UNION

Increasing the effectiveness of recalls remains a top priority for the Commission of the European Union (EU) and is explicitly addressed in the recently enacted EU’s General Product Safety Regulation (Regulation (EU) 2023/988) which will come into force on December 13, 2024. Rutger Oldenhuis, a leading EU recall expert, summarizes this priority as follows:

“In the EU, enhancing the efficiency of product recalls continues to be a key focus for the EU Commission and is explicitly addressed in the upcoming EU General Product Safety Regulation (Regulation (EU) 2023/988). Research indicates that one-third of consumers who have read a recall notice still continue to use the unsafe product in question. Therefore, the new Regulation includes extensive new recall obligations for manufacturers of consumer products. The impact of these new measures could be significant.”⁷

The new regulation includes several measures described below to improve recall effectiveness:

- Providers of online marketplaces that collect their customers’ personal data shall make use of that information for recalls and safety warnings.
- Product registration by consumers for direct notifications regarding recalls and safety warnings shall be encouraged. This includes integrating direct contact mechanisms into customer loyalty programs and product registration systems.
- The Commission shall be empowered to adopt implementing acts in order to specify that for some specific products or categories of products, consumers should always have the possibility to

It is exceedingly difficult to defend cases where a recall has occurred unless you can show that the consumer read the recall notice and decided not to return the product to the manufacturer.



register a product they have purchased in order to be directly notified about a recall or a safety warning related to that product.


- Recall notices should not minimize the risk at stake or be drafted in a complex way. Recall notices should be clear and transparent, and describe risks clearly. The recall notice must avoid any elements that may decrease consumers' perception of risk, for example by using terms and expressions such as "voluntary," "precautionary," "discretionary," "in rare situations" or "in specific situations" or by indicating that there have been no reported accidents.
- Economic operators must offer consumers at least two options between repair, replacement, or adequate refund of the recalled product unless the second remedy would be impossible or impose disproportionate costs on the recalling party.

On the issue of recall effectiveness, Oldenhuis has also stated:

"Effectiveness in product recall management introduces an intriguing paradox. The more successful and efficient a recall is in reaching and persuading consumers to return or stop using the recalled products, the greater the costs incurred, and consequently, the more significant the financial and reputational damage inflicted upon the manufacturer. One might assume that manufacturers would therefore opt for recall insurance. However, in practice, this is mostly not the case. Companies often seem to rely on the belief that a recall won't affect them."⁸

Many of the requirements in these new regulations are based on a 2021 behavioral study done by the EU on strategies to improve the effectiveness of recalls.⁹ In addition, the UK Office for Product Safety and Standards issued a report in 2020 based on research it performed in 2017. The research tested behaviourally-informed product recall messages with a consumer panel. Responses were measured in terms of perception, sense of urgency, emotional response and likely action.¹⁰

CONCLUSION

It is exceedingly difficult to defend cases where a recall has occurred unless you can show that the consumer read the recall notice and decided not to return the product to the manufacturer. Therefore, manufacturers should spend sufficient time to carefully prepare before sale and after sale for the possibility of a recall. This includes carefully designing a program that will be defensible if there is a class-action suit alleging an inadequate remedy or a lawsuit for injury, damage, or economic loss brought by an individual consumer or to satisfy or exceed the requirements or desires of the applicable government authority. 

ENDNOTES

1. Erazo v. Shimano, et al, USDC, Central District of California, filed October 3, 2023.
2. <https://incompliancemag.com/article/preparing-for-and-implementing-product-recalls-in-2022>
3. See "Recall Effectiveness Research: A Review and Summary of the Literature on Consumer Motivation and Behavior." <https://www.cpsc.gov/s3fs-public/RecallEffectiveness.pdf>
4. <https://www.cpsc.gov/Recall-Effectiveness>
5. <https://www.gao.gov/products/gao-21-56>
6. <https://www.youtube.com/watch?v=a0Y-drY4qa4> (starting at the 12-minute mark)
7. From Rutger Oldenhuis, RecallDesk, <https://www.recalldesk.com>, in an email to the author dated November 27, 2023.
8. From Rutger Oldenhuis, RecallDesk, <https://www.recalldesk.com>, in an email to the author dated November 26, 2023.
9. <https://op.europa.eu/en/publication-detail/-/publication/1a695500-9e31-11ed-b508-01aa75ed71a1/language-en>
10. <https://www.gov.uk/government/publications/insights-into-product-recall-effectiveness>

DIFFERENCE AMPLIFIER: COMMON MODE AND DIFFERENTIAL MODE VOLTAGES

By Bogdan Adamczyk

This column describes the operation of an ideal difference amplifier. First, the input-output relationship for the generic input voltages is derived. Subsequently, the differential mode and common mode voltages are introduced. Then, the difference amplifier driven by the common mode and differential mode input voltages is analyzed. It is shown that an ideal difference amplifier (with no resistance mismatches) eliminates the common mode portion of the input voltage and amplifies only the differential mode portion of the input voltage.

1. DIFFERENCE AMPLIFIER – GENERIC INPUT VOLTAGES

Figure 1 shows a classical difference amplifier circuit with generic input voltages v_a and v_b , [1].

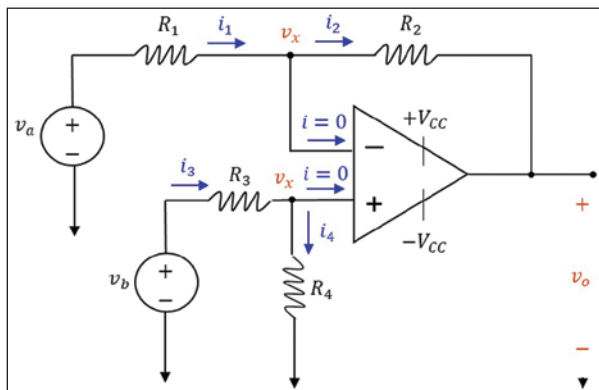


Figure 1: Difference amplifier with generic input voltages

Let's derive the relationship between the two input voltages and the output voltage. Assuming the ideal operational amplifier model, we have

$$i_1 = i_2 \quad (1.1a)$$

$$i_3 = i_4 \quad (1.1b)$$

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 EMC certificate courses for industry. He is an iNARTE certified EMC Master Design Engineer. He is the author of the textbook *Foundations of Electromagnetic Compatibility with Practical Applications* (Wiley, 2017) and the upcoming textbook *Principles of Electromagnetic Compatibility: Laboratory Exercises and Lectures* (Wiley, 2024). He has been writing this column since January 2017. He can be reached at adamczyk@gvsu.edu.



or

$$\frac{v_a - v_x}{R_1} = \frac{v_x - v_o}{R_2} \quad (1.2a)$$

$$\frac{v_b - v_x}{R_3} = \frac{v_x}{R_4} \quad (1.2b)$$

From Eq. (1.2a) we obtain

$$v_o = \frac{R_1 + R_2}{R_1} v_x - \frac{R_2}{R_1} v_a \quad (1.3a)$$

while from Eq. (1.2b) we get

$$v_x = \frac{R_4}{R_3 + R_4} v_b \quad (1.3b)$$

Substituting Eq. (1.3b) into Eq. (1.3a) we get

$$v_o = \left(\frac{R_1 + R_2}{R_1} \right) \left(\frac{R_4}{R_3 + R_4} \right) v_b - \frac{R_2}{R_1} v_a \quad (1.4)$$

or

$$v_o = \frac{\frac{R_1 + R_2}{R_1}}{\frac{R_3 + R_4}{R_4}} v_b - \frac{R_2}{R_1} v_a \quad (1.5)$$

leading to

$$v_o = \frac{(1 + \frac{R_2}{R_1})}{(1 + \frac{R_3}{R_4})} v_b - \frac{R_2}{R_1} v_a \tag{1.6}$$

which is equivalent to

$$v_o = \frac{R_2}{R_1} \frac{(1 + \frac{R_1}{R_2})}{(1 + \frac{R_3}{R_4})} v_b - \frac{R_2}{R_1} v_a \tag{1.7}$$

when

$$\frac{R_1}{R_2} = \frac{R_3}{R_4} \tag{1.8}$$

the relationship in Eq. (1.7) becomes

$$v_o = \frac{R_2}{R_1} (v_b - v_a) \tag{1.9}$$

which describes the input-output relationship of the difference amplifier.

2. DIFFERENTIAL AND COMMON MODE SIGNALING

Consider a circuit shown in Figure 2, with the load between nodes *A* and *B* and the two sources sharing node *C* [2].

Writing KVL for the circuit shown produces

$$-v_s - v_s + v_L = 0 \tag{2.1}$$

or

$$v_L = 2v_s \tag{2.2}$$

To make the load voltage, v_L , equal to the source voltage, v_s , while retaining both sources, we could simply half the voltage source values as shown in Figure 3.

Figure 3 also shows the forward current, I_D , flowing from the sources to the load and return currents of the same value and opposite direction flowing from the load back to the

sources. We refer to this differential mode current to the sources as the differential mode sources.

Circuit 2, shown in Figure 3, is equivalent to the one in Figure 4, where the polarity and value of the lower source have been reversed, and the names of the sources have been changed from v_s to v_{dm} to emphasize that these are differential mode sources.

Let's add an additional source, v_{cm} , to the circuit between the reference node and node *C*, as shown in Figure 5 on page 40.

This common-mode source injects the common-mode current, I_c , into the forward and return path, as shown in Figure 5.

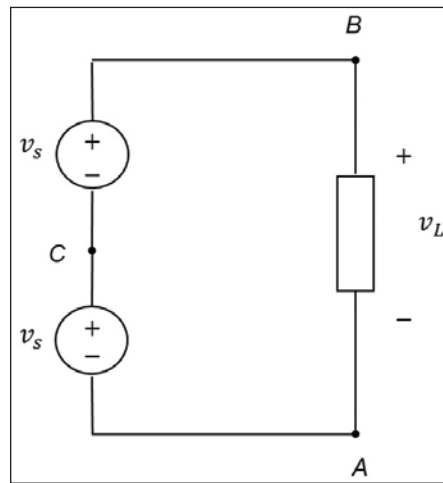


Figure 2: Differential signaling circuit 1

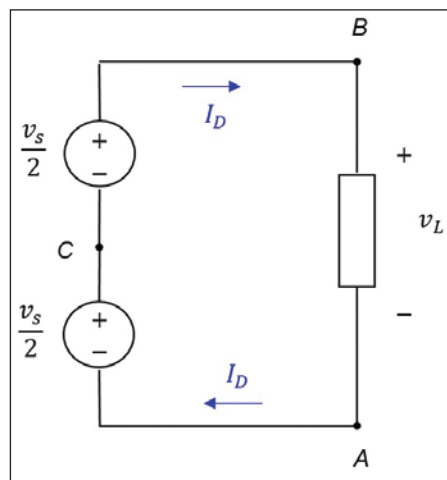


Figure 3: Differential signaling circuit 2

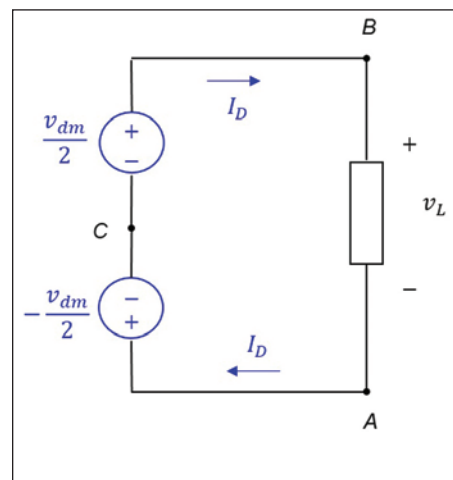


Figure 4: Differential signaling circuit 3

The voltage at node *A* with respect to the reference node is

$$v_a = v_{cm} - \frac{v_{dm}}{2} \tag{2.3}$$

while the voltage at node *B* with respect to the reference node is

$$v_b = v_{cm} + \frac{v_{dm}}{2} \tag{2.4}$$

3. DIFFERENCE AMPLIFIER – DIFFERENTIAL AND COMMON MODE INPUT VOLTAGES

Let’s return to the difference amplifier circuit shown in Figure 1 and replace the generic input voltages v_a and v_b with the ones given in Eqs. (2.3) and (2.4). This is shown in Figure 6.

Let’s substitute Eqs. (2.3) and (2.4) into Eq. (1.4) repeated here as Eq. (3.1)

$$v_o = \left(\frac{R_1+R_2}{R_1}\right)\left(\frac{R_4}{R_3+R_4}\right)v_b - \frac{R_2}{R_1}v_a \tag{3.1}$$

Thus

$$v_o = \left(\frac{R_1+R_2}{R_1}\right)\left(\frac{R_4}{R_3+R_4}\right)\left(v_{cm} + \frac{v_{dm}}{2}\right) - \frac{R_2}{R_1}\left(v_{cm} - \frac{v_{dm}}{2}\right) \tag{3.2}$$

or

$$v_o = \left[\left(\frac{R_1+R_2}{R_1}\right)\left(\frac{R_4}{R_3+R_4}\right) - \frac{R_2}{R_1}\right]v_{cm} + \left[\left(\frac{R_1+R_2}{R_1}\right)\left(\frac{R_4}{R_3+R_4}\right) + \frac{R_2}{R_1}\right]\frac{v_{dm}}{2} \tag{3.3}$$

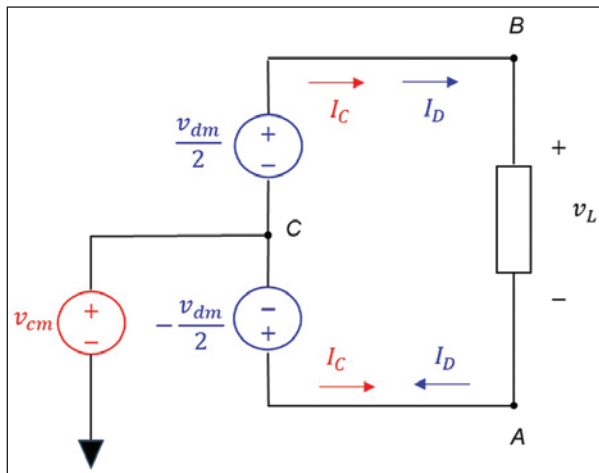


Figure 5: Differential mode and common mode signaling circuit

leading to

$$v_o = \left[\frac{R_1R_4 - R_2R_3}{R_1(R_3+R_4)}\right]v_{cm} + \left[\frac{R_4(R_1+R_2) + R_2(R_3+R_4)}{2R_1(R_3+R_4)}\right]v_{dm} \tag{3.4}$$

or

$$v_o = A_{cm}v_{cm} + A_{dm}v_{dm} \tag{3.5}$$

where A_{cm} is the common mode gain and A_{dm} is the differential mode gain.

Equations (3.4) and (3.5) express the output of the difference amplifier in terms of the common mode and differential mode input voltages.

when

$$R_1R_4 - R_2R_3 = 0 \tag{3.6}$$

we have

$$v_o = (0)v_{cm} + A_{dm}v_{dm} \tag{3.7}$$

Thus, an ideal difference amplifier (with no resistance mismatches) eliminates the common mode portion of the input voltage and amplifies only the differential mode portion of the input voltage. [\[4\]](#)

REFERENCES

1. James W. Nilsson and Susan A. Riedel, *Electric Circuits*, Pearson, 2015.
2. Bogdan Adamczyk, *Foundations of Electromagnetic Compatibility with Practical Applications*, Wiley, 2017.

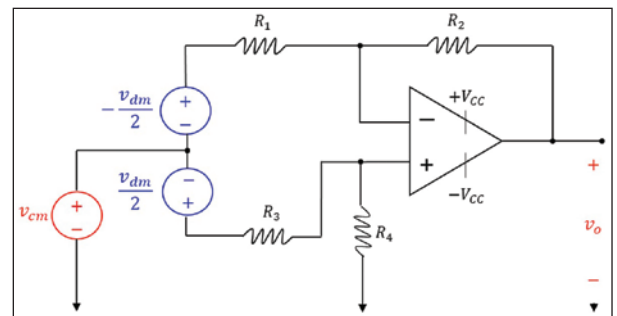




Figure 6: Difference amplifier with common mode and differential mode input voltages

PRODUCT Showcase




Trust Matters!



New Dual FFT
FFT-based Modal EMI Receiver

EMSCOPE

Innovative EMI receiver for modal measurements



A double channel receiver for complete measurements of conducted emissions up to 110 MHz.

- Fast and accurate EMI measurements
- 16 amp LISN Built-in (optional)
- Innovative Modal Measurements
 - Simultaneous Common and Differential Mode
- Effective Filter Design
 - Reduce cost and space of your EMI filter

ABSOLUTE-EMC.com



One Stop Shop for All Your Testing Needs

- Wireless Coexistence
- HazLoc/ATEX
- RoHS
- FCC
- FDA 510K
- NEMA 250/IP
- CE
- ISED Canada
- Other Sources of RF Emitters


AND MORE...

Let us assist you with testing your
Medical Devices, Machinery,
IT Devices, Lab Devices, Controllers,
Wireless Devices, Lighting,
or Electric Tools.

Call Us Today!



877-407-1580 sales@f2labs.com

F2 Labs is an accredited regulatory testing laboratory with more than 25 years of experience performing EMC and Safety evaluations on an extensive range of products.



Smart Test System For MIL-STD-461 & DO-160 Tests

MIL-MG3 is tailored to MIL-STD-461 CS106, CS115 and CS116 test requirements. One coupler for CS115 and all CS116 test frequencies enables faster and more efficient calibration and test setups. Plug-in modular design gives users the flexibility to add DO-160 Section 17 and Section 19 tests. Optional automation software available.

USA sales, service and support by HV TECHNOLOGIES, Inc.
emcsales@hvtechnologies.com | www.hvtechnologies.com



Stay informed and empowered with **In Compliance Weekly** eNewsletter, your source for the latest compliance engineering news and insights.

IN COMPLIANCE
Magazine

<https://incompliancemag.com/subscribe/enewsletters>



FOR YOUR CONDUCTIVE IMMUNITY TESTING NEEDS




IEC TESTING MADE EASY

SALES@LIGHTNINGEMC.COM




Current and voltage - our passion



The Static Control Flooring Experts

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



www.staticstop.com
877-738-4537

CHALLENGES OF CDM MODELING FOR HIGH-SPEED INTERFACE DEVICES

By Emanuele Groppo for EOS/ESD Association, Inc.

The Charged Device Model (CDM) qualification level is essentially correlated to the peak ESD discharge current [1]. Hence, several modeling approaches have been proposed to predict CDM peak current for a given package and CDM voltage level based on lumped-element equivalent circuits [2, 3]. However, the behavior of ultra-high-speed interfaces is more complex, involving fast rise time waveforms and on-die transient phenomena that cause device failure at lower CDM levels [4]. Distributed parasitics models of both on-chip circuitry and package wiring are required to capture such phenomena properly.

STATE OF THE ART

Figure 1 shows the field-induced CDM tester schematic and the corresponding 3-capacitor circuit model described in the JEDEC standard [1]. The following capacitance contributions are considered in this model:

- Field plate to device under test (DUT) capacitor CDUT, considering the contribution of package conductors and on-die traces.
- Ground plane to DUT capacitor CDG, always significantly smaller than CDUT.

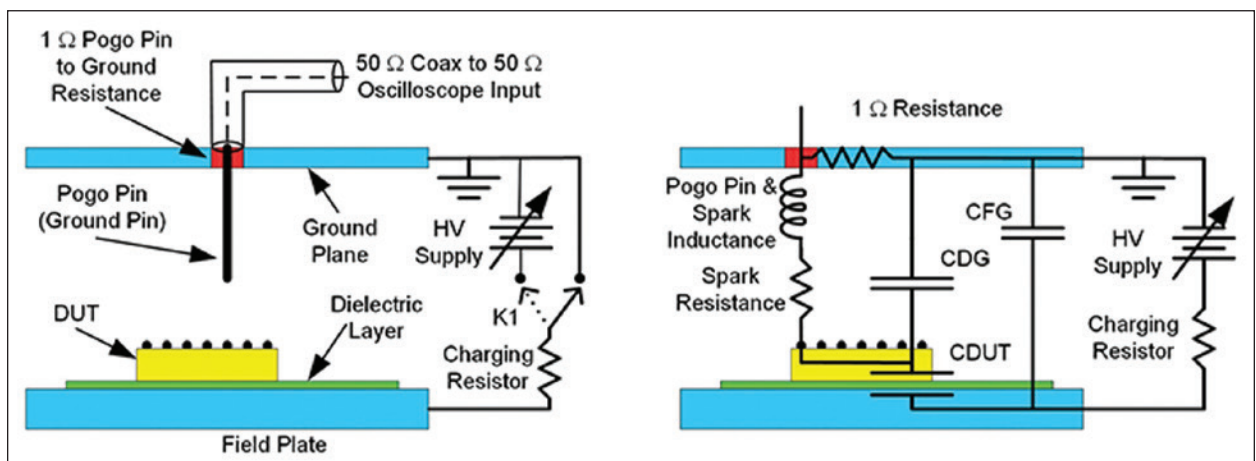


Figure 1: CDM tester scheme (left) and equivalent 3-capacitor circuit model (right) [1].

Emanuele Groppo received his B.Sc. (2020) and M.Sc. (2022) in Electronic Engineering from Politecnico di Torino, Italy. He is currently pursuing a Ph.D. at the Technical University of Munich (TUM), Chair of Circuit Design. In 2023, he joined the ESD team at Intel in Munich, Germany. The focus of his research is on novel ESD devices and solutions for advanced semiconductor technologies.



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.



- Ground plane to field plate capacitor CFG, including the chassis contribution (separated in more complex 5-capacitor models [3]).

The equivalent circuit is then completed by the spark resistance, a series inductor accounting for the contributions of arc and pogo pin, and a 1 Ω current sensing resistance from pogo pin to ground. This model is suitable to describe the initial peak of the CDM discharge current, which has been shown to correlate well with the CDM failure threshold in many cases.

PROBLEM STATEMENT

However, when dealing with ultra-high-speed interface devices, the model described in the previous section yields a significant mismatch with respect to experimental data. To understand its limitations, consider the Spice schematic shown in Figure 2.

1. The DUT is modeled as a lumped capacitor CDUT. This approach is suitable for peak current estimation but does not allow the evaluation of the actual voltage at the pad and the voltage drop on internal nodes (critical for deeply scaled, overshoot-sensitive technologies).
2. With respect to the model shown in Figure 1, package trace and bonding impedance are modeled as a lumped RL series (R_{pkg} , L_{pkg}). However, the actual discharge channel behavior is more complex than an RL series, with reflections and delays that may affect the input waveform.

To overcome such limitations, distributed parasitics models are required to successfully predict the CDM behavior of ultrafast devices, providing a more reliable description of fast transient phenomena that can occur in the tester structure and within the DUT.

PROPOSED APPROACH

The most sensitive victims for high-speed interfaces are thin gate oxides directly connected to the pad to optimize RF and high-speed performance. To assess the design solutions, a distributed DUT model, as presented in Figure 3 on page 44, can be plugged into the CDM tester model, replacing the lumped DUT capacitor. An example of a protection concept of a single-stage ESD diode protection with a power clamp (PC) is included in the model. The maximum voltage difference between V_{dut} and V_{ss} (V_{dd}) should not exceed the breakdown voltage of the gates. On-die parasitics of V_{ss} and V_{dd} nets strongly influence the actual voltage waveform at the input gate oxide. In particular, oscillations and spikes in the voltage waveform are sensed by the gate oxide and can lead to damage.

To account for the package trace behavior at fast transients as well, the lumped R_{pkg} and L_{pkg} need to be replaced by a more accurate channel model, capturing fast rise time slopes and possible reflections. Since the channel behavior strongly depends on the topology and layout of the substrate wiring, the most accurate modeling approach will require S-parameter extraction through calibrated EM simulations.

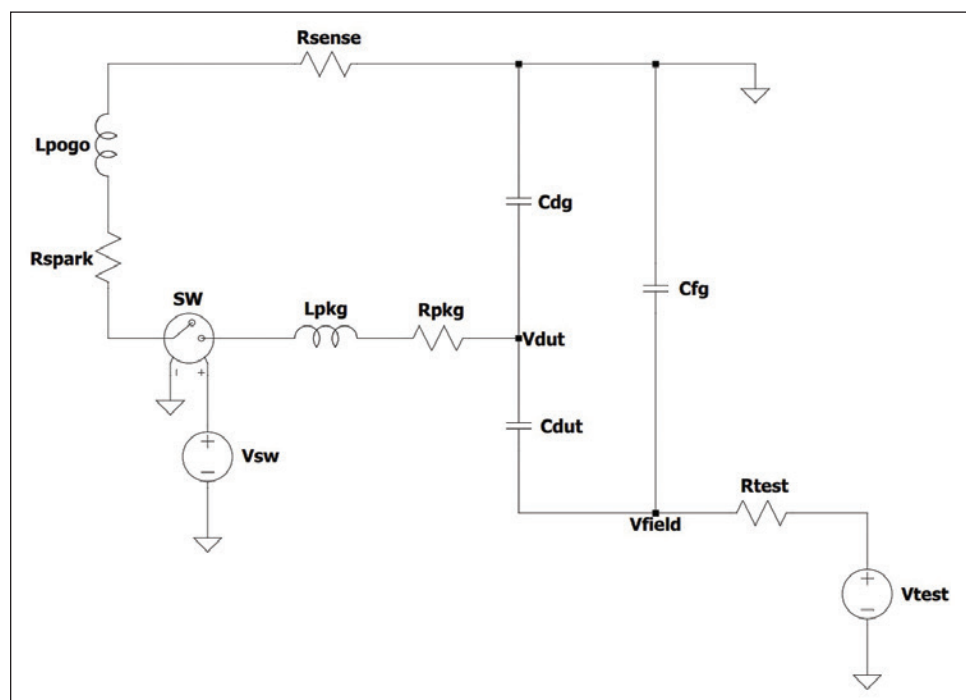


Figure 2: Spice implementation of the 3-capacitor circuit model.

However, a simple lossy transmission line (TL) already represents a good trade-off between accuracy and complexity, which can be included in the Spice model.

Figure 4 shows the comprehensive CDM tester model with two building blocks representing the distributed DUT model and the distributed discharge channel model (S-parameter or lossy TL).

A comparison of the current waveforms obtained with different models is shown in Figure 5, obtained with $V_{test} = -250\text{ V}$. The simple lumped model yields a smooth current waveform flowing through R_{sense} (blue dashed curve). A similar current behavior is obtained when including a distributed DUT model while keeping the RL channel (orange curve). On the other hand, including a distributed channel model allows the capture of reflections and delays that affect the current waveform (green curve), with variations in slope that could affect rise time-sensitive devices.

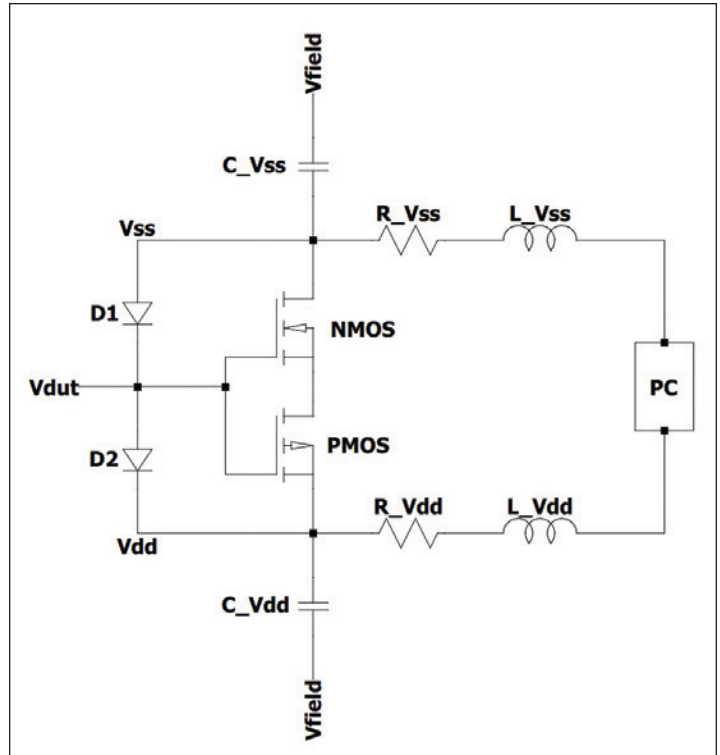


Figure 3: Distributed DUT model including resistance and inductance parasitics. The NMOS and PMOS gates represent the sensitive victims.

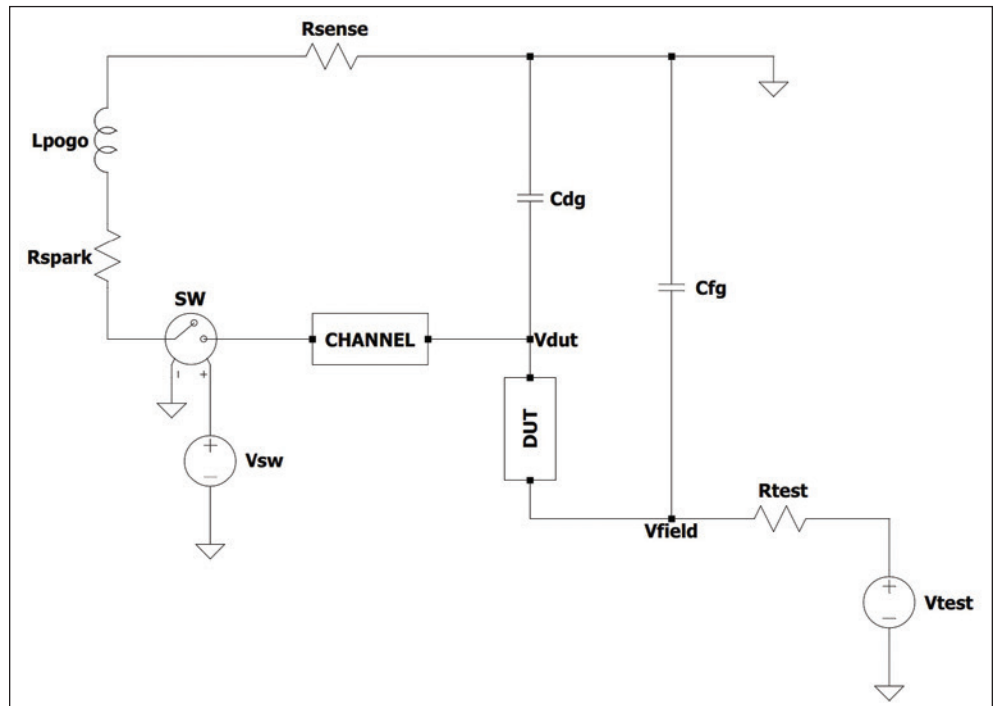


Figure 4: CDM tester model with distributed DUT and channel.

The voltage waveform at the input gate oxide can only be evaluated in the presence of a distributed DUT model. Hence, the following cases are considered in Figure 6:

- To model the voltage without on-die parasitics, a distributed DUT model with no inductance and resistance contributions on Vdd and Vss branches is considered. This yields the smooth voltage waveform indicated as “lumped” DUT (blue dashed curve) with a low peak voltage below 4V.
- The presence of on-die parasitic resistance and inductance in the distributed DUT model leads to an additional voltage drop and increases the peak voltage to more than 6 V at the input gate oxide (orange curve).

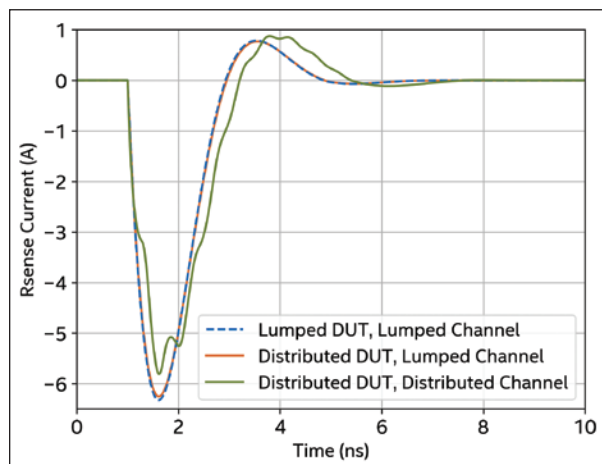


Figure 5: Current waveforms comparison.

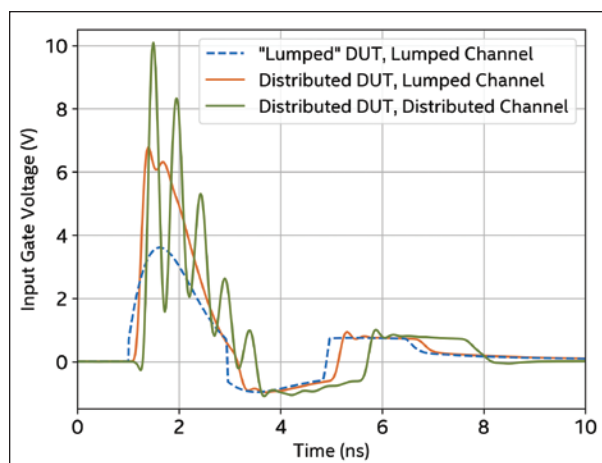



Figure 6: Voltage waveforms at the gate oxide.

- More severe voltage spikes up to 10 V are obtained by adding the distributed channel model on top (green curve).

These peak values must be compared against the gate oxide breakdown voltage to assess whether the device is able to withstand the targeted CDM stress. It clearly shows that the simple “lumped” model can be too optimistic for high-speed interfaces where ultrafast CDM transients can reach a thin gate oxide.

CONCLUSIONS

A simple lumped CDM tester model is suitable to evaluate the peak current at the I/O pads of the DUT for regular interface devices working at frequencies up to the low GHz range. However, fast transient phenomena such as current reflections and voltage overshoots can strongly degrade the overall CDM robustness when considering high-speed interfaces working at frequencies beyond 5 GHz. This is due to their capability to conduct ultrafast transients of the CDM pulse to the input gates. More complex distributed models are required to capture these phenomena, offering a methodology to assess the ESD performance of such designs. 

REFERENCES

1. ANSI/ESDA/JEDEC JS-002-2022, “Joint Standard for Electrostatic Discharge Sensitivity Testing – Charged Device Model (CDM) – Device Level.” <http://www.esda.org/standards/esda-documents>
2. Shukla, Vrashank, et al., “Predictive Modeling of Peak Discharge Current During Charged Device Model Test of Microelectronic Components,” 2013 35th Electrical Overstress/Electrostatic Discharge Symposium, IEEE, 2013.
3. Atwood, Bruce C., et al., “Effect of Large Device Capacitance on FICDM Peak Current,” 2007 29th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), IEEE, 2007.
4. Ishfaq, Umair, et al., “Advanced CDM Simulation Methodology for High-Speed Interface Design,” 2022 44th Annual EOS/ESD Symposium (EOS/ESD), IEEE, 2022.

USING A NEAR-FIELD PROBE TO TROUBLESHOOT TRANSIENT FAILURES

By Dr. Min Zhang

Solving EMI problems isn't only about ensuring that a product can meet EMC regulations and standards (although it's a significant part of the job). Another crucial reason for addressing EMI issues is to enhance product reliability, especially when a product operates in public or industrial areas where there are many different types of noise sources.

European and international immunity standards are based on typical operating environments and statistical data. Meeting these standards should be considered the minimum requirement for reliable equipment operation in the real world, given the increasing electromagnetic interference levels.

A product that incorporates EMC considerations from the beginning may not necessarily perform better, but its immunity to interference will improve its reliability in the field and make installation easier. This also leads to fewer service calls, particularly those troublesome "no fault found" cases that consume valuable time. It also reduces warranty costs and enhances customer perception, resulting in increased repeat business.

CASE STUDY: FIXING INTERMITTENT TIMER RESETS

A recent case illustrates this point. A product installed in an industrial kitchen environment experienced frequent timer resets, causing significant downtime and frustration for the manufacturer. After sending their engineers to the field multiple times, they gave up and tried to seek some expert advice on this.

To address this intermittent issue, the first step was to analyze the ambient electromagnetic noise. In such environments, various devices like fans and pumps are typically driven by variable speed drives (VSDs), which can produce noise ranging from a few kHz to about 100 MHz. However, these noise sources are usually continuous and don't align with the intermittent timer trip outs.

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



Another characteristic of such environments is that inductive loads, like motors and relays, generate voltage spikes or kickback voltages each time they're switched off. These spikes can appear on the public mains network and also signal lines (via near-field



Figure 1: Using an EFT/Burst generator for troubleshooting

coupling). The IEC 61000-4-4 standard tests such phenomena using electric fast transient (EFT) events coupled to the device under test (DUT) via a CDN (to the power port) or a capacitive coupling clamp (to the signal port).

In this case, the second characteristic seemed to align more with the field failures. To troubleshoot a potential transient failure, an EFT/Burst generator or an ESD simulator was needed. (An ESD simulator set to 10 or 20 pulses per second may be used to approximately simulate EFT pulses as suggested in [1], though the pulse shapes between the two types are quite different.)

Not all companies have an EFT/Burst generator or a capacitive coupling clamp, but one can rent a generator from a specialized EMC rental company. A quick way of testing the signal port without using a clamp is to directly connect the CDN output of the EFT generator to the signal port while keeping the voltage level moderate (starting with 200V and staying below 1kV). That approach proved effective in this case (Figure 1).

FINDING THE FAILURE SOURCE

When the failures were reproduced, the next step was to identify the weak point on the PCB. A useful technique involves connecting the HV output of the EFT/Burst generator to a near-field probe. Engineers can then inject noise into suspected weak areas on the PCB while taking HV safety precautions:

- Ensure the coaxial cable connected to the EFT/Burst HV output uses a suitable connector (e.g., SHV) due to the HV nature.
- If a commercial near-field probe designed for HV operation isn't available, engineers can create their own probe, ensuring proper insulation.
- The ground side of the loop must be securely connected to the shield of the coax from the pulse generator to prevent open circuit voltage issues.
- When using a near-field probe, it's advisable not to exceed 1kV of the EFT/Burst generator's output.

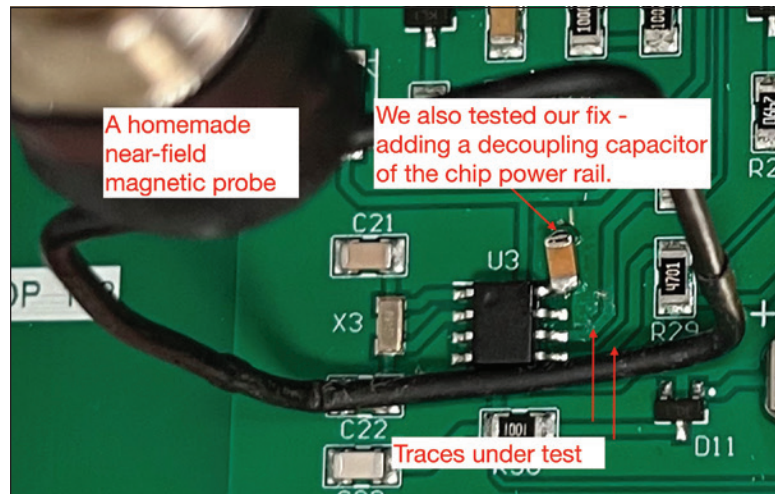



Figure 2: Using a near-field probe to inject pulses

SOLVING THE PROBLEM

Using this approach (see Figure 2), I found that moving the near-field probe (a homemade unshielded magnetic field loop) close to a trace that runs beneath the timer chip repeatedly triggered a timer reset error. This occurred due to the parallel orientation of the probe's conductor to the trace, resulting in strong near-field magnetic field coupling. Because the mutual coupling between the trace and the near-field loop conductor is less than unity, one can expect a similar pulse voltage (but with less amplitude) to be induced on the trace being investigated. If such a trace could cause problems, it indicates the need for a redesign to resolve the issue.

In this case, we provided the following recommendations for fixing the issues:

1. Adding ferrite cores on the signal input cables.
2. Adding a decoupling capacitor (100nF) on the power rail of the chip, as shown in Figure 2.
3. For the next revision of the PCB, re-route critical traces, adding C-L-C filters on the signal ports. 

REFERENCES

1. Ken Wyatt, *Workbench Troubleshooting EMC Immunity (Volume 3)*.
2. Douglas C. Smith, "Noise Injection for Design Analysis and Debugging." https://emcesd.com/pdf/DC09_DCSmith.pdf

Banana Skins

437 Financial costs of delayed EMC compliance

A manufacturer of electrical test equipment took an order worth several million dollars for new product to be used worldwide to help service the vehicles manufactured by a major multinational. It failed to meet the EMC standards required for compliance (which had also been made a part of the contract).

Testing and consultancy to discover the causes and find do-able fixes for the EMC problems (several low-cost options not being possible due to the late stage of the project) cost around \$20,000; iterating the PCBs to a compliant build standard cost around \$60,000; and refurbishing non-compliant units already supplied to the customer cost around a further \$70,000.

The delivery of the (eventually) EMC-compliant units was also delayed by five months from the target date, causing equivalent delays in receiving the first payments and incurring greater costs of financing the project (by putting the financial break-even point back around half a year on what was intended to be an 18 month project). Whether any harm has been done to the test equipment manufacturer's reputation with their customer, or with the marketplace as a whole, remains to be seen.

(A contribution in June 1999, the source wishes to remain anonymous.)

438 Pump at ski resort causes interference

In 1996, a ski resort near Silverthorne, Colo, installed a pumping system to lift water up to a river, whose water flows into a lake at the base of the resort and is then used on the mountain for snowmaking. At that time, the pumping system consisted of a 350-hp, 480VAC,

3-phase, SCR, variable-frequency drive (VFD), which was located at the base village. Because the pump and motor were positioned 900 feet below the river and VFD, the resort used 4,1560V as the distribution voltage from the VFD to the motor and pump. The power source for the pumping system was, and still is, a 1000kVA transformer fed by a 25kV, 3-phase overhead power line located five miles from the ski resort. This line also runs beyond the pumping system and serves a local community.

This pumping system worked well for several years with only the 350-hp pump, but as the ski resort expanded its snowmaking system, more water was needed. As a result, a 750-hp VFD, pump, motor and new pipe to the river were installed in 2002. At this point some real operational problems surfaced.

During the 2002-03 ski season, the resort could not run the 750-hp VFD at full capacity by itself, let alone together with the 350-hp VFD running at full capacity. The drives would drop off-line because of their under-voltage protection. Another concern was that homeowners and businesses in the area and nearby community complained of flickering lights.

(Extracted from: "Solving a Power System Compatibility Problem," Vaughn DeCrausaz, EC&M, June 1st 2006, <https://ecmweb.com>. The rest of the article describes how the problem was solved with careful measurement and the application of reactive power factor correction to achieve a unity power factor for the VFD systems.)

439 Electric 'bum' hazards

I've been reading up on various standards relating to test equipment safety and stumbled across BS EN 50110-1 1996 section 3.1.6 Injury (electrical) which cites "electric bum" as a potential hazard! I zoomed in and re-read it several times, it's definitely B U M and not B U R N.

'Electric bum' sounds quite painful, I'm definitely taking all the necessary precautions to avoid that one!

(Sent in by James Toddington of BAE Systems Electronics & Integrated Solutions, Rochester, 9th May 2007.)

440 Switching of power-factor correction capacitor interferes with contactor

A case study illustrates negative impulses of 366V followed by positive impulses of 420V at the terminals of a LV load when a power factor correction capacitor was switched on within an adjacent installation. These transients caused a contactor within a switch panel to fail to latch correctly.

(From subclause 9.2 of IEC/TR 61000-2-14:2006, "Environment – Overvoltages on public electricity distribution networks," Clause 9: "Case Studies," <https://www.iec.ch>)

441 Interference from insulation breakdown caused by vibration

This case study shows how high levels of vibration in a three-phase induction motor could cause insulation breakdowns causing momentary earth-faults on one phase. The resulting short voltage peaks on the mains distribution networks caused frequent misoperation of electronic regulators.

(From subclause 9.3 of IEC/TR 61000-2-14:2006, "Environment – Overvoltages on public electricity distribution networks," Clause 9: "Case Studies," <https://www.iec.ch>)

442 Switching MV power factor correction trips LV circuit breaker

This case study concerns frequent operation on a circuit breaker protecting a PVC moulding plant, causing lost production. It was found that the cause was the switching of a 120kV power factor correction capacitor in the upstream substation.

(From subclause 9.4 of IEC/TR 61000-2-14:2006, "Environment – Overvoltages on public electricity distribution networks," Clause 9: "Case Studies," <https://www.iec.ch>)

443 Wireless interference problems in the home

Take a look at any Sunday newspaper's advertising section for stores that sell electronics, and it is clear that wireless devices are everywhere. Visit these stores and listen to the salespeople selling wireless local-area-networks (WLANs), cordless phones, and all else wireless to often-naïve consumers.

What salespeople fail to tell consumers is that before consumers buy the latest wireless gadget, they should make sure that it will function properly in their home environment. For an unknowing consumer, it can be frustrating to buy a microwave, a 2.4GHz cordless phone, a 2.45GHz video transfer system, and a 2.4GHz WLAN, and then find that only some work error-free once installed in the home.

Manufacturers often take the view that as long as their products are certified, interference is the other guy's problem. What most manufacturers fail to acknowledge is that the consumer ultimately ends up with the problem. Unfortunately, consumers don't necessarily know why it doesn't work, just that it doesn't. These devices often end up as returns or consumer complaints.

(Extracted from: "Residential Spectrum Management: The Manufacturer's Role," David A Case, *Compliance Engineering 2005 Annual Reference Guide*, pages 106-107.)

444 Interference with household appliances from living too close to a transmitter

Residents living near the ABC's main radio transmitter at Liverpool have complained repeatedly of interference from the powerful signals it emits, amid concerns that planners have overlooked the impact of electromagnetic radiation on the area. Residents in a new housing estate at Prestons, which is across the road from the tower, have had the signal from the ABC radio station 702 interrupting phone calls, throwing lines across television screens and turning electronic equipment on and off without warning.

"There would be music at the back of our phone calls," one resident, Arvin Prasad, said.

"Telstra kept saying it was not their problem but finally they fixed it. They put some kind of filter on the lines."

Another resident, Marina Baldin, said: "I had one of those touch lamps. It used to go off and on by itself. I got rid of it."

The Herald reported last week that the five AM radio transmitters at Homebush Bay will have to be moved because Planning NSW has given approval for a multistorey building 200 metres from the 2UE-2SM transmitter. No one is yet living at Homebush Bay, and the issue is who will pay the \$40 million cost of moving the transmitters.

But at Prestons people have been living for more than a year in two-storey houses within 350 metres of the ABC tower. The ABC broadcasts at 50 kilowatts – ten times the power of

the AM stations at Homebush. The packaging company Amcor, which is investigating a new plant on the old Liverpool showground site 400 metres away, commissioned a study which yielded alarming results.

Readings at ground level were well below safe levels for non-ionising electromagnetic radiation, but at five metres were above the safe limit. The company has been advised it would need to shield equipment in the factory to avoid malfunctions.

The ABC's director of technology, Colin Knowles, disputed the Amcor findings yesterday, saying the ABC's own testing at Prestons showed radiation levels were well below those permitted under Australian standards. "This is the same problem that airports experience. People complain about airport noise, but they build out near the airport," he said.

The ABC tower has been at Liverpool for 67 years. One resident who complained to the ABC was told to direct his concerns to Liverpool Council, which gave permission for the new housing development. A council spokesman was not available yesterday.

(Extracted from: "Neighbours find ABC has turned the radio up too far," Anne Davies, *Urban Affairs Editor, Sydney Morning Herald*, 24 February 2003. Also see: "Planning debacle forces radio towers to seek new home," 17 February 2003, <http://www.smh.com.au/articles/2003/02/16/1045330466812.html>, and "Government admits radio towers, units were too close", 18 February 2003, <http://www.smh.com.au/articles/2003/02/17/1045330538774.html>, also by Anne Davies in the *Sydney Morning Herald*.)

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

Advertiser Index

A.H. Systems, Inc.	Cover 2
Absolute EMC	41
AR	3
Coilcraft	11
E. D. & D., Inc.	7
EMC & Compliance International	27
ETS-Lindgren	Cover 4
F2 Labs	41
HV TECHNOLOGIES, Inc.	41
ISPCE 2024	Cover 3
Kikusui America, Inc.	13
Lightning EMC	41
Raymond EMC	21
StaticStop by SelecTech, Inc.	41
Suzhou 3ctest Electronic Co. Ltd.	15

Upcoming Events

February 15
mmWave Communications Technologies

February 28 - March 1
Battery Japan

March 12-14
EMV

March 14
EU Radio Equipment Directive Update

April 11
Adding UNII-4 Band to Previous UNII Approvals

April 21-24
A2LA Annual Conference 2024

April 30- May 2
IEEE International Symposium on Product Compliance Engineering (ISPCE 2024)

May 14
Annual Chicago IEEE EMC Mini Symposium

May 16
EMC Fest 2024

May 16
Japan Radio Regulations

Visit the In Compliance Events page for more events:
<https://incompliancemag.com/event-directory>

Thank you to our Premium Digital Partners



CALL FOR PAPERS

Annually, the IEEE International Product Safety Engineering Society (PSES) hosts a premier symposium (ISPCE) on current topics relevant to people who are challenged to make products safe and compliant with ever-changing global codes, standards, & regulations.

The fundamental activities covered in this symposium are critical aspects of virtually all Engineering endeavors AND they are now consuming greater time and attention from business leaders. This event provides an opportunity for inclusion and crosscompany collaboration that results in collective educational growth for all participants.

The Ask

- ✓ With so many recent regulatory changes, including the publication of a new National Electrical Code, record attendance is anticipated. Increase your recognition as an expert and contribute to IEEE.
- ✓ Support Product Safety Engineering Society by educating our audience of members & guests at ISPCE 2024.
- ✓ Submitting a presentation or formal paper is both a personally & professionally rewarding experience.
- ✓ Visit the Authors & Presenters page on the ISPCE 2024 website for author registration, comprehensive submission instructions, and the biography, paper and presentation templates to be used.
- ✓ Compliance Management - Technical and Documentation

Decorum

Educational presenters speaking at ISPCE 2024, are permitted to reference the company they represent and/or company activities, when necessary for context within their presentation.

However, other promotional activities or sales should be conducted outside of the actual presentations.

Topics for ISPCE 2024

The IEEE international Product Safety Engineering Society seeks original and unpublished formal papers, presentations without formal papers, tutorials, and workshops on any and all aspects of product safety and compliance engineering - including, but not limited to:

- | | | | |
|--|--|--|---|
| » Arc Flash | » EMC & Wireless Compliance | » Field Inspections & Evaluations | » Introductory or Advanced Design for Compliance |
| » Batteries & Energy Storage Systems | » Emerging Technologies & Innovations | » Forensics, Failure & Risk Analysis | » Laboratory Safety |
| » Codes & Standards Development | » Energy Efficiency Codes Engineering & Safety Science | » Global Hazardous Locations | » Legal Regulations, Directives & Consumer Protection |
| » Compliance Management, Compliance and Technical Documentation Management | » Environmental Regulations, Sustainability & Circular Economy | » Global Market Access | » Medical Devices |
| » Cybersecurity | » Importance of Ethics for Effective Compliance | » Grounding & Bonding | » Product Labeling |
| » Data Center Safety | | » Hazard Based Safety Evaluations | » Safety of Education and Healthcare facilities |
| | | » Instrumentation and Laboratory Equipment | |

Important Dates

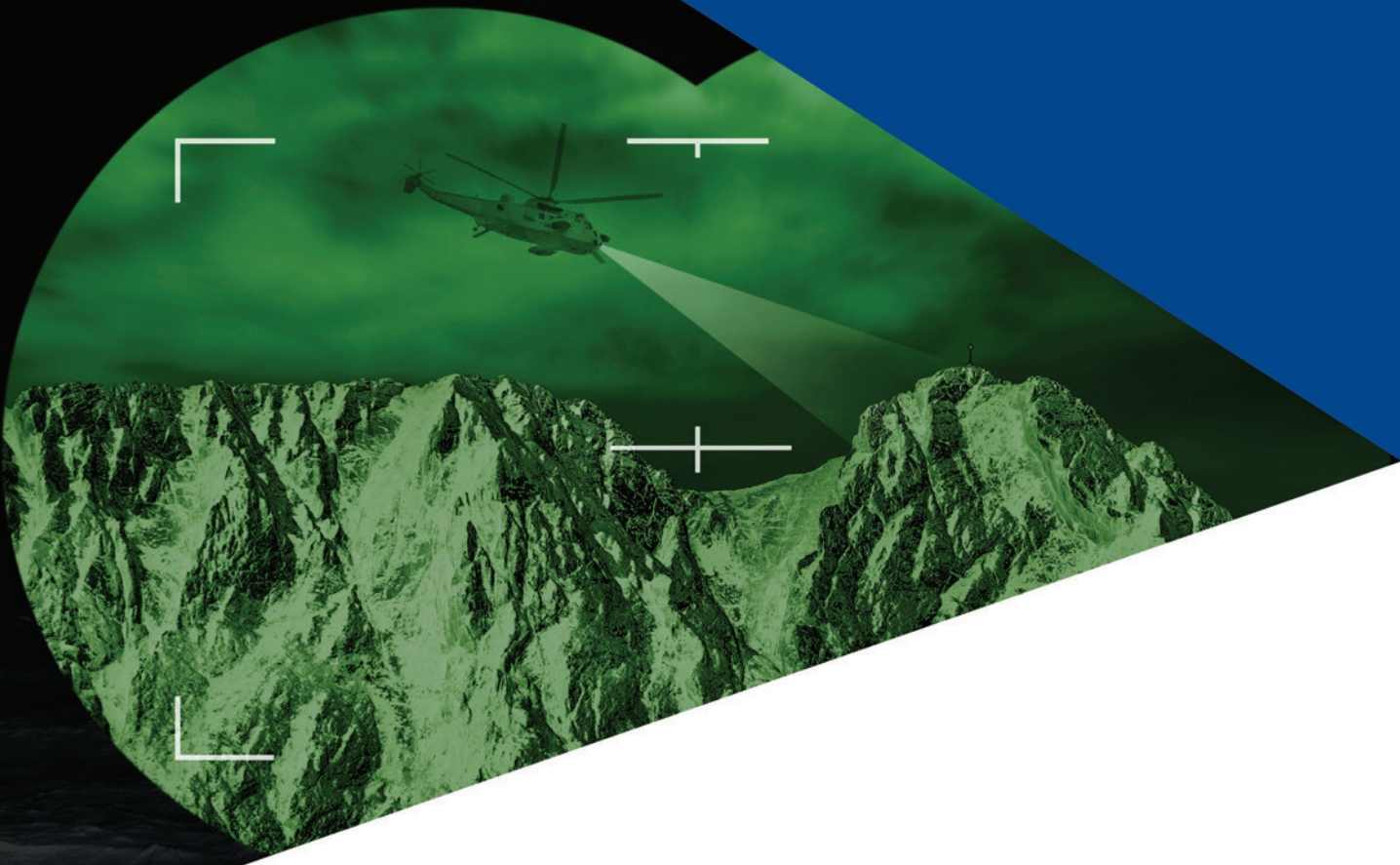
February 15, 2024
Formal Paper/Reviewable
Presentation Submission
Deadline

March 15, 2024
Acceptance Notification
Deadline

April 1, 2024
Final Paper/ Presentation
Submission Deadline

Conference Dates

April 30 - May 2, 2024



SILENT TECHNOLOGY: THE STRENGTH BEHIND OUR NATION'S SECURITY

Continuous innovation and a high level of quality are required to keep our nation secure and troops well supplied. From product inception to deployment, there are many requirements to delivering and deploying products to the field. ETS-Lindgren's Acoustic Research Lab can assist with MIL-STD-1474E tests to assist you in assessing the products that help keep our nation secure and troops well equipped.

NVLAP Accredited Testing Laboratory (Laboratory Code 100286-0) for MIL-STD-1474E – (Appendix C) Aural Non-detectability Requirements. A commercially-available third-party independent testing laboratory.

The right test environment – Ambient noise levels well below 0dB re 20 μ Pa from 125 Hz to 10000 Hz for accurate measurements. Precision Grade Test conditions to 2m.

Highly secure testing environment.

Optimized Multichannel test setup with low-noise microphones at all positions that can detect emissions down to -10 dB re 20 μ Pa in the mid-bands.

Experienced Test Personnel who have performed 100s of MIL-STD-1474E Aural Non-detectability tests. Fast turnaround on data summaries and test reports.

Ability to perform customized data analysis and results presentations if necessary.

Remove the uncertainty from your measurements with ETS-Lindgren, Committed to a Smarter, More Secure Future.

Connect with us at:



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

ETS·LINDGREN
An ESCO Technologies Company

Offices Worldwide | ets-lindgren.com

2/24 RR © 2024 ETS-Lindgren v1.0