


EMBEDDED DEVELOPER

A Diverse Set of Applications Shows the **Versatility** of the **60 GHz** Band

Accelerating Bluetooth
Low Energy Development 

Securely Control Sensors
and IoT Nodes with the
MAXREFDES143 

Now Available
On-Demand
with Registration



Eliminating Counterfeits

with Elliptic Curve Based Authentication

Every year, the electronics industry loses billions of dollars to counterfeiting. As the volume/value of the product increases, the incentive for the counterfeiter increases and a higher security level is needed to keep down the value to the counterfeiters as well as to detect counterfeits that do emerge.

The NXP Authentication Webinar Covers

- » The basics of authentication for anti-counterfeit applications.
- » Use cases and applications, hardware vs. software, symmetric vs. asymmetric crypto protocols, host and device requirements, attacks and countermeasures, and “beyond the chip” security concerns.
- » Multiple options for adding anti-counterfeit technology to your products to protect the integrity of your brand and reputation, as well as your revenue stream, and the health and safety of your customers.

Who Should Attend

- » Design engineers
- » Design managers
- » System architects



Speaker



Joe Salvador
Global Product Marketing Director,
Authentication Products,
NXP Semiconductors

Joe Salvador is Marketing Director for Anti-Counterfeit and Smart Analog Products at NXP Semiconductors. He has more than 20 years of experience in the semiconductor and technology industry.

59
min

**ELIMINATING COUNTERFEITS
WITH ELLIPTIC CURVE BASED
AUTHENTICATION**



EXTERNAL USE **NXP** | SECURE CONNECTIONS
FOR A SMARTER WORLD

REGISTER

EDITORIAL STAFF

Content Editor
Karissa Manske
kmanske@aspencore.com

Digital Content Manager
Heather Hamilton
hhamilton@aspencore.com

Director, Creative Development
Jeff Chavez
jchavez@aspencore.com

Graphic Designer
Carol Smiley
csmiley@aspencore.com

Audience Development
Claire Hellar
chellar@aspencore.com

Register at EEWeb
<http://www.eeweb.com/register/>

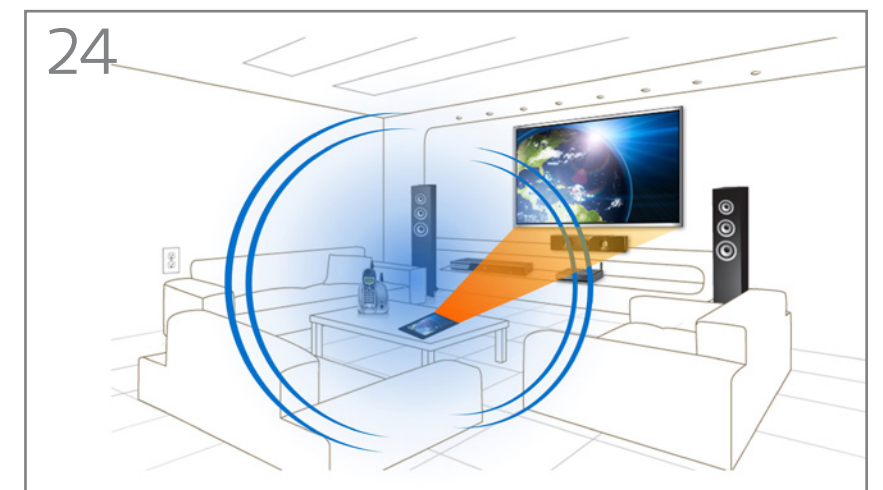
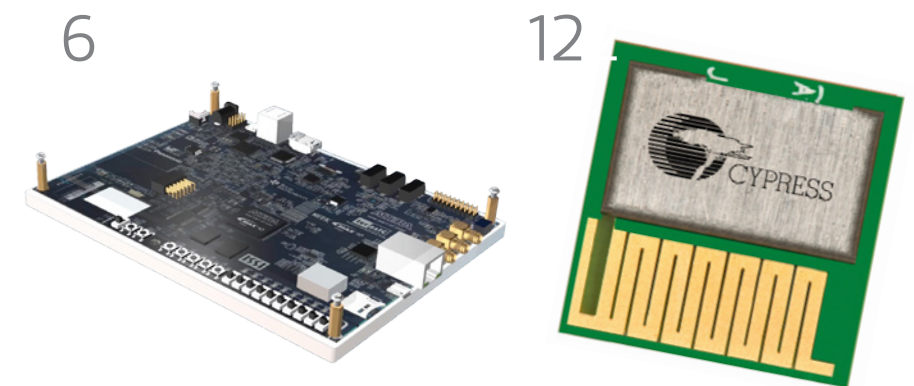
Published by
AspenCore
950 West Bannock
Suite 450
Boise, Idaho 83702
Tel | 208-639-6464

Victor Alejandro Gao
General Manager
Executive Publisher

Cody Miller
Global Media Director
Group Publisher

Glenn ImObersteg
Publisher
Contributing Editor
Embedded Developer

	PRODUCT INSIGHTS
4	NXP Security
6	Altera Max 10 NEEK
10	Securely Control Sensors and IoT Nodes with the MAXREFDES143#
	TECH REPORT
12	Accelerating Bluetooth Low Energy Development
	COVER FEATURE
24	A Diverse Set of Applications Show the Versatility of the 60 GHz Band



EEWeb



ARROW PRODUCT INSIGHTS

NXP Security

For this Arrow Product Insights, we present six communication and security product families from NXP that are driving innovation in safe and secure connected transportation, smart connected solutions, and end-to-end security and privacy applications across a wide technological landscape.

NXP's QorIQ processor family integrates crypto acceleration that allows you to develop secure connections without a performance penalty for the world's new virtualized networks ranging from the wireless infrastructure, to the smart grid, to the home.

One product within this family is the **QorIQ LS1012A**. This processor is the world's smallest and lowest power 64-bit processor, making it ideal for battery-powered and space-constrained applications such as those found in smart homes.

An alternative cyber security microcontroller is the **MPC5748G**, which delivers a secure central node connecting all vehicle domains across all interfaces. An ideal application is the automotive gateway, which connects advanced safety features such as radar and night vision along with the vehicle's infotainment system.

NXP's family of **i.MX** application processors deliver many hardware-enabled security features including secure boot, secure software downloads, and on-the-fly DRAM encryption for digital rights management, secure e-commerce, and information encryption applications. Many retail stores and popular coffee shops—where customers' sensitive digital information is constantly flowing—could take advantage of these hardware-enabled security features.

The **i.MX 6UL**, or the 6 UltraLite, is a high-performance, ultra-efficient processor family featuring an advanced implementation of a single ARMbCortex-A7 core. An ideal application for this processor would be a smart-home where there exist

home network hubs, security systems, and energy metering equipment.

NXP's family of high-performance Kinetis K8x ARM Cortex-M4 microcontrollers builds upon the **Kinetis** microcontroller portfolio. Both the Kinetis K81 and the Kinetis K82 are 150 mega-hertz advanced security microcontrollers with scalable memory. The K81 comes with Anti-Tamper Features while the K82 has a cryptographic co-processor. Large retail stores and smart homes could find this security microcontroller a necessity given today's hacking environment.

NXP's NTAG I2C plus is designed to be the perfect enabler for NFC in home-automation and to benefit from the increased security and convenience level achieved by NFC network commissioning. This device can be embedded to just about any electronic device with a very low bill of materials cost and easy integration. Think IoT devices such as light bulbs, security sensors, and wireless audio speakers. **EE**

For more info on the latest products, join us for the next Arrow New Product Insights. Visit Arrow.com.





Altera® Max® 10 NEEK

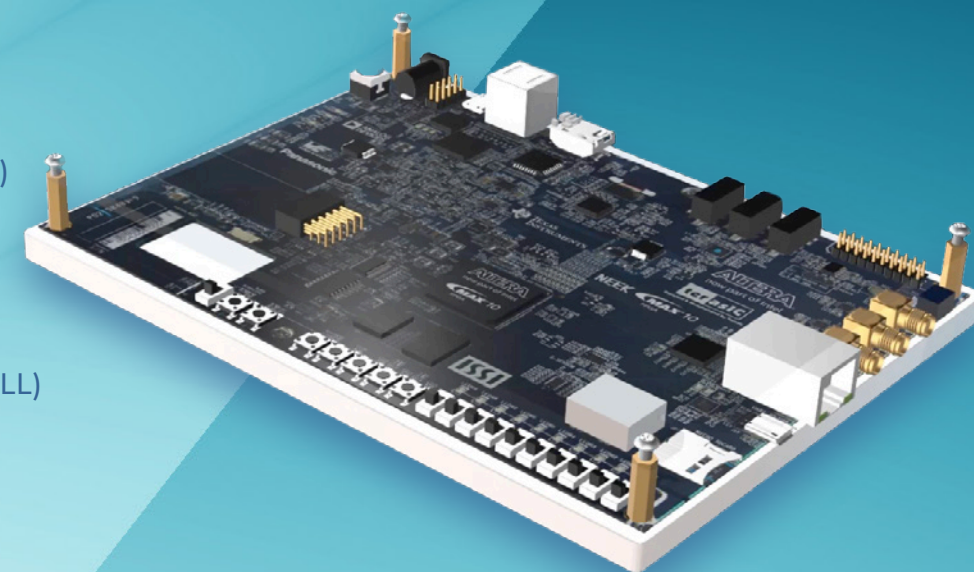
The ubiquitous microcontroller has become increasingly popular as consumers have demanded more intelligence in their products. However, as the pace of technology continues to surge, the drawbacks of microcontrollers, primarily their inflexibility, become more pronounced. FPGAs, such as Altera's MAX 10, use a softcore CPU, capable of on-the-fly changes both before and after product deployment. Changing peripherals as needed, FPGAs can integrate with changing sensor and communication technologies, keeping products current and relevant.

NEEK Features


- Logic Array Blocks (LABs)
- Analog-to-digital Converter (ADC)
- User Flash Memory (UFM)
- Embedded Multiplier Blocks
- Embedded Memory Blocks (M9K)
- Clocks and Phase-locked loops (PLL)
- General Purpose I/O
- High Speed LVDs I/O
- External Memory Interfaces

In order to practically eliminate the learning curve of working with FPGAs, Terasic, in partnership with Altera, created the Nios® II Embedded Evaluation Kit, or NEEK. The NEEK is the ideal way to familiarize yourself with the MAX 10 devices and quickly develop powerful, flexible applications. The NEEK has a wide range of features designed to demonstrate the different capabilities of the MAX 10 FPGAs as well as provide an integrated platform for custom product development.

Take advantage of the NEEK's LCD-capacitive, multi-touch panel as well as the eight-megapixel image sensor. An ambient light sensor, audio input and output, as well as a three-axis accelerometer make this ideal for multimedia and HMI applications. Combined with a wide variety of digital and analog interfaces, variable memory allocations, buttons, switches and status LEDs, the NEEK makes everything an embedded developer needs readily available.



With these tools, you can evaluate several different configurations of the Nios II processor to ascertain the ideal setup for your specific need. Change from testing and development to production configurations with ease and without any performance changes.

Ideal for high volume, cost sensitive applications in communications, consumer products, industrial, and automotive applications, discover the benefits and flexibility offered by using an Altera FPGA using the Nios II Embedded Evaluation Kit. For more information about the NEEK and Altera's MAX 10 line of FPGAs, please visit altera.com. 



Click image
to view video.



SCHEMATICS.COM

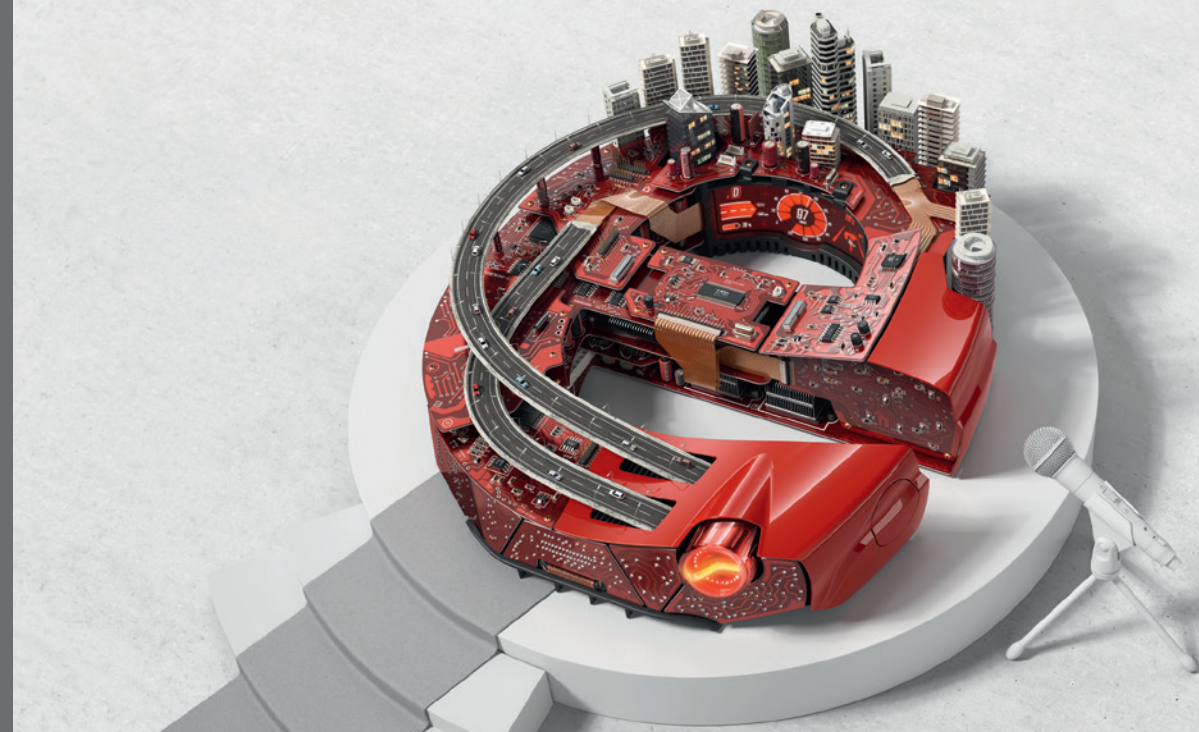
Your Circuit Starts Here.

Sign up to design, share, and collaborate on your next project—big or small.

[Click Here to Sign Up](#)



Messe München
Connecting Global Competence



electronica Automotive Conference.

International Conference on Technologies and Strategies for Automotive Electronics and Components.










Topics:

- Safety and security
- Autonomous driving
- Interior electronics

Information & Registration:

electronica.de/en/automotiveconference

List of speakers (excerpt):

								
Simon Furst BMW Group for AUTOSAR	Andreas Klage DRÄXLMAIER Group	Dr. Ludger Laufenberg Kostal	Wolfgang Lenders BMW Car IT	Steve Nadig Daimler Trucks	Dr. Reinhard Ploss Infineon Technologies	Dr. Stefan Poledna TTTech	Martin Schleicher Elektrobit	Dirk Wollschläger IBM

electronica Automotive Conference
November 7, 2016 | Messe München

The conference is held within the scope of electronica, the World's Leading Trade Fair for Electronic Components, Systems and Applications.

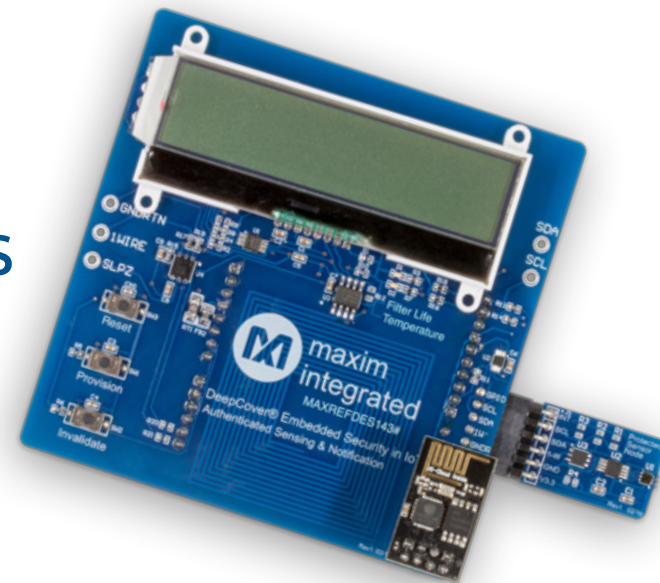


electronica 2016
inside tomorrow

Tech Trends

Securely Control Sensors and IoT Nodes with the MAXREFDES143#

Hi, I'm Ian Benz and I'm an applications engineer here at Maxim and today we're going to be taking a look at the [MAXREFDES143](#), Maxim's newest reference design for Industrial Internet of Things applications. This is the MAXREFDES143 and we're going to be using it to show how authentication and data integrity can easily be brought into an IoT ecosystem. What we have is a sensor node. In our case this will represent a water filter. We also have a light sensor to monitor the remaining life of the filter, a temperature sensor to measure the temperature of our water, and the DS28E15 that we use to authenticate the sensor and to provide data information on the device for things such as remaining filter life and other life cycle management.



Each one of these sensor nodes will connect up locally to a controller node. These controller nodes are WI-FI enabled and they can, in turn, connect to a web server, one centralized web server that can manage everything in the ecosystem. As this is running, you'll see the DS2465 on our controller will connect up to and authenticate our sensor node. From there, we'll begin taking data from the sensor node, um, you'll see it displayed locally here, and it will also be reformatted for transmission to the web server.

Before we can transmit to the web server, we need to compute to a digital signature, or MAC, that's used for verification of the data that ties into our whole authentication and data's integrity, so we request a challenge from the web server and use this to prevent replay attacks where old data would be reused by an attacker. Once we have our challenge, we'll put that data, along with our sensor data, back into the DS2465, and when that's combined with a secret shared between the controller and the web server, we're able to generate our MAC, your secret is always stored in the DS2465 secure memory and never leaves.

Once we have all of our data, we can send it out through our WI-FI connection. The web server is able to validate our signature and ensure that the data came from an authentic controller that's part of the system and can also verify that no errors were introduced and no tampering occurred with the sensor data. We're now ready to fire this up and take a look.

To begin, we'll insert an invalid sensor node that will tell if the DS28E15 is counterfeit or has not been programmed with the valid secret. As you can see, it is displayed locally that the sensor node is not authentic and the controller simply sends a message to the web server that indicates that an invalid sensor was detected. From there it returns back, prompting us to insert another sensor node. So, we'll try again with a valid Maxim sensor node.

We'll insert that, press provision, and you can see that our valid data is displayed here and on the web server.

You can shade this light sensor to change the sensor data, and you can see those changes reflected with the filter life of 61% here. You'll notice that even though the filter life has remained at 61 and the temperature at 25 degrees, the MAC has changed and this is a result of our challenge that we received from the web server, which causes a constant rotation of the MAC value.

Next we'll simulate what would happen if you used an invalid controller. By pressing

the invalidate button once, we cause the controller to use an invalid secret, which is then reflected on the website. You can see the expected MAC did not match the MAC that was received from the controller and, therefore, the data was rejected by the web server. Pressing the invalidate button again returns to normal operation, and you can see that the MAC now matches the expected MAC again and the data was accepted and cataloged.

There are a couple of key advantages to this design: This metric approach to authentication is easy to implement, as well as cryptographically sound. All cryptographic hash functions are handled by the DS2465, so minimal additional resources are required, which is great for IoT devices that are cost sensitive. Additionally, the DS2465 provides secure key storage for the secrets that are used in the authentication scheme and this means that your processor needs no secure memory or other security related features, so it's easy to implement this in an existing design.

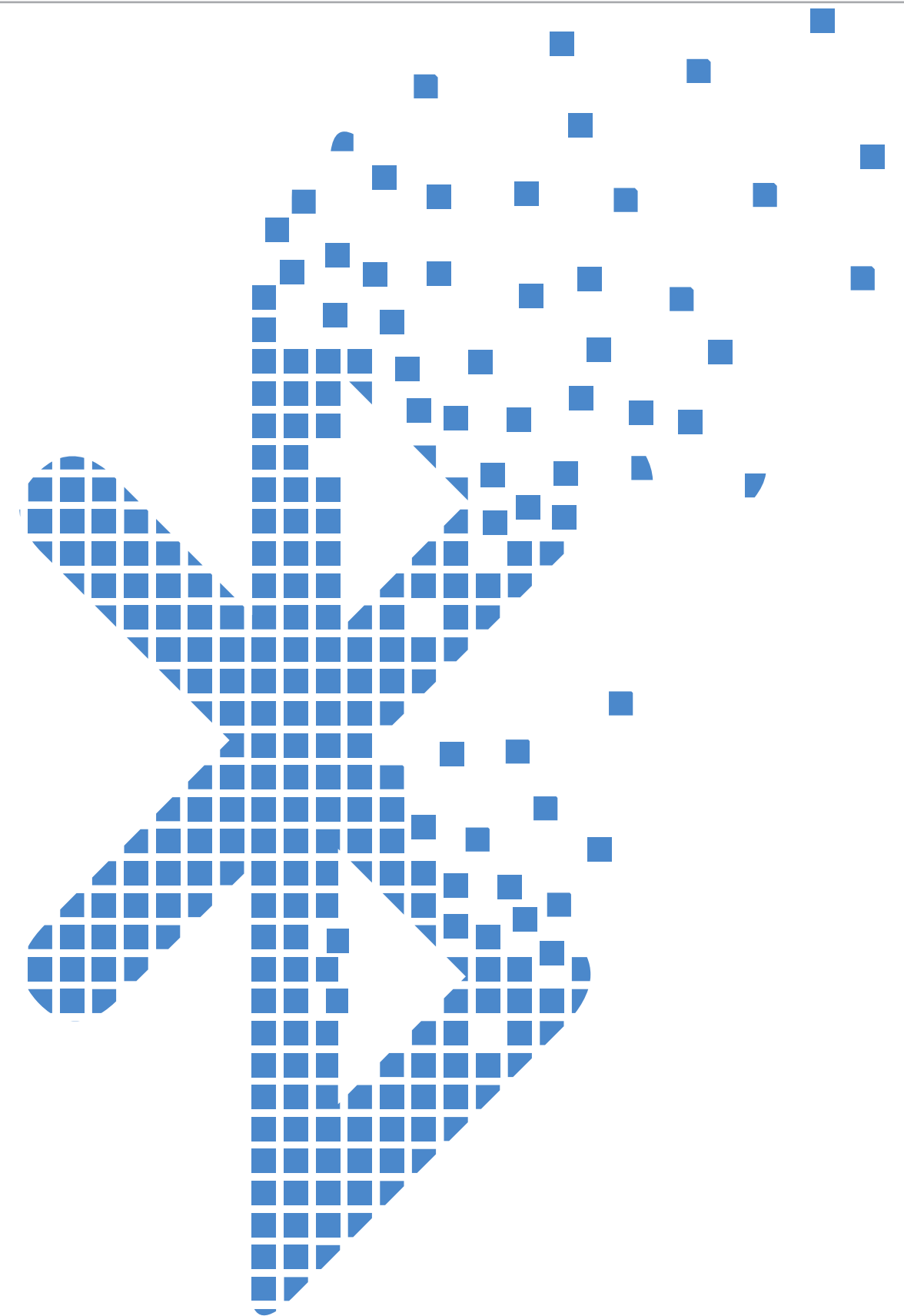
All of our code has been made available on mbed for immediate use and download. If you're using a platform board such as our MAX32600MBED, or any other mbed enabled board, you should be able to get up and running very quickly. For more information, please visit the MAXREFDES143 page on our [website](#), or on mbed. [EE](#)



Accelerating **BLUETOOTH LOW ENERGY** Development

*By Gagan Luthra and Pushek Madaan,
Cypress Semiconductor*

There's a mad rush in the consumer electronics space to capture customers mindshare by being first-to-market with the next-generation IoT products. With everything from fitness monitors, smart door locks, and light bulbs to a smart water cup, product companies are rushing to establish dominance in these newly emerging markets. The differences in many of these products today are often minimal as they all offer similar features. Besides differentiating on product design and aesthetics, the winning product is typically the one that is the first to become commercially available. Today's intelligent consumers are now wary of 'vaporware' through the many painful examples of crowd-funded projects that have failed to make it past a successful marketing and awareness campaign.



Wireless standards are important. They unify the magic of radiowaves into specified, deterministic standards and specifications that engineers can use without worrying too much about how the magic happens.

The need of the hour is to conceptualize new IoT products with differentiating features, and more importantly, deploy them to market quickly. However, if you're ever tried developing commercial-grade wireless products, you will realize that going to market with shortened product development cycle-times is excruciatingly difficult, especially when the development team does not have prior expertise in dealing with wireless standards qualification and regulatory approval for selling these products in established consumer markets. Moreover, as second-generation IoT products are beginning to differentiate on features, physical size, and battery life, developers are faced with a myriad of challenges in integrating these seemingly orthogonal feature requirements.

Qualification for Standards-Based Technology

Wireless standards are important. They unify the magic of radiowaves into specified, deterministic standards and specifications that engineers can use without worrying too much about how the magic happens. While this enables industries to develop wireless products that can talk to each other (common radio specifications) and speak common languages (common protocol stacks), it comes with the added challenge of getting these wireless products tested and qualified by the governing body that defines the standard.

Bluetooth Low Energy (or Bluetooth Smart) has emerged as a popular wireless standard for IoT products, mostly stemming from its simplified protocol stack (read as simpler compared to Classic Bluetooth or WiFi, but still not very simple) and an architecture defined for low-power radio communication. Developers making Bluetooth Smart products are required to go through the Bluetooth Special Interest Group (SIG) to test and qualify their products as per the specifications defined by the Bluetooth 4.x standard. Once a product has been successfully qualified by the Bluetooth SIG, it is assigned a Qualification ID (QDID). Furthermore, to market the end-product as Bluetooth Smart compliant, the product needs an additional, albeit less complex and expensive, Declaration ID which allows the product to carry the Bluetooth compliant sticker on its box.

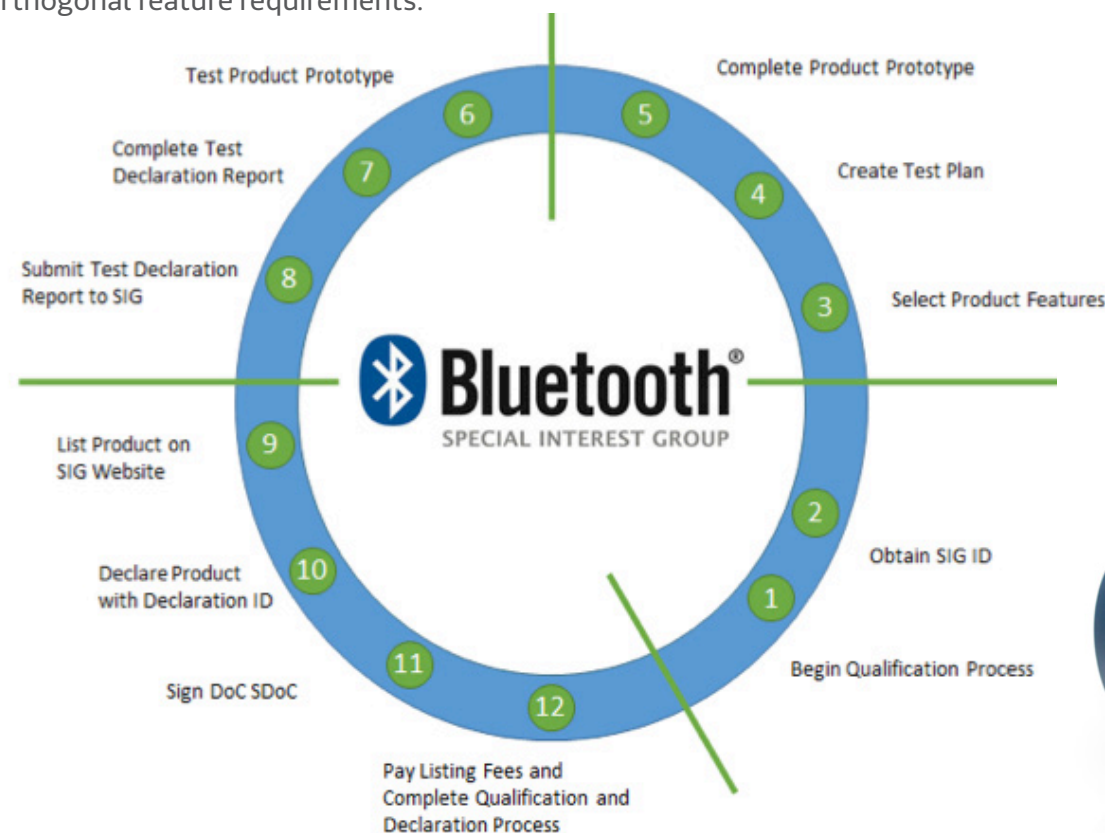


Figure 1. Bluetooth SIG's Complex Qualification Process



Exhibit A: Bluetooth SIG Qualification Testing and Documentation Process

Step	Process Description	Help Resources
1.	Create a Qualification Project Using the online Test Plan Generator (TPG): <ol style="list-style-type: none"> Choose the applicable design Product Type (End Product, Subsystem, Component, Development Tool or Test Equipment) Select the design's supported Bluetooth specification features Verify feature compliance using the automated consistency checker in the TPG Generate Test Plan 	Process Experts
2.	Perform Qualification Testing <ol style="list-style-type: none"> Execute all test cases listed in the Test Plan Generate Test Evidence Report(s) Document test verdicts in Test Plan—once complete, becomes Test Declaration 	Test Requirements Test Facilities
3.	Create and store a Compliance Folder <ol style="list-style-type: none"> Includes all required documentation defined in the PRD Section 3.2 (e.g. product description, design information, and test evidence) 	
4.	Submit Test Evidence <ol style="list-style-type: none"> Upload Test Declaration and Test Evidence Reports 	

Reference: <https://www.bluetooth.org/en-us/test-qualification/qualification-overview>

**Exhibit B:
Bluetooth SIG Product Listing
and Declaration Process**

Step	Process Description
1.	<p>Purchase a Declaration ID</p> <p>Price depends on membership level—see the fees page for more information</p>
2.	<p>Create a New Listing</p> <p>Using the online Qualification Listing Interface (QLI):</p> <ol style="list-style-type: none"> 1. Reference the new project or QDID(s) of the Qualified Design(s) being declared 2. List your product(s)
3.	<p>Sign a Declaration of Compliance (DoC)</p> <p>There are two versions of the DoC:</p> <ul style="list-style-type: none"> • New or changed Qualified Designs • Used or branded Qualified Designs <p>The QLI will automatically generate the correct version based on your selections. The signed DoC must be added to the Compliance Folder of new or changed Qualified Designs (e.g. Start A)</p>

Reference: <https://www.bluetooth.org/en-us/test-qualification/qualification-overview>



**Approval from
Regulatory Authorities**

Once you’ve gotten past acquiring the blessing of the governing standard, and indeed comply with their specified requirements, you aren’t done! You are now faced with the challenge of seeking approval from the various regulatory government-backed agencies that determine whether or not you can sell your product in a given country or geography. Within the USA, for example, this regulatory body is the Federal Communications Commission, commonly referred to as the FCC. The FCC regulates interstate communications by radio, television, wire, satellite and cable in all 50 States. Specifically around wireless communication, they regulate the frequency spectrum in which devices can transmit/receive radio signals. Furthermore, the FCC requires that any device that radiates RF energy must be tested for compliance with their rules.

There are a plethora of authorized companies who have made a living out of this need, and can help you in achieving the required wireless certification from the FCC. A typical process involves extensive wireless design and testing, re-design and re-testing! Rise and repeat until you’re told that you are ready to pass the FCC requirements. Once ready, you submit your end-product to the FCC for final testing and certification, and along

the way you’ve spent an average of 8-12 weeks of calendar time (if you’re lucky and have minimal iterations) and are out of pocket upwards of six-figures in US Dollars to account for test equipment, agency fees, test and approval fees, etc. Want to sell your product in another country? Repeat this process, with varying levels of requirements for other regulatory bodies like the IC (Canada), KC (Korea), CE (Europe) and so on. If successful, you can look back and realize that you wanted to become an expert at designing products for smart human interaction, like a fitness monitor, but have instead spent a large chunk of your resources on understanding and perfecting the intricacies of voodoo wireless communication standards and certification.

FCC ID

The FCC-ID is a unique identifier of 4-17 characters for an end-product. It consists of two elements—a Grantee Code, a 3-character string representing the applicant assigned permanently to a company for the authorization of all RF equipment, and an Equipment Product Code that is the non-grantee code portion of the FCC ID and can be between 1-14 characters. The FCC-ID must be permanently marked either directly on the wireless transmitter, or on a sticker or tag attached to it. It is important that the FCC ID be clearly visible to the purchaser of the product.

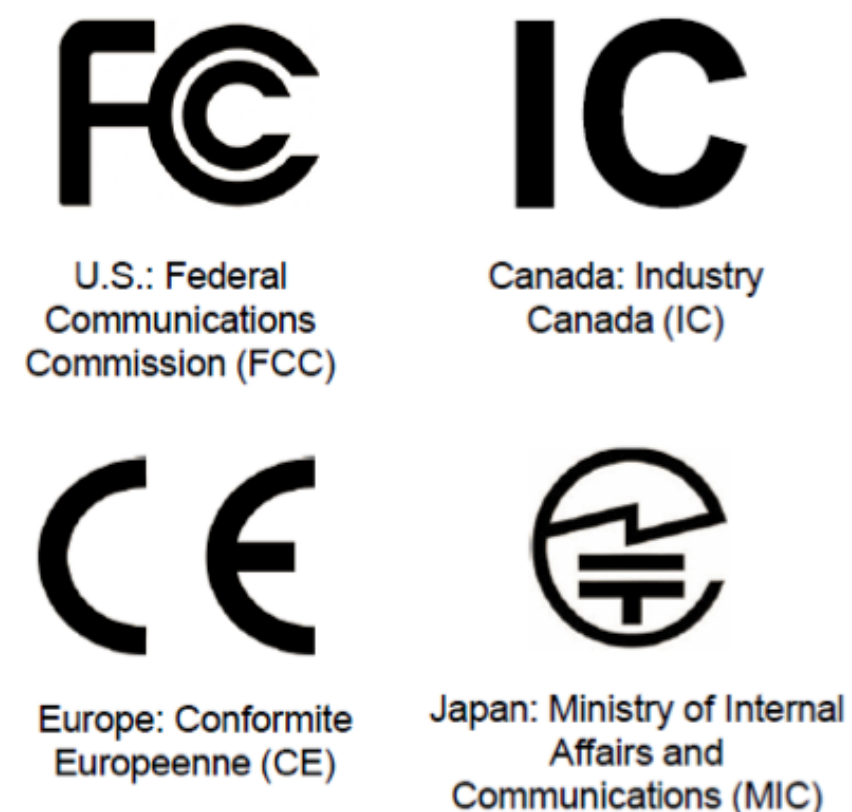


Figure 2. Regulatory Authorities Around the Globe

The FCC-ID must be permanently marked either directly on the wireless transmitter, or on a sticker or tag attached to it.



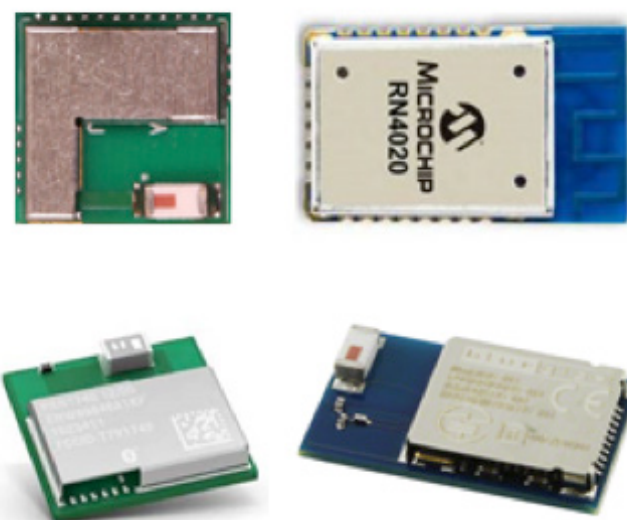


Figure 3. Popular Pre-Certified Bluetooth Smart Modules

Pre-Certified Modules for Accelerated Time-to-Market

One commonly used approach to navigate the challenge of wireless qualification and certification is to use pre-qualified and pre-certified modules. Traditionally available from vendors who specialize in the design and manufacture of such modules, these offer a viable alternative to designing your own wireless systems and taking them through the long and expensive qualification and certification processes. One drawback of using modules can be that they are available have restricted form-factors and features, but these can often be overlooked when ticking schedules must be met.

By loose definition, modules commonly include a wireless controller IC, any crystals required for timing purposes, an RF antenna, and the required circuitry to complete the antenna matching network and power system. Besides offering

integrated hardware on moderate-to-easy solderable packages, modules often also include pre-loaded firmware on the wireless IC, typically the supported wireless protocol stack and a command-set to easily interface with the wireless controller.

Modules almost always carry the wireless standard's qualification, e.g. a QDID for Bluetooth Low Energy modules, such that the end-product developer can easily refer to the pre-qualified ID and avoid having to go through the qualification process themselves. A product declaration still needs to be completed for the end-product to get the appropriate marketing symbols and logos from the governing standard (e.g. Bluetooth SIG), but the requirements for such declarations is typically much simpler than that of the qualification process. Certain modules that feature an integrated RF antenna (of various types, for example a ceramic chip antenna or a printed circuit board trace antenna) include additional regulatory certification and approval. Having an FCC ID on a pre-certified module also has the added benefit of eliminating worry about whether or not your wireless system will pass the required stringent tests regulated by the FCC. Your end-product may still require FCC certification for other parts in the system that radiate waves, but having the primary wireless subsystem of your product pre-certified saves a lot of time and money in the long run.

Choosing the Right Bluetooth Smart (Low Energy) Module

With Bluetooth Smart becoming a very popular choice in low-power wireless for IoT products, there are several module options with pre-qualification for this standard available in the market today. Many of these modules are offered by companies who specialize in the design and manufacture of modules, as it takes specialized expertise in wireless design and reliable small form-factor manufacturing. While knowing that your module is designed by an expert company is useful, it often has the drawbacks of support (or the lack of) when you have to go to a different vendor to troubleshoot issues with the wireless controller IC (from the chip manufacturer) or the wireless protocol stack (from the software vendor).

To aid developers, some companies in the industry today offer in-house end-to-end solutions with IC design, software development, and module manufacturing capabilities. Cypress Semiconductor, for example, recently extended its successful touchpad module manufacturing capabilities to its wireless modules, and Silicon Labs with its recent acquisition of Bluegiga, a popular module manufacturer. Other wireless IC vendors like CSR and Dialog Semiconductor rely on 3rd party module manufacturers like Microchip or Panasonic to offer pre-certified module solutions.

Another way module vendors offer product differentiation is by integrating more features into their modules. The

most commonly available modules are simple communication modules, i.e. they rely on your system having its own microcontroller and simply latch on to it over a standard serial communication interface such as UART/SPI/I2C to manage the wireless communication in the system.

Panasonic's popular PAN1740 uses Dialog Semiconductor's wireless controller IC and offers a low-power Bluetooth Smart module that is also small in size (9x9.5x1.8mm), albeit a no-frills modules with lower feature integration. The wireless controller IC from Dialog Semiconductor includes a 16MHz ARM® Cortex®-M0 CPU, serial communication interfaces for UART/I2C/SPI, 42KB SRAM, 32KB OTP (One-Time Programmable) for Bluetooth Smart Profiles and 84KB ROM that hosts the Bluetooth Smart protocol Stack.

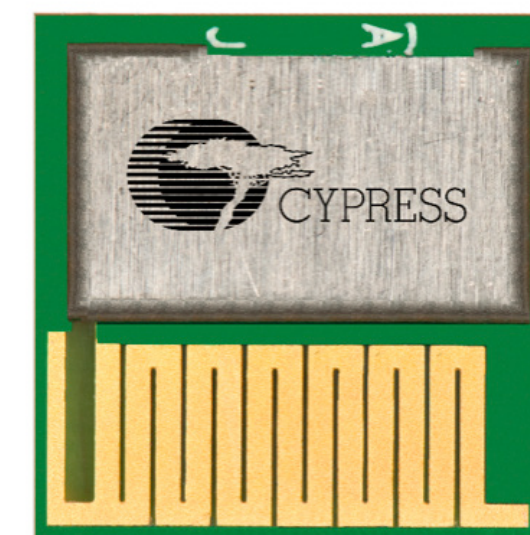


Figure 4. The Highly Integrated EZ-BLE PSoc Module from Cypress Semiconductor

With the industry trending towards smaller form-factors for end-products, higher feature integration is key in choosing the right Bluetooth Smart module for your system. The BLE113 module from Silicon Labs includes an 8-bit 8051 CPU with 8KB SRAM and up to 256KB Flash for the application firmware and Bluetooth Smart Profiles, an ADC for converting analog sensor data into digital formats, and also a PWM to drive LEDs or simple buzzers. The module does make a size tradeoff to offer the higher feature integration (15.75x9.15x2.1mm), and is also limited in configurability by only offering a UART interface to configure and exercise the wireless protocol stack. The EZ-BLE PSoC module from Cypress Semiconductor presents a balanced combination of size, feature integration and programmability. At 11x11x1.8mm, the module is not the smallest available, but offers the highest amount of feature integration per square mm. The integrated PSoC 4 BLE wireless controller IC features a 48MHz ARM® Cortex®-M0 CPU with a variety of communication interfaces (UART/SPI/I2C/I2S) and also a programmable analog front end to eliminate the need for any external ICs to interface with analog sensors—a very common requirement for IoT products that feature on-board sensors.

In addition, the EZ-BLE PSoC module features Cypress's industry-leading CapSense® touch-sensing technology making it easy to add sophisticated user interfaces to your end-product. Cypress's module has another key advantage as discussed previously, with them being one of the only vendors in the industry that has its own in-house MCU and wireless IC, protocol stack software, and module manufacturing capabilities.

All of the modules above offer pre-qualified QDID for Bluetooth Smart compliance and feature regulatory approvals from various agencies like the FC, CE, IC, KC and so on. All of the available modules are also more-or-less equal on demonstrable wireless range, as they have to comply with the standards specified by the Bluetooth SIG. Thus, engineers have available to them several good options for pre-certified and pre-qualified Bluetooth Smart modules, depending on the end-product's feature and size requirements. By using such modules, designers can expect to shave off anywhere between 8-12 weeks of product development time and upwards of \$100k+ that would normally be spent on the wireless qualification and certification process. [EE](#)

All of the modules above offer pre-qualified QDID for Bluetooth Smart compliance and feature regulatory approvals from various agencies like the FC, CE, IC, KC and so on.



Embedded systems: The future of the industry

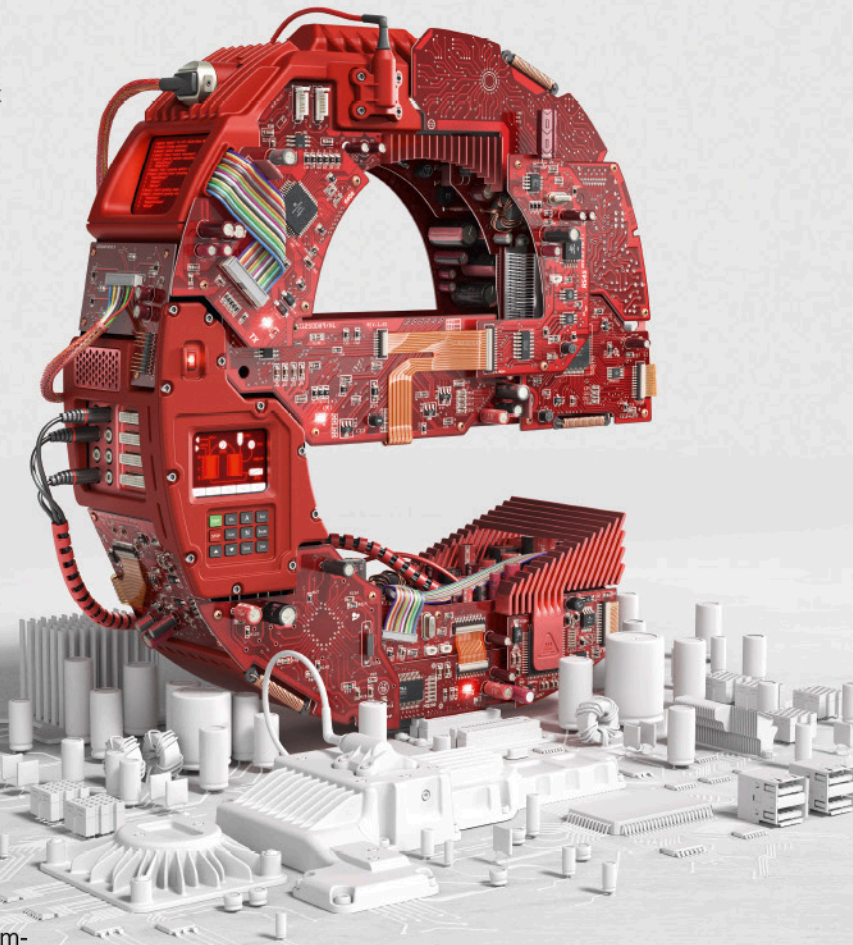
"Connected Worlds—Safe and Secure" is the motto of an exhibition sector at **e**lectronica, the World's Leading Trade Fair for Electronic Components, Systems and Applications, that revolves around the latest operating systems and networking technology in the electronics applications sector.

More than 2,800 international exhibitors will present the latest embedded solutions and products that pertain to key themes such as the Internet of Things (IoT), industrial electronics and automation. Besides the Embedded exhibition sector in Hall A6, the Embedded Platforms Village is another visitor highlight where companies can demonstrate their know-how. Experts will discuss the industry's latest developments at the Embedded Platforms Conference and the Embedded Forum.

Embedded Platforms Conference

Future trends such as Industry 4.0, autonomous driving, the smart grid, smart buildings, wearables, 3D printing and virtual reality call for intelligent and networkable embedded platforms. The objective: New kinds of functions and services that work reliably and give rise to new business models. In this regard, the Embedded Platforms Conference serves as a valuable communication platform for users and solution providers of components and tools.

This year, the conference will shed light on modern embedded platforms from the perspective of microcontrollers, peripherals, security, sensor technology, energy supplies and communication—and the Internet of Things is always in sight. Together with the unique range of information at **e**lectronica, the program of the Embedded Platforms Conference offers you a number of new ideas. It takes place at the Press Center East during the fair, i.e. on November 9 and 10.



More information:
electronica.de/en/embedded

HARDWARE DESIGN MADE EASY.

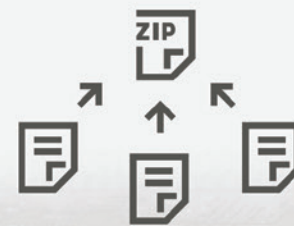
pcbWEB

PCBWeb Designer is a free CAD desktop application for designing and manufacturing electronics hardware. The tool supports schematic capture and board layout, including integrated "click-to-order" manufacturing.

www.PCBWeb.com



Simple. Custom. Quality.



Upload



Quote



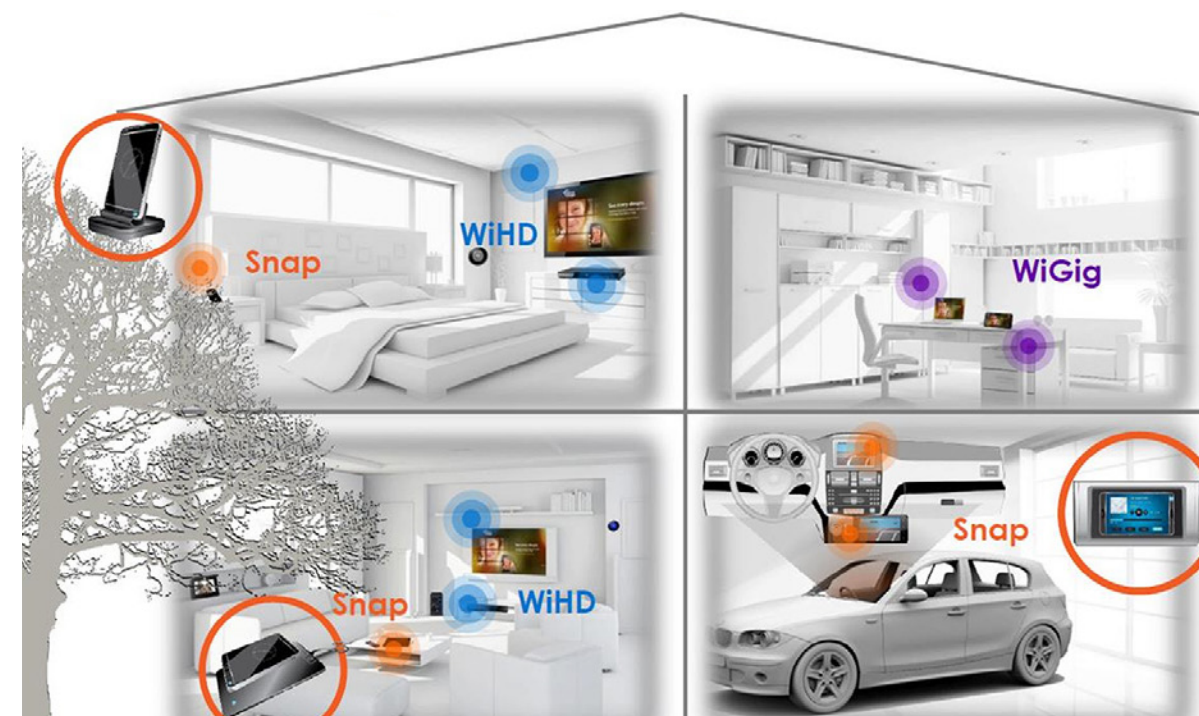
Order



A Diverse Set of Applications Shows the **Versatility** of the

60 GHz Band

*By Neil Bullock,
Director of Strategic Marketing,
SiBEAM Technology Group,
Lattice Semiconductor*



The potential of the license-free 60 GHz band has long been recognized. The very high capacity supported by 7 GHz of spectrum and the robustness to interference offered by millimeter wave propagation sets this unlicensed band apart from others and makes it ideal for a number of applications. The challenge has been in the development of the semiconductor and packaging technology that can exploit these characteristics and enable new, large markets. Since 2004, SiBEAM™ (now the SiBEAM Technology Group of Lattice Semiconductor) has been focused on overcoming these challenges

through the creation of innovative silicon and software. The portfolio of solutions based on SiBEAM technology includes WirelessHD® for in-room AV distribution, 802.11ad (WiGig™) for high-speed data, SiBEAM Snap™ technology for connector elimination on mobile devices, and wireless infrastructure products for outdoor backhaul and access that enable next-generation wireless connectivity on the road to 5G. Each solution delivers a unique capability to the segment that it addresses, and SiBEAM works closely in partnership with other industry leaders to help accelerate 60 GHz adoption.

AS WIRELESS CHARGING BECOMES COMMONPLACE, IT BECOMES RELEVANT TO CONSIDER WHETHER THE DATA TRANSFER FUNCTIONS OF THE USB INTERFACE COULD ALSO BE PERFORMED WIRELESSLY.

WirelessHD: The Pioneer

In-room wireless video distribution presents many challenges. The image quality should be as good as wired video. Lag should be unnoticeable. The link should be robust, both to interference from other devices and to changes in the physical environment as people and equipment move. The 60 GHz band is ideally suited to this application as sufficient capacity exists to carry high quality HD video. The technical challenge is in establishing and maintaining connections in a dynamic in-room environment. WirelessHD was introduced in 2008 with the support of industry leaders LG, Panasonic, Philips, Samsung, SiBEAM (now Lattice), Sony, and Toshiba to standardize the solution across a wide array of video devices. The technology is particularly suitable for use in products for which wired video connections are impractical or unacceptable; for example, mobile devices, enterprise video projectors and medical displays.

802.11ad (WiGig): Instantaneous Data

Building on the very high capacity and robustness to interference offered by WirelessHD, WiGig was developed to enable data services at much higher data rates and with lower latency than is possible in the existing Wi-Fi bands. This capability is essential to new wireless use cases: gigabit-speed Internet access, low-latency desktop video display and virtual reality. The wireless industry has collaborated within the WiGig Alliance and, more recently, the Wi-Fi Alliance to develop the foundation for a high-speed wireless data ecosystem. The results of this work have recently been demonstrated with the announcements of successful interoperability testing between Intel and Qualcomm and between Qualcomm and Lattice. WiGig products certified by the Wi-Fi Alliance are expected to be available by the end of this year.

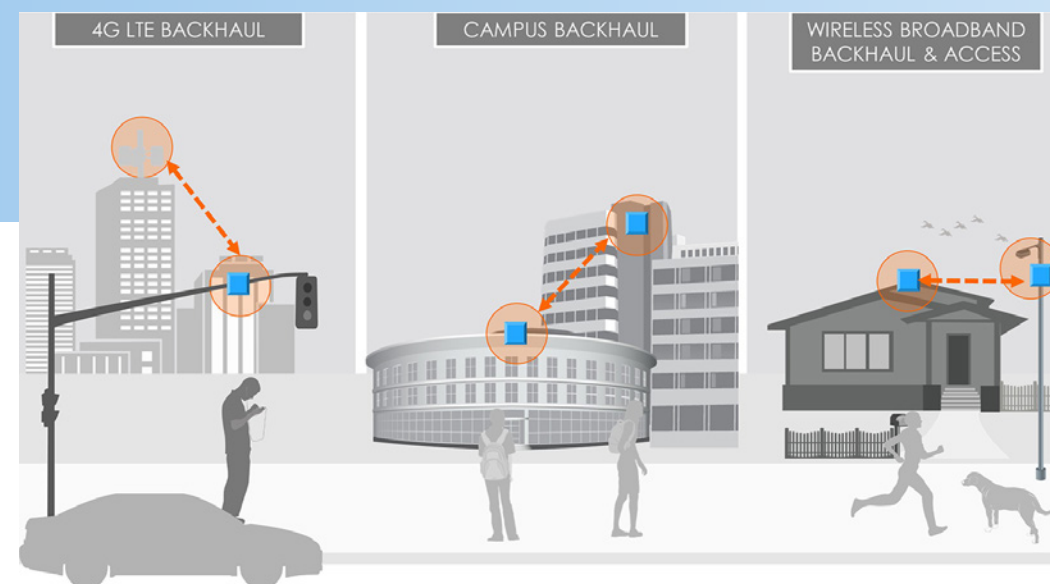
Snap: True Mobility

Mobile devices rely heavily on wireless technologies for key interfaces: Bluetooth to connect to keyboards and speakers, Wi-Fi to connect to printers and access points to the internet. One physical interface—USB—remains ubiquitous on mobile devices because “it just works” in performing the basic functions of battery charging and data transfer. As wireless charging becomes commonplace, it becomes relevant to consider whether the data transfer functions of the USB interface could also be performed wirelessly. There are significant benefits to this: devices can be made waterproof, product aesthetics can be improved and elegant device use models such as ‘casual’ docking on desktops (as exemplified by Microsoft Continuum) and in cars (as exemplified by Android Auto and Apple Carplay) can be created. The challenge of supporting the very high data bandwidth implicit in USB 3.0 (5Gbps in each direction) can only be met in the 60 GHz band. Lattice’s SiBEAM Snap 60 GHz technology provides 6Gbps in each direction and replaces the USB connector with wireless “place and play”.

Wireless Infrastructure: The Great Outdoors

Next-generation networks will be characterized by dense meshes of high capacity outdoor wireless links, both for access (to the client device) and backhaul (to the core network). The limited signal propagation in the 60 GHz band due to atmospheric absorption (the absorption

by oxygen molecules signals at their resonant frequency), means that the same channels can be reused at a significantly higher density than in other bands. This, along with the high capacity of the band and the robustness to interference due to the narrowness of the beams makes the 60 GHz band ideal for both access and backhaul. The phased array antenna and electronic beam-steering technologies developed by Lattice’s SiBEAM Technology Group can be applied to outdoor wireless infrastructure and deliver substantial benefits over conventional 60 GHz infrastructure equipment. As the beams are steered electronically, links can be established dynamically. This significantly reduces the installation and maintenance cost compared to conventional fixed antenna installations. The technologies also result in improved equipment size, weight, power consumption and cost. In its first deployment, Lattice’s 60 GHz phase array RF transceiver using SiBEAM technology has been integrated into equipment installed as part of the Bristol is Open experimental network, which demonstrates gigabit-speed wireless mesh networking for dynamic data backhaul applications. This is the first mesh network trial in Europe to use 60 GHz and OpenFlow software-defined networking. The recent announcement of [Facebook Connectivity Lab’s Terragraph program](#) is a great endorsement of the promise of wireless networks using the 60 GHz band to address the challenge of serving rapidly increasing data demands in dense urban environments. No other technology can be deployed as quickly or cost-effectively and provide gigabit speeds.



NO OTHER BAND HAS THE NEAR-TERM POTENTIAL TO PROVIDE SO MUCH CAPACITY FOR NEW APPLICATIONS.



A Peek Into the Future

In October 2015, the Federal Communications Commission (FCC) issued a Notice of Proposed Rulemaking that would make the 64GHz-71GHz band available for non-federal use. This would increase the total spectrum to 14 GHz, or approximately 20 times more spectrum than is available in the 5GHz band. The FCC is proposing that the additional spectrum be license-free, in common with the existing 60 GHz (57-64GHz) band. Regulators in other regions are proposing similar changes.

This expansion allows a significant increase in both data throughput and link density. No other band has the near-term potential to provide so much capacity for new applications.

The single application—wireless video distribution—that drove the development of Lattice’s SiBEAM technology has now multiplied into a range of applications that demonstrates the versatility of the 60 GHz band and drives its use into many aspects of our technology lives. As more industry leaders apply their support, the momentum of 60 GHz is unstoppable. **EE**

ROBO Business

INVEST ▶ INNOVATE ▶ IMPLEMENT

SEPTEMBER 28-29, 2016

San Jose Convention Center, San Jose, CA

WORLD-RENOWNED KEYNOTE SPEAKERS



James Kuffner
CTO –Toyota Research Institute



Dr. James Canton
Chief Futurist, CEO – Institute for Global Futures



Will Allen
HP Fellow & VP, Inventor & Innovator – Hewlett-Packard Labs

POWERING BUSINESS WORLDWIDE

Meet industry leaders, startups, investors and end users all at the forefront of robotics.

The RoboBusiness Conference Shows You How to Benefit From Robotics:

- Identify New Business Opportunities & Global Trends
- Learn How to Apply Robotics with Success
- Build Strategic Relationships with the Industry Elite
- Make Informed Technology Purchasing Decisions
- Get Exclusive Insights into Cutting-Edge Technology Development
- Access Market Forecasts & Application Breakthroughs in Key Markets:
 - ▶ *Business | Technology | Unmanned Systems*
 - ▶ *Manufacturing & Logistics | Consumer | Service & Healthcare*

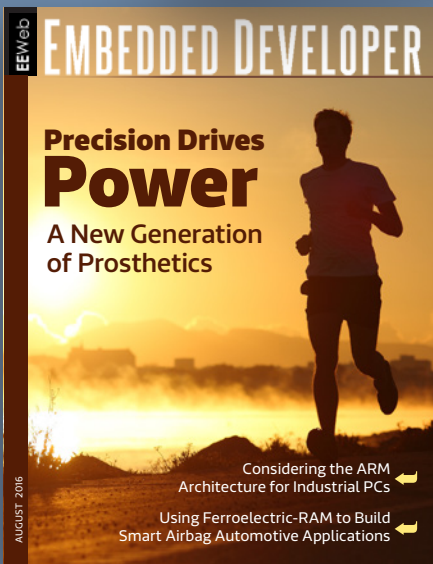
The Expo is the hub for hands-on learning with hundreds of robots from around the world.

SAVE OVER 50%!
USE CODE RB16ED



A **NEW** issue is coming!

Until then, enjoy these **current** magazines.



EEWeb
Electrical Engineering Community

News » Tools » Resources » Ideas



Read more
EEWeb magazines

New issues are coming up!