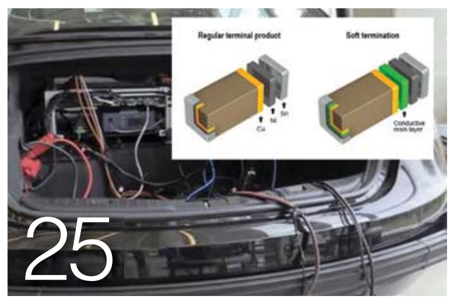
Electronic Design®

THE AUTHORITY ON
EMERGING TECHNOLOGIES
FOR DESIGN SOLUTIONS

SEPTEMBER/OCTOBER 2020
electronicdesign.com

IN THIS ISSUE

ID 163725043 © Roman Samborskyi | Dreamstime.com



FEATURES

COLUMNS & DEPARTMENTS

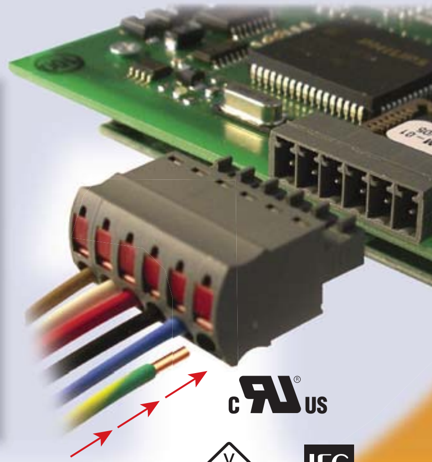
31

EDITORIAL MISSION:
To provide the most current, accurate, and in-depth technical coverage of the key emerging technologies that engineers need to design tomorrow's products today.

ELECTRONIC DESIGN (ISSN 0013-4872) is published bi-monthly in Jan/Feb, Mar/Apr, May/June, July/Aug, Sept/Oct and Nov/Dec by Endeavor Business Media, 1233 Janesville Ave., Fort Atkinson, WI 53538. Paid rates for a one-year subscription are as follows: $60 U.S., $90 Canada, $120 International. Periodicals postage paid at Fort Atkinson, WI and additional mailing offices. Printed in U.S.A. Title registered in U.S. Patent Office. For subscriber services or to order single copies, write to Electronic Design, PO Box 3257, Northbrook, IL 60065-3257. POSTMASTER: Send change of address to Electronic Design, PO Box 3257, Northbrook, IL 60065-3257. Canadian GST #R126431964.

PRINTED CIRCUIT BOARD Terminal Blocks from Altech®

PCB Plug-In Connectors	PCB Fixed Terminal Blocks	PCB Push-In / Spring Clamp Technology



Fixed
- Tubular Screw Clamp
- Screw-Cage Clamp
- Dual Pin Screwless Spring Clamp

Pluggable
- Tubular Screw Clamp Plug & Pin Headers

Mini Pluggable
- Screw-Cage Clamp Plug & Headers

Standard Pluggable
- Screw-Cage Clamp Plug
- Headers
- Double Level Headers

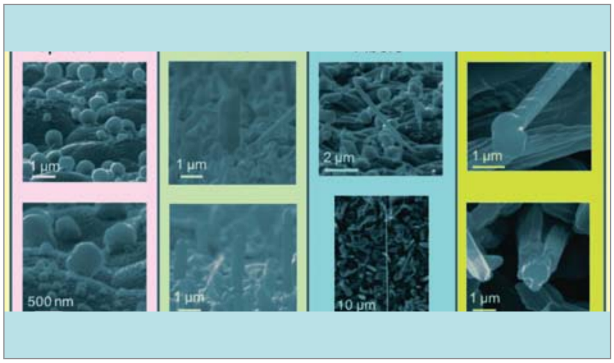
Altech Corp.®

Your Source for Automation & Control Components

info@altechcorp.com • 908.806.9400

Altechcorp.com/PCB

ON ELECTRONICDESIGN.COM



Hey, Lithium Dendrites: We're Looking at You—Very Closely

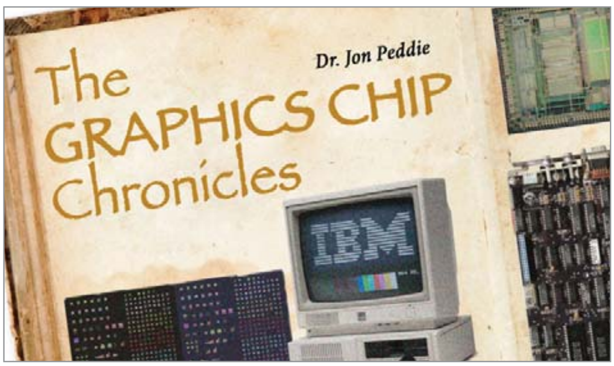
Researchers are devising ways to accurately assess the mechanical properties of lithium-battery dendrites, as these nanomaterials limit the usefulness and safety of such power cells.

https://www.electronicdesign.com/power-management/whitepaper/21141009/hey-lithium-dendrites-were-looking-at-youvery-closely

How Self-Driving Systems are Ushering in a New Era of Transportation

This article discusses the roles of software and hardware in the realm of autonomous-vehicle design and how the new generation of transportation will be led by self-driving systems.

https://www.electronicdesign.com/markets/automotive/article/21139392/how-selfdriving-systems-are-ushering-in-a-new-era-of-transportation



The History of the Integrated Graphics Controller

Moore's Law has turned the integrated graphics processing unit (GPU) into one of the key components of personal computers, smartphones, and even automobiles.

https://www.electronicdesign.com/technologies/embedded-revolution/article/21135920/the-history-of-the-integrated-graphics-controller

11 Myths About Cellular IoT Design

Laird Connectivity's Jonathan Kaye discusses the most common misconceptions about cellular IoT design—a growing area of IoT thanks to two new versions of the cellular standard that enable battery life of up to 10 years for wireless devices.

https://www.electronicdesign.com/technologies/iot/article/21140960/11-myths-about-cellular-iot

FOLLOW US ON FACEBOOK AND TWITTER (ElectronicDesign) (@ElectronicDesgn)

Fast Pulse Test Systems from Avtech

Avtech offers over 500 standard models of high-speed pulsers, drivers, and amplifiers ideal for both R&D and automated factory-floor testing. Some of our standard models include:

AVR-E3-B: 500 ps rise time, 100 Volt pulser

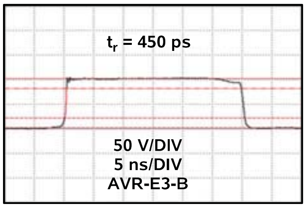
AVRQ-5-B: Optocoupler CMTI tests, >120 kV/us

AVO-8D3-B: 500 Amp, 50 Volt pulser

AV-1010-B: General purpose 100V, 1 MHz pulser

AVO-9A-B: 200 ps t_r, 200 mA laser diode driver

AV-156F-B: 10 Amp current pulser for airbag initiator tests



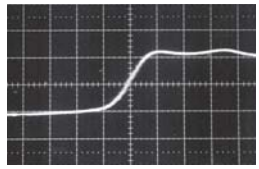
AVTECH

Nanosecond Electronics
Since 1975

Pricing, manuals, datasheets and test results at:
www.avtechpulse.com

AVTECH ELECTROSYSTEMS LTD.
Tel: +1-613-686-6675 Fax: +1-613-686-6679
info@avtechpulse.com

High Output - Low Risetime Pulsers from Avtech



Sub-nanosecond rise time pulsers for every amplitude range!

Model AVP-3SA-C provides up to 10V with < 50 ps rise times.
← Typical waveform, 50 ps/div, 5V/div.

At the other extreme, Model AVI-V-HV2A-B provides up to 100V with < 300 ps rise times.

Ampl	t_{RISE}	Max. PRF	Model
100 V	500 ps	0.1 MHz	AVR-E3-B
100 V	300 ps	0.02 MHz	AVI-V-HV2A-B
50 V	500 ps	1 MHz	AVR-E5-B
20 V	200 ps	10 MHz	AVMR-2D-B
15 V	100 ps	25 MHz	AVM-2-C
15 V	150 ps	200 MHz	AVN-3-C
10 V	100 ps	1 MHz	AVP-AV-1-B
10 V	50 ps	1 MHz	AVP-3SA-C
5 V	40 ps	1 MHz	AVP-2SA-C

AVTECH

Nanosecond Electronics
Since 1975

Pricing, manuals, datasheets and test results at:
www.avtechpulse.com/

AVTECH ELECTROSYSTEMS LTD.
Tel: +1-613-686-6675 Fax: +1-613-686-6679
info@avtechpulse.com

Pulsed Laser Diode Drivers from Avtech

Each of the 19 models in the Avtech **AVO-9 Series** of pulsed laser diode drivers includes a replaceable output module with an ultra-high-speed socket, suitable for use with sub-nanosecond pulses.

Models with maximum pulse currents of 0.1A to 10A are available, with pulse widths from 400 ps to 1 us.

GPIB, RS-232, and Ethernet control available.

AVTECH

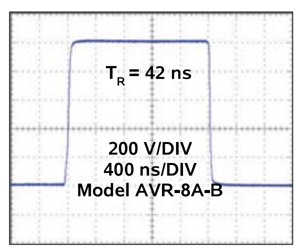
Nanosecond Electronics
Since 1975

Pricing, manuals, datasheets and test results at:
www.avtechpulse.com/laser

AVTECH ELECTROSYSTEMS LTD.
Tel: +1-613-686-6675 Fax: +1-613-686-6679
info@avtechpulse.com

100 to 1000 Volt Lab Pulsers

Avtech offers a full line of 100, 200, 500, 700 and 1000 Volt user-friendly pulsers capable of driving impedances of 50 Ω and higher. The **AVR Series** is suitable for semiconductor and laser diode characterization, time-of-flight applications, attenuator testing, and other applications requiring 10, 20, or 50 ns rise times, pulse widths from 100 ns to 100 us, and PRFs up to 100 kHz. GPIB & RS-232 ports are standard, VXI Ethernet is optional.



See additional test results at:
http://www.avtechpulse.com/medium

AVTECH

Nanosecond Electronics
Since 1975

Pricing, manuals, datasheets and test results at:
www.avtechpulse.com/medium

AVTECH ELECTROSYSTEMS LTD.
Tel: +1-613-686-6675 Fax: +1-613-686-6679
info@avtechpulse.com

ElectronicDesign.

SEPTEMBER/OCTOBER 2020

EDITORIAL

SENIOR CONTENT DIRECTOR: **BILL WONG** bwong@endeavorb2b.com
SENIOR EDITOR: **DAVID MALINIAK** dmaliniak@endeavorb2b.com
SENIOR STAFF WRITER: **JAMES MORRA** jmorra@endeavorb2b.com
CONTRIBUTING EDITOR: **LOUIS E. FRENZEL** lfrenzel@endeavorb2b.com
ASSOCIATE EDITOR/COMMUNITY MANAGER: **ROGER ENGELKE** rengelke@endeavorb2b.com

ART DEPARTMENT

GROUP DESIGN DIRECTOR: **ANTHONY VITOLO** tvitolo@endeavorb2b.com
ART DIRECTOR: **JOCELYN HARTZOG** jhartzog@endeavorb2b.com

PRODUCTION

GROUP PRODUCTION MANAGER: **GREG ARAUJO** garaujo@endeavorb2b.com
PRODUCTION MANAGER: **DEANNA O'BYRNE** dobyrne@endeavorb2b.com

AUDIENCE MARKETING

USER MARKETING MANAGER: **DEBBIE BRADY** dmbrady@endeavorb2b.com

FREE SUBSCRIPTION / STATUS OF SUBSCRIPTION / ADDRESS CHANGE / MISSING BACK ISSUES
OMEDA **T** | 847.513.6022 **TOLL FREE** | 866.505.7173 **FAX** | 847.291.4816 electronicdesign@omeda.com

SALES & MARKETING

REGIONAL SALES REPRESENTATIVES:

AZ, NM, TX: **GREGORY MONTGOMERY** gmontgomery@endeavorb2b.com

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

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: **STUART BOWEN** sbowen@endeavorb2b.com

INTERNATIONAL SALES:

GERMANY, AUSTRIA, SWITZERLAND: **CHRISTIAN HOELSCHER** christian.hoelscher@highcliffemedia.com

BELGIUM, NETHERLANDS, LUXEMBURG, UNITED KINGDOM, SCANDINAVIA, FRANCE, SPAIN, PORTUGAL:
LARA PHELPS lara.phelps@highcliffemedia.com

ITALY: **DIEGO CASIRAGHI** diego@casiraghi-adv.com

PAN-ASIA: **HELEN LAI** helen@twoway-com.com

PAN-ASIA: **CHARLES LIU** liu@twoway-com.com

ARTICLE REPRINTS: reprints@endeavorb2b.com
LIST RENTALS/ SMARTREACH CLIENT SERVICES MANAGER: **MARY RALICKI** mralicki@endeavorb2b.com

DIGITAL

SENIOR DIGITAL INNOVATION & STRATEGY DIRECTOR: **RYAN MALEC** rmalec@endeavorb2b.com

DESIGN ENGINEERING & SOURCING GROUP

EVP, DESIGN & ENGINEERING GROUP: **TRACY SMITH** tsmith@endeavorb2b.com
GROUP CONTENT DIRECTOR: **MICHELLE KOPIER** mkopier@endeavorb2b.com
VICE PRESIDENT OF MARKETING SOLUTIONS: **JACQUIE NIEMIEC** jniemiec@endeavorb2b.com

ENDEAVOR BUSINESS MEDIA, LLC

331 54th Ave N., Nashville, TN 37209 USA | www.endeavorbusinessmedia.com
CEO: **CHRIS FERRELL**
CRO/CMO: **JUNE GRIFFIN**
CFO: **WILLIAM NURTHEN**
COO: **PATRICK RAINS**
CHIEF ADMINISTRATIVE AND LEGAL OFFICER: **TRACY KANE**
EVP KEY ACCOUNTS: **SCOTT BIEDA**
EVP SPECIAL PROJECTS: **KRISTINE RUSSELL**

ENDEAVOR BUSINESS MEDIA

Electronic Design | Machine Design | Microwaves & RF | Hydraulics & Pneumatics | Source ESB | Source Today | Evaluation Engineering

Editorial

WILLIAM WONG | Senior Content Director
bwong@endeavorb2b.com

Good Code Means Secure Code

Good, clean code is the starting point for secure software, and having the right tools is essential when that's not the case.

No one wants to write bad, buggy code, but that's often what we get from developers who don't follow best practices. This problem is worse when one considers the requirements for safe and secure applications. These days, safe and secure code covers just about everything. If you're sharing the code, then people depend on its quality. If you're designing a product for self-driving cars, aircraft, or medical devices, then it's even more important to use the right tools and procedures to deliver reliable software that's also secure.

I do recommend Ada and SPARK for programming in general because of features like contract-based programming. However, I know C still dominates for embedded programmers. For those who haven't moved to C++, I would push that as a better solution even if object-oriented programming (OOP) isn't part of your repertoire. C++ is significantly better when it comes to everything from namespaces to type management to references. The new C++20 standard will incorporate new features like modules.

Many assume C++ is less efficient because C and C++ have more overhead. That's not really the case, but if you use some features like virtual class functions, then, yes, there's overhead. It's on par with any overhead of providing similar functionality in C, although in a much cruder fashion. Using C++ features like non-virtual methods in a class allows for the same efficiency as C while enabling methods to be hidden as well.

So, what does code quality have to do with safety and security?

It's difficult to have either without good code to back them up. Though coding standards can help in writing good code, it's just a starting point. Code reviews can also help, but many developers overlook tools like static analysis that have the advantage of enforcing rules by a computer, which brings a level of consistency to the process as well as enforcement.

One well-known standard is MISRA C. It started in the automotive space where it remains important, but MISRA C and MISRA C++ are applicable to any application. The standards include a multitude of rules that limit the functionality available within the programming language, as well as how features are used. Some, like Rule 1.3, address undefined behavior, which covers a lot of ground when it comes to C. The C90/C99 standard has over 200 instances of undefined behavior.

Other MISRA C rules might appear less useful, such as preventing local variable and type names from hiding more global definitions. This can result in a debugging nightmare if one isn't aware, because he or she may be looking at the more global definition and wondering why it's not operating as expected.

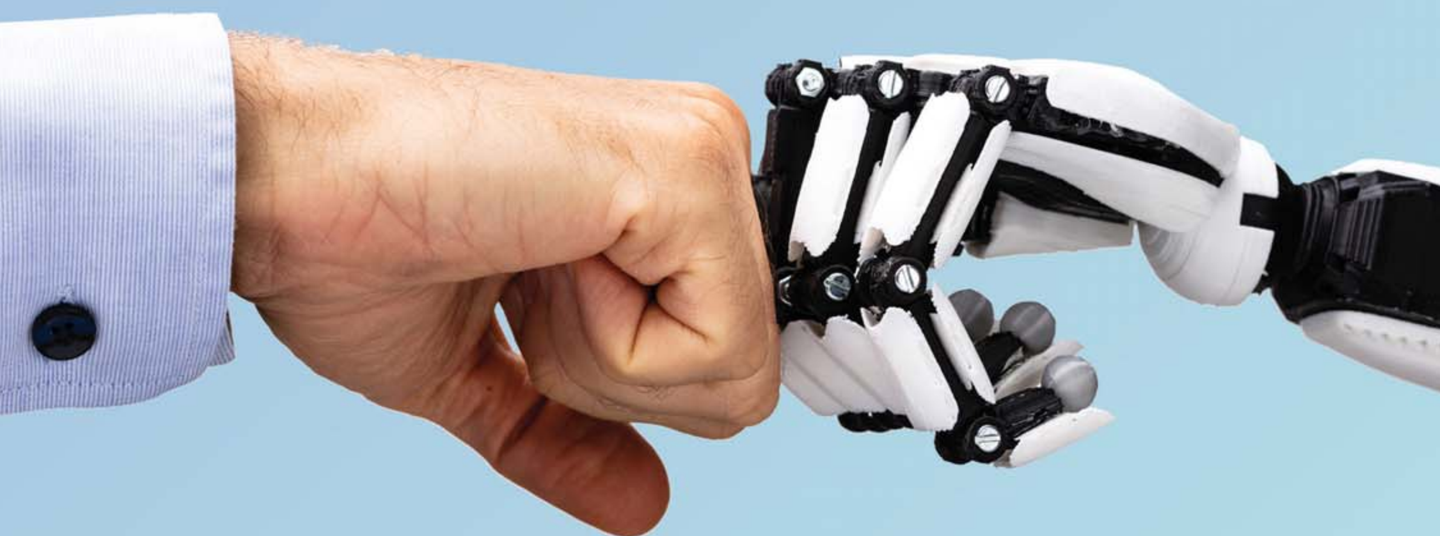
I've been working with IAR Systems' Embedded Workbench, which has MISRA C support built-in, along with GigaDevice's GD32V RISC-V board. It was an interesting exercise getting the demo code working. Turning on MISRA C with the default settings results in hundreds of errors, but disabling or tweaking a few rules cuts this number down to a dozen, so it's worth making the code changes.

Following the rules when writing code and having the compiler check it doesn't eliminate all errors. However, it can force better programming practices and highlights errors that would otherwise be overlooked until the code was running in the field. Debugging costs rise exponentially as it moves farther from the original developer.

Developing safe and secure code should be part of the goals for any developer. Using the right procedures and tools can help, especially for larger projects and groups. ed

THINK™ DESIGN SOLUTIONS

Compact Multi-Purpose Coin Cell Power Pack



Designers & Manufacturers of Electronic Components and Hardware

• Built-in on/off toggle switch for multi-purpose applications (safety, battery life extension, switchable power) • Accepts all 2032 Coin Cells • Available in Single (3 Volt) or Dual (6 Volt) battery configurations • Polarized to prevent improper battery installation • Designed for high shock and vibration applications • Self-locking cover secures batteries within holder with retaining screws • Supplied with 6” wire leads

IT’S WHAT’S ON THE INSIDE THAT COUNTS

KEYSTONE® ELECTRONICS CORP.

View our Dynamic Catalog M70 at www.keyelco.com

(516) 328-7500 (800) 221-5510

ZIA SARDAR | Applications Engineer, Maxim Integrated

Cryptography: Why Do We Need It?

This article address the escalating need for cryptography in this ever-more connected world, from developing confidentiality to avoiding modifications to transmitted messages.

In our day-to-day lives, the use of cryptography is everywhere. For example, we use it to securely send passwords over vast networks for online purchases. Bank servers and e-mail clients save your passwords using cryptography as well. Cryptography is used to secure all transmitted information in our IoT-connected world, to authenticate people and devices, and devices to other devices.

If all of the cryptographic engines/functions stopped working for a day, modern life as we know it would stop. Bank transactions wouldn't go through, internet traffic would come to a halt, and cell phones would no longer function. At this point, all of our important information would be exposed, and it then could be exploited to do unimaginable harm to us all.

Cryptography is an essential way of preventing that from happening. It secures information and communications using a set of rules that allows only those intended—and no one else—to receive the information to access and process it.

IN THE OLD DAYS

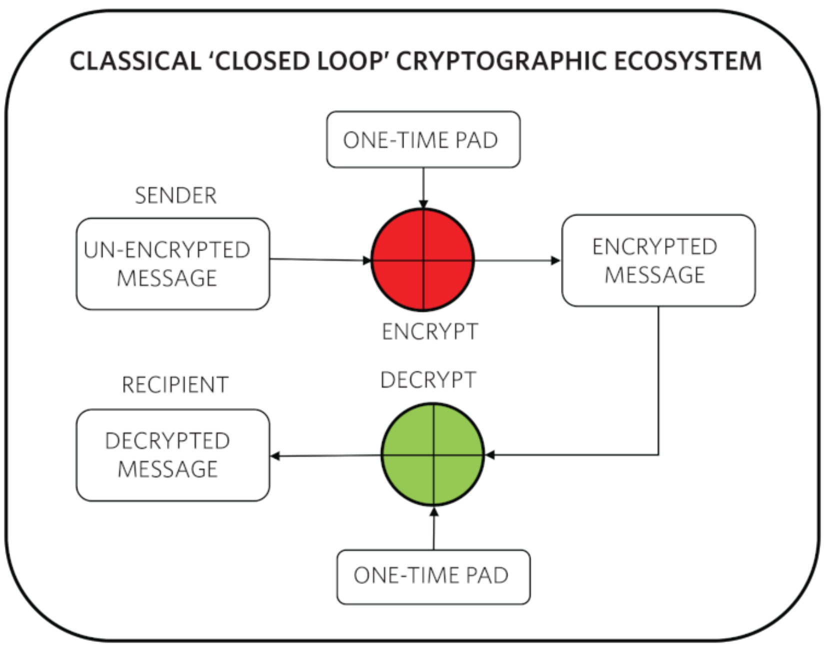
Classically, cryptography used *"security by obscurity"* as way to keep the transmitted information secure. In those cases, the technique used was kept secret from all but a few, hence the term *"obscurity."* This made the communication secure, but it was not very easy to implement on a wide scale. Classical cryptographic methods are only secure when two parties can communicate in a secure ecosystem.

In *Figure 1,* we show a classical cryptographic system. The sender and the receiver first agree upon a set of pre-shared encryption/decryption keys. These keys are then used sequentially to encrypt and then de-crypt each subsequent message.

One-time pad is an encryption technique that requires the use of a pre-shared key that can be used only once. The same key must be used for encryption and decryption. The term *"One-Time Pad"* is an artifact from having each key on a page of a pad that was used and then destroyed. Once the pre-shared keys are exhausted, the sender and the receiver need to meet in a secure location to securely exchange a new set of keys and then store them in a secure location for the duration of the next set of message exchanges.

But...

Clearly, obsolete classical techniques are no longer viable. A vast system of electronic communication, commerce, and intellectual properties need to be secured across oceans and continents that would otherwise be intercepted by people with hostile intentions.



1. A classical closed-loop cryptographic system uses one-time pad as an encryption technique.

NEXT PHASE OF CRYPTOGRAPHY

So, how do you implement an excellent level of security in such a massive system that can carry out billions of transactions in a short period? That's where modern cryptography comes in. It's an essential part of *secure but accessible* communication that's critical for our everyday life.

Next, we will learn how this is achieved on a day-to-day basis all around us. We rely on publicly known algorithms for securing the massive amount of information that's exchanged around the clock. These algorithms are standards-based and vetted in an open environment so that any vulnerabilities can be quickly found and addressed.

Figure 2 shows a simplified modern cryptographic system. Let's investigate these systems and algorithms a bit more in depth.

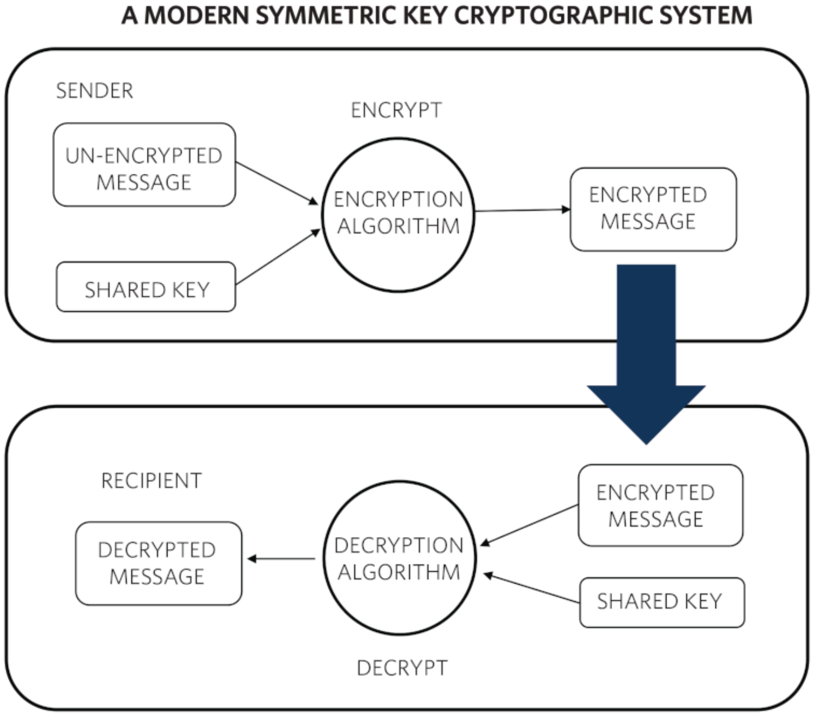
The basic tenet of a modern cryptographic system is that we no longer depend on the secrecy of the algorithm used, but rely on the secrecy of the keys. There are four essential goals of a modern cryptographic system:

- **Confidentiality:** Information can never be disclosed to someone who is not authorized to see it.
- **Identification and Authentication:** Before any information is exchanged, identify and then authorize both the sender and the recipient.
- **Integrity:** Information must not be modified in storage or transit. Any modification must be detectable.
- **Non-repudiation:** Cannot disclaim the creation/transmission of the message. This provides "digital" legitimacy and traceability of a transaction.

Current cryptographic systems provide all of the above or a combination of the above in various forms for an intended application. Let's explore each of these goals a little more to get a basic idea of how they are achieved.

CONFIDENTIALITY

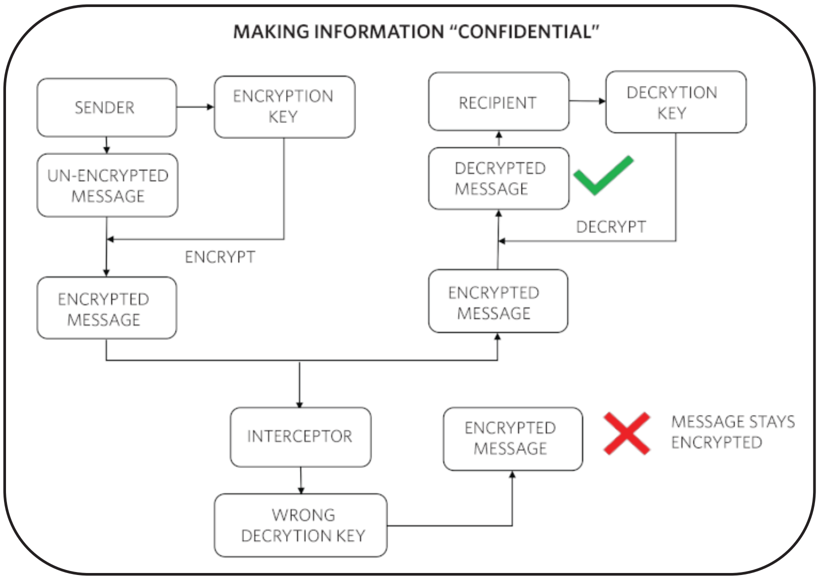
Confidentiality requires informa-



2. A modern symmetric key cryptographic system provides a greater level of security.

tion to be secured from unauthorized access. This is accomplished by encrypting a sent message using a cryptographic algorithm with a key that's only known by the sender and recipient. An interceptor might be able to obtain an encrypted message but will not be able to decipher it.

In *Figure 3*, we show how encryption is used. In this case, the sender and recipient have worked out a system to share the encryption/decryption key. They both use the key to encrypt/decrypt the messages they exchange between each other. If a malicious individual intercepts the message, no harm is done since that person will not have the key to decrypt the message.

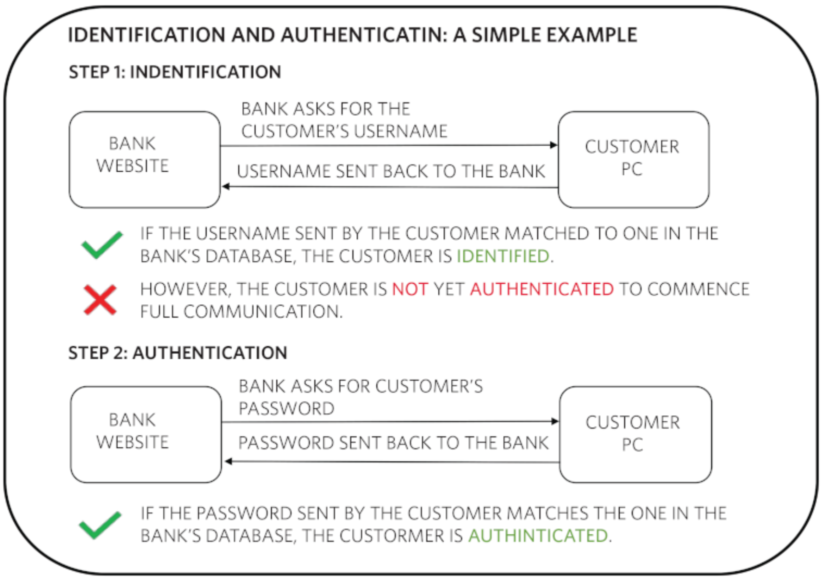


3. Encryption ensures information is kept confidential.

IDENTIFICATION AND AUTHENTICATION

The goal here is to first identify an object or a user and then authenticate them prior to initiating communication or other operations. Once the Sender has authenticated the Recipient, further communication can begin.

In *Figure 4*, we show how authentication works in one direction. The bank (Sender) authenticates the customer's PC (Recipient) using a simple username and password combination before letting the customer use the bank's website. The actual process is much more complex, but we are using this simple example to illustrate the basic concepts of cryptography. Identification and authentication can also be a bidirectional process, where the Sender and Recipient both need to identify each other before starting message exchanges. We will explore all those topics in detail later.



4. Identification and authentication, basic concepts of cryptography, shown in a simple example.

INTEGRITY

How do we make sure that a message sent and then received over a communication network or data link hasn't been altered during transit? For example, there could be an attempt to intercept a message and insert a virus or malicious program to take control of the Recipient's PC or other equipment without their knowledge. To prevent this from happening, it's vital to ensure that any message transmitted isn't modified.

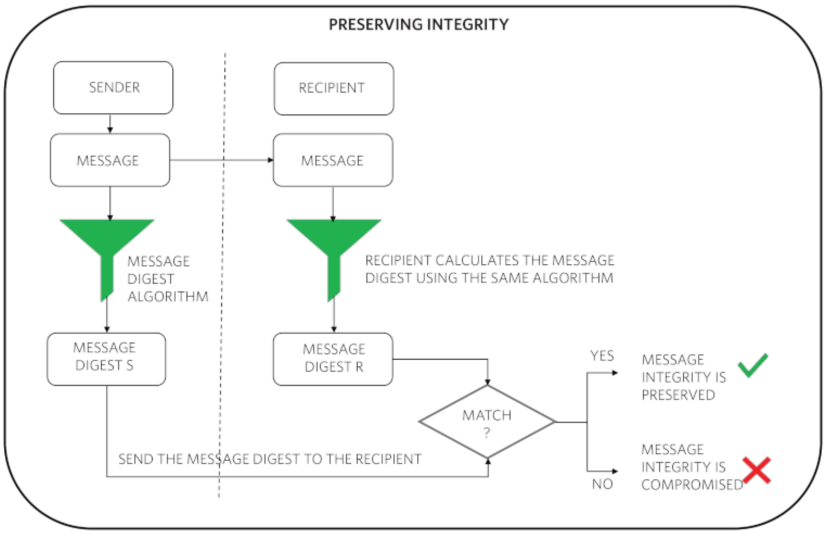
As shown in *Figure 5 (on page 14)*, one way to do this is to use a message digest. The Sender and Recipient use an agreed-upon Message Digesting Algorithm to create and verify the message digest output. If the message is altered, the message digests will not match, and the Recipient knows that either tampering has occurred or there was a transmission error. Many Message Digesting Algorithms are used in modern cryptographic applications, including SHA-2 and most recently SHA-3.

NON-REPUDIATION

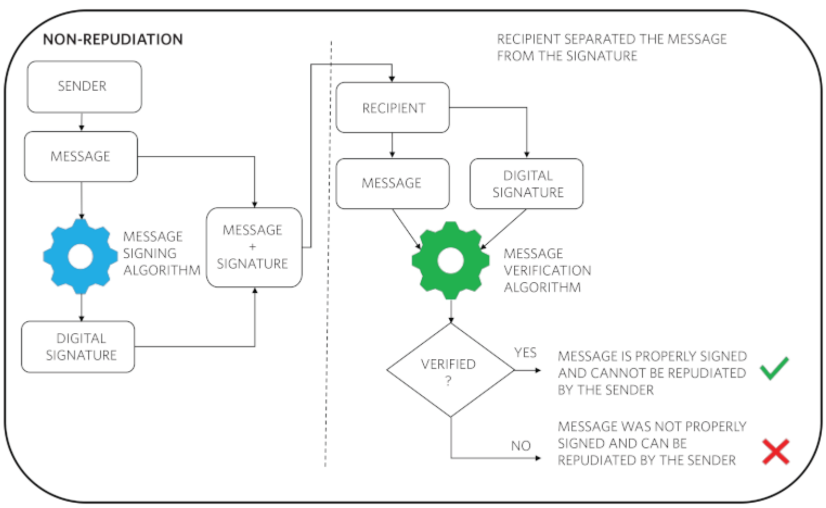
In a communication system where a

multitude of messages are exchanged, there's a need to trace the incoming message back to the Sender. This is required to ensure that the Sender doesn't deny sending the message. Very similar to a pen-and-paper legal document where we sign on the dotted line to finalize a contract, a digital signature is used to achieve similar goals in the digital domain.

Figure 6 shows a simplified view of the digital signature generation, transmission, and verification process. First, the Sender takes the outgoing message and puts it through a Message Signing Algorithm to generate a digital signature related to the message and the Sender's verified identity. The Sender then attaches the digital signature to the original message and sends it to the Recipient. The Recipient takes the incoming combined message and separates the original message and the digital signature. Both are then input into a Message Verification Algorithm. The result can then be used by the Recipient to prove that the message was signed by the Sender. ed



5. Using a message digest helps both a sender and recipient to preserve integrity.



6. The non-repudiation process includes digital signature generation, transmission and verification.

BROADCOM OPTOCOUPLERS

Take the Risk Out of High Voltage Failure!

Only Optocouplers Meet or Exceed International Safety Standards for Insulation and Isolation.

Stringent evaluation tests show Broadcom optocouplers deliver outstanding safety performance and exceptional high voltage protection. Alternative galvanic isolation technologies such as capacitive and magnetic isolators do not perform anywhere near the levels of insulation and isolation provided by Broadcom optocouplers.

GO with OPTO! 50 YEARS
BROADCOM® OPTOCOUPLERS

IEC 60747-5-5 Certified

To learn more visit
broadcom.com/optocouplers

BROADCOM®
connecting everything®

SHAWN PRESTRIDGE | U.S. Field Applications Engineer Team Leader, IAR Systems

Fast Functional-Safety Certification for Your Project

Getting an application functional-safety-certified is often a very difficult process, requiring multiple steps along with testing to complete the functional-safety "checklist." This article reviews ways to fast-track certification.

Though many tweaks can be done to development processes to speed your certification, everything starts with code quality. But how can you ensure code quality? Fortunately, there are some easy ways to almost instantly upgrade your code-quality game with as little pain as possible.

GET HELP FROM STANDARDS

Did you know that in C99, about 190 different ambiguities exist in the code specification? What we mean is that in C99, 190 different syntactically legal C constructs aren't spelled out in the C language specification. It actually gets a bit worse when you go to C18 and even more so in C++, where you start introducing concepts of multiple and virtual inheritance. Of course, a compiler must turn source into concrete code, so it has to pick an interpretation of what your code means and run with it.

Practically, this means that different compilers can interpret your source code differently. In a high-reliability system, this is a nightmare scenario, especially since many companies pursuing functional safety-certification are cross-compiling their code on multiple platforms for ease of testing. As you can imagine, this could have a detrimental impact on the time it takes to get your certification because you must test around all of these situations to prove the repeatability and reliability of the code.

How do we get through this? The short answer is that you avoid these ambiguities in your code. But how do we do that? Using coding standards like MISRA is a quick way to solve the problem because they're designed to prevent those types of common pitfalls in code. They also promote safe and reliable coding practices to reduce the number of defects in the code. But how can we make sure we follow those standards?

Design Note

Dual-Channel, 8.5 A, 18 V, Synchronous Step-Down Silent Switcher Device with 16 μA Quiescent Current

Dong Wang, Applications Manager

Introduction

The LT8652S is a dual-channel, synchronous, monolithic, step-down regulator featuring a 3 V to 18 V input range. It can deliver up to 8.5 A of continuous current from both channels and supports loads up to 12 A from each channel. It features peak current-mode control with an extremely low 20 ns minimum on-time, which allows high step-down ratios even at high switching frequencies. Fast, clean, low overshoot switching edges enable high efficiency operation at high switching frequencies, leading to a small overall solution size.

The LT8652S enables low EMI and a small solution size, a combination that few solutions can achieve. It features the proprietary Silent Switcher® 2 architecture, which minimizes EMI, while delivering high efficiency at high switching frequencies. In this architecture, the bypass capacitors are brought into the package, and by doing so, high di/dt loops are factory set in an optimized layout.

For battery-powered applications, current draw at light load and no load idle is a critical parameter, as minimizing this current preserves battery run time. Idle conditions are where many applications spend most of their time. The LT8652S features 16 μA ultralow quiescent current during Burst Mode® operation, preserving battery life as long as possible. Integrated top and bottom N-channel MOSFETs contribute to an impressive light load efficiency. The LT8652S also includes forced continuous mode that can control frequency harmonics across the entire output load range, with spread spectrum operation to further reduce EMI emissions.

The LT8652S offers both internal and external compensation options. Internal compensation yields smaller solutions by minimizing external components. External compensation via the VC pins enables fast transient response at high switching frequencies. The VC pins also simplify current sharing between channels for parallel, single output operation. CLKOUT and SYNC pins enable synchronizing other LT8652Ss to further expand current ability. To ensure tight output

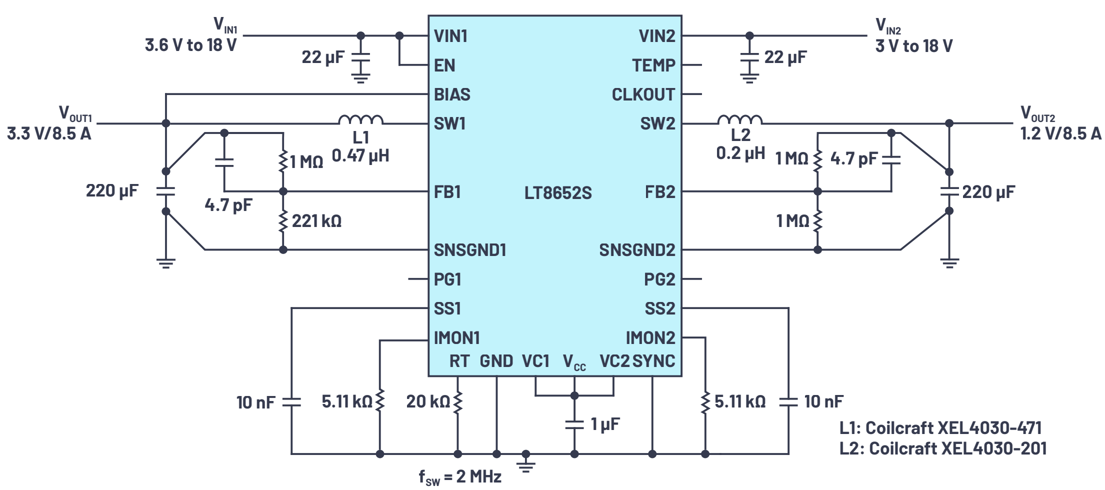


Figure 1. Ultralow EMI emission, dual output LT8652S-based 12 V to 3.3 V and 1.2 V synchronous step-down converter.

voltage regulation at the load for low voltage, high current applications, the LT8652S features a differential output voltage sensing function that allows Kelvin connections for output voltage sensing and feedback directly from the output capacitor.

In some high current applications, output current information is required for telemetry and diagnostic purposes. Limiting or derating the maximum output current based on operating temperature may be required to prevent damage to the load. The LT8652S's IMON pins can be used to monitor and reduce the load current. Load-based or board temperature-based derating can be programmed by using a positive temperature coefficient thermistor from IMON to GND. LT8652S can effectively control the load or board temperature by comparing IMON pin voltage with the internal 1 V reference. When IMON drops below 1 V, there is no effect.

Circuit Description and Functionality

A 3.6 V to 18 V input to 3.3 V/8.5 A and 1.2 V/8.5 A with 2 MHz switching frequency power supply is shown in Figure 1. Each channel can supply up to 12 A continuous load current. Figure 2 shows that the circuit in Figure 1 achieves 94% peak efficiency.

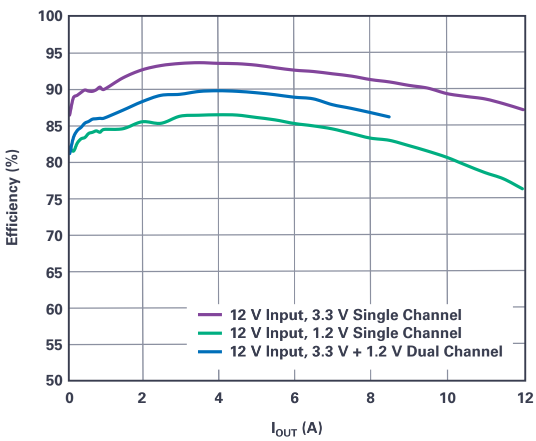


Figure 2. Efficiency vs. load current for an LT8652S-based, 12 V input to 3.3 V/1.2 V synchronous step-down converter.

Differential Voltage Sensing Provides Tight Load Regulation

For high current applications, every inch of PCB trace incurs significant voltage drop. For low voltage, high current loads that require very tight output voltages, this voltage drop can cause serious problems. LT8652S features a differential output voltage sensing function, which allows the customer to make Kelvin connections for output voltage sensing and feedback directly from the output capacitor. It can correct up to ±300 mV of the output ground line potential.

High Switching Frequency with Ultralow EMI Emission and Improved Thermal Performance

EMI/EMC compliance has become a significant concern in many electronic environments. With integrated MOSFETs, advanced process technology, and up to 3 MHz operation frequency ability, LT8652S can achieve fast, clean, low overshoot switching edges, which enable high efficiency operation at high switching frequencies, leading to a small overall solution size. With the leading-edge Silent Switcher 2 technology and integrated hot-loop caps, LT8652S can simultaneously deliver top level EMI performance and reduced switching losses. Spread spectrum operation of the switching frequency can also assist in passing EMI tests. Integrated hot-loop caps make circuits insensitive to board layout and layers. Figure 3 and Figure 4 show the CISPR 22 and CISPR 25 Class 5 EMI performance of the application in Figure 1.

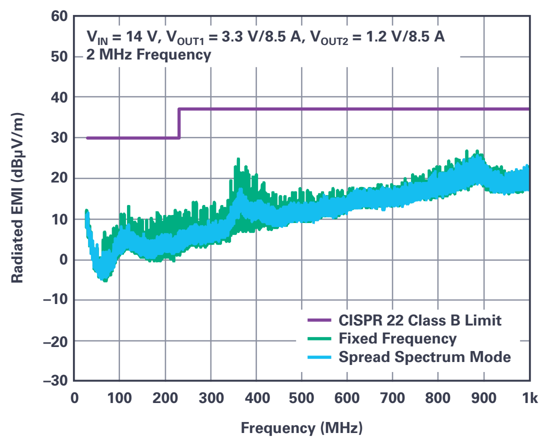


Figure 3. CISPR 22 radiated EMI performance for the circuit in Figure 1.

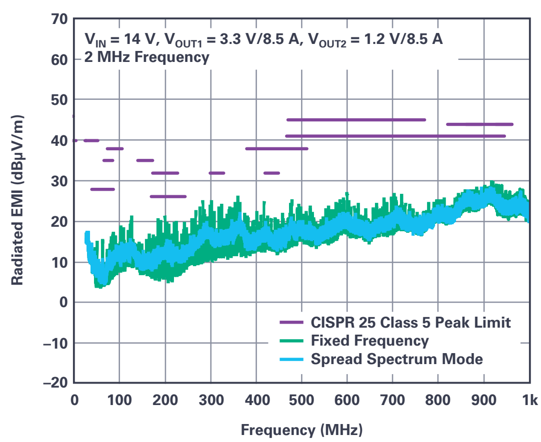


Figure 4. CISPR 25 Class 5 radiated EMI performance for the circuit in Figure 1.

Fortunately, functional-safety standards give us a way to accomplish the task.

STANDARDS REQUIRE CODE ANALYSIS

Virtually every functional-safety standard requires that you do static analysis of your code, and highly recommends that you do runtime (or dynamic) analysis of your code. The most broad-reaching of these standards is IEC 61508, which covers safety-related systems in general.

In section C.4.2 of that standard, using C without coding standards that remove ambiguous and dangerous behavior isn't recommended for anything above Safety Integrity Level (SIL) 1. In other words, you must use static analysis to make your code more robust if you're looking to get SIL 2-4 certification for your product. Why is this? These static-analysis tools can force a developer to implement coding standards like MISRA. Moreover, static and runtime analysis helps you to up your code-quality game by quickly pointing out when you're getting into risky coding behavior, especially with the aforementioned coding standard ambiguities.

However, these types of automated tools can also have a huge impact on your certification timeline. Many organizations employ hard-to-configure, hard-to-use code-analysis tools that are relegated to running on a build server as part of a nightly build.

Such a scenario doesn't really help much because the individual developer isn't getting instantaneous feedback on what's wrong with the code they just wrote. Moreover, sometimes the warning messages that come from these tools are inscrutable. Thus, the developer wastes time trying to figure out what they mean and how the code can be corrected to make the warning go away.

If you can run code analysis during development—and before you check it into a formal build—then it's like the defect never even happened. You get a lower defect injection rate for your project that certification entities love to see, because it means you have a very mature development organization.

MAKING CODE ANALYSIS PART OF THE DAILY WORKFLOW

The easier code-analysis tools are to configure and use, the more likely and quickly developers are to use them and realize the benefits. Having these automated tools as part of the developer's toolbox means that you can check and improve the code quality as you write your application, while you're "in the zone" of understanding what that section of code is meant to do and how it interacts with other modules in the system. To do this effectively, the tools must be integrated into the daily workflow.

> "Compiler errors are displayed early in the development process and integrated into the developer workflow. We have found expanding the set of compiler checks to be effective for improving code quality at Google."

When looking through what others are saying in regards to integrated code analysis, I found that Google published an article, "Lessons from Building Static Analysis Tools at Google," in *Communications of the ACM*, looking at the merits of code analysis. Though the article takes a holistic view of their entire codebase including C, C++, and Java, their results are very clear:

"Compiler errors are displayed early in the development process and integrated into the developer workflow. We have found expanding the set of compiler checks to be effective for improving code quality at Google."

The authors stated that moving static-analysis checks into the compiler workflow and making them appear as errors drastically improved the attention paid to the tool's findings, and that it ultimately meant that their code was of a much higher quality. Further on, they talk about a survey sent to developers who recently encountered a compiler error and developers who had received a patch with a fix for the same problem:

"Google developers perceive that issues flagged at compile time (as opposed to patches for checked-in code) catch more important bugs; for example, survey participants deemed 74% of the issues flagged at compile time as 'real problems,' compared to 21% of those found in checked-in code."

The article also talks about the importance of having code analysis part of the workflow by stating that when they automatically ran commits through a static-analysis tool and invited engineers to look at the analysis dashboard, very few engineers followed through. Having instant feedback in the compilation process made static analysis easier to use and harder to ignore. Therefore, they chose to integrate static analysis by default in everyone's workflow. They believe that for code-analysis tools to succeed, developers must feel they benefit from their use and enjoy using the tools.

But what kind of results can you expect to see from adding code analysis to your workflow? One thing is an improvement in the overall security of your application—having high code quality can eliminate exploits like buffer overflows, illegal pointers, and the like, as described in the article, "Improving Software Assurance through Static Analysis Tool Expositions."

While this in and of itself is a compelling reason to use code analysis, it's sometimes hard to convince people of

the maxim that "an ounce of prevention is worth a pound of cure." You often need even more significant results to convince developers and management alike of the merits of code analysis.

A paper by Stefan Wagner and others used empirical data to calculate the benefit of code-analysis tools vs. traditional testing on different code bases. Their results are very telling: Out of the 769 identified defects, 76% were caught by code-analysis tools and only 4% by traditional testing (the remaining 20% found by code review).

How fast could you achieve your mean-time-to-failure (MTTF) goal in software if you could eliminate 75% of your bugs before you even begin testing? The answer is "awfully quick." The time and money savings on testing alone make the investment in code-analysis tools worthwhile, not to mention the savings in time to market. These are the types of processes that functional-safety certification entities love to see because it drastically reduces the risk of defects making it into the field in your final product.

HIGH-QUALITY CODE SPEEDS YOUR PATH TO FUNCTIONAL SAFETY

The key to accelerating the functional-safety certification process is to improve your code quality. By improving code quality, you lower your defect injection rate, which means you more quickly reach the software release criteria. Thus, your development organization looks very mature to a functional safety-certification entity. While you can never know exactly how many defects are left in an application, you can minimize the number by using code-analysis tools early and often. ed

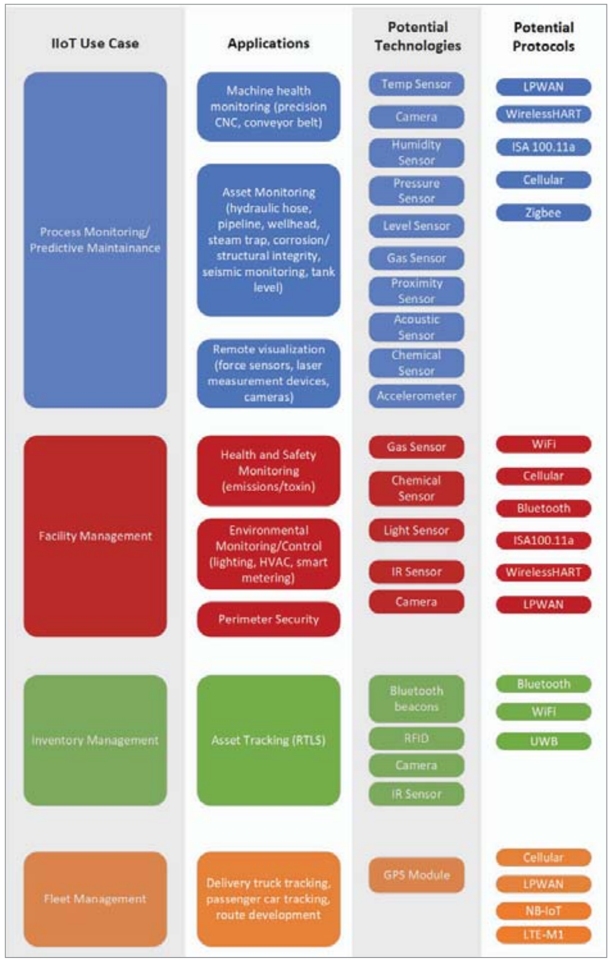
TINU OZA | IoT Product Manager, L-com

Understanding the Underlying Sensor and Wireless Technologies in IIoT Apps

This article details some of the more common industrial IoT applications that utilize wireless sensor technology to control, monitor, and report on critical processes and control functions.

From the connected home and smart wearables to Industry 4.0 and smart-city applications, wireless sensor networks (WSNs) permeate nearly every conceivable application. They bring automation to simple manual tasks with remotely controlled actuators and monitoring/tracking environments with evolving microelectromechanical-systems (MEMS) sensors. These relatively simple, energy-constrained devices reveal a massive potential in data collection and data analytics to better assess human, machine, and even plant systems.

In industrial IoT (IIoT), short-range wireless solutions, cellular, and low-power wide-area networks (LPWANs) can be leveraged to support the various sensor nodes. The choice of industrial communications depends on whether the process is time-critical with the need for real-time data or is non-time critical with either frequent or infrequent transmissions. Depending on the industrial application at hand, there are numerous IIoT use cases in which many sensor technologies and/or communication protocols may be brought to bear *(Fig. 1)*.



1. Depending on the industrial application at hand, there are numerous IIoT use cases in which many sensor technologies and/or communication protocols may be brought to bear.

PROCESS MONITORING

Process monitoring is likely to be the largest application for industrial WSNs (IWSNs) as it requires the placement and tracking of thousands to tens of thousands of sensor nodes over vast distances. This centralized method of tracking industry operations is what leads to realizing predictive maintenance strategies that systematically minimize factory downtime and save on operational overhead.

MACHINE-HEALTH USE CASES AND COMMON SENSOR TYPES

Hyper-specialized equipment is leveraged all over IIoT because monitoring common faults is critical to maintain optimal performance of machine equipment. For instance, while a high-end computer-numerical-control (CNC) system can perform precision machining on a massive scale, it can encounter the common faults of spindle unbalance.

Should such a fault occur, the mass unbalance in the spindle system can cause the machine tool to vibrate, ultimately degrading machine accuracy and potentially causing further machine damage if left unrepaired.[1] Typically, the bearings within the spindle are analyzed for vibrations as they allow the shaft to stay

Wireless Technologies Used in IoT

Parameters	Operating Frequency	Maximum Range	Throughput	Latency	Bandwidth	Battery life	Device #
WirelessHART	2.4 GHz	~200m	250 kbps	10-50 ms	3 MHz	several years	30,000
ISA 100.11a	2.4 GHz	~200m	250 kbps	~ 100 ms	5 MHz	several years	unlimited
LoRa	915 MHz (US), 868 MHz (Eur), 433 MHz (Asia)	5-20km	0.3-50 kbps	-	7.8-500 kHz	10+ years	50,000
NB-IoT (LTE Cat NB2)	Cellular bands	1- 10 km	159 kbps	1.6-10s (NB1)	180 kHz	10+ years	100,000
LTE-M2 (LTE Cat M2)	Cellular bands	>11 km (M1)	4 Mbps (DL), 7 Mbps (UL)	10-15ms (M1)	5 MHz	-	>>100,000
Sigfox	868 MHz, 902 MHz	>50km	100-600 bps	-	100-600 Hz	10+ years	-
Bluetooth 5 Low Energy	2.4 GHz	<200 m (PtP), <1.5km (mesh)	1 to 3 Mbps	<3ms	~ 2 MHz	-	32,767
WiFi	2.4, 3.6, 4.9, 5, 5.9 GHz	< 300 ft	>54 Mbps	1-3ms	~22 MHz	-	-

802.15.4-based

LPWAN

Popular Protocols

in place while rotation occurs—uncharacteristic vibrations would therefore be apparent with these components.

Accelerometers are able to monitor and detect such machine-tool failures by collecting vibration data. Ultrasonic and acoustic emission sensors can detect damage within the bearings of the spindle before any noticeable vibrations occur by discerning the ultrasonic acoustic emissions resulting from metal degradation. Armed with knowledge of the nominal thermal operation, temperature sensors can also note temperature anomalies in various critical components within the machine. An inductive current sensor would detect variations in the current consumed by the electrical motor, too, and similarly detect anomalies.

These same principles can be applied to any large machine that includes a large electric motor. Cranes, for instance, are often used in manufacturing facilities to move large, heavy equipment from passenger cars to airplanes. Pulleys and electric motors will be found in conveyor belts that are leveraged in a broad array of applications including coal mining, food processing, and chemical segregation. Accelerometers, temperature sensors, and inductive current sensors are all useful in adequate monitoring of such machines.[2]

ASSET-MONITORING USE CASES AND COMMON SENSOR TYPES

Oil and gas manufacturers monitor assets such as pipelines over vast distances. In this application, leaks and ruptures are avoided at all costs to prevent the potential loss of life and damage to the environment. Pipelines have several significant failure modes, including construction/manufacturing defects; damage during installation; corrosion; and earth forces such as earthquakes, land slips, and extreme weather-related incidents.[3]

External accelerometers can monitor the pipeline's flow rate by tracking flow-induced vibrations. Crack monitoring can be accomplished through ultrasonic detection or transverse magnetic-flux leakage. Failures due to corrosion can be prevented through several sensors with technologies like RFID and fiber optics. Seismic sensors can provide a subsurface map for offshore drilling rigs, improving rig efficiency.

In chemical, food, and pharmaceutical processing facilities, mixing tanks rotate chemicals and ingredients that are added in precise values. Sensors placed at key locations on these tanks measure parameters such as temperature, humidity, pressure, pH value, and fill level, thus ensuring optimal plant operational procedures with little to no manual intervention.

IoT protocols for process monitoring vary greatly depending on the application. The *table above* lists some commonly used IoT protocols and some of their respective key parameters. Oftentimes, WSNs monitor machine health within a facility that, when compared to some asset-monitoring applications such as tracking pipeline health, is contained within a relatively small area.

In cases where small payloads of data are transmitted infrequently, LPWANs such as LoRa, Sigfox, and NB-IoT offer narrowband modulation schemes at sub-gigahertz frequencies—two qualities that increase signal range. The LPWANs are known not only for large transmission distances, but also for long battery lifetimes beyond 10 years and one-to-many architectures in which thousands of devices can be wirelessly connected to a gateway (when sensor nodes can be deployed on the scale of tens of thousands, energy-harvesting techniques and battery lifetime are critical considerations).

However, LPWAN protocols are often asynchronous with unscheduled transmissions. Thus, they're susceptible to data collisions at high network capacities. This would not be ideal for time-critical IIoT applications that require deterministic and reliable transmissions with a low bit error rate (BER). Industry-specific wireless networks such as WirelessHART and ISA100.11a are based on IEEE 802.15.4, low-rate wireless personal-area networks (LR-WPANs). With a maximum range of 200 meters, these offer up to a 250-kb/s throughput and latencies of 10 to 100 ms for more real-time communication on critical processes.

HEALTH AND SAFETY

Monitoring the environmental conditions with the respective intelligent alarm installations is essential in protecting industrial workers and maintaining smooth operations. This often involves the use of gas/chemical-based sensor nodes around areas of particular risk.

In the oil and gas industry, tracking highly combustible methane leaks is paramount in preventing any potential explosions around wellheads. Steam traps leverage a huge range of manufacturing facilities to filter out condensate from air without letting steam escape. A faulty steam trap would fail to remove water droplets from steam, causing water to accumulate and rupture steam lines, leading to expensive downtime and safety hazards.

Acoustic sensors and temperature sensors have been used to monitor the behavior of these critical components to prevent any costly failures. Underground mines are notorious for hazardous safety conditions; environmental parameters such as carbon-monoxide emissions, methane emissions, and airflow are actively monitored to ensure a safe working environment.

Reliable and deterministic protocols are necessary for these applications, often calling for WirelessHART or ISA100.11a communications within the facility. While these protocols may consume more power on sensor nodes than other WSN technologies such as Bluetooth Low Energy (BLE) or LPWANs, the ability to perform real-time analysis and control on data is critical to ensure adequate safety measures.

Both WirelessHART and ISA100.11a were specifically designed for industrial applications. WirelessHART is the wireless alternative to the existing HART technologies and ISA100.11a was developed by the International Society of Automation (ISA) to support multiple protocols already used in industrial applications, including HART, Modbus, Foundation Fieldbus, and ProfiBus. Both networks support star and mesh networking with bidirectional communication from the host to the sensor node.[4]

ASSET TRACKING WITH RTLS

Compared to outdoor tracking systems that rely on GPS and typically yield an accuracy around 10 m, indoor position systems (IPSs) such as real-time location systems (RTLSs) can achieve accuracies on par or lower without the major consideration of satellite signals penetrating factory walls. The *table above* lists some of the more commonly used RTLSs.

Such IPSs can be applied on the plant floor to actively track moving indoor equipment like forklifts and actively track inventory in transport within a facility. Outdoor environments, e.g. truck yards, can leverage RTLSs to monitor and manage truck movement by assigning docks and tracking loading/unloading of cargo.

Indoor positioning systems will employ either a trilateration or a fingerprinting localization method, depending on the wireless protocol in use. Trilateration uses estimated distances to calculate the likeliest coordinates of an object. The fingerprinting method compares current signal characteristics with a previously catalogued set of signal characteristics obtained from fingerprint locations—implementing this is often more technically involved. The movement of a sensor can then be obtained by comparing the online measurements with the "fingerprint." For brevity, this section will cover two popular RTLS protocols: Bluetooth and Ultra-wideband (UWB).

LEVERAGING A UWB SYSTEM FOR RTLS

Ultra-wideband (UWB) technology essentially sends a burst of energy of extremely short duration.

For RTLS applications, the short pulses in UWB modulation allow for precise delay estimates, ultimately yielding position/location data. Typically, UWB technology leverages time-of-arrival (ToA) and time-difference-of-arrival (TDoA) information generated by tags that emit low-power UWB pulses which are received by the sensors or UWB readers. Those pulses are used to determine the precise 3D location for a tag with centimeter accuracy. However, precise time synchronization is needed between the UWB readers within a network to successfully gain location data.

The UWB frequencies have frequency allocations between 3.1 and 10.6 GHz. Typically, a planar monopole antenna is employed in these applications due to their omnidirectional radiation pattern and ability to yield stable input impedance over the large frequency bandwidth. Because of their performance into the X-band and the fact that trace dimensions grow smaller at higher frequencies, these antennas offer a small form-factor solution that can be printed on the same PCB holding the transmitter/receiver.[5]

RTLS Technologies

RTLS Technology	Accuracy	Real-time Tracking	Range
Bluetooth	1m to 4m	Yes	~75m
WiFi	5m to 15m	Yes	~50m
UWB	sub-meter	Yes	~50m
Passive RFID	<1 m	No	~50m

BLUETOOTH BEACONS

While already a prolific short-range protocol, BLE modules are utilized in RTLS applications by delivering Bluetooth beacons to disseminate localized content. These beacons can act as proximity sensors by broadcasting low-energy signals with packets of data at predetermined intervals of time (>100 ms).

Distances are calculated with received signal-strength indicator (RSSI) readings, ultimately extrapolating distances between nodes based on the mathematical relationship between the strength of the received signal and the propagation of an RF signal through space.[6] This creates a live map of inventory outfitted with unique IDs and BLE tags with actively updated location data. Because most smart devices are Bluetooth-enabled (i.e., smartphone, tablet, laptop), this can potentially eliminate the need for custom hardware, leading to dramatic cost savings.

While BLE does support mesh topologies with bidirectional communications, BLE beacons generally support one-way communications and are therefore limited to star topologies. In such configurations, beacons connect to a Bluetooth-enabled device/router and relay information to the cloud, typically via cellular or Wi-Fi.

As alluded to earlier, many of these beacons can include multi-protocol SoCs with a sub-gigahertz, long-range wireless network to control/monitor factory environments with smart lighting or HVAC control. The large window for the advertising packet can allow for the sub-gigahertz radio to be in a receiving state, obtaining non-frequent and unpredictable packets of information from distant locations within the facility.

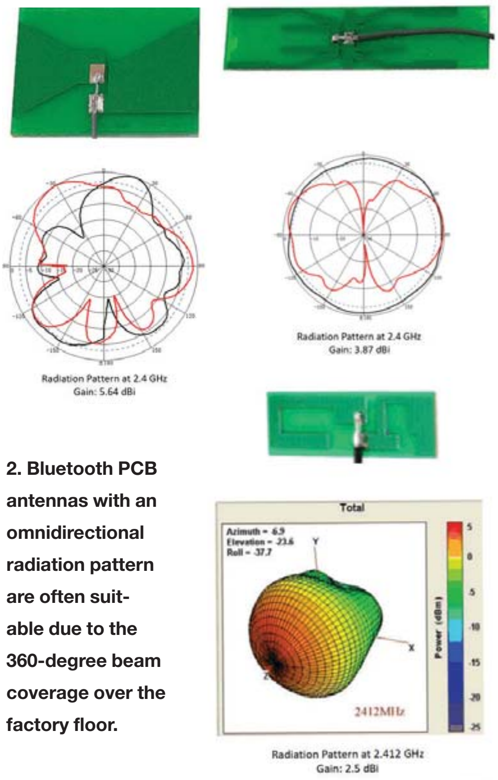
Typically, BLE beacon designs will involve a 2.4-GHz PCB antenna combined with a vendor-specific Bluetooth chip. In some cases, the Bluetooth chip will have an integrated chip antenna. If the board employed a sub-gigahertz frequency protocol, a PCB antenna would not be viable as it would be too large.

As stated earlier, BLE typically uses trilateration (RSSI) to determine location areas. In this case, an omnidirectional radiation pattern is often suitable due to the 360-degree beam coverage over the factory floor, so long as the antenna matches the transmitter's impedance for maximum signal transfer and range *(Fig. 2 on page 24)*. However, a TDoA algorithm can be implemented, calculating either two angles from a singular beacon signal, or three angles from two beacon signals. In this case, a 3D map can potentially be created with the use of the complex mapping and placement of BLE beacons outfitted with more sophisticated antenna arrays.[7]

FLEET MANAGEMENT

Industrial fleet management can vary with passenger cars, tractor trailers, railways, airplanes, ships, and heavy equipment. Trucks alone account for 70% of the goods transported in the United States, making tracking logistics such as repairs, replacements, and scheduled maintenance all the more important to prevent poor fleet operation. Typically, the cellular infrastructure is used for applications that transcend plant-wide boundaries. However, in the case of localized equipment such as heavy equipment operation within a mine, LPWANs can be considered.

Fleet telematics can communicate with 2G, 3G, and 4G infrastructures or IoT-specific cellular alternatives such as NB-IoT or LTE-M1. Sensor nodes can consist of GPS modules, gyroscopes, level sensors, and accelerometers. Where the GPS provides location data, the accelerometer offers the orientation of the vehicle, and the level sensor measures fuel in real time. More complex systems are also utilized for fleet management; autonomous mining trucks have been in operation since 2008, outfitted with over 200 sensors, a GPS receiver, and radar guidance system.[2]



2. Bluetooth PCB antennas with an omnidirectional radiation pattern are often suitable due to the 360-degree beam coverage over the factory floor.

SUMMARY

An array of sensors and communication protocols can serve industrial networks depending on the required level of reliability, latency, and flexibility. Process monitoring and health and safety applications often require real-time communications with IEEE 802.15.4-based protocols (e.g. ISA100.11a, WirelessHART), while some asset-monitoring applications can benefit from the long range offered by LPWAN applications.

Indoor asset-tracking applications have specific localization systems with ToA- or RSSI-based algorithms for accuracy. Fleet-management systems, on the other hand, can rely on GPS for location data but must transfer all sensor data to a centralized point via cellular backhaul. They can even benefit from LPWAN if the fleet is based in a restrictive geographic location. ed

REFERENCES

1. Wang, Zhan, et al. “Optimization and Experiment of Mass Compensation Strategy for Built-In Mechanical On-Line Dynamic Balancing System.” *Applied Sciences, vol. 10, no. 4,* 2020, p. 1464., doi:10.3390/app10041464.

2. Zhou, C et al. “Industrial Internet of Things: (IIoT) applications in underground coal mines.” *Mining engineering vol. 69*,12 (2017): 50-56. doi:10.19150/me.7919

3. Kishawy, H. and Gabbar, H., 2010. Review of pipeline integrity management practices. *International Journal of Pressure Vessels and Piping,* 87(7), pp.373-380.

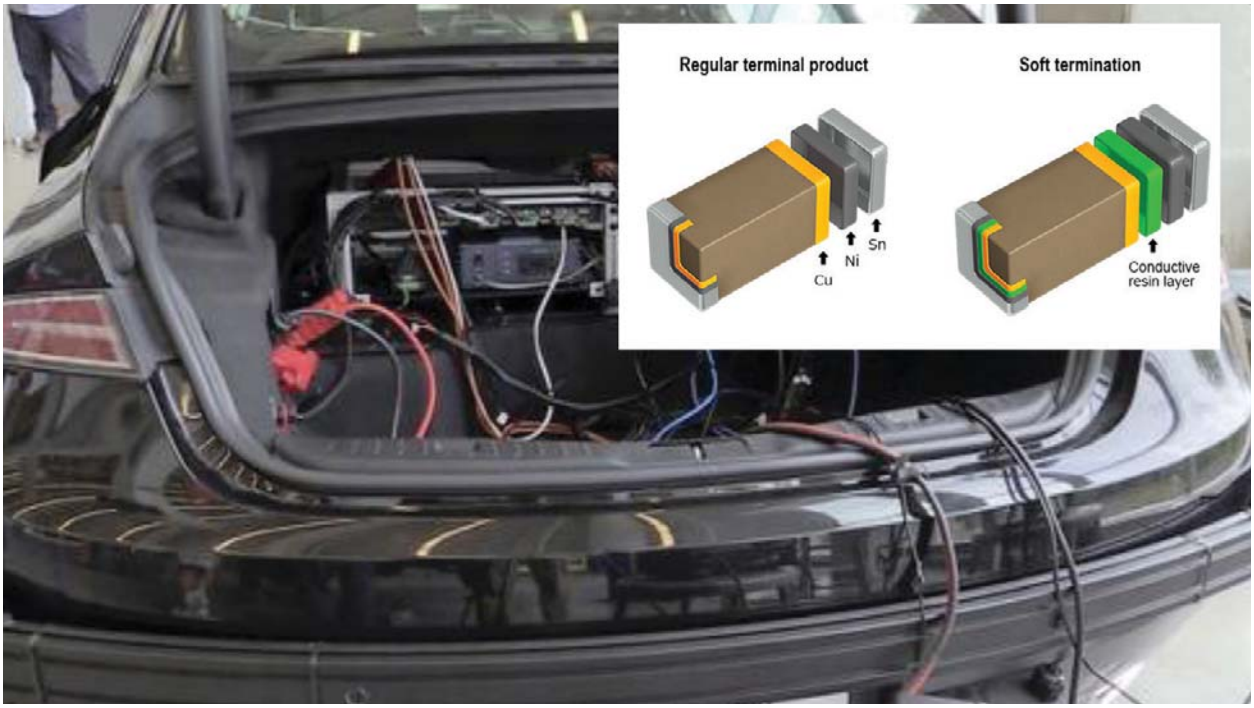
4. Peter M (2017) Industrial wireless mesh network architectures. L-com Global Connectivity. *https://www.l-com.com/images/downloadables/white-papers/wp_wireless-industrial-mesh-networks.pdf*

5. Y. Lu, Y. Huang, H. T. Chattha and P. Cao, “Reducing Ground-Plane Effects on UWB Monopole Antennas,” *IEEE Antennas and Wireless Propagation Letters,* vol. 10, pp. 147-150, 2011, doi: 10.1109/LAWP.2011.2119459.

6. A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura and A. A. F. Loureiro, “Localization systems for wireless sensor networks,” *IEEE Wireless Communications, vol. 14, no. 6,* pp. 6-12, December 2007, doi: 10.1109/MWC.2007.4407221.

7. https*://www.bluetooth.com/wp-content/uploads/Files/developer/1903_RDF_Technical_Overview_FINAL.pdf*

MICHAEL CANNON | Product Manager, TDK Corporation of America



Optimize Reliability in ADAS and EV Applications with Soft Termination

As automotive electronic content increases due to ADAS and EVs and autonomous driving grows more prevalent, rugged passive components have become critical to vehicle performance, safety, and reliability.

Advanced driver-assistance system (ADAS) applications form one of the fastest-growing segments of automotive electronics. Stringent government regulations and consumer interest in safety applications that protect drivers and reduce accidents are fueling this rise. In parallel, government legislation and the effect of CO_2 or EPA regulations are driving the industry to move away from traditional fossil fuels to electric powertrains. According to a Frost & Sullivan study released in November 2019, global sales of electric vehicles (EVs) are set to increase to about 34 million in 2025, 121.2 million in 2030, and 636.7 million by 2040.

As a result of both trends, the auto industry is incorporating more multifunctional capabilities into automobiles. For example, high-power electronic control units (ECUs) support image processing for ADAS, whereas low-power ECUs are ideal for sensor and body applications. Moreover, to reduce latency in gathering data, these ECUs are now being installed in closer proximity to environmentally challenging locations, such as the engine compartment.

To meet the industry's ISO 26262 functional safety standard for automotive electronic equipment, reliability is a critical factor. ADAS applications need, more than ever, passive components that have the durability required for mechanical strength and the ability to withstand rapid temperature cycles. These include multilayer ceramic chip capacitors (MLCCs), inductors for decoupling and power-supply circuitry, and chip beads for signal and power-supply lines.

One strategy to support this requirement is to use components with resin electrodes (soft termination), which address the two common failure mechanisms: flex cracks and solder cracks.

MAJOR CAUSES OF FLEX CRACKS

Flex cracking is due to excessive circuit board flexure. This can happen during the manufacturing process, such as solder stress due to an inappropriate amount of solder, stress applied at the time of de-paneling, or screw fastening. It can also occur during final assembly and during use, stemming from exposure to continuous vibration.

MLCCs and ferrite components tend to be strong when under compression, but weak in tension. This discrepancy is due, in part, to the brittle nature of ceramics. When subjected to a tensile load, they're unable to yield and relieve the stress, unlike metals. Thus, when a soldered component experiences excessive board flex, a crack is easily generated in the element.

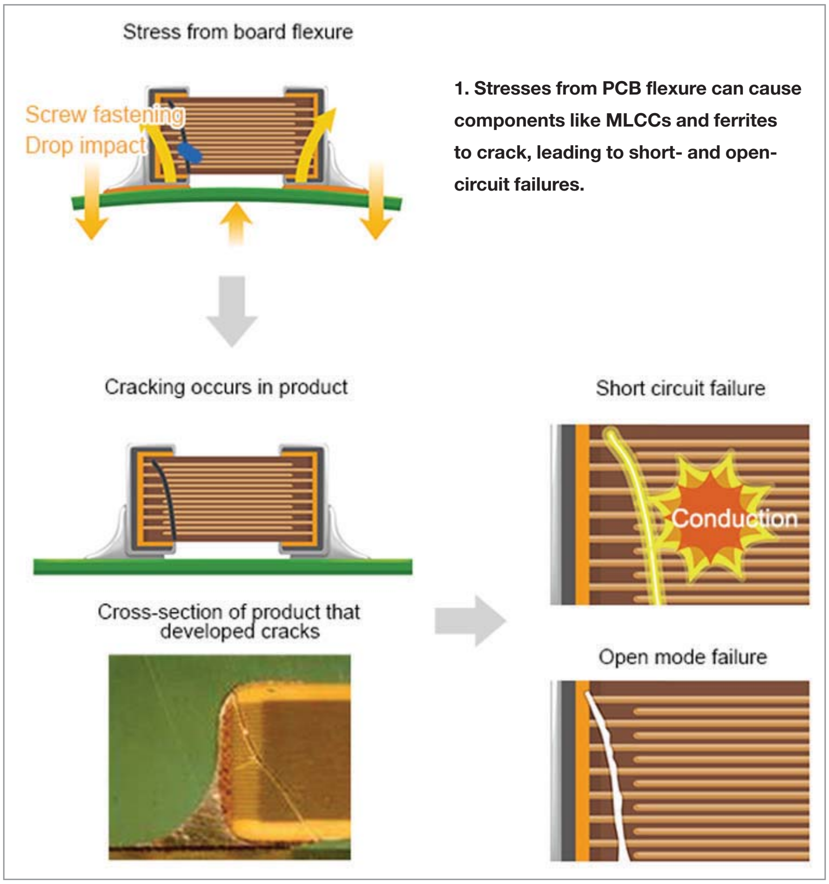
A flex crack can cause the formation of an electrical conduction path between opposing internal electrodes. It's also possible that a flex crack can propagate to a fail short condition with continued voltage and temperature cycling *(Fig. 1).* If a crack in a component progresses to a short-circuit failure, it may lead to problems such as heat generation, smoking, or ignition.

HOW TO MITIGATE FLEX CRACKS

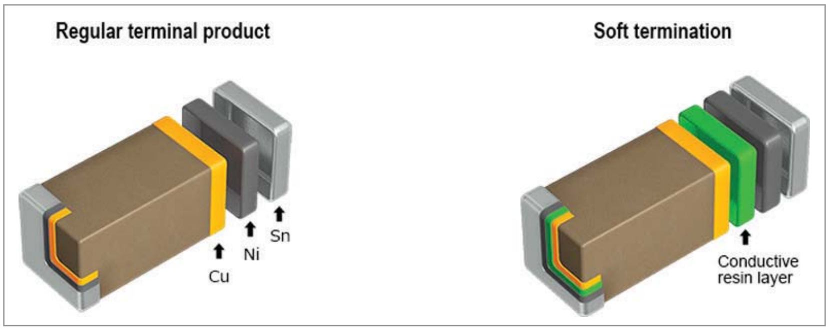
In the terminal electrode of a traditional MLCC, the copper (Cu) underlayer is electroplated with nickel (Ni) and tin (Sn). Soft termination is achieved by adding a conductive resin layer in between the Cu and Ni plating layers *(Fig. 2).* This resin layer acts to reduce the stresses accompanying expansion or shrinkage of the solder joints due to thermal shock or flex stress on the board, which lead to cracking of the capacitor element.

A flexure strength test comparison in *Figure 3 (on page 28)* shows the onset of cracking in the standard product at about 4 mm of deflection. In contrast, no cracking occurred in the soft-termination product even with over 10 mm of bending stress applied. Although there was peeling of the nickel layer and the conductive resin layer, cracks in the ceramic body were prevented.

Taking it one step further, in battery power lines, safety can be greatly enhanced by replacing a traditional MLCC with one that features a dual fail-safe function. MLCCs with dual safety design provide the highest protection



1. Stresses from PCB flexure can cause components like MLCCs and ferrites to crack, leading to short- and open-circuit failures.



2. Soft termination is achieved by adding a conductive resin layer in between the Cu and Ni plating layers, which serves to dampen the physical stresses of expansion or contraction of solder joints.

from cracking and short-circuit occurrences. Firstly, the conductive resin is layered in the terminal electrodes, preventing crack occurrences. Secondly, the internal electrodes adopt a special structure, which is equivalent to a series-connection of two capacitors.

Such a structure will reduce the risk of short-circuiting, even if a crack does occur on the capacitor element. Moreover, since just one serial design MLCC can achieve AEC-Q200-compliant safety, instead of requiring two standard MLCCs connected in series, the parts count, PCB space, and mounting costs are cut in half.

Similarly, in the terminal electrode structure of traditional inductors and chip beads, the silver (Ag) underlayer is plated with Ni and Sn. Soft termination is achieved by applying a conductive resin layer between the Ag and Ni plating layers.

In comparison tests, multilayer inductors and chip beads—with resin electrodes—have nearly twice the board flex resistance (critical bending) of products with conventional electrodes. In traditional products, cracks developed on the ceramic element with a flex of about 4 mm. In contrast, products with soft termination can safely withstand cracking at 7 mm of flex.

MAJOR CAUSES OF THERMAL CRACKS IN SOLDER JOINTS

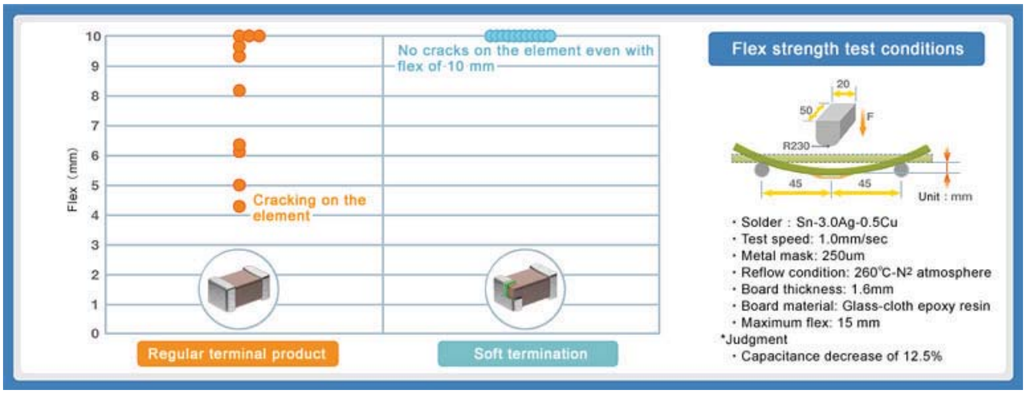
Solder cracks occur mainly because of thermal fatigue due to thermal shock or temperature cycles and/or the use of lead-free solder, which is more brittle than lead-bearing solders. Therefore, special caution is required when mounting passive components near sources of excessive heat that may experience sudden temperature changes (thermal shock).

When thermal stress is applied repeatedly to a solder joint, the coefficient of thermal expansion (CTE) mismatch of the passive component and PCB could cause solder cracks. This can also occur when temperature control is insufficient during the soldering process.

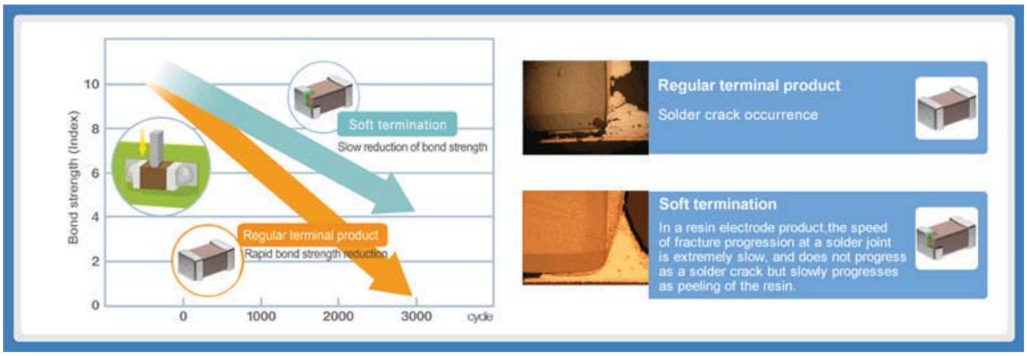
HOW SOFT TERMINATION MITIGATES THERMAL CRACKING

MLCCs with resin electrodes help to reduce thermal cracks in solder joints due to their outstanding thermal shock resistance *(Fig. 4 on page 28)*. In shear strength tests, a standard termination product is compared with a resin electrode product after 3,000 thermal shock cycles from −55 to +125°C. While the push strength of the conventional product decreases by approximately 90%, the soft-termination MLCCs maintain 50% of their shear strength.

The 2,000-cycle thermal shock test data of inductors and chip beads (−55 to



3. In a comparison of the flex strengths of a regular terminal product and a soft-termination device, element cracks occurred in the regular product after it was flexed up to about 4 mm. In contrast, no cracking occurred with soft termination, even after it was flexed 10 mm.



4. Bond strength is significantly greater with soft termination; this comparison illustrates the rate of bond-strength decrease in normal terminal devices compared with soft terminations.

150°C) shows that the anchoring strength of the conventional product declined approximately 50%, as compared to around 20% for the resin electrode.

CONCLUSIONS

Mechanical stresses can produce cracking in passive components, resulting in circuit failure. Similarly, solder cracking will occur when there's excessive stress between the board and the solder joint, causing an open circuit or the component to lose adhesion to the PCB.

Therefore, caution is required when placing components in locations that may experience significant post-solder handling stresses, such as near mounting screws, PCB edges, and corners. Additional attention should be paid to locations where extreme temperature changes (thermal cycling) occur, such as in an automobile's engine compartment. Due to the enhanced robustness of soft-termination products, the effects of board flexure and thermal shock stresses can be suppressed, improving connection reliability. ed

Lab Bench

WILLIAM WONG | Senior Content Director

bwong@endeavorb2b.com

Checking Out GigaDevice's RISC-V with IAR's MISRA-C

Editor Bill Wong checks out IAR's GigaDevice GD32V RISC-V development board.

IAR Systems is known for its IAR Embedded Workbench along with a host of security and embedded development tools like the Visual State state-machine model development toolkit. It complements these with evaluation kits that highlight the hardware and their software.

The focus of this article is the IAR RISC-V GD32V evaluation board built around the GigaDevice Semiconductor GD32VF103 microcontroller *(see figure)*. This micro has up to 128 kB of on-chip flash memory compared to the SiFive HiFive RISC-V chip I looked at earlier that used an off-chip SPI flash chip for application code.

The GD32VF103 is based on the Bumblebee core. This is the same core used by Andes Technology's AndeStar V5 chip. The Bumblebee core supports the RV32IMAC instruction set, which means that it's a 32-bit integer core (RV32I) with multiply/divide (M), atomic instructions (A), and compressed instruction (C) support. The system employs a two-stage variable-length pipeline architecture.

The platform's register file includes 32 registers. The 32-bit instructions are the norm with 16-bit compressed instructions as well. This is very similar to other popular 32-bit microcontroller architectures. The compressed 16-bit instructions can result in a 25% to 30% reduction in code size.

The 32-bit chip runs at 108 MHz and has the usual complement of micro peripherals. These include multiple timers, UARTs, SPI, I^2C, I^2S and an external memory controller. There are dual CAN 2.0B controllers and a USB 2.0 OTG controller. There's a mix of RISC-V 16- and 24-bit timers and GigaDevice adds a 64-bit real-time timer to the mix. Analog peripherals include a 1-Msample/s ADC plus dual 12-bit, 16-channel ADCs and dual 12-bit DACs. Versions are available with up to 80 GPIOs.

IAR's development board is built around the GD32VF103RBT6 RISC-V microcontroller from GigaDevice Semiconductor. The I-Jet Lite provides JTAG support.

The system needs a power supply from 2.6 to 3.6 V dc and has 5-V-tolerant I/O pins. It has multiple low-power modes and a standby-current requirement of 6.3 µA. Package options include QFN36, LQFP48, LQFP64, and LQFP100. Available development tools include Nuclei Studio, IoT Studio, and SEGGER Embedded Studio in addition to the IAR Embedded Workbench. It's compatible with a variety of operating systems including µC/OS II, FreeRTOS, RT-Thread, TencentOS-tiny, and LiteOS.

BUILDING BETTER CODE

The IAR Embedded Workbench comes with IAR's C/C++ compiler. This includes support for more than the typical open-source C/C++ compiler, such as support for MISRA C and IAR's C-STAT static-analysis tool. C-STAT adds MISRA C++ support. It also maps checks to Common Weakness Enumeration (CWE) issues.

If you want to write better C code, then including MISRA C in the mix is a good idea. The Workbench provides fine-grain control of the rules that are enabled. It defaults to the required set, but you can add or remove them at will.

I did try out MISRA C and C-STAT on the sample applications. It's obvious that IAR didn't do this, as each project kicks out hundreds of notifications. This is typical as most C/C++ programmers don't follow these rules. However, most tend to be trivial details. For example, disabling a few of the rules like 2.2, 5.1, and 16.5 significantly reduces the number of notifications.

The use of single-line comments is where rule 2.2 comes in, and limiting the number of characters in a symbol to 51 is rule 5.1. The use of f() versus f(void) in a function definition is rule 16.5.

MISRA C is still a far cry from Ada and SPARK, but it's much better than coding without the use of a static-analysis tool. IAR provides sufficient customization to allow for additional checks without causing problems in development. It works best when using it on a new source code file, but working it into existing code can be worthwhile as well.

Overall, I'm a fan for IAR Embedded Workbench, especially its MISRA C support. It has fewer bells and whistles than something like Eclipse, but that's an advantage for many projects, especially if your focus is the micro. ed

United States Postal Service

Statement of Ownership, Management, and Circulation **(Requester Publications Only)**

1. Publication Title: ELECTRONIC DESIGN
2. Publication Number: 172-080
3. Filing Date: 8/31/20
4. Issue of Frequency: Bi-monthly - Jan/Feb, Mar/Apr, May/Jun, Jul/Aug, Sep/Oct, Nov/Dec
5. Number of Issues Published Annually: 6
6. Annual Subscription Price: Free to Qualified
7. Complete Mailing Address of Known Office of Publication (Not Printer): Endeavor Business Media, LLC, 1233 Janesville Ave, Fort Atkinson, WI 53538 — Contact Person: Debbie M Brady, Telephone: 941-208-4402
8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not Printer): Endeavor Business Media, LLC,331 54th Ave N., Nashhville, TN 37209
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor - Publisher: Tracy Smith, Endeavor Business Media, 331 54th Avenue N., Nashville, TN 37209; Editor: William Wong, Endeavor Business Media, 331 54th Avenue N., Nashville, TN 37209; Managing Editor: ,
10. Owner - Full name and complete mailing address: Endeavor Media Holdings I, LLC, 905 Tower Place, Nashville, TN 37205; Endeavor Media Holdings II, LLC, 905 Tower Place, Nashville, TN 37205
11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities: None
12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes: N/A
13. Publication Title: ELECTRONIC DESIGN

14. Issue Date for Circulation Data: July/August 2020 15. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)	37,629	37,643
b. Legitimate Paid and/or Requested Distribution (By Mail and Outside the Mail)		
(1) Outside County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.)	33,142	33,380
(2) In-County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies.)	0	0
(3) Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS®	1,707	1,674
(4) Requested Copies Distributed by Other Mail Classes Through the USPS (e.g. First-Class Mail®)	0	0
c. Total Paid and/or Requested Distribution (Sum of 15b (1), (2), (3), and (4))	34,849	35,054
d. Nonrequested Distribution (By Mail and Outside the Mail)		
(1) Outside County Nonrequested Copies Stated on PS Form 3541 (include Sample copies, Requests Over 3 years old, Requests induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)	1,876	1,770
(2) In-County Nonrequested Copies Stated on PS Form 3541 (include Sample copies, Requests Over 3 years old, Requests induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)	0	0
(3) Nonrequested Copies Distributed Through the USPS by Other Classes of Mail (e.g. First-Class Mail, Nonrequestor Copies mailed in excess of 10% Limit mailed at Standard Mail® or Package Services Rates)	0	0
(4) Nonrequested Copies Distributed Outside the Mail (Include Pickup Stands, Trade Shows, Showrooms and Other Sources)	108	0
e. Total Nonrequested Distribution (Sum of 15d (1), (2), (3), and (4))	1,985	1,770
f. Total Distribution (Sum of 15c and 15e)	36,834	36,824
g. Copies not Distributed	795	819
h. Total (Sum of 15f and g)	37,629	37,643
i. Percent Paid and/or Requested Circulation (15c divided by 15f times 100)	94.61%	95.19%
16 Electronic Copy Circulation		
a. Requested and Paid Electronic Copies	-	-
b. Total Requested and Paid Print Copies (Line 15c)+ Requested/Paid Electronic Copies (Line 16a)	34,849	35,054
c. Total Requested Copy Distribution Distribution(Line 15f) + Requested/Paid Electronic Copies (Line 16a)	36,834	36,824
d. Percent Paid an/dor Requested Circulaltion (Both Print & Electronic Copies) (16b diveded by 16c x 100)	94.61%	95.19%

[x] I certify that 50% of all my distribution copies (electronic and print) are legitimate requests or paid copies:

17. Publication of Statement of Ownership for a Requester Publication is required and will be printed in the: September/October 2020 issue of this publication.

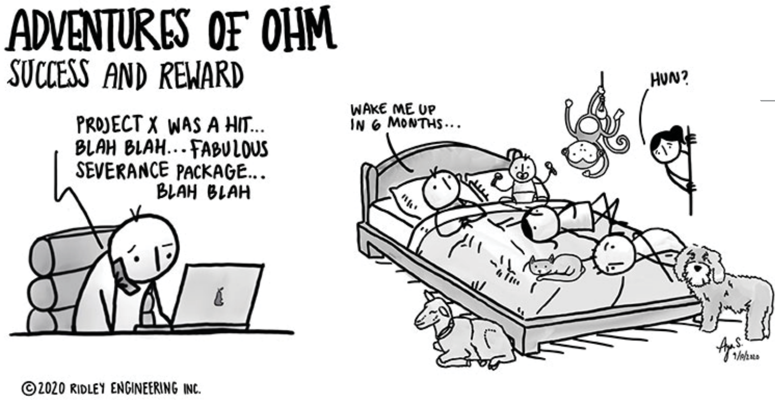
18 Debbie M Brady, Manager User Marketing — Date 8/31/20

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

PS Form 3526-R, July 2014

Ohm Confinement

DR. RAY RIDLEY | President, Ridley Engineering Inc.



OHM HAS DISCOVERED what many engineers have been through. Engineering is valuable until it's not. Nobody understands what engineers do, so it must be easy and they can be replaced at any time—or so the managers think.

OHM HAS SET UP his own microgrid and is providing power to all of the neighbors. You aren't legally allowed to sell power to others, so he has set up a bartering system. Not sure how many kWh a goat is worth, but they will work it out.

Advertisers Index


ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™
Quad-Channel Precision ADC Eases Signal Chain Design and Implementation
AD7134
▸ Alias-free sampling up to 1.5 MSPS eliminates external filter and improves phase matching.
▸ Easy-drive resistive input reduces requirements on ADC driver.
▸ New synchronization features simplify digital interface designs in multidevice distributed systems.
ANALOG DEVICES
AD7134
Buy Now at mou.sr/ADI-AD7134
MOUSER ELECTRONICS