MARCH/APRIL 2024 | mwrf.com

Microwaves&RF®

COMBATING IoT's CYBERSECURITY RISKS

Matchmaker

0402DC Series Designer's Kit (C472-2):
20 samples each of 112 inductance values,
including 0.1 nH increments from 2.8 nH to 10 nH

Looking for the perfect high-Q inductor for impedance matching in RF/microwave antenna circuits? This kit has it!

Coilcraft 0402DC Series wirewound chip inductors offer the industry's highest Q factors in an 0402 (1005) size for super low loss in high frequency circuits. And with 112 values from 0.8 to 120 nH, including **0.1 nH increments from 2.8 nH to 10 nH**, you'll have exactly what you need for all your RF and Microwave applications.

The 0402DC also features wirewound construction for extremely high self resonance – up to 28.8 GHz – and offers DCR as low as 25 mΩ, significantly lower than other inductors this size.

Equip your lab with the ultimate impedance matching resource. Our C472-2 Designer's Kit has 20 samples of all 112 values! Purchase one online at **www.coilcraft.com/0402DC.**

Coilcraft®
WWW.COILCRAFT.COM

coilcraftdirect.com
No min order. Next day delivery.

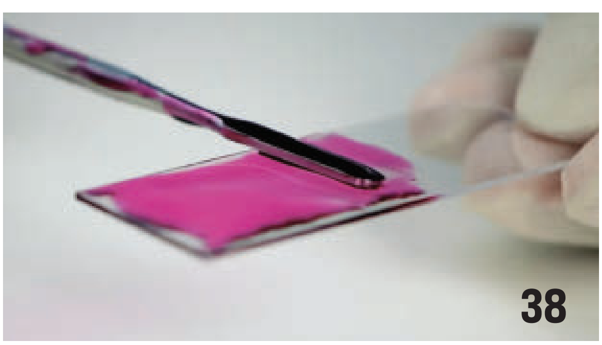
CONTENTS

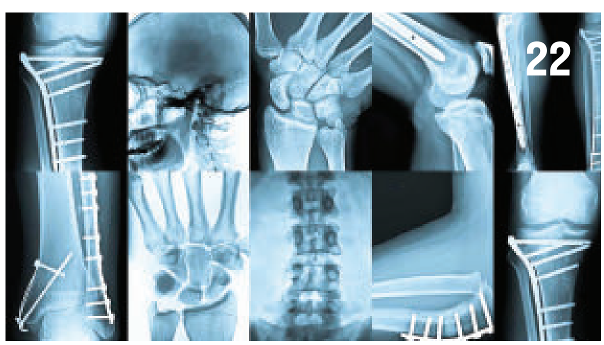
MARCH/APRIL 2024 | VOLUME 63, ISSUE 2

FEATURES

Cover photo credits:
bekisha_521421311 | iStock / Getty Images Plus
your_photo_1222889675 | iStock / Getty Images Plus

DEPARTMENTS





DAVID MALINIAK, Executive Editor

5G's Disparity Between **Promise and Reality**

It's time to grudgingly admit that 5G has been overhyped and underdelivered. Why has it not fulfilled its promise?

WE'VE BEEN TOLD for several years now that 5G technology is going to change everything about our interconnected digital lives. There's been reams of editorializing about it, particularly about mmWave 5G and how it will deliver insanely fast connectivity with minuscule latency. I've been as guilty of that as anyone among industry observers.

Certainly, 5G has been a moneymaker for service providers. One market report estimates the global value of the 5G services market at $121.8B in 2023 and projected at $1,002.3T by 2028. From those market numbers, one might extrapolate that 5G is ubiquitous and successfully bearing out its early promise.

Sadly, though, the reality is different from what the hype promised, and its past time to reckon with that reality. As of today, 5G hasn't been the game-changing technology envisioned for enterprises. But why not?

Why 5G hasn't met expectations:

- *Slow rollout*
- *Lack of compelling use cases*
- *Technical limitations*
- *Infrastructure challenges*
- *Return-on-investment concerns*

290014294 © Dmytro Zaharchuk | Dreamstime.com

For one thing, coming as it did during the pandemic, the rollout took forever and is still ongoing in much of the world. Even where rollout has been reasonably successful, such as in India (165M users between the top two carriers), monetization lags due to the lack of truly compelling use cases for 5G.

Here in the United States, a big difference exists between what 5G users were being sold and what they got. Verizon, which spent some $45B on spectrum when the FCC auctioned licenses in 2021, touted mmWave 5G as the "be all, end all" of connectivity. Of course, mmWave 5G delivers extremely high data rates, but it was quickly revealed to be too limited in range for many use cases in which it would be beneficial.

The infrastructure buildout itself has proved more difficult, time-consuming, and expensive than carriers bargained for. Urban and suburban regions require a great deal of equipment for adequate coverage. It's going to be a while before carriers get rural areas fully built out, as the return on investment (ROI) will suffer.

If you look at the history of rollouts for successive generations of cellular technologies, it's fair to say that the odd-numbered generations have fared rather poorly in terms of ROI. For millions of cellular users, 4G is still the best bet—sometimes 4G data rates are faster than low-band 5G rates anyway. It could well be that 5G suffers the same fate as did 1G and 3G, serving as placeholders until technology matured in the 2G and 4G eras. If you're waiting for a 6G bailout, please don't hold your breath. ■

dmaliniak@endeavorb2b.com

EDITORIAL ADVISORY BOARD

AD INDEX

Microwaves&RF

mwrf.com

EDITORIAL

Group Content Director: Michelle Kopier
mkopier@endeavorb2b.com

Senior Content Editor: Bill Wong
bwong@endeavorb2b.com

Executive Editor: David Maliniak
dmaliniak@endeavorb2b.com

Managing Editor: Roger Engelke
rengelke@endeavorb2b.com

Editor-at-Large: Alix Paultre
apaultre@endeavorb2b.com

Senior Staff Writer: James Morra
jmorra@endeavorb2b.com

Technical Editor: Jack Browne,
jack.browne@citadeleng.com

ART & PRODUCTION

Group Design Director: Anthony Vitolo

Art Director: Jocelyn Hartzog

Production Manager: Brenda Wiley

Ad Services Manager: Deanna O'Byrne

AUDIENCE MARKETING

User Marketing Manager: Debbie Bouley
dbouley@endeavorb2b.com

Article Reprints:
reprints@endeavorb2b.com

LIST RENTAL

Smartreach Client Services Manager:
Kelli Berry, kberry@endeavorb2b.com

DIGITAL & MARKETING

VP Digital & Data Innovation: Ryan Malec

SALES

AL, AR, SOUTHERN CA, CO, FL, GA, HI, IA, ID, IL, IN, KS, KY, LA, MI, MN, MO, MS, MT, NC, ND, NE, OH, OK, SC, SD, TN, UT, VA, WI, WV, WY, CENTRAL CANADA:
Jamie Allen, jallen@endeavorb2b.com

AZ, NM, TX: Gregory Montgomery
gmontgomery@endeavorb2b.com

CT, DE, MA, MD, ME, NH, NJ, NY, PA, RI, VT, EASTERN CANADA:
Elizabeth Eldridge
eeldridge@endeavorb2b.com

AK, NORTHERN CA, NV, OR, WA, WESTERN CANADA, AUSTRIA, BELGIUM, FRANCE, GERMANY, LUXEMBURG, NETHERLANDS, PORTUGAL, SCANDINAVIA, SPAIN, SWITZERLAND, UNITED KINGDOM:
Stuart Bowen,
sbowen@endeavorb2b.com

ITALY: Diego Casiraghi,
diego@casiraghi-adv.com

PAN-ASIA: Helen Lai
helen@twoway-com.com

PAN-ASIA: Charles Liu
liu@twoway-com.com

ENDEAVOR BUSINESS MEDIA

ENDEAVOR BUSINESS MEDIA, LLC

30 Burton Hills Blvd., Suite 185.,
Nashville, TN 37215 | 800-547-7377

CEO: Chris Ferrell

President: June Griffin

COO: Patrick Rains

CRO: Paul Andrews

Chief Digital Officer: Jacquie Niemiec

Chief Administrative and Legal Officer: Tracy Kane

EVP, Design & Engineering Group: Tracy Smith

DESIGN & ENGINEERING GROUP

Electronic Design, Machine Design, Microwaves & RF, Power & Motion, SourceESB, Source Today, 3DX

Microwaves & RF Magazine ID Statement 2024:

Microwaves & RF, ISSN 2162-1411 online, is published 6 times a year (January/February, March/April, May/June, July/August, September/October, November/December) by Endeavor Business Media, LLC, 201 N Main St, 5th Floor, Fort Atkinson, WI 53538.

POSTMASTER: Send address changes to Microwaves & RF, PO Box 3257, Northbrook, IL 60065-3257. **SUBSCRIPTIONS:** Publisher reserves the right to reject non-qualified subscriptions. Subscription prices: U.S. $68.75 per year; Canada/Mexico $81.25 per year; All other countries $93.75 per year. All subscriptions are payable in U.S. funds. Send subscription inquiries to Microwaves & RF, PO Box 3257, Northbrook, IL 60065-3257. Customer service can be reached toll-free at 877-382-9187 or at microwavesRF@omeda.com for magazine subscription assistance or questions.

Video► Containers Speed Embedded Software Development

A collaboration between MicroEJ and NXP Semiconductors has resulted in the NXP Platform Accelerator, which promises easier integration, faster time-to-market, scalability, and portability to users of NXP's processors.
www.mwrf.com/21284793

Video► Four-Port Single-Sweep VNA Serves D- and G-Band Apps

Anritsu's VectorStar ME7838x4 broadband vector-network-analyzer (VNA) systems provide four-port measurements. According to the company, they offer better calibration stability and better measurement stability with significantly longer time between calibrations.
www.mwrf.com/21275986

CONNECT WITH US

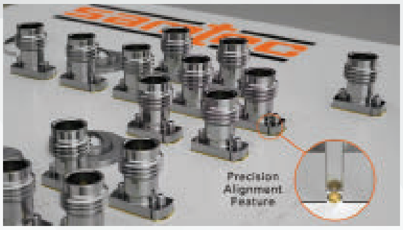
www.facebook.com/microwavesrf

@MicrowavesRF

linkedin.com/groups/3848060/profile

www.youtube.com/@engineeringtvEBM

Visit *www.mwrf.com* for more information on stories in this issue, plus exclusives on pertinent topics in the RF, Communications, and Microwaves Technology industry.



Improve Alignment of Compression-Mount Connectors in Wireless Designs

This article explains how compression-mount connectors are used in RF and microwave systems and why alignment is so important, and then examines the impact of misalignment on performance.
www.mwrf.com/21285333

MWC 2024: A Showcase for the Latest Wireless Solutions

Recently, the wireless community came together at GSMA MWC (Mobile World Congress) Barcelona 2024, one the world's most influential connectivity events, with a combination of an exhibition, conferences, and the largest gathering of policymakers enabling the digital economy.
www.mwrf.com/21284654

Matter Underpins the Future of the Smart Home

In the rapidly evolving smart-home landscape, the Matter connectivity standard emerges as a beacon of promise, offering consumers enhanced security, reliability, and seamless experiences.
www.mwrf.com/21284175

dB Control's

2-46 GHz GaN & TWT

MPMs Meet Your Critical Requirements

High-Performance Microwave Power Modules for Radar, EW, ECM, Data Links, Secure SATCOM

- Form, fit, function replacements
- QUAL-by-SIM opportunities
- Air-, liquid- or conduction-cooled
- Continuous wave or pulsed power
- Designed to meet SWaP-C requirements
- Modular design for easy customization
- Multiple prime power options (270-280 VDC, or AC 3-Phase)

C, X, Ku, Ka and Q-Band TWT MPMs, CW or Pulsed

2-18 GHz GaN SSPA MPM, up to 200W CW or Pulsed

dB Control
a HEICO company
Reliability by Design®

For specs and customization info, call **510-656-2325**
or email **info@dBControl.com**
www.dBControl.com

SCAN ME: MPM24

IMS
Connecting Minds. Exchanging Ideas.

See us at IMS Booth 2112

Photo courtesy U.S. Air Force photo/Master Sgt. Kevin J. Gruenwald

LATEST NEWS

Wireless MCUs Ready for Incoming Cybersecurity Regulations

STMicroelectronics' highly integrated chips handle a range of wireless technologies and the latest security standards.

SUPPORTING MULTIPLE WIRELESS technologies and the latest security standards, STMicroelectronics' new short-range wireless microcontrollers are all-in-one components that enable wearables and smart objects to become more miniaturized, easy to use, and secure. The cost-effective MCUs leverage short-range wireless technologies like Bluetooth LE, Zigbee, and Thread to connect smart devices to home bridges, gateways, and controllers, including smartphones.

The STM32WBA5 family offers a compact one-chip solution that reduces the bill of materials and shortens time-to-market. It accomplishes those goals by relieving wireless design challenges while being compatible with the development tools and software packs of the STM32 microcontroller development ecosystem.

The flagship STM32WBA55 microcontroller can communicate using multiple protocols simultaneously, like Bluetooth LE 5.4, Zigbee, Thread, and Matter. ST also supports the latest Bluetooth LE Audio specifications, enabling next-generation products that offer a better listening and hearing experience, including Bluetooth Auracast.

"Lead customers are already appreciating the enhanced wireless performance, flexibility, and security of our latest STM32WBA wireless microcontrollers," said Benoit Rodrigues, Wireless MCU Division General Manager, STMicroelectronics. "They are creating diverse products including smart thermostats, tracking devices, smart chargers, headsets, power tools, and smart meters."

STMicroelectronics

He added, "The extensive software ecosystem that provides communication stacks, microcontroller-specific software packs, sample code, and tools helps developers bring new products to market based on these MCUs quickly and efficiently."

Satisfying SESIP and Other Upcoming Mandates

Presented as the first wireless MCU currently available that can achieve the important SESIP (Security Evaluation Standard for IoT Platforms) Level 3 security certification, products based on STM32WBA microcontrollers can satisfy the U.S. Cyber Trust Mark and EU Radio Equipment Directive (RED) regulations due to become mandatory in 2025. The company will also introduce a ready-to-use module with the STM32WBA and all necessary external components, including a power supply and antenna-balancing circuitry.

Olivier Hersent, CEO, Abeeway (Actility Group), said, "We work with smart asset-tracking devices which are connected through Bluetooth to mobiles and through mobile apps to the cloud, enabling us to deliver complete asset-tracking management for our customers. ST's microcontrollers bring wireless connectivity to our multi-mode trackers.

"We have selected the new wireless connectivity product, STM32WBA5, for its enhanced performance with ultra-low-power radio capabilities, which is key for our battery-powered devices. They ensure stable connectivity in the harsh industrial environment where we operate, combined with security that meets the highest industry standards."

Tom Roberts, CTO, Performance Designed Products (PDP), stated, "We believe that gaming peripherals should be as unique and accessible as the gaming community itself. ST and PDP have worked together through several video game generations, and we have used STM8 and STM32 devices for many years. ST products consistently provide the features we need in our highly competitive market segment.

"We recently selected ST's short-range wireless connectivity product, the STM32WBA5, based on the integrated MCU and Bluetooth low-energy technology, as the right solution for a new, groundbreaking game controller. The STM32WBA offered us an ideal combination of performance, peripherals, cost efficiency, and ecosystem support that enabled simple and fast development."

The STM32WBA54 and STM32WBA55 each contain a 100-MHz Arm Cortex-M33 core with TrustZone architecture and up to 1 MB of flash memory. Offering inherently low power consumption, they have a background autonomous mode and flexible power-saving states to extend operational battery life in portable products.

ST's latest 2.4-GHz radio is integrated alongside the MCU. It's the first to let the application control the RF output power, with an adjustment range of up to +10 dB to ensure reliable wireless connections even under adverse conditions. ■

Ingestible Thermo Sensor Performs Core Body-Temperature Monitoring

LEVERAGING A CONNECTED ingestible thermometer for Sports and Occupational Health Research applications, French MedTech BodyCAP has developed the eCelsius Performance Connect System. The solution has connectivity to smartphones and tablets provided by Insight SiP's ISP1807-LR RF module for continuous core body-temperature monitoring.

The thermometer is integrated into an ingestible capsule, which monitors and measures the core body temperature as it passes through the gastrointestinal tract. The innovative connected core body-temperature data-collection device will transmit data until it's expelled, which usually takes a couple of days but can last up to six days.

The eCelsius Performance research device uses a small 2-cm ingestible electronic capsule, accurate to within ±0.1°C, with a communication protocol for data security. The capsule transmits data via a sub-gigahertz radio to a wearable watch-type device. Called ePerf Connect, the wrist device relays data via Bluetooth, which can be read by any compatible system such as a smartphone or tablet.

Flexible ISP1807-LR Module

Chosen for its high memory capacity and flexible I/O set, the ISP1807-LR module enables the ingested capsule to relay information via Bluetooth in real-time every 15 seconds to 5 minutes. The ePerf Connect then records the data and triggers alerts if the threshold temperature is exceeded.

Insight SiP's ISP1807-LR RF module's compact size and low power consumption ensures unobtrusive integration with an extended operational life. The module offers a Bluetooth 5 stack along with IPv6 connectivity and Mesh capabilities.

According to Sébastien Moussay, co-founder & Chairman of BodyCAP, "Insight SiP's RF module is ideal for the connectivity of the eCelsius System, a complex application requiring fast, reliable processing and best-in-class power consumption. The module's small size made it ideal for our wearable gateway product, and the sophisticated features allowed it to form the core of this product. Our system is a breakthrough for research and medical applications in which measuring core body temperatures is key to symptom diagnosis and finding the best solutions for patients."

Dr Nick Wood, director, Sales & Marketing, Insight SiP, added, "We are proud to work with BodyCAP on its highly innovative eCelsius System and contribute our RF expertise and module to enable this connected medical device to provide patients with more effective diagnosis and optimal care." ■

Test Cases Certify Non-Terrestrial-Network Chipset

KEYSIGHT TECHNOLOGIES EXTENDED the number of test cases for Skylo Technologies' non-terrestrial-network (NTN) certification program to 21 in the Keysight RF/RRM Carrier Acceptance Toolset (RCAT). Offering developers new ways to certify 3GPP 5G Release 17 (Rel-17) NTN chipsets, modules, and devices, the test cases address narrowband Internet of Things (NB-IoT) solutions for Skylo's network.

Keysight and Skylo are creating seamless NTN certification testing solutions with tools to validate and certify products targeting these new networks for organizations such as the Global Certification Forum (GCF) and the PTCRB. The test cases cover radio frequency (RF) and functional performance aspects of NB communication unique to NTN, like the technical challenges posed by Doppler effects arising from the distance and relative speed between devices and satellites.

Real-World Emulation

The RCAT Skylo release addresses this by emulating real-world conditions, such as geostationary orbit, geosynchronous orbit, and the signal-to-noise-plus-interference ratio, balancing test complexity and real-world network emulation. Keysight and Skylo continue to collaborate on supplementary tests for future releases of Skylo's NTN certification program.

According to Ian Milne, Head of Quality and Standards at Skylo Technologies, "The journey between our two companies has been exceptional, and we are thrilled to witness the results, with our certification program gaining interest from key industry players. We eagerly anticipate continuing our collaboration with Keysight to achieve our shared goal of ensuring high-quality service to hybrid terrestrial and non-terrestrial networks, in which Skylo plays a key role."

Jose Ignacio Espinola, Director of NTN Certification Solutions at Keysight added, "Keysight is a pioneer in supporting the scale-up of NTN by using a combination of 3GPP and service provider standards to develop and prioritize certification testing.

"Our commitment is reflected in bringing advanced test solutions to market first, and we are leading certification efforts with every major vendor and chipset maker on testing critical aspects of satellite communications. This significant milestone with Skylo validates our efforts and inspires us to contribute continuously to the successful development of NTN." ■

Software/CPU Duo Yields Efficient, Flexible Open RAN Implementations

AMD's EPYC 8004 chipsets and Parallel Wireless's GreenRAN software platform combine to free Open RAN implementations from specific hardware requirements while also optimizing power efficiency.

AMD

The Overview: Open RAN Collaboration

Parallel Wireless is collaborating with AMD to pair its GreenRAN hardware-agnostic software platform with AMD's EPYC 8004 Series CPUs. The collaboration, it's hoped, will boost Open RAN adoption as it reduces end-product power consumption and frees OEMs from hardware constraints.

Who Needs It & Why: Those Seeking Interoperability

The Open RAN movement, which promises to break the shackles that bind network operators to monolithic providers of radio-access network (RAN) equipment, continues to make progress. Yet, it still seeks solutions that will leverage hardware-agnostic RAN software with processors optimized for edge and telecom use cases.

Use of the AMD EPYC processors with Parallel Wireless's GreenRAN software gives cellular network operators greater control over their components. The software operates seamlessly across various general-purpose CPUs, which represents a significant advance compared with earlier Open RAN solutions that were tied to specific hardware configurations. As a result, OEMs of Open RAN gain more of the openness and flexibility that was key to the Open RAN movement.

Under the Hood: Software & CPU Highlights

Both the software and the CPU bring attributes to the table that make the collaboration seem like a great fit as OEMs pursue the goals of innovation, scalability, and cost reductions.

Parallel Wireless's GreenRAN software suite includes its xApps Suite, which provides software-driven layer switch-off and MIMO channel shutdown. These capabilities give operators the ability to fine-tune network activity based on demand. Together, they form an intelligence layer that optimizes network cluster power efficiency while maintaining quality of experience in both uplink and downlink.

The xApps also optimize the user MIMO configuration between MIMO 4x4 and MIMO 2x2 while maintaining user-equipment channel quality. Shutdowns are performed in near real-time, which offers rapid response to frequent changes in network behavior. It all adds up to significant energy savings compared with older solutions.

For its part, AMD's fourth generation EPYC 8004 Series (Siena) processors are optimized for edge and vRAN deployments. They contribute high core counts and energy efficiency to the overall solution, both of which are integral to enhancing the performance, scalability, and cost-effectiveness of Open RAN hardware. Core counts range from 8 to 64 and number of threads from 16 to 128. Maximum boost clock rates are 3.1 GHz with base clocks ranging from 2 to 2.65 GHz.

In its collaboration with Parallel Wireless, AMD gains a stronger foothold in the telecom network market by aiding in the industry's ongoing shift to more flexible and adaptable architectures.

RF Power Transmitter Ushers Over-the-Air Wireless Charging into Homes

Powercast's RF power transmitter means to slash RF transmitting technology costs and make convenient, contactless power ubiquitous.

Powercast's Ubiquity RF power transmitter is hoped to make a pervasive presence of RF wireless power in smart homes. With this transmitter, Powercast claims to have lowered the barrier to entry into having multiple RF wireless power transmitters covering every home.

The idea of the Ubiquity transmitter is to make wireless charging a "set-and-forget" proposition, much like Wi-Fi. Powercast's over-the-air wireless power architecture has two sides:

- A transmitter sends RF over the air.
- A receiver embedded in end devices harvests that RF from the air and converts it into dc (direct current) to both communicate data and power devices.

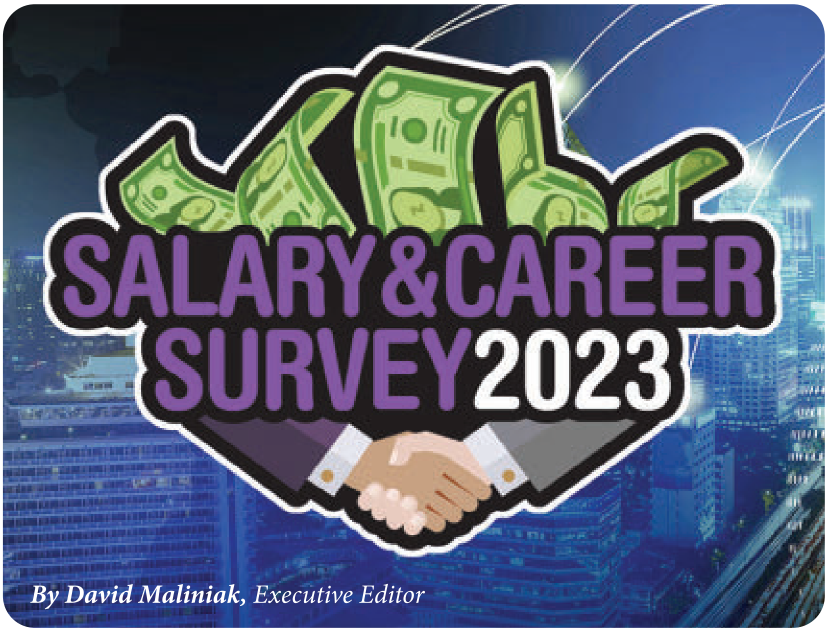
On the transmitter side, Powercast's Ubiquity will come in several forms, all able to both charge RF-enabled devices and communicate data back and forth with them throughout a home. Manufacturers have two options to turn their own products—such as home appliances, TVs, game systems, computer monitors or AI-enabled home assistants—into Ubiquity RF transmitters:

- A licensable reference design provides flexibility and ultimate cost savings for manufacturers to integrate just the electronics needed onto their own circuit boards for $5 or less bill-of-materials (BOM) cost.
- An easy-to-integrate, drop-in embeddable module contains all of the electronics and hardware needed. Manufacturers will add a power supply and antenna. Powercast will work with manufacturers on an antenna design that best fits their specific product size.

On the receiving side, manufacturers can embed Powercast's tiny Powerharvester PCC110 receiver chip and a small antenna into their end devices for around $1 to enable them to work with an RF transmitter—either Powercast's standalone Ubiquity, or RF-transmitting products created using the Ubiquity embeddable module or reference design.

This wireless power-over-distance architecture is perfect for charging low-power devices with continuous, reliable, background trickle charging. End-device examples include TV remotes, electric toothbrushes, keyboards and mice, game controllers, earbuds, headphones, smart watches, fitness bands, hearing aids, clocks, electric shavers, home-automation devices, and many other applications.

The Ubiquity transmitter can output up to 1 W (3 W EIRP) and automatically charges multiple RF-enabled devices that come into its charging zone, with no charging mats needed. Power-hungry devices charge faster within several feet of the transmitter, while ultra-low-power devices like IoT sensors can charge up to 120 feet.



How Do You Stay on **Top of Technology?**

Technology marches on, but are you lagging in your proficiency? Our 2023 Annual Salary and Career Report survey provides a glimpse into the state of continuing engineering education.

WHEN ASKED ABOUT challenges in staying up to date with evolving technologies, one respondent to our *2023 Salary & Career Report* survey answered in a way that may be indicative of industry employment trends: "I'm expected to be current in a wide range of disciplines because of under-resourcing and hiring of junior engineers who need mentoring and bring little to the table initially."

If this situation sounds familiar—needing to wear multiple hats even as you help new talent—then you've got to somehow find time to learn about new technologies. It could be what enables you to prove your value to your organization, both through innovative work of your own and in getting newcomers up to speed.

Needing to scramble to accommodate accelerating change, with precious little time to do so, is a perennial requirement for electronic design engineers. Our survey asked about your current level of education and your preferred means of learning new tricks. We wanted to know whether your employer pays for continuing education, and if so, in what modes?

In this article, we'll look at these topics with facts, figures, and representative anecdotal responses. Bear in mind that for most questions, we asked you to "select all that apply," so results won't necessarily add up to 100%.

Education Levels on the Rise

How well are engineers educated, and how do this year's results compare with the 2022 survey? The largest chunk of respondents holds a master's degree (33.3% vs. 32% in 2022). Then there's 25.6% with bachelor's degrees (22% in 2022).

Respondents with a bachelor's degree plus some graduate studies are at over 14% this year, a slight increase from last year. Doctorates made a bit of a comeback in 2023 at nearly 13% vs. last year's 11%. Overall, current education levels are improving year-on-year compared to last year's survey results.

Educational Options Abound

Regardless of whether you graduated from a prestigious technical college or worked your way up from the mailroom, there's no getting around the need to refresh your knowledge and skills. So, as we do each year, we asked, "What are some of the ways in which you continue your engineering education?"

While last year was something of an off year for continuing education, this year's results indicate that more of you are taking advantage of opportunities to learn and grow professionally. It's fair to say that coming out from under the pandemic cloud could be the reason.

As usual, we've asked about your usage of various modes of education. You can always count on industry vendors to produce webcasts, videos, and white papers in large volumes. These items are invariably free for the asking (or registering). Most webcast providers make their events available on demand if you've missed the live streams.

In 2023, your most preferred means of getting up to speed on technology is engineering videos (62.4%). That's followed by engineering/technology publications at 62.2%, a significant rebound from 47% in 2022. Last year's #1 option, seminars, fell to #3 this year, but it still climbed to 62% from 51% in 2022.

We broke out engineering/technology publications' websites in this year's survey, and 56.4% rely on those for news and information. White papers came in with 59% vs. 48% last year. You're turning to engineering textbooks more this year (48.7% vs. 35% in 2022); the same goes for eBooks (41% vs. 35% last year).

In-person education options are a mixed bag: Fewer of you are attending in-classroom college courses (11.3% vs. 14% in 2022) or showing up at user-group meetings and meetups (18.3% vs 20% last year). But your tradeshow/conference attendance rose from 26% last year to 29% in 2023.

We asked about a few new education modes this year, beyond publication websites. Some 34% of respondents avail themselves of vendor-sponsored events while 19% stop in at in-house education sessions sponsored by your employers. We wanted to know if you take advantage of online tradeshows/conferences, and about 17.6% say they do. Another category of education mode that's resurfaced in the wake of COVID-19 is podcasts, with 15.3% tuning in.

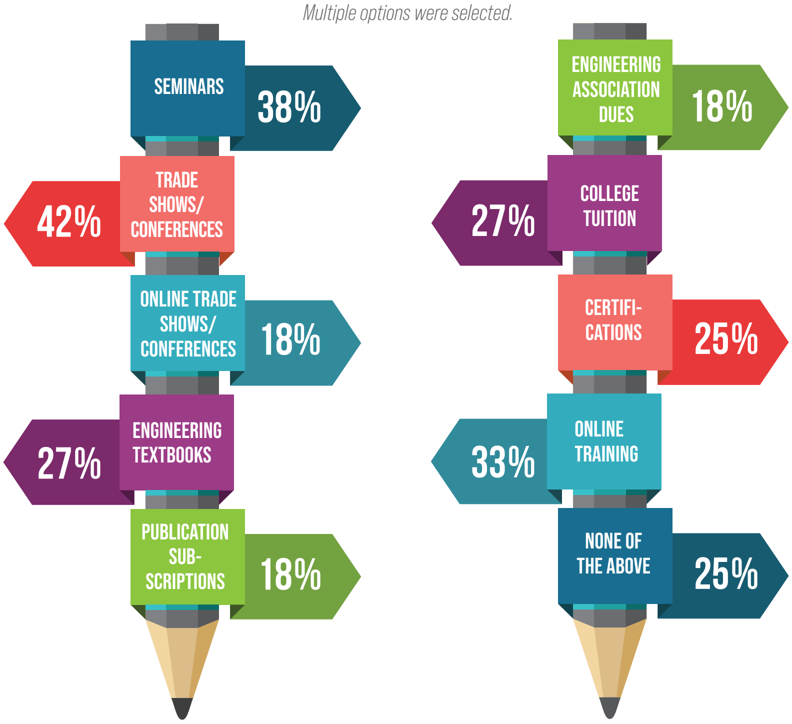
Some educational options are free of charge, but there's quite a few that are not. We asked whether your employers reimburse you for those costs. Sadly, 25% report that you're on your own in this regard. But over 42% say they'll recoup costs for attending tradeshows/conferences. Nearly 38% say the same about seminars, and about 32.5% get repaid for the costs of online training sessions. If you're taking college courses, over 27% get tuition costs back as well as costs for textbooks. Close to 18% are reimbursed for dues to engineering associations.

Time and Time Again

While fears of contracting disease have largely receded, enabling you to more readily attend shows, conferences, and seminars, lack of time remains the perennial thorn in the side of the knowledge hungry. Compared to the general population, electronic engineers are a well-paid lot, but your employers often get more than their money's worth out of you. That's clear from the number of anecdotal responses to our survey decrying the surfeit of time for continuing education.

For which of these forms of education does your company reimburse costs to engineers?

Multiple options were selected.



"[It's difficult to] make time available outside of work and personal time to stay current with advances in engineering and technology."

"[It's difficult to] make time available outside of work and personal time to stay current with advances in engineering and technology," said one respondent. "The technology moves along too fast to keep up," offered another, while a third observed, "Lots of information is becoming obsolete very quickly."

The imbalance between work and private life remains a concern for many engineers, as any time spent with technical journals or watching videos at home means less time for the family and/or friends. "Any study of new tech has to be done on my own time with my own funds," offered one respondent.

Then there's the problem of the sheer volume of material to be had. What's the source? What the heck do they know, anyway ("…sources who claim expertise when their knowledge is superficial")? Which material is useful now and which might be useful in the future ("…just filtering out the far-future stuff from that which might be relevant soon")?

The rate of technology change is a constant refrain among design engineers, who cite anxiety about keeping up with emerging technologies such as machine learning and artificial intelligence. "It's a matter of navigating hype-fueled spam, focusing on content relevant to my job," said one survey respondent. "It's about filtering out all the 'executive summary' and 'infomercials' promoted as educational for engineers (generalized puffery)," added another.

Without a doubt, staying abreast of technology trends and project-relevant information is a difficult endeavor. Here's hoping you're able to maintain and expand your knowledge base sufficiently in 2024 to keep you at the top of your game. ■

REGISTER NOW FOR IMS2024

Pack Your Bags!

"Capitol"ize Your IMS Experience:

- RF to Optical
- Systems Applications
- The Human Dimension

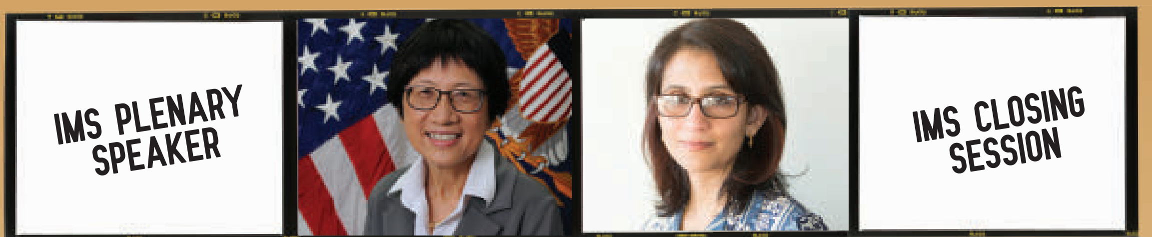
IEEE

MTT-S IEEE MICROWAVE THEORY & TECHNOLOGY SOCIETY

IMS & RFIC PLENARY SPEAKERS/ WEEK AT-A-GLANCE

Peter Vetter, (Nokia),
President of Bell Labs
Core Research

Prof. Tsu-Jae King Liu,
Dean of the College of
Engineering at UC Berkeley



Heidi Shyu
Under Secretary of Defense for Research and Engineering,
Chief Technology Officer for the Department of Defense

Dr. Monisha Ghosh
Professor of Electrical Engineering, University of Notre Dame, Policy Outreach Director for SpectrumX and Former Chief Technology Officer at the Federal Communications Commission (FCC)

WEEK AT-A-GLANCE

	Sunday 16-Jun-24	Monday 17-Jun-24	Tuesday 18-Jun-24	Wednesday 19-Jun-24	Thursday 20-Jun-24	Friday 21-Jun-24
Workshops	■	■				
RFIC Technical Lectures	■					
RFIC Plenary Session, Reception, Industry Showcase	■					
Quantum Bootcamp	■					
AI/ML Bootcamp	■					
RF Bootcamp		■				
WPT Bootcamp		■				
RFIC Technical Sessions and Interactive Forum		■	■			
Three Minute Thesis		■				
IMS Industry Showcase, Plenary and Welcome Reception		■				
IMS Technical Sessions			■	■	■	
Interactive Forum				■		
Panel Sessions		■	■	■	■	
Future G Summit				■		
Exhibition			■	■	■	
MicroApps and Industry Workshops			■	■	■	
Amateur Radio Reception			■			
Young Professionals Reception			■			
Industry Hosted Reception				■		
Women In Microwaves Reception			■			
IMS Closing Ceremony					■	
103rd ARFTG						■

Workshops   Technical Lectures   RFIC   Bootcamp   Three Minute Thesis   IMS
Panel Sessions   Future G Summit   Exhibit Hall Activities   Focus Groups   ARFTG

What's the Difference Between **Matter 1.0, Matter 1.1, and Matter 1.2?**

Across its three iterations to date, the Matter connectivity protocol has significantly expanded its reach. Learn what's new in the latest revision.

***By Rob Alexander,** Principal Product Manager - Matter, Silicon Labs*

IN 2019, AMAZON, APPLE, GOOGLE, and Zigbee Alliance members came together to form Project Connected Home over Internet Protocol (CHIP). That working group built a new standard that enables IP-based communication across smart-home devices, mobile apps, and cloud services, and ultimately unites the smart home.

In 2021, the Zigbee Alliance rebranded as the Connectivity Standards Alliance (CSA), and Project CHIP rebranded to Matter. These rebrands were necessary as the new Matter mark authenticates devices, ensuring that any object built on this standard is reliable by nature, secure by design, and compatible at scale.

Fast forward to today, and Matter is here! Officially released in October 2022, the Alliance and Matter have seen tremendous growth with 600+ members, 750+ Matter-certified devices, and multiple updates to Matter. Before we dive into these updates, let's learn more about the Matter standard and why Matter matters.

What Exactly is Matter?

Matter is an application-layer protocol developed specifically to address device interoperability within the smart home, more specifically across different smart-home device platforms. That means your Amazon Alexa can work with your Google Home or Apple HomeKit. Beyond interoperability, its other biggest benefits include simplified device setup, significantly better reliability and latency, and improved security through standardization.

Matter is designed to support existing protocols, such as Thread, Wi-Fi, Bluetooth Low Energy, Zigbee, and Z-Wave, bringing greater flexibility to manufacturers and consumers alike.

For developers, Matter simplifies product development while lowering development and operational costs. Because Matter is completely open source, anybody can read and propose changes to source code, resulting in collaboration from the industry, improved quality, and expedited processes.

With Matter, device manufacturers only need a single SKU per product instead of separate ones for each ecosystem. This reduces costs, shortens development and production time, and simplifies the entire supply chain.

Furthermore, consumers have the power to choose how they want to control their homes and with what devices—they're not limited to certain ecosystems. Consumers can have peace of mind when using their devices as privacy and security are central to Matter, with built-in encryption, over-the-air updates, and standardization to keep data safe.

Another benefit for consumers is simplified setup for new IoT devices in their homes. Matter uses a simple and secure onboarding process to connect new devices and is as easy as scanning a QR code to add a new Matter device. Lastly, Matter is compatible with existing devices—non-Matter-certified devices—via Matter bridges so that consumers can continue to use the devices they already have.

Matter 1.0: Certification Now Open

In 2022, the CSA launched Matter 1.0, along with eight authorized test labs for product certification, the test tools needed to certify devices, and the open-source reference design software development kit (SDK) to develop Matter devices.

Consumers started to see the first ever Matter-certified devices. The Matter 1.0 release supported a variety of common smart-home products, such as lighting and electrical, HVAC controls, window coverings and shades, safety and security sensors, door locks, media devices (including TVs), controllers as both devices and applications, and bridges.

In addition to new devices, Matter 1.0 enabled companies to upgrade existing, already deployed devices to Matter-certified devices via over-the-air updates.

Matter 1.1: Enhancements for Developers and Devices

May 2023 saw the release of Matter 1.1, an update with enhanced support for many smart-home products in the Intermittently Connected Devices (ICDs) category, also known as "sleepy devices." Typically, ICDs represent battery-powered devices like sensors, door locks, and switches that are connected via wireless networks and need to conserve power for optimal operation and lifespan.

ICDs aren't constantly connected. Rather, they "wake up" and connect periodically, drawing power and, thus, making energy efficiency vital. Matter 1.1 allows for ICDs to sleep for longer periods of time before checking in with parent devices without having to reconnect to the network. Fewer check-ins mean power conservation and longer battery life.

Matter 1.1 fixed many of the bugs from the initial launch of Matter, especially from the developer side. Given the code is publicly available and relies on an open-source SDK, it's important that these tools are easy to work with. In this update, the CSA gathered feedback from developers throughout the process to make clarifications on how to make the tools easier to operate, helping developers to work with Matter.

The CSA also launched a testing center in Portland that offers interoperability testing services to alliance members developing Matter products for certification. In addition, Silicon Labs launched its Connectivity Lab, which simulates a modern smart home, with a range of IoT devices, applications, ecosystems, and networks. Customers can test their Matter prototypes operating within real-world scenarios across a variety of protocols and device brands.

Matter 1.2: More Device Types

Fast forward another six months, and Matter 1.2 introduces new device types and brings other improvements that enhance interoperability and user experience. This release expands device types to washing machines, refrigerators, dishwashers, room air conditioners, robotic vacuums, air-quality sensors, air purifiers, smoke/CO_2 alarms, and fans. Matter 1.2 also adds key foundational elements to enable more device types, such as operational modes, that are important to adding more appliances in the future.

This is exciting as many of these devices tend to be Wi-Fi-enabled but often have limited ecosystem support and require proprietary app control. With Matter 1.2, manufacturers can simplify the user experience—including commissioning—while enabling integration into key smart-home ecosystems.

Matter 1.2 also includes new features that improve the user experience for commissioning to better identify the product and its description. For example, to help the user verify which device is the one they're interacting with, the color of the device is listed in the Matter controller's user interface. Or, a light with multiple bulbs can describe the location or position in a controller user interface to indicate which bulb is bound to a smart switch.

Final Thought: Matter 1.3 and Beyond Only Gets Bigger

Support for Matter will only continue to grow. In fact, Amazon has already added Matter to more than 100 million Echo and eero devices. The CSA has indicated that it hopes to share new Matter updates every six months, so we can continue to expect more Matter device types, specifically cameras and energy-management devices to further unify smart-home ecosystems, as well as more updates that help widespread adoption across the smart home. ■

What is the **12-Term VNA Calibration Model?**

Learn about the 12-term error model used to characterize systematic errors encountered during VNA measurements.

*By **Brian Walker,** RF Engineer, Copper Mountain Technologies*

This is the third in a multi-part series of articles on vector network analysis. Part 1 introduced the VNA, how such instruments work, and some of their applications in the lab. Part 2 introduced S-parameter network flow diagrams and how to manipulate them to solve real-world problems.

BECAUSE TEST CABLES experience loss and delay, vector network analyzers (VNAs) must be calibrated to make precise measurements. Those cable losses mean that phase measurements made at the VNA ports will not be the same as those made at the device under test (DUT).

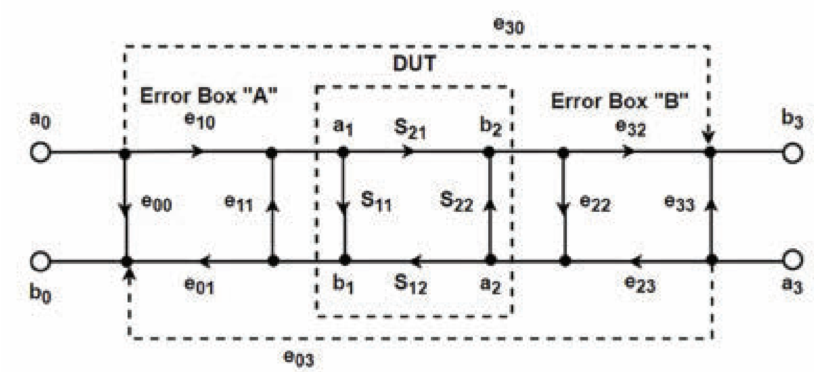
If the characteristic impedances of the test cables are not precisely 50 Ω, the effective source and load match of the VNA will be slightly off, resulting in measurement ripple. In addition, the directivity error in the VNA measurement bridges must be corrected to ensure accurate reflection measurements. This short primer will quantify the various systematic errors and introduce the 12-term error-correction model, which serves as a basis for VNA calibration.

The S-parameter network diagrams, as seen in the previous article in this series, will be used to describe the various error terms.

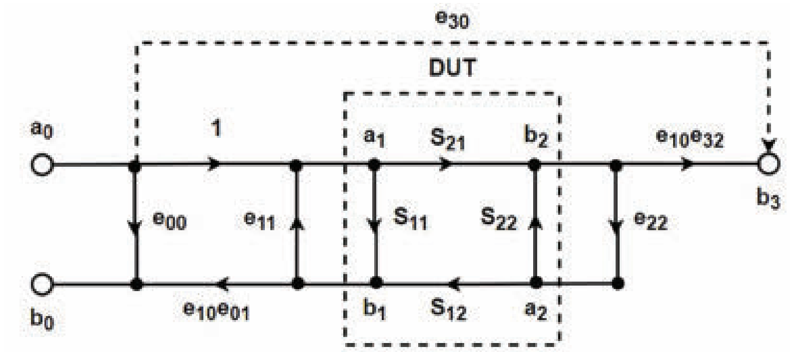
What is the 12-Term Error Model?

Our model starts with a perfect VNA. We create two error boxes and put them on either side of the DUT and attach the perfect VNA to the left and right sides of *Figure 1*.

Error box A is defined by its four S-parameters—e_{00}, e_{01}, e_{10}, e_{11}—and error box B by S-parameters e_{22}, e_{23}, e_{32}, and e_{33}. The DUT is defined by its S-parameters S_{11}, S_{12}, S_{21}, and S_{22}. The S-parameters measured by the perfect VNA attached to the system, S_m, are altered by error boxes A and B. The isolation terms e_{30} and e_{03} are usually small and may be ignored for the moment.



1. Our model starts with a perfect VNA. We create two error boxes and put them on either side of the DUT and attach the perfect VNA to the left and right sides. Images courtesy Copper Mountain Technologies



2. This diagram depicts the 6-term forward error model of the DUT.

The measured S-parameters, S_m, may be expressed as in Equation 1:

$$S_m = A * S_a * B \qquad (1)$$

where S_a are the actual S-parameters of the DUT.

Unfortunately, you can't multiply S-parameters as shown in Equation 1, but you can recast them as cascade (or transfer) parameters, and then matrix multiplication is valid. The conversion to cascade parameters is accomplished with Equations 2, 3, and 4:

$$T_{DUT} = \frac{1}{S_{21}}\begin{vmatrix} -\Delta_S & S_{11} \\ -S_{22} & 1 \end{vmatrix} \qquad (2)$$

$$T_A = \frac{1}{e_{10}}\begin{vmatrix} -\Delta_{eA} & e_{00} \\ -e_{11} & 1 \end{vmatrix} \qquad (3)$$

$$T_B = \frac{1}{e_{32}}\begin{vmatrix} -\Delta_{eB} & e_{22} \\ -e_{33} & 1 \end{vmatrix} \qquad (4)$$

where:

$$\Delta_S = S_{11}S_{22} - S_{21}S_{12}$$

$$\Delta_{eA} = e_{00}e_{11} - e_{10}e_{01}$$

$$\Delta_{eB} = e_{22}e_{33} - e_{32}e_{23}$$

Then:

$$T_m = T_A * T_{DUT} * T_B \qquad (5)$$

And we can find T_{DUT} by inverting T_A and T_B:

$$T_{DUT} = T_A^{-1} * T_m * T_B^{-1} \qquad (6)$$

We then convert the cascade parameters back to S-parameters, and we will have our calibrated measurement assuming we know the eight **e** values:

$$S = \frac{1}{T_{22}}\begin{vmatrix} T_{12} & \Delta T \\ 1 & -T_{21} \end{vmatrix} \qquad (7)$$

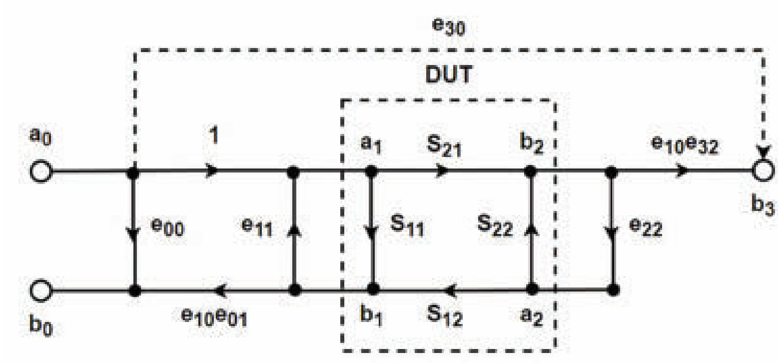
where the T parameters are T_{DUT} from above. And:

$$\Delta T = T_{11}T_{22} - T_{21}T_{12}$$

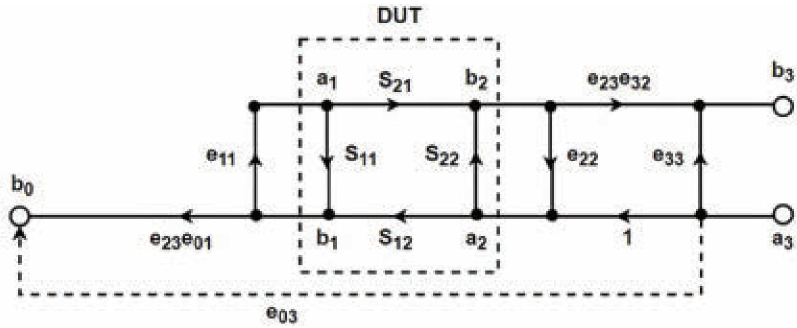
The e values for the A and B boxes can be determined by making a few measurements of known calibration standards such as an Open, a Short, a Load, and a Thru.

But this is an 8-term error model, and the individual error terms don't correspond well to any physical error contributor. The 8-term model can be modified into two 6-term models—one for each measurement direction—where the stimulus is emitted by Port 1 and received on Port 2 or the other way around. The error terms in this model relate to actual physical phenomena.

Referring to *Figure 2*, for a forward 6-term model, we can normalize e_{10} to 1. In doing so, any signal that comes back through e_{01} had to pass through e_{10} first, so we change e_{01} to $e_{10}e_{01}$. The same is true for e_{32}, so we changed it to $e_{10}e_{32}$.



2. This diagram depicts the 6-term forward error model of the DUT.



3. Shown is the 6-term reverse error model of the DUT.

Lastly, we eliminated node a_3 in the forward model because there's no driven signal on the right side to feed it. With a_3 gone, e_{33} and e_{23} go with it and we have *Figure 2* with six error terms. Similarly, the reverse model is shown in *Figure 3*.

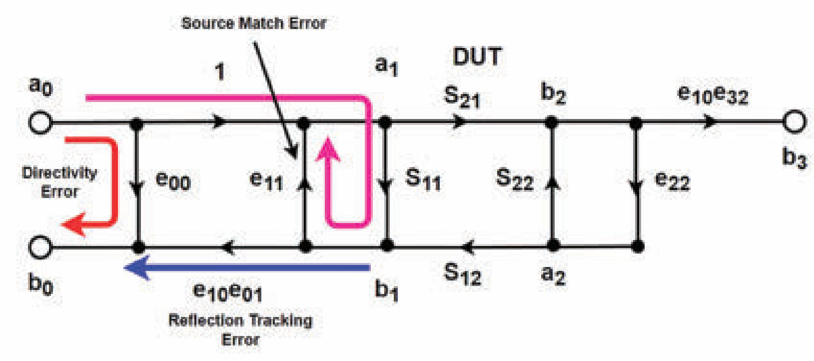
Focusing on the forward model, we can name these errors based on physical causes. a_0 is the driven node and, ignoring isolation term e_{30} for now, the input signal from a0 immediately sees e_{00}, which sends a signal right back to b_0.

This is the *directivity* error, the signal that leaks from the incident signal into the reflection port of the directional bridge. The remaining forward traveling signal then encounters S_{11} of the DUT, generating a reflection, which heads back to the source.

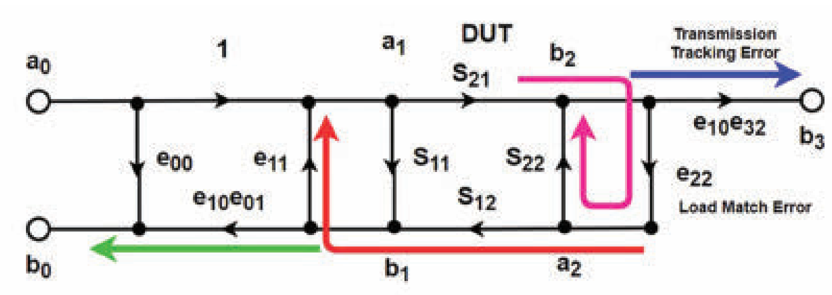
That reflection encounters e_{11}, the *source-match error*. The source-match error is seen right at the end of the test cable and is caused by any deviation from 50 Ω due to the cable, the connectors, and to some extent, the raw source-match error of the VNA itself. This source-match reflection is pushed back up to the top of the network diagram and reenters the DUT along with the incident signal.

The remaining S_{11} reflection, that which was not diverted by e_{11}, passes through $e_{10}e_{01}$, the *reflection tracking error*. The reflection tracking error is essentially the frequency response of the test cable, the connectors (twice), and the internal hardware of the VNA in the reflection path of the measurement bridge. This error will be a gentle low-pass response, as the test cable will always be more lossy at higher frequencies. These first three reflections are shown in *Figure 4*.

That part of the incident signal not reflected by the directivity error, or S_{11} of the DUT, enters the DUT and is affected by S_{21}. This modified signal then sees e_{22}, the load-match error, passes to the bottom of the diagram, and heads back toward a_2. The load-match error is seen at the end of the test cable and is caused by any deviation from 50 Ω due to the cable, the connectors, and the raw load match of the VNA itself.



4. Here's a depiction of the first three reflections: directivity error, source-match error, and reflection tracking error.



5. In this diagram, we see the reflections after the DUT: the load-match error, the transmission tracking error, and the reflection tracking error.

Some of that reflected signal at a_2 is reflected upward again by S_{22} and rejoins the incident signal. The rest passes through S_{12} of the DUT—some is reflected once again by the source-match error e_{11}, and the rest passes through the reflection tracking error $e_{10}e_{01}$, and into Port 1 of the VNA.

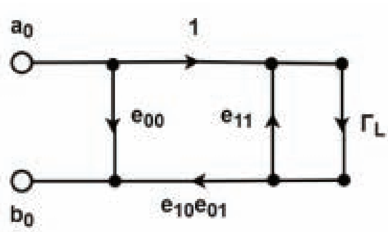
Finally, the remaining incident signal not reflected by the load match passes through $e_{10}e_{32}$, the *transmission tracking error*. This error is the frequency response of the Port 2 test cable, the connectors, and the internal hardware of the VNA behind Port 2. It looks like a gentle low-pass response, much like the reflection tracking error.

These reflections are shown in *Figure 5*. The reflections that occur in the reverse model are identical in nature and needn't be shown again.

How are the 12 Error Terms Found?

The first step to the full 2-port correction is to perform a full 1-port correction on each side. This means finding e_{00}, e_{11}, and $e_{10}e_{01}$ on the left side and e_{33}', e_{22}', and $e_{23}e_{32}$' on the right, where the primed error terms are for the reverse direction.

First, we place a load with reflection coefficient Γ_L after a network defined by its S-parameters as in *Figure 6*.



6. Shown here is a port bearing a load with reflection coefficient ΓL after a network is defined by its S-parameters.

We know that the reflection coefficient looking into this network, Γ_{in}, is given by Mason's Rule:[1]

$$\Gamma_{in} = e_{00} + \frac{e_{10}e_{01}\Gamma_L}{1 - e_{11}\Gamma_L} \qquad (8)$$

This is an equation with three unknowns, as we don't need to know e_{10} and e_{01} separately. We need only apply three known Γ_L loads and measure three Γ_{in} values to find them. The three Γ_L values may be Open, Short, and Load, or +1, −1, and 0, if we had perfect calibration standards. Note that if a perfect Load is applied, the fraction will be zero and the input reflection coefficient will be simply e_{00}, the directivity error. This is an important result, because it highlights the significance of this error in the total 1-port measurement error.

There's a very convenient matrix operation to find e_{00}, $e_{10}e_{01}$, and e_{11}. Form two matrices **C** and **V**:[2]

$$C = \begin{vmatrix} \Gamma_{a1} & 1 & \Gamma_{a1}\Gamma_{m1} \\ \Gamma_{a2} & 1 & \Gamma_{a2}\Gamma_{m2} \\ \Gamma_{a3} & 1 & \Gamma_{a3}\Gamma_{m3} \end{vmatrix} \text{ and } V = \begin{vmatrix} \Gamma_{m1} \\ \Gamma_{m2} \\ \Gamma_{m3} \end{vmatrix}$$

where Γ_{a1}, Γ_{a2}, and Γ_{a3} are the three actual load values, which must be known. These are usually the Open, Short, and Load calibration standards. Γ_{m1}, Γ_{m2}, and Γ_{m3} are the three measured input reflection coefficients with the three known loads applied.

Note that the three applied loads might also be three total reflections with different delays, whereby they're widely separated on the Smith Chart, such as 0°, 120°, and 240°. Any three calibration standards may be used if they remain far apart on the Smith Chart over the frequencies of calibration. Open, Short, and Load are the simplest because the Open and Short will maintain a 180° difference on the circumference if they have equal internal delays, and the 50-Ω load is at (or near) the center.

Next, we calculate matrix **E**:

$$E = (C^H \cdot C)^{-1} \cdot C^H \cdot V = \begin{vmatrix} E_1 \\ E_2 \\ E_3 \end{vmatrix}$$

where H is the Hermitian transpose operator, or the matrix transposed with its entries conjugated.

From **E**, we can find the three error terms:

$$e_{00} = E_2\ ,\ e_{11} = E_3,\ \text{and}\ e_{10}e_{01} = E_1 + E_2 * E_3$$

Note that $(C^H * C)^{-1} * CH$ is a least-squares calculation. If our measurements are a little noisy, we can improve our results by making more known measurements and add more rows to C and V. Matrix E will still have three values in the end, and the results will be somewhat better in the face of slightly noisy measurements.

The last three error terms can be found now that the error terms on the left-hand side are known. e_{22} and $e_{10}e_{32}$ are found mathematically and e_{30}, the isolation, is found by a last measurement with no connection between the two ports.

We'll find $e_{10}e_{32}$ and e_{22} on the right-hand side of the forward model. First, the test cables are terminated, and measuring S_{21} gives isolation term e_{30} directly. Then with the two ports—or test cables—connected directly together:

$$e_{22} = \frac{S_{11m} - e_{00}}{S_{11m}e_{11} - \Delta e}$$

where:

$$\Delta e = e_{11}e_{22} - e_{12}e_{21}$$

and:

$$e_{10}e_{32} = (S_{21m} - e_{30})(1 - e_{11}e_{22})$$

This process is repeated in the reverse direction to obtain the six primed error terms of the reverse model. With all 12 error terms, we can now convert measured S-parameters into actual S-parameters of the DUT. The equations for this are given in Reference 4.

The assumption that the two cables are connected directly together greatly simplified these last two calculations. If using a Thru with some loss and delay instead, it's easier to revert to the 8-term error model and use the "unknown Thru" or SOLR calibration calculation.[5] This method doesn't require precise knowledge of either the loss or the delay of the Thru calibration standard.

Conclusion

We've seen here how the measurement system can be modeled as a perfect VNA with error boxes on either side and how those errors can be related to real-world phenomena. We provided an example of the 1-port calibration calculation and then the final calculations to achieve a 2-port calibration.

With these error terms characterized, do we now have a perfect measurement? No, we will still have residual errors. These residual errors may be traced back to several factors, not the least of which are the uncertainties of the calibration kit standards. This will be a topic for the next article in the series. ■

ACKNOWLEDGMENTS

The great majority of the work on VNA calibration was done by Douglas Rytting,[3] and this paper draws extensively from his published work. The intention of this article is to elaborate on that work and make it more accessible to those without extensive VNA experience.

REFERENCES

1. Mason, Samuel, "Feedback Theory – Further Properties of Signal Flow Graphs", Proceedings of the IRE (Volume: 44, Issue: 7, July 1956).

2. Walker, Brian, "One-Port VNA Calibration: A Look Under the Hood," Microwaves & RF, Jan 11, 2021.

3. Rytting, Douglas, "Network Analyzer Error Models and Calibration Methods," University of Illinois, Urbana-Champaign.

4. Walker, Brian, "Introduction to the Metrology of VNA Measurement," Appendix A, May 31, 2022.

5. Walker, Brian, "VNA Master Class: Full 2-Port VNA Calibration Math Explained," Webinar.

Maximize X-ray Imaging Performance with Low-Noise Precision Voltage References

By Jackson Wightman, *Applications Engineer, Texas Instruments*

Boosting the resolution of X-ray images ultimately leads to better healthcare. Making it happen typically requires a redesign of the front end, which means careful selection of the voltage reference.

X-RAY IMAGING IS one of the most widespread medical imaging technologies, and as such, many efforts are underway to improve X-ray imaging performance—specifically, increasing the resolution of the image produced.

One of the most effective ways to improve the image resolution of an X-ray is to reduce the noise present in the front end. Careful design of the data-acquisition portions of the front end can help achieve this goal. Using a low-noise series voltage reference in the data-acquisition circuit is one design choice that can lead to lower noise and thus a higher-resolution image.

[In this article, to differentiate between a custom chip-on-film device and the front end of the X-ray system, any use of "analog front end (AFE)" will refer to a chip-on-film device, and any mention of "front end" will refer to the section of the X-ray system that contains a chip-on-film device, a voltage reference, and other devices.]

General Overview of X-ray Imaging Operation

In an X-ray system, an AFE receives the generated signal from the X-ray panel. An AFE is a specially designed integrated circuit where data acquisition in the front end takes place. X-ray systems include multiple AFEs that are specifically designed to be used in X-ray systems, all of which use a common voltage reference. *Figure 1* shows a simplified block diagram of an X-ray device front end.

The AFE converts a charge coming from the X-ray panel into a voltage by using a charge-summing amplifier (CSA). This voltage is then fed into a multiplexer that provides an analog signal to an analog-to-digital converter (ADC). The ADCs present in the AFE use an external precision voltage reference to provide accurate data conversion. A field-programmable gate array (FPGA) or other processor then processes the output.

Once the front end has a digital signal, digital subtraction radiography helps improve the image quality. Digital subtraction radiography compares a scan of the patient and a scan without the patient to remove image flaws. The two images are taken within a short time frame.

In this short period of time, because the X-ray system is in a temperature-controlled environment, the change in temperature is minimal. However, the process of digital subtraction radiography compensates for image discrepancies caused by any small temperature change in the front end.

Implementing a Low-Noise Circuit

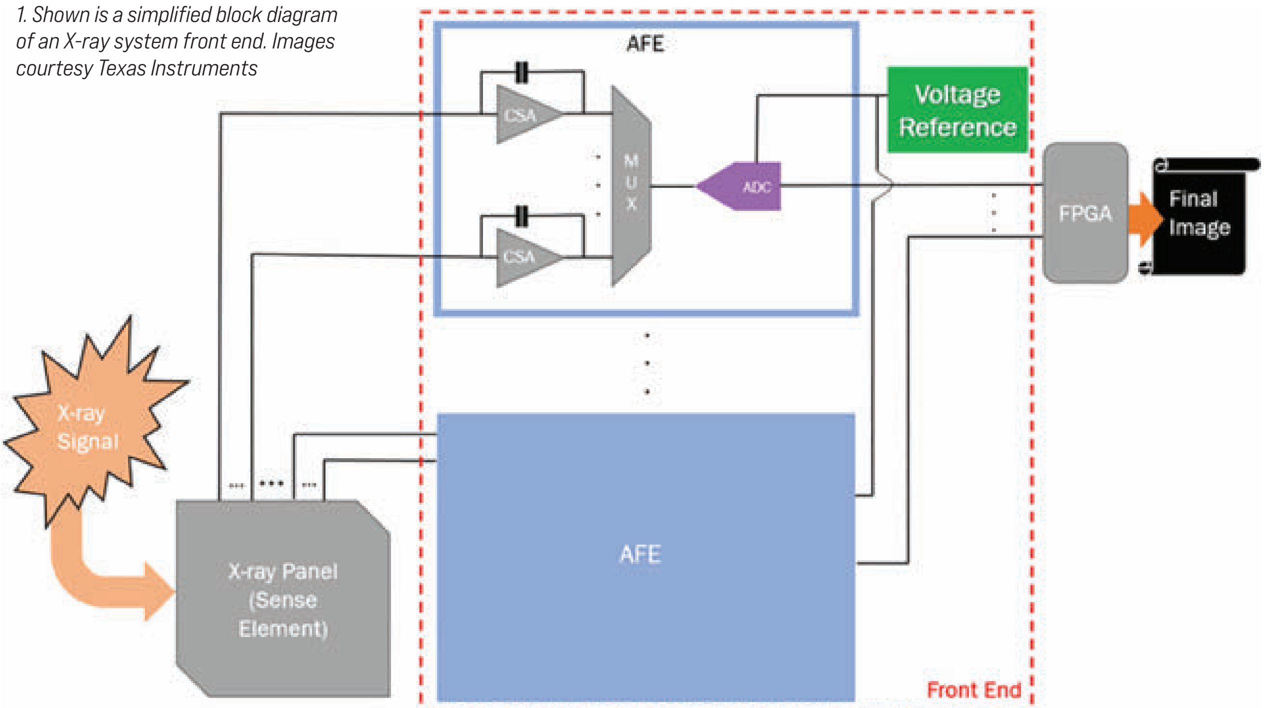
The noise of a circuit may change drastically in a very short amount of time. Therefore, digital subtraction radiography isn't effective in removing image flaws caused by noise in the circuit. Noise is a random event, and not something that can be controlled. Any noise present in the front end—including in the precision voltage reference and the AFE—will propagate through all channels and decrease the final image resolution, leading to a low-quality image.

In high-precision applications, an internal voltage reference in an ADC, digital-to-analog converter (DAC), or AFE can't meet the application's accuracy, noise, temperature drift, or long-term drift specifications. Often, an internal voltage reference isn't even available, or doesn't meet the noise specifications necessary to produce a high-quality image.

An external precision voltage reference with ultra-low noise can help improve image resolution and reduce the number of X-rays taken, thus reducing patient and medical professional exposure as well as healthcare costs. *Table 1* defines voltage-reference parameters to consider.

Table 1: Important Voltage-Reference Parameters

Parameter	Description
Flicker noise	Noise present at low frequencies (0.1 Hz to 10 Hz)
Output voltage noise	Noise present from 10 Hz to 1 kHz on the output signal
Temperature drift	How the output of the voltage reference will change with temperature over a certain range



1. Shown is a simplified block diagram of an X-ray system front end. Images courtesy Texas Instruments

Depending on the number of bits or effective number of bits (ENOB) of a DAC or ADC, the parameters in *Table 1* can directly affect the gain error and signal-to-noise ratio (SNR) of the circuit. In an X-ray system, a higher gain error translates to decreased image quality. Also, the flicker noise of a voltage reference affects the SNR of the ADC.

Equations 1 and 2 show the noise and SNR in an ADC:

Boosting the quality of X-ray images can only improve the medical care that people receive. Given the expansive use of this type of medical imaging, a plethora of opportunities for technological advances are possible in this space. Such advances will continue to help improve healthcare around the world.

$$\text{Total ADC Noise (RMS)} = \sqrt{(\text{Inherent ADC Noise})^2 + (\text{Voltage Reference Noise})^2 + (\text{Buffer Noise})^2}$$
(1)

$$SNR_{ADC} = 20 \log \left(\frac{\text{Vref}}{2\sqrt{2} \times \text{Total ADC Noise}}\right) \qquad (2)$$

From Equation 1, you can see that as the noise of the voltage reference decreases, the total ADC noise drops as well. Looking at Equation 2, you can see that decreasing the voltage reference noise leads to an increase in the SNR of the ADC. A higher SNR would lead to a higher ENOB, which is necessary for higher system resolution. Therefore, it's important that the voltage reference noise be much less than the noise of the ADC.

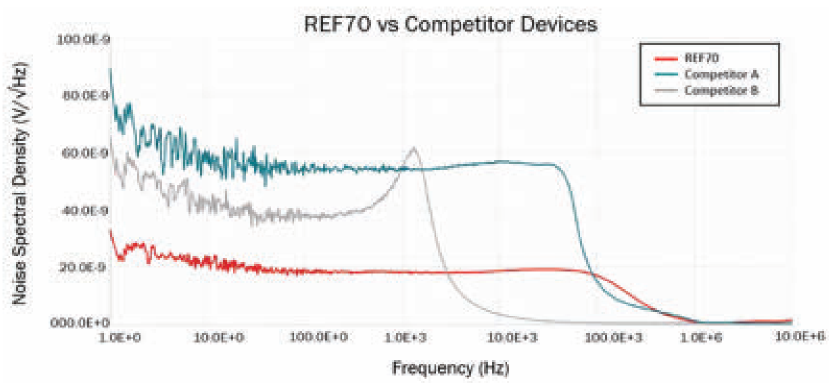
In addition, using a filter to decrease the noise on the output of the voltage reference would slow down the system. For this reason, having low noise would be valuable in applications such as X-ray imaging because it would help avoid any need for filtering.

In many cases, opting for an external voltage reference such as the REF70 from Texas Instruments can assist in improving the SNR of the ADC. A precision voltage reference with low noise would be an essential consideration. *Table 2* lists the parameters of the REF70 series voltage reference.

Lowering the noise present in the analog front end by choosing a low-noise precision voltage reference like the REF70 will also increase the SNR in the ADC, which would enable improved image resolution in X-ray systems. *Figure 2* compares the noise of the REF70 (from 1 Hz to 10 MHz) with competing devices.

Table 2: REF70 Series Voltage-Reference Parameters

Parameter	REF70
Flicker noise	$0.23\ ppm_{p\text{-}p}$
Output voltage noise	$0.35\ ppm_{rms}$
Temperature drift	2 ppm/°C



2. This graph compares the noise spectral density of the REF70 to that of competing devices.

Conclusion

Boosting the quality of X-ray images can only improve the medical care that people receive. Given the expansive use of this type of medical imaging, a plethora of opportunities for technological advances are possible in this space. Such advances will continue to help improve healthcare around the world.

When designing an X-ray system, the goal is to produce the best image possible. There are many ways to achieve that, but among the most important is choosing the best voltage reference for the design of the X-ray system's front end. Choosing a device such as the REF70 can help improve the resolution of the image and the overall image quality. ■

187308977 © Maksim Laptanovich | Dreamstime.com

The Critical Role of Timing in 5G Networks

Gain insights into the impact of timing on the quality of service of 5G networks and learn how that impact defines the requirements of a proper timing architecture.

***By Jim Olsen,** Senior Technical Applications Engineer, Frequency and Time Systems Business Unit, Microchip Technology*

THE CRITICAL ROLE of timing in 5G networks and its impact on network performance isn't a subject that's widely covered or examined in detail. This article will deliver insights into the role timing plays regarding the quality of the services being provided. The ways in which timing affects these services define the requirements of a proper timing architecture. Dive in to explore the fascinating concepts and intricacies of 5G timing architectures and technologies.

The source of time used to generate timing signals for 5G networking technologies is one that's traceable to Universal Coordinated Time (UTC). Global Navigation Satellite Systems (GNSS) receivers are commonly used to obtain the UTC-traceable reference needed to satisfy the 5G timing requirements. Other technologies can also be used to obtain UTC traceable timing that aren't mentioned in this article.

TDD Timing Requirements are Critical to 5G Networks

As LTE evolved from frequency-division-duplex (FDD) to time-division-duplex (TDD) technologies in 5G radio-access networks (RANs), new stringent timing requirements have emerged. FDD operation required only a frequency reference for frequency alignment of the RAN equipment, but TDD technology requires both a frequency reference and UTC-traceable phase reference.

The additional requirement of TDD technology is like the CDMA requirements in the RAN networks that were deployed several years ago. The CDMA base stations had integrated GNSS receivers to satisfy the timing requirements. One major difference between CDMA and 5G is that the CDMA base stations had high-quality rubidium atomic-clock oscillators for timing holdover functions if GNSS was compromised, whereas 5G base stations and radio technology don't have rubidium atomic-clock holdover capability.

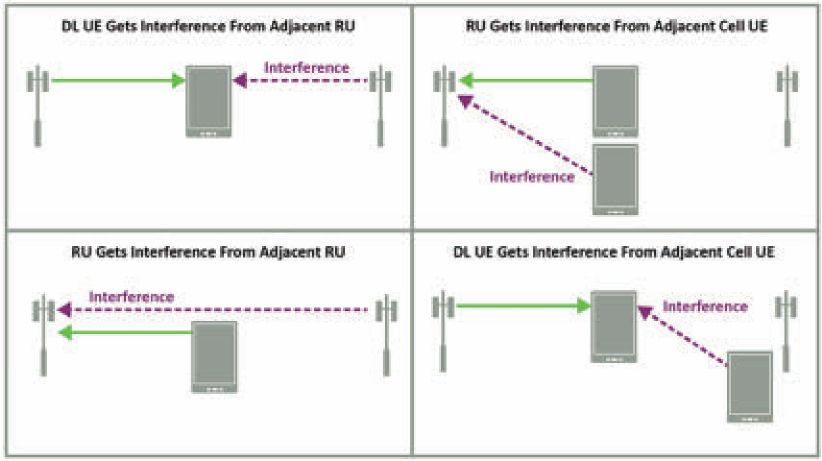
The 5G RAN technologies use low-cost, low-performance oscillator technology as a cost-saving measure. An important topic of this article is how this holdover-related vulnerability will be addressed in the overall timing solutions.

Single Frequency Bands for TDD

Both frequency- and phase-alignment requirements define how timing impacts 5G network performance. The internal clocks in the radios can hold the 50-ppb frequency requirement for several days, so losing the timing reference to the radio isn't something that needs backup or to be addressed quickly. If the radio's clock frequency drifts outside the 50-ppb accuracy window, the network will drop more calls when a radio hands off to an adjacent radio in mobility applications.

Phase alignment is a much more critical parameter. There are two different types of requirements: absolute phase alignment of a radio to UTC and relative phase alignment from radio to radio. First, let's examine the role that timing plays in the category where the requirements for radio units (RUs) are ±1.5 µs to absolute UTC.

The 5G RAN technology is based on TDD that adds the absolute phase-alignment requirement to UTC in addition to the frequency requirements. In TDD operation, a single frequency band is shared for uplink and downlink transmission. *Figure 1* shows the difference between FDD and TDD where the uplink and downlink for TDD share the same frequency band.



2. Shown here are some interference scenarios for TDD applications. The abbreviations denote radio unit (RU), downlink (DL), and user equipment (UE).

This means that transmission must be executed in assigned time slots. If the time slots overlap, the data transmitted in the time slots will be compromised, and, to some extent, related to interference. To prevent overlap, guard bands are placed around the time slots. These guard bands will at least partially absorb the offset in the event of timing errors. In 5G TDD networks, there's a desire to reduce the size of the guard bands or eliminate them.

Timing Impairments Create Interference Issues

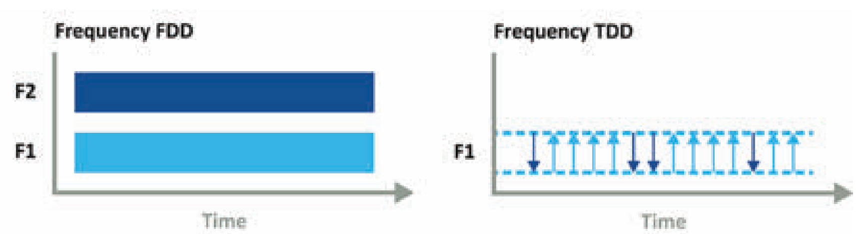
If the timing of the absolute requirement to UTC (±1.5 µs) is outside the specifications at the radio locations, this will result in interference between radios that share the same frequency spectrum. Timing errors result in degradation of service; for unregulated frequency bands, these can result in additional issues.

If multiple operators share the same spectrum, an operator with a timing issue can impact the service of a neighboring service provider operating with overlapping coverage. *Figure 2* depicts interference scenarios for TDD applications.

The timing-related interference issues in TDD technologies elevate the role of timing in 5G networks to a critical status. It's clear from the perspective of ITU and Open Radio Access Networks (O-RANs) standards that the possibility of timing-related interference makes preferable a network-based, Precision Time Protocol (PTP) timing architecture.

The 5G radios don't have high-quality, high-performance oscillators that can hold time or phase for an extended period. When there's loss of GNSS reception in a radio with an integrated GNSS receiver, that radio must be taken out of service quickly before it begins interfering with adjacent radios due to the lack of holdover quality.

Using network-based timing services, whereby the radios are connected to one source clock offering quality holdover, is a suitable mechanism to keep the radios in phase alignment if the GNSS timing receiver function in the source clock is compromised. If the GNSS is compromised in the source clock, all of the radios connected to the same source clock will drift in the same



1. This graphic shows the difference between FDD and TDD, where the uplink and downlink for TDD share the same frequency band. Images courtesy Microchip Technology direction at the same rate, thus avoiding interference issues.

Common Clocks Support Relative Phase Requirements

The 5G carrier-aggregation feature introduces a relative phase-alignment requirement (as opposed to a UTC-traceable absolute phase-alignment requirement) between radios that operate at FR1 (Frequency 1: 4.1 to 7.125 GHz or sub-6-GHz) or FR2 (Frequency 2: 24.5 to 52.6 GHz or mmWave). *Figure 3* depicts frequency-band coverage models for these spectrum segments.

The relative phase-alignment requirements for carrier aggregation are associated with the use of multiple component carriers that must be aggregated into the same frequency or multiple frequency bands. In the carrier-aggregation feature, it's possible for a user handset to connect to the same or multiple radios simultaneously using multiple component carriers.

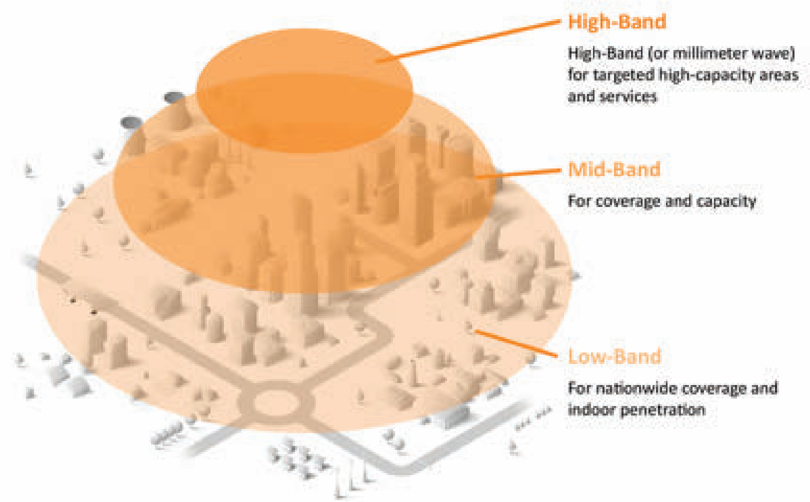
The relative phase requirements for the use cases are typically met by the timing concept referred to as a common clock. For 5G radio clusters, the nearest common clock is a boundary clock (BC) function that's located in the closest switch common to the adjacent radios in the cluster. *Figure 4* depicts use cases for common clocks.

The carrier-aggregation feature will not operate properly if the radios aren't phase-aligned within the specifications for the frequency band in which they operate. The common clock must be located where the relative time error that's accumulated between the common clock and radio doesn't exceed the time-error budget for the application.

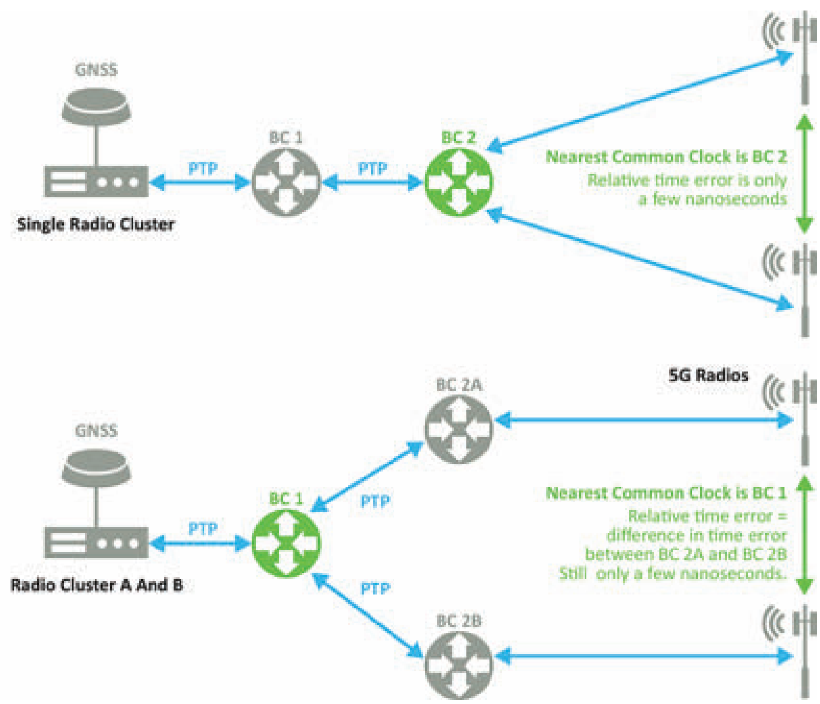
A GNSS timing receiver used as a source clock, per the ITU standards, must operate within the Primary Reference Time Clock (PRTC) requirements, which are <100 ns of time error relative to UTC. It's the best technical approach to use network-based PTP timing services that support the concept of the nearest common clock that could be either a PRTC or BC function.

Conclusion

The timing designs and architectures for 5G networks are important planning and engineering considerations when building out the footprints. Both absolute and relative timing requirements must be accounted for when deploying TDD wireless technology. Poor timing quality or not planning for timing failure scenarios can have service-affecting consequences such as issues related to interference and throughput. ■



3. This diagram depicts 5G coverage models for low-, mid-, and high-band segments of the spectrum.



4. Shown are some use cases for common clocks in meeting relative phase timing alignment.

CYBERS

Critical to Safeguarding IoT/IIoT Connections

Learn how the latest IoT and IIoT devices ensure secure connectivity against cyber threats, whether wired or wireless. Explore cybersecurity measures in this comprehensive guide.

By Jack Browne, *Technical Editor*

164743075 © Adam121 | Dreamstime.com

ECURITY

SECURE CONNECTIONS ARE ESSENTIAL for many internet-based devices. As the number of devices connected to the internet escalates, opportunities to steal data or information also increase, heightening the need for internet cybersecurity protection. Networked information can be captured from any internet interconnection, including Internet of Things (IoT) and industrial IoT (IIoT) devices.

If not properly protected, those devices can become unintended access points. They can allow data to be subtracted and malware to be added to a network. It's possible to make safer IoT/IIoT devices by adding circuitry and software to the devices, although more-effective IoT/IIoT protection is usually achieved by incorporating cybersecurity circuitry and software at the network level.

Understand Cybersecurity Risks with IoT/IIoT Devices

As the number of global IoT/IIoT devices grows steadily, and in turn adds network access points with each connection, services, software, and solutions to boost cybersecurity for those devices and their networks become vital for practical internet use. Furthermore, the number of people and things seeking to take advantage of any internet-based network access points also ramps up.

The total amount of IoT and IIoT devices already exceeds the number of people in the world, with IoT activity expected to expand significantly in the coming years. Increasing IoT use signifies how fully these devices have been embraced across major industries.

IoT devices are things that can provide information about themselves or their surroundings via the internet. They use sensors, control circuits, and communications devices to interact with the internet and enable visitors to the internet to remotely use them.

Such devices ultimately become part of the internet, allowing instant access to information like rainfall in a forest, the presence of an intruder within a home or facility, or temperatures throughout a warehouse or production line. IoT and IIoT devices serve a variety of markets, including automotive, building security, government, healthcare, information technology (IT), manufacturing, retail, transportation, and utility areas.

TABLE 1: SALIENT CHARACTERISTICS OF IoT AND IIoT DEVICES		
Aspect	**IoT devices**	**IIoT devices**
Operating Environment	Typically located in homes or small offices	Typically located in factories and manufacturing facilities
Data Analysis	Communicate data to cloud-based computers	Interact with a local server for data analysis
Security	Less secure due to cloud-based data transmission	Typically more secure due to local server interaction
Computing Power	Limited due to cost constraints	May have more computing power due to industrial usage
Data Sensitivity	Often involves less sensitive data	Often involves more sensitive data due to industrial processes
Connection Method	May use Wi-Fi or other wireless connectivity	Often connected through wired networks
Functionality	Designed for remote monitoring and control	Focuses on process control and automation
Application Areas	Commonly used in consumer electronics, home automation, etc.	Predominantly used in manufacturing, utilities, and industrial sectors
Security Concerns	Vulnerable to cyberattacks due to limited security features	Potential targets for cyberattacks due to critical infrastructure involvement

How IoT and IIoT Devices Differ

IoT and IIoT devices constrast from one another because of their typically different operating environments (see *Table 1* for salient characteristics of both categories). Often located in homes or small offices, IoT devices usually communicate data to cloud-based computers for analysis.

IIoT devices, typically located in factories and manufacturing facilities, are more likely to interact with a local server for data analysis, although that server will be connected to the internet. Because of their greater isolation, they tend to be more secure than IoT devices, although they too can benefit from cybersecurity solutions. And because of the nature of their data, such as supply-chain statistics, better security is needed for the increased capital nature of their data.

Connected IoT devices offer many benefits, including remote monitoring and control of their associated equipment. Because multiple IoT devices may be used in some applications, they're often designed to be cost-competitive. But to keep costs low, they may be limited in computing power, meaning the lack of resources for some functions, such as data encryption, needed for essential cybersecurity.

Without integrated protection, IoT and IIoT devices are vulnerable to those seeking external access to a network, such as hackers. Hackers may desire access to a network to steal its data or introduce damaging malware into that network. An IoT device may not contain harmful data, but it can serve as an access point for cybercriminals. Thus, cybersecurity supporting these devices on any network is essential for the protection of that network and all networks it interconnects via the internet.

Assessing Safety Measures to Enhance IoT/IIoT Cybersecurity

Multiple safety measures are practiced for enhanced IoT/IIoT cybersecurity. Identification of all IoT devices authorized for a business or home network is usually a first step, followed by some form of authentication of those devices within the application software, such as by password. Carefully planning the addition of any IoT/IIoT devices to a network, rather than using automatically connected IoT/IIoT devices, such as plug-and-play components, helps maintain cybersecurity when adding IoT/IIoT devices.

Security of the IoT control software can be maintained by software patches, especially after the software is found to have flaws that can be compromised. Encrypting data handled by IoT/IIoT devices helps strengthen network security, too.

Authentication is critical when maintaining cybersecurity for any IoT/IIoT devices added to a network. Rather than a simple one-step process, greater cryptosecurity is possible via a two-factor authentication or identification process.

Any IoT device can serve as an entry point to a network if not guarded by suitable cybersecurity, and some IoT devices, e.g., routers and webcams, are difficult to secure. Smaller IoT devices, such as smartwatches, can also be security risks, making it possible to track a wearer's location. Cybercriminals will tirelessly probe any internet interconnection endpoints, such as IoT and IIoT devices, for an opening.

For those in need of an introduction to issues caused by widespread use of IoT, the IoT For All site offers a wide range of educational articles.

Key Players and Strategies in IoT and IIoT Cybersecurity

Along with identifying and authenticating as many IoT/IIoT devices on a network as possible, reasonable network cybersecurity can be achieved with edge- or cloud-based systems and software (see *Table 2* for a summary of cybersecurity vendors). For example, Alarm.com works

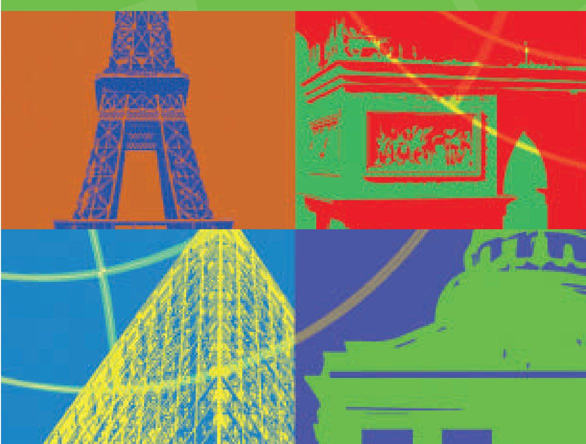


TABLE 2: COMPANIES CONTRIBUTING TO ENHANCED IoT/IIoT CYBERSECURITY

Company	URL	Product types
Alarm.com	www.alarm.com	Smart homes, offices
Alibaba.com	www.alibaba.com	SKYLAB software
Alleantia	www.alleantia.com	IoT device drivers
Amazon Web Services	https://aws.amazon.com	End-to-end network security
Amper Technologies	www.amper.xyz	Amper FactoryOS
Armis Security	www.armis.com	IoT network protection
HPE Aruba Networking	www.arubanetworks.com	ClearPass Wi-Fi security
AT&T Business	www.business.att.com	Network security
Augury	www.augury.com	Machine monitoring
AutomationDirect	www.automationdirect.com	MQTT gateways
Axonius	www.axonius.com	Asset management software
Bosch	https://bosch-iot-suite.com	IoT Suite
Broadcom	www.broadcom.com	Industrial networking
CDW	www.cdw.com	Encryption
Cisco	www.cisco.com	IoT threat defense
CradlePoint	https://cradlepoint.com/	NCX services
CrowdStrike	www.crowdstrike.com	Network security software
Dell Technologies	www.dell.com	Network security software
Enmify	www.emnify.com	Wireless SIM cards
Entrust	www.entrust.com	Encryption
Ericsson	www.ericsson.com	AI-based network security
Fortinet	www.fortinet.com	AI-powered cybersecurity
FreePoint Technologies	www.shiftworxmes.com	ShiftWorx software
GE Digital	www.ge.com/digital	MES software
Google Cloud	https://cloud.google.com	IoT protection
Honeywell	www.honeywell.com	Industrial IoT sensors
IBM	www.ibm.com	Risk-based cybersecurity
Infineon Technologies	www.infineon.com	IoT for "green" buildings
Intel	www.intel.com	IoT platforms
Intertrust	www.intertrust.com	PKI for IoT
Karamba Security	www.karambasecurity.com	ADAS vehicle security
Leverege	www.leverege.com	IoT network security
Lumen	www.lumen.com	Endpoint threat detection
Micron Technology	www.micron.com	Memory support for Intel IoT
Microsoft	https://azure.microsoft.com	Azure IoT software suite
NXP Semiconductors	www.nxp.com	IoT security tools
Palo Alto Networks	https://www.paloaltonetworks.com/	IoT security
Portainer	www.portainer.io	IIoT container devices
qbee.com	www.qbee.com	IoT protection suite
Relayr	www.relayr.io	IoT predictive maintenance
Rockwell Automation	www.rockwellautomation.com	Industrial automation
Samsung Electronics	www.samsung.com	AI-based software
Schneider Electric	www.se.com	Software, services
Siemens	www.siemens.com	Risk-based cybersecurity
Texas Instruments	www.ti.com/iot	IoT protection devices
Telefonica	www.telefonica.com	Secure communications
Thales	www.thalesgroup.com	IoT cybersecure solutions
Trend Micro	www.trendmicro.com	VPN for homes/home offices
Trihedral	www.vtscada.com	SCADA software suite
Verizon	www.verizon.com	Network protection
Webroot	www.webroot.com	MSP program
Wi-Next	www.wi-next.com	end-to-end IoT protection

closely with a customer and its connected IoT and IIoT devices to develop the optimum security solution.

Alarm.com's sensor-enabled IoT/IIoT solutions provide intrusion detection, video perimeter protection, and automated lock control. They also enable energy monitoring so that power and thermostat schedules can be controlled cost-effectively according to a facility's requirements.

An organization synonymous with telecommunications, AT&T, and its Business Center provides security for highly IoT-populated networks. Its product lines used licensed frequency spectrum to avoid interference from too many IoT/IIoT devices within a small area, in contrast to wireless connectivity methods such as Wi-Fi. As an example, the LTE-M/NB-IoT product line supports low-power, wide-area (LPWA) networks and provides effective cybersecurity for IoT/IIoT devices integrated into utility meters, smart homes, and wearable devices.

AT&T's Cybersecurity business unit aids the AT&T Business Center with its array of cybersecurity consulting services and network security solutions. The firm recently announced its intention to create a standalone cybersecurity services business, with funding help from WillJam Ventures, an investor from the cybersecurity industry. The new business will provide security software and consulting services while AT&T will retain an ownership stake in the new operation.

The action enables AT&T to boost enhanced network-based security capabilities without disrupting its existing Managed Security Services. Products from the new entity will improve network-embedded security for small- and medium-sized businesses.

Siemens employs a risk-based, "zero-trust" approach to IoT cybersecurity *(Fig. 1)*. Its tools analyze the types of data to be processed and model responses to develop cyber controls that will protect the data.

In partnership with Siemens, Anguil has developed an IIoT-based solution for environmental pollution control. Siemens employs a risk-based approach

1. Device makers such as Siemens are rapidly deploying IoT/IIoT cybersecurity solutions to protect homes and businesses from cybercriminals. Siemens

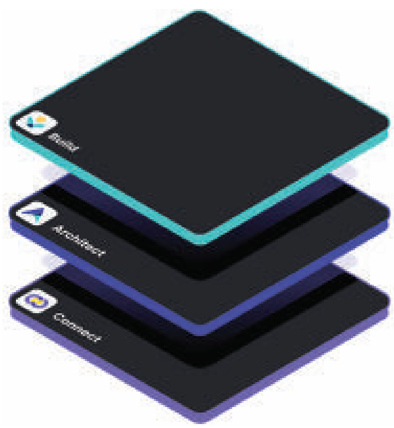
to IoT cybersecurity tools, analyzing data and modeling responses to best protect the data. Anguil teams Siemens' Insights Hub program with their own IIoT software. The resulting IIoT platform saves data from connected IIoT devices via an Ethernet IP connection to an on-site edge computing device. Raw data is transferred from an edge device to an Insights Hub cloud platform, where it can be analyzed and used to create formatted results.

The formatted data includes graphical presentations of trends useful to engineers for equipment maintenance and making improvements in performance. Anguil is working with pilot customers to enhance and refine the IIoT platform according to feedback from those customers.

IoT/IIoT Cybersecurity Heads to the Clouds

Another partnership, software developer Leverege and Google Cloud, has resulted in a multilayer IoT software stack from Leverege. Building upon its own BigQuery software, which analyzes IoT data for problems, the company developed its Leverege IoT Stack.

The three-layer software stack consists of Leverege Connect for device management, Leverege Architect for data management, and Leverege Build for creating optimized applications from



2. Running on Google Cloud, the Leverege IoT Stack is a three-layer software solution for IoT/IIoT cybersecurity. Leverege

the analyzed data *(Fig. 2)*. The Leverege IoT Stack, which runs natively on Google Cloud, uses artificial-intelligence (AI) and machine-learning (ML) technologies to gain the greatest benefits from data collected from millions of IoT/IIoT devices.

The Proficy Smart Factory software suite from GE Vernova protects IIoT devices in industrial and manufacturing facilities. Featuring Manufacturing Execution System (MES) software for smart factories, the software suite provides in-process quality management via IIoT control using cloud-based and on-premises software access.

A firm long associated with the Internet, Microsoft provides IoT/IIoT software tools through its Azure cloud platform of products and services. By taking advantage of widely distributed data and tools available on cloud-connected computers, Azure can help customers develop applications using IoT/IIoT data more quickly *(Fig. 3)*. Using cloud-based resources helps overcome challenges often associated with applications designed from IoT/IIoT data, such as fragmented data and lack of standardization. Azure applies AI and ML technologies for high-resolution analysis of captured data and identification of usable trends in the data.

Lumen offers security services to battle problems left by cybercriminals, such as malware and distributed denial of service (DDoS) attacks. A DDoS attack attempts to disrupt the traffic of an organization's server or network by creating a flood of internet traffic, usually from multiple previously compromised computer systems. A DDoS attack is noticeable when a site becomes slow or unavailable. But Lumen's AI-based tools and services have been effective at mitigating cyberattacks, many against government users.

For a host of organizations and their networks, adding a large amount of IoT and IIoT devices has resulted in a splintered security perimeter. Symptoms include inconsistent communications and slow response times across the network. For a network with a large population of IoT/IIoT devices, a perimeter-based security model may not apply. For that reason, Fortinet developed an AI-powered end-to-end network security approach using what it calls zero-trust network access (ZTNA) to ensure high security at all access points.

As a self-contained solution for IoT/IIoT connectivity, emnify.com provides full, redundant worldwide coverage for IoT devices using what it calls its IoT SuperNetwork. The network combines cellular and satellite-communications (satcom) technologies to reliably interconnect IoT and IIoT devices. The firm's low-power Global IoT SIM cards enable

3. The Azure cloud-based platform of products and services works with IoT/IIoT data to develop optimum cyber-protection solutions. Microsoft

4. A system-level approach developed by Texas Instruments provides IoT/IIoT cyber protection for smart offices, factories, and cities. Texas Instruments

over-the-air (OTA) updates to adapt IoT devices to available communications methods, including 5G. The firm provides secure IoT/IIoT access via more than 540 global cellular networks in more than 180 countries in addition to satellite coverage.

For network protection from advanced threats, the CrowdStrike Falcon software from CrowdStrike is an AI-based cloud-native platform that analyzes IoT data for problems. The extended detection and response (XDR) tool incorporates an extensive high-threat library and modular program design with built-in automation to quickly adapt and respond to new threats. Based on the company's Threat Graph security analytics software engine, it automatically detects and prevents internet threats in real-time.

Texas Instruments provides a system-level approach to IoT/IIoT cyber protection. It offers IoT building blocks for all major applications, including interconnections for wired and wireless devices in smart offices and cities *(Fig. 4)*. Components include MCU, Zigbee, and power control devices (including devices for harvesting power and extending battery life), as well as hardware and software to establish gateway reference designs for enhanced protection of servers and network-interconnected devices.

When setting out to enable users to manage fleets of IoT/IIoT devices securely and as simply as possible, qbee.io considered available software development tools and decided that Go was the optimum programming language to create a dependable, efficient, and secure IoT/IIoT control platform. A complete suite of IoT protection tools from Bosch Global Software Technologies GmbH is contained in the firm's IoT Suite.

For educational purposes, it offers users faced with IoT/IIoT cybersecurity issues several excellent white papers including "White paper: 12 tips for successful IoT data management" and "A guide to successful IoT device management" free of charge from their website.

Trend Micro assists operators of smaller networks with software protection for IoT devices. While the company's Trend Micro Security Suite serves users of larger networks, its VPN Proxy One Pro established virtual private networks (VPNs) within homes and home offices for enhanced cybersecurity. It works with any device, such as computers, tablets, and smartphones, as well as with all operating systems including MS Windows and macOS.

Navigating Regulations for IoT/IIoT Security

The importance of IoT/IIoT cybersecurity is apparent from attention given to it by government organizations. The U.S. Food and Drug Administration maintains a page on cybersecurity and how it relates to various IoT devices, in particular medical equipment. The organization provides recommendations on medical-device cybersecurity in its "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" guidance.

In addition, the National Institute of Science and Technology (NIST) provides multiple publications with guidance on IoT security, including government agencies and businesses. NIST's studies, which consider different device types and network architectures, emphasize that IoT/IIoT devices are now a permanent part of life and achieving security for them is an essential part of sustaining life. ■

Surface-Mount Filter Screens 25 to 27 GHz

Mini-Circuits' model WSBP-26G+ is a substrate-integrated-waveguide (SIW) bandpass filter with passband of 25 to 27 GHz. Passband insertion loss is typically 2.3 dB while passband return loss is typically 12.0 dB. Stopband rejection is typically 41 dB or better from DC to 23 GHz and typically 35 dB from 31 to 32 GHz. Suitable for 5G n258 band applications, the 50-Ω surface-mount filter measures 1.20 × 0.210 × 0.015 in. (30.54 × 5.33 × 0.38 mm) and weighs 0.35 g.

MINI-CIRCUITS

https://tinyurl.com/26a5cy24

EMI Filters Meet Demands of Advanced Space Applications

Available in feed-thru, Pi, and L circuits in panel- and surface-mount packages, Spectrum Control's Space-Grade EMI filters meet the tough demands of existing and emerging space technologies. The hi-rel EMI filters are provided with either feed-thru circuits or Pi circuits (with ferrite beads) to occupy less space on the PCB. The reliable space-grade hermetic- and resin-sealed panel-mount EMI filters support MIL-PRF-28861 and MIL-PRF-15733 requirements, with additional screening for space-level applications.

SPECTRUM CONTROL

https://tinyurl.com/2aafqq4d

One-Part Epoxy Changes from Red to Clear Under UV Light

Master Bond's UV15RCL is a low-viscosity UV curing system with a special color-changing feature. The cationic-type red material changes to clear once exposed to UV light, showing that the UV light passed through the adhesive material. The change in color from red to clear confirms that the UV light has reached the polymer, but doesn't necessarily indicate a full cure. The immediate visual feedback provides processing and handling advantages over conventional systems, with a curing time from 30 to 60 seconds and a lamp emitting a wavelength of between 320 to 365 nm.

MASTER BOND

https://tinyurl.com/25mn26mo

Signal Generator Spans 0.1 to 44.0 GHz

Mini-Circuits' model SSG-44G-RC is a versatile signal generator that provides CW and pulsed outputs (as narrow as 0.5 μs) from 100 MHz to 44 GHz. It offers signal levels from -40 to +17 dBm at a 2.92-mm female output connector and can operate in swept-frequency and frequency-hopped modes. Typical harmonic levels are -30 dBc, with typical spurious content of -40 dBc. The compact signal generator, which can be controlled via USB or Ethernet bus, includes full software support.

MINI-CIRCUITS

https://tinyurl.com/2xn8ud9l

High-Power RF Fixed Attenuators Tout Precision, Power, and Versatility

Fairview Microwave's RF fixed attenuators with 2.4-mm connectors boast power ratings of up to 5 W (CW) and frequencies up to 50 GHz. The RF fixed attenuators meet the developing needs of RF applications, providing precise control over RF signals while ensuring stability and reliability. Features include a design that ensures secure and dependable RF connections with customized attenuation levels from options of 1, 2, 3, 6, 10, 20, or 30 dB. Able to withstand the rigors of high-intensity RF applications, the attenuators deliver consistent performance under challenging conditions and excel in high-frequency environments up to 50 GHz, ensuring reliable performance in demanding RF setups.

FAIRVIEW MICROWAVE

https://tinyurl.com/2c6g8m7y