Electronic Design®

ENDEAVOR BUSINESS MEDIA™

SPECIAL REPORT

THE WIRELESS INTERNET OF THINGS

How engineers are overcoming complexity in multiprotocol wireless IoT designs

Table of Contents

Engineering the Multiprotocol Future of the IoT

This special report dives into the challenges and engineering solutions behind today's multiprotocol wireless IoT devices.

By ***James Morra, Senior Editor***

AT ITS CORE, the IoT is all about connecting the unconnected — and doing so on a massive scale. According to IoT Analytics, a technology and market research firm, the number of connected IoT devices, largely via Wi-Fi and Bluetooth, reached 18.5 billion in 2024, up by 12% from 2023. Their forecast projects this number will rise 14% to 21.1 billion by the end of 2025 before growing to approximately 39 billion by 2030.

But as more "things" are connected to the IoT, wireless complexity is emerging as a key challenge for engineers.

The IoT is one of the most complex, fragmented areas in the world of wireless connectivity due to the wide range of technologies at play. A single device can use Wi-Fi, Bluetooth, and Thread for different roles: Wi-Fi for high-speed cloud access, Bluetooth for short-range communication with mobile devices, and Thread for low-power, direct device-to-device communication in a local mesh network.

The multiprotocol approach allows for both control and connectivity. It gives engineers more ways to enhance performance, latency, and power at the expense of design complexity.

The Matter standard is breaking down the barriers between devices in the smart home, making sure they can securely and seamlessly connect to each other in a multiprotocol world. But the underlying reality is more complex.

Many of these devices integrate several different IoT radios that tend to operate in overlapping or very close frequency bands. This can raise the risk of RF interference and cause performance degradation.

For engineers, universal IoT connectivity continues to come with a growing list of technical tradeoffs. In this Special Report eBook, *Electronic Design* wanted to give engineers a lay of wireless landscape and how it's reshaping IoT devices from inside-out. We consulted industry insiders and technical experts to spotlight short-range wireless solutions, from multiprotocol wireless SoCs to RF front-end modules (FEMs). In a future report, editors will take a closer look at cellular IoT and other long-range technologies.

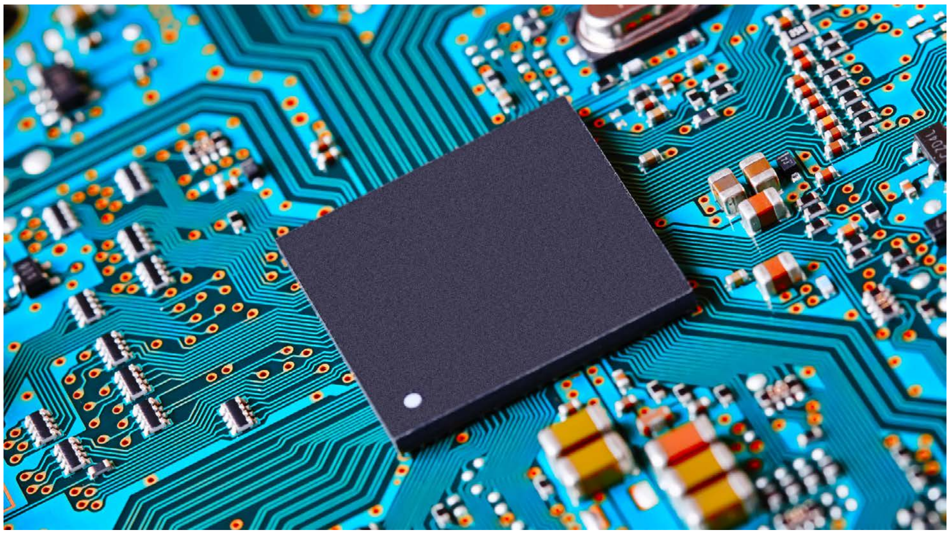
To fill in the blanks, we went through the archives to highlight technical content on everything from managing power used for wireless connectivity in IoT devices to antenna placement on space-constrained circuit boards.

CHAPTER 1

What's Inside a Wireless IoT SoC?

Is the IoT SoC transforming into a separate class of embedded processor?

JAMES MORRA, Senior Editor



dreamstime_Raimundas_52332363.jpg

The IoT continues to expand, but engineers continue to wrestle with a web of challenges: fragmented standards, tight constraints on power and space, and constant tradeoffs between performance and cost. However, a new wave of wireless SoCs is untangling these issues. By bringing together wireless connectivity, computing, and security, these IoT chips can help reduce hardware complexity and time-to-market for everything from sensors embedded on factory floors to smart-home devices, said Silicon Labs CTO Daniel Cooley.

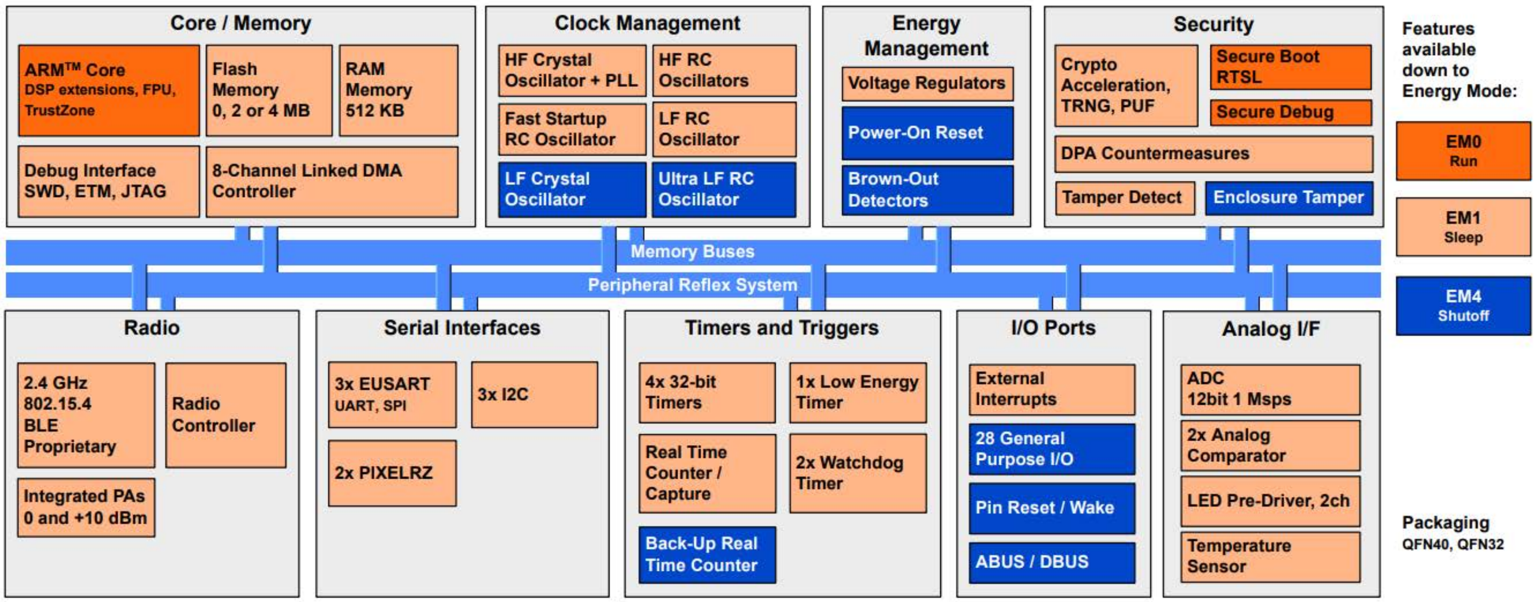
"You're eventually not going to have a wireless application that doesn't have some degree of processing in it," he said in a briefing with reporters at Silicon Labs' 2025 Works With conference in Austin, Texas.

In October 2025, Silicon Labs introduced the first chips in its Series 3 platform — its vision for the future of IoT SoCs. The new chips will support a wide range of long- and short-range wireless protocols, including Wi-Fi, Bluetooth, and Thread. Many of them are specifically designed to work with the Matter standard to bridge the gap between them.

By upgrading from 40 nm to 22 nm, the company said Series 3 brings generational gains in computing, connectivity, and security to the table, outperforming the capabilities of its Series 2 platform without replacing it.

No single chip is ideally suited for every IoT device—the design requirements are too diverse. But Cooley explained that the Series 3 platform features the fundamental building blocks for connecting these devices to the IoT. These comprise:

- **Wireless connectivity**, including the RF transceiver as well as power amplifiers (PAs), RF switches, LNAs, and most or all other RF front-end components plus interfaces to external PAs.
- **Application processor**, typically a Cortex-M MCU that's increasingly used to run real-time operating systems (RTOS) and comes paired with more on-chip memory to manage the complexity.
- **AI accelerators**, through a neural processing unit (NPU) or hardware accelerator to run AI and machine-learning (ML) models more efficiently than software running on the MCU.
- **Hardware security,** based on a secure enclave that acts as a hardware root of trust (RoT) and runs cryptographic operations to help keep hackers out of the system.
- **Sensor interfaces**, including serial interfaces and general-purpose I/Os,



Inside the SiMG301, one of the first chips based on the Series 3 platform from Silicon Labs. (Image credit: Silicon Labs)

supplemented by analog-to-digital converters (ADCs) and other parts of the analog front end (AFE) to capture the data.

- **Peripherals**, for saving PCB space and reducing the cost of integrating external components. For instance, it integrated LED pre-drivers in its SiMG301 to control dimming in smart lighting.

By focusing in on the demands of IoT devices, Cooley said it distilled everything in the Series 3 — starting with its SiXG301 and SiXG302 — into a platform purpose-built for secure, robust, intelligent connectivity without excessive power and cost.

"We are focused on IoT connectivity, and we are squarely focused on this one market," noted Cooley. "We have the widest portfolio of wireless technologies, and we believe that we're the technology leader in the space."

Silicon Labs is betting that its IoT focus gives it the engineering edge over other companies that spread out its R&D over several different markets. "We don't have those distractions — in terms of the level of investment in the company—and so we don't have to dilute what we're doing when it comes to our chip-level engineering," said Cooley. "We make technology decisions because we know exactly what we're going into. There is nothing we're doing that our competitors can't do, but long-term, we think we're ahead."

The Move to Multiprotocol Wireless SoCs

The IoT is running into a wall of wireless complexity that the latest SoCs are equipped to solve, according to Cooley.

Today, IoT devices use a wide range of wireless protocols that operate in overlapping or very close frequency bands, which can potentially cause RF interference, signal degradation, and increased latency. Each protocol plays a distinct role: For instance, in a connected door lock, users can pair it with a smartphone over Bluetooth; control it remotely and connect it to the cloud using Wi-Fi; and integrate it to home automation through Thread for mesh networking. Many IoT devices must rapidly shift between protocols or run them at the same time.

"It's a multiprotocol world," said Cooley. "There will never be one wireless protocol to rule them all."

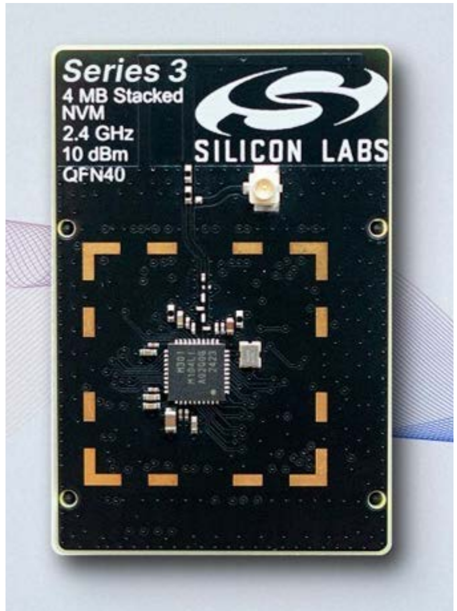
To cut through the tangle of wireless technologies, companies are racing to roll out chips that can handle several different protocols at a time — integrating Wi-Fi and Bluetooth, Bluetooth and Thread, and Wi-Fi, Bluetooth, and Thread. These chips are all about reducing hardware complexity and saving PCB space, which is critical for compact IoT devices, while managing complex protocol stacks and reducing the RF interference between them all.

The first multiprotocol Series 3 SoC — the SiMG301 — brings Bluetooth LE, [Zigbee](), and [Thread]() into a single chip that's targeted at smart lighting and other line-powered smart plugs, sensors, switches, and controllers.

At the heart of it is the high-performance 2.4-GHz radio that offers up to +10 dBm of transmit (TX) power while supporting −98.6 dBm of receive (RX) sensitivity for Bluetooth and −106.3 dBm for Thread and other protocols that use the 2.4-GHz band. This reduces the impact of interference in increasingly crowded RF areas like smart homes.

"If you could hear what is happening in the 2.4-GHz band, it would sound like this cacophony of clicks and chirps," said Cooley. "We have very high-performance, congestion-tolerant radios."

It uses a separate radio CPU core to control all of the wireless connectivity, from the protocol stacks to the firmware that enables it to shift between protocols dynamically or run protocols such as Zigbee and Thread at the same time using its "concurrent multiprotocol" technology. That enables continuous communication between IoT devices, regardless of the protocols in use, and allows for backwards compatibility. By bringing Bluetooth and Matter over Thread into a single chip, it saves space for additional integrations like Wi-Fi.



Silicon Labs said the Series 3 platform brings upgrades in connectivity, compute, and security. (Image credit: Silicon Labs)

The SIMG301 has a scalable PA architecture. In high-power mode, the PA provides a +10-dBm output for maximum range or signal strength; in low-power mode, the PA output is 0 dBm for optimized power.

Transforming the RF SoC into the IoT SoC

The first generation of IoT radios required external co-processors to run applications. But now most wireless SoCs come with a dedicated processor, which makes it easier for engineers to develop Matter-ready IoT devices.

Like many major IoT chip companies, Silicon Labs is betting on Matter to become the standard way for the smart home to communicate. It would unite a market that has long been fragmented by the lack of compatibility between devices from different manufacturers and linked by different wireless protocols. Such compatibility problems pushed Apple, Google, Samsung, and a wide swath of semiconductor firms (including Silicon Labs) to create the open standard through the Connectivity Standards Alliance (CSA).

The standard, which started as part of Project Connected Home over IP (Project CHIP), enables everything from smart thermostats to smart door locks, switches, and lighting to connect locally without using the cloud.

The SiMG301 is one of the first chips in the CSA's Matter Compliant Platform Certification program, as it comes with a software development kit (SDK) that's been certified with the hardware for core Matter functionality. By building on top of a certified platform, Silicon Labs said engineers can inherit pre-tested commissioning, networking, and security, cutting down on the complexity, cost, and time required for product certification.

Series 3 is based on a multicore architecture that separates application processing from wireless connectivity and security, giving it headroom to handle larger wireless protocol stacks and more computationally intense jobs. The SiMG301 features a Cortex-M33 clocked at up to 150 MHz that's supplemented by a relatively large amount of memory: up to 4 MB of co-packaged flash for program memory and 512 kB of on-chip RAM for data memory.

It's also integrating more general-purpose I/Os to interface with the sensors embedded in many edge devices as well as other AFE components to convert and condition analog signals from the sensors.

Silicon Labs plans to integrate its second-generation Matrix Vector Processor in several of its Series 3 SoCs to enable fast, power-efficient execution of AI. That parallels what it did with its most advanced Series 2 SoC, the MG26. It uses hardware accelerators to offload machine-learning operations off of the main CPU, specifically ones for audio, vision, and other sensor-powered features, such as keyword spotting and motion detection. The NPU is up to 10X faster while using 80% less power than the CPU alone, drastically reducing power draw in wireless IoT devices.

Series 3 integrates a power management unit (PMU) on-chip to boost efficiency, which is bound to be even more important in Silicon Labs' SiXG302 family for battery-powered IoT devices, due out in 2026.

Hardware-Secure Connectivity for the IoT

As more unconnected "things" are connected to the IoT, security at the hardware level is becoming critical, said Cooley.

The SiXG301 family features the company's latest secure vault for IoT security. The secure enclave comes with what Silicon Labs calls the first PSA Level 4 certification, the highest level recognized by PSA Certified.

Silicon Labs said the secure vault "raises the bar for edge protection" by defending against physical attacks such as laser fault injection, side-channel analysis, micro-probing, and voltage manipulation. It incorporates a hardened RoT, lifecycle controls, and secure OTA updates for devices that can be deployed for a decade at a time. The Series 3 SoCs also feature a quad-SPI (QSPI) memory interface with runtime authentication and encryption.

The secure vault in the Series 3 SoCs helps developers reach compliance with emerging regulations, including the EU's RED and CRA and the U.S. Cyber Trust Mark, among others.

"Our parts are ready for all of this," Cooley remarked about the tightening IoT security regulations. "We don't have to reengineer the entire portfolio because it requires circuitry down into the hardware. You need a physically unclonable function (PUF), you need a hardware root of trust, and you need cryptographic key management. These are not just software solutions."

One of its latest innovations relates to execute-in-place (XIP), in which the processor executes code directly from external flash instead of copying it to on-chip memory first. The Series 3 secure vault authenticates the code as it enters the processor.

"In a world where IoT devices are more feature-rich and adopting real-time operating systems, you have to enable memory expansion, and so now we have basically the world's most secure serial memory interface, and we can prove it," said Cooley.

The Future of IoT SoCs is All About Integration

With the demand for wireless connectivity on the rise, companies are adding more of everything to these SoCs, from radios and memory to processors, to enable more intelligent connectivity while balancing power and cost. While others are adopting FD-SOI, Silicon Labs said it's upgrading to more advanced CMOS nodes such as 22 nm to not only reduce area, but also to save space to integrate more features and more memory in the same package.

Cooley said there will be a higher degree of integration in the future. "We're able to take advantage of the benefits of Moore's Law. But this is the last Bulk CMOS node and then it's down to FinFET."

view this article online

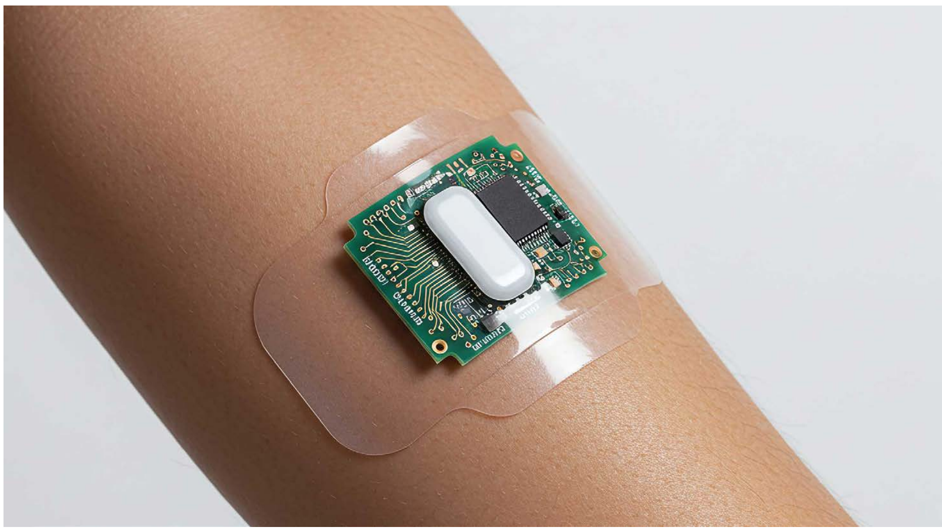
BACK TO TABLE OF CONTENTS

CHAPTER 2

RF Module Brings It All Together for the Wireless IoT

A small multiprotocol RF FEM aims to improve the reliability, range, and speed of IoT connectivity.

JAMES MORRA, Senior Editor



dreamstime_Tedy-Dwi-Prayoga_404690021.jpg

Multiprotocol wireless SoCs handle most of the heavy lifting in today's IoT devices. Still, the final stretch of the RF signal path — those last several inches to the antenna — can be critical. Bridging this gap is the RF front-end module (FEM).

While companies are integrating power amplifiers (PAs), low-noise amplifiers (LNAs), and switches (SW) directly into their IoT SoCs, a separate FEM can be used to extend range and connection robustness in noisy RF environments.

"Unlike integrated PAs or RF front ends found on SoCs, external FEMs deliver superior performance," said Xinliang Wang, senior director of product portfolio management at pSemi. "This is achieved through higher output power, enhanced receive sensitivity, and greater flexibility in power control."

However, it tends to be a challenge to cram all of the different building blocks of the FEM — notably the PA, LNA, and SW — into a single module that works within the context of a low-cost, space-constrained IoT device.

As engineers grapple with the tightening cost and space constraints of the IoT, pSemi tries to bring these components closer together with its RF silicon-on-insulator (SOI) technology. Using what the company calls its UltraCMOS technology, it can integrate the main parts of the FEM into a single monolithic unit that saves space while competing with other RF technologies in terms of power amplifier output and receiver sensitivity.

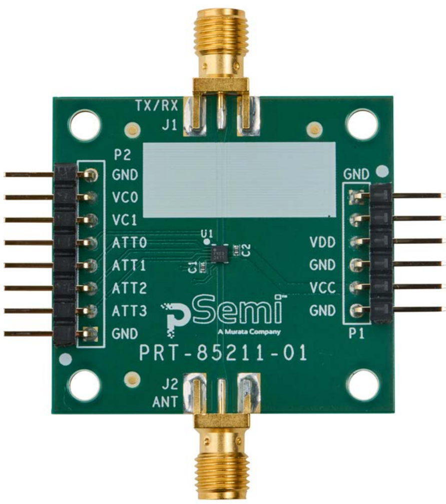
The UltraCMOS technology underpins its most compact RF FEM to integrate the PA, LNA, and SW into a single module — the PE562212. The 2.4-GHz FEM features very low noise that enables extended wireless range. It connects everything from smart speakers, smart lighting, smart thermostats, and other home appliances to wireless audio and medical wearables to sensors embedded on factory floors to ensure link robustness.

The multiprotocol FEM supports Bluetooth and Bluetooth Low Energy (LE) for short-range communications, Zigbee and Thread for mesh networking, and low-to-medium throughput Wi-Fi, giving more flexibility to IoT device makers **(Fig. 1)**.

Reducing RF Tradeoffs in the Wireless IoT Landscape

The reliability, range, and speed of wireless connectivity in IoT devices depends on RF front-end and the PA inside it, which directly impacts the robustness of the wireless connection and power consumed by the device.

In most cases, these power amplifiers are based on bulk CMOS technology and integrated directly into IoT SoCs. While these RF components can enable robust performance and range, they tend to be optimized for power efficiency above all. The output power of these PAs is also often limited by harmonic generation, which may reach the limits set by regulations and certifications, or by the tight requirements of battery-powered IoT devices.



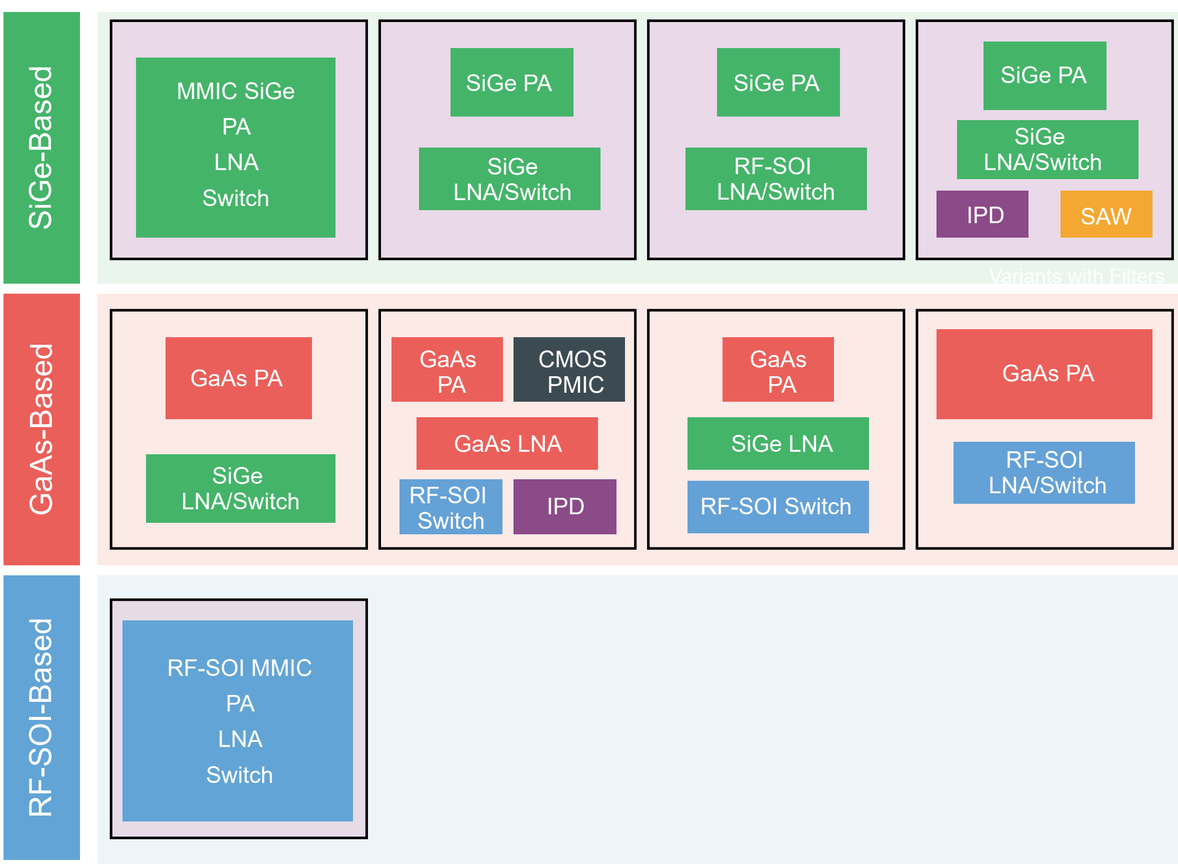
1. The new multiprotocol IoT FEM comes in a very compact 1.8- × 1.8-mm package. (Image credit: pSemi)

Multiprotocol wireless SoCs are designed to deliver the best link budget for the power envelope. That's largely determined by the receive sensitivity, but it's also defined by how efficiently the RF transceiver in the SoC has been designed.

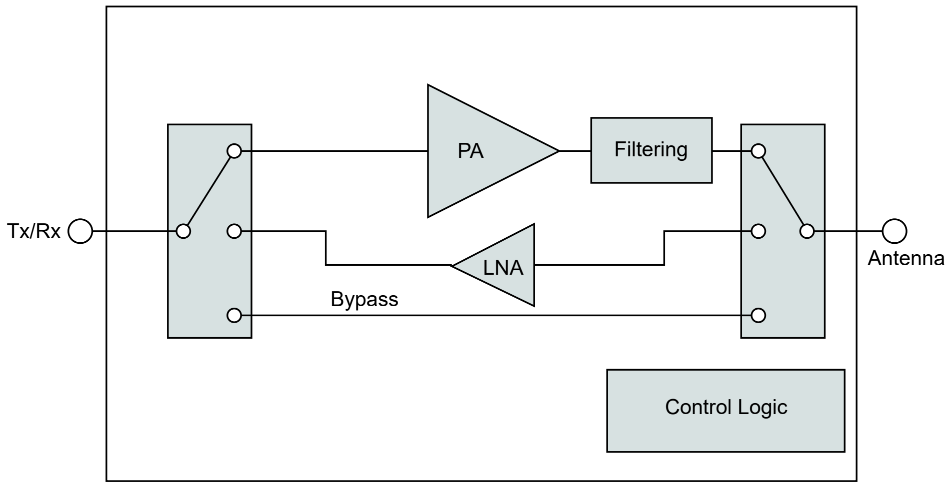
Integrating digital, analog, and RF functions on a single chip has its difficulties and often leads to tradeoffs. These include reducing transmit power and receiver sensitivity, or how frequently the wireless SoC transmits.

Wang said it can make sense to use a separate FEM to boost the link budget, making sure that signals are transmitted and received with maximum efficiency and minimal loss. In many cases, these modules rely on RF-focused process technologies, such as [silicon germanium (SiGe)] and [gallium arsenide (GaAs)], to boost power efficiency at the expense of tight integration.

But that means traditional IoT FEM solutions are typically assembled in parts: Power amplifiers based on SiGe or GaAs to enable efficient, long-range



2. Most RF modules mix and match different process technologies, including RF-SOI. (Image credit: pSemi)



3. pSemi uses its UltraCMOS technology to integrate the PA, LNA, and RF switch in a single module. (Image credit: pSemi)

transmission are frequently paired with separate LNAs and SWs based on RF-SOI, which is well-suited for faster switching and better signal reception, in a module **(Fig. 2)**. Though it's ideal for switching between different frequency bands or amplifying weak wireless signals, RF-SOI can have its limits when used in PAs.

pSemi claims to close the performance gap with its UltraCMOS technology. UltraCMOS is based on RF-SOI, which is widely used in the RF front ends crammed into 4G and 5G smartphones. However, the company said it brings improvements in power capacity, linearity, isolation, and switching performance ($R_{ON} \times C_{OFF}$) on top of it by uniquely using a sapphire substrate.

Using the monolithic integration made possible by CMOS, it can build the PAs, LNAs, and RF switches into a single IC, eliminating the mixing and matching of different RF blocks **(Fig. 3)**.

"RF front ends in smartphones are highly complex and optimized for speed and high data rates across many cellular bands, while IoT devices prioritize simplified RF designs for extreme low-power, long-range, and protocol-specific communication," said Wang. "Smartphones use advanced filtering and integration to manage interference from multiple radios, whereas IoT devices are more focused on power efficiency to maximize battery life."

The Monolithic Integration for RF Modules

The high-performance PA at the heart of the PE562212 delivers up to +21-dBm output to improve signal transmission, while supporting application-specific output power requirements through 1-dB gain steps.

The IoT FEM also incorporates LNAs with a 1.6-dB noise figure to strengthen signal reception and RF switches designed for minimal loss. Furthermore, it features integrated RF filters to reduce harmonics and distortion as well as a bypass path with 0.6-dB loss. The combination of high output power and low noise provides a robust link budget, which is critical for penetrating walls and ensuring extended range and reliability, according to the company.

pSemi said the PE562212 has the ability to support the most widely used wireless protocols in the IoT. For instance, it can be used in a smart-home device that uses Bluetooth LE to connect to a smartphone while it downloads firmware updates over Wi-Fi at the same time. That tends to require more linearity than what's possible with a wireless SoC alone.

"For IoT devices, especially wearables and smart sensors, maintaining robust RF performance is a key design challenge given their increasingly compact size," said Wang.

While it reduces excessive packet drops and power consumption by increasing link budget, the RF FEM has robustness against ESD and ruggedness to handle the harsh environmental conditions inherent to the IoT.

The new module comes in a compact 1.8- × 1.8- × 0.63-mm LGA package suited for space-constrained applications. It enables easier PCB design with I/O interfaces requiring no external matching, said pSemi.

view this article online

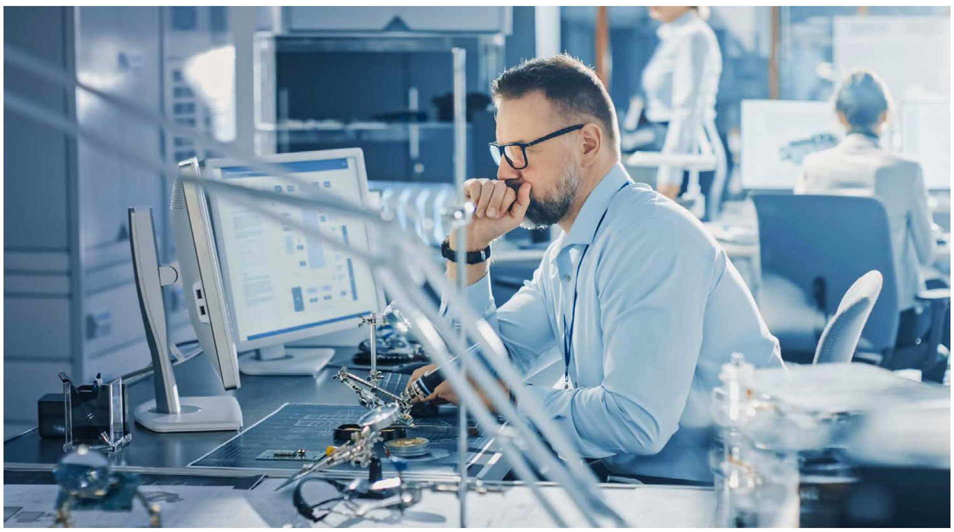
BACK TO TABLE OF CONTENTS

CHAPTER 3

Addressing RF Coupling in Wireless SoC System Design

RF coupling is one of the most important and tricky issues that RFIC designers always must confront while developing wireless SoCs.

KARIM SALEH, Manager, and MOHAMMED TAWFIK ABDELHAFEZ, Senior Principal Engineer, Si-Vision, https://www.si-vision.com



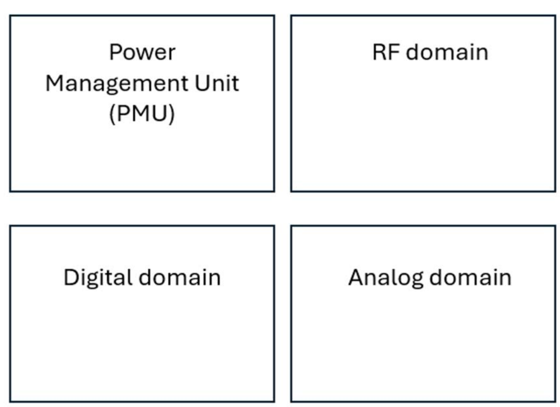
dreamstime_Aleksei-Gorodenkov_308693970.jpg

Wireless system-on-chip (SoC) designs require implementing all circuit domains on the same die. This enables manufacturers to reduce cost and support integrity. On the other hand, crosstalk between these domains can be problematic and degrade the overall performance.

Electromagnetic interference (EMI) is caused by radiated radio-frequency (RF) signals. Various techniques are available to lower EMI in system design. For instance, radiated RF can be addressed with filtering and shielding; however, this doesn't mitigate on-chip RF coupling.

Channels for RF Coupling

RF coupling is an example of crosstalk between the RF domain and other domains (**Fig. 1**). Wireless transmitters are required to generate output power in the range of ~10 dBm. Power amplifiers (PAs) generate these levels of power while sometimes incorporating on-chip inductors or transformers.



1. The annotated domains are typically found within wireless SoCs (Credit: Si-Vision).

Due to electromagnetic radiation of the inductors, a fraction of the transmitted power can couple to other domains inside the SoC. Whether the coupled component is at the same transmitted frequency or its harmonics, it degrades transceiver performance. This becomes evident when the output signal spectrum of the integrated frequency synthesizer becomes spurious.

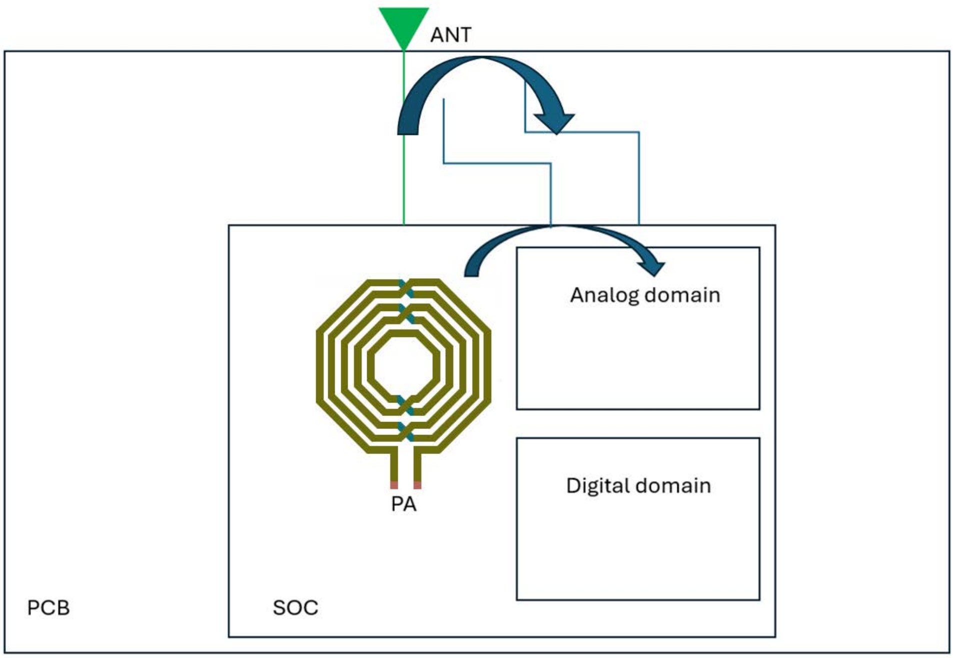
The same coupling mechanism can happen outside the SoC on the PCB level, where the antenna will radiate and impact critical PCB routes of other domains near to it (**Fig. 2**).

Reducing RF Coupling

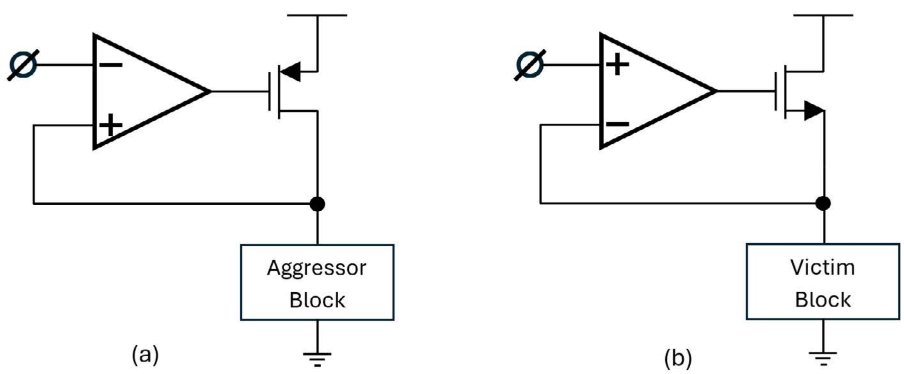
Generally, any block that operates at an arbitrary frequency (f1) is considered an aggressor for a victim block that operates at another frequency (f2) and vice versa. There can be exceptions when one frequency is an exact integer multiple of the other.

The links through which the aggressors affect victims include:

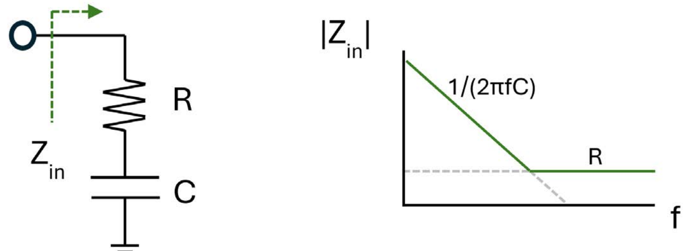
- Supply networks
- Parasitic capacitive coupling
- Parasitic magnetic coupling
- Substrate coupling



2. The arrows indicate possible RF coupling mechanisms in a wireless module (Credit: Si-Vision).



3. Shunt regulators protect the supply from aggressor blocks (a). Series regulators protect sensitive blocks from supply noise (b) (Credit: Si-Vision).



4. Parasitic resistors in series with supply decaps degrade their performance (Credit: Si-Vision).

Reduction of Supply Network Coupling

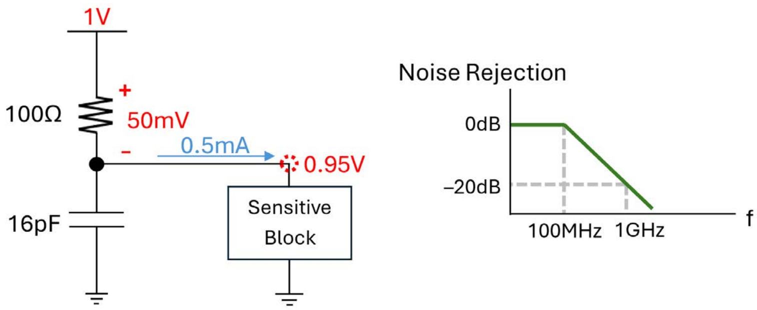
Different regulators can be used to decrease coupling through supply networks. Consider an aggressor block that's insensitive to supply noise. Such a block should be supplied from a shunt regulator,[1] like that in **Figure 3a**. The reverse power-supply rejection ratio (PSRR), which is the signal transfer function from the regulator output to its supply, is small.

Similarly, sensitive blocks to supply noise, which have negligible contribution to supply contamination, should be supplied from series regulators[1] (**Fig. 3b**). Forward PSRR, which is the transfer of supply noise to the regulator output, is small in series regulators.

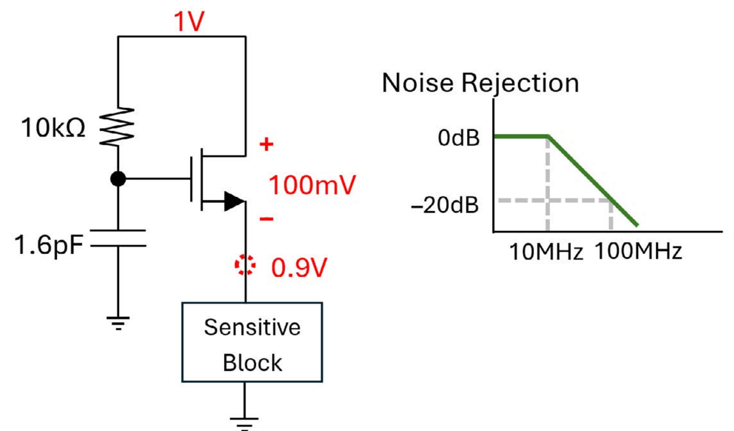
Another common way to decrease coupling through supply networks is by adding an ample capacitance of supply decoupling capacitors near each block. However, this must be done carefully to maximize the range of frequencies in which the decoupling capacitors are effective.

Parasitic resistance of the decoupling capacitor routing should be minimized to increase its quality factor. When the decoupling capacitors are

CHAPTER 3: **Addressing RF Coupling in Wireless SoC System Design**



5. This is an example of a reasonable tradeoff between supply headroom and noise filtration in a passive supply filter design (Credit: Si-Vision).

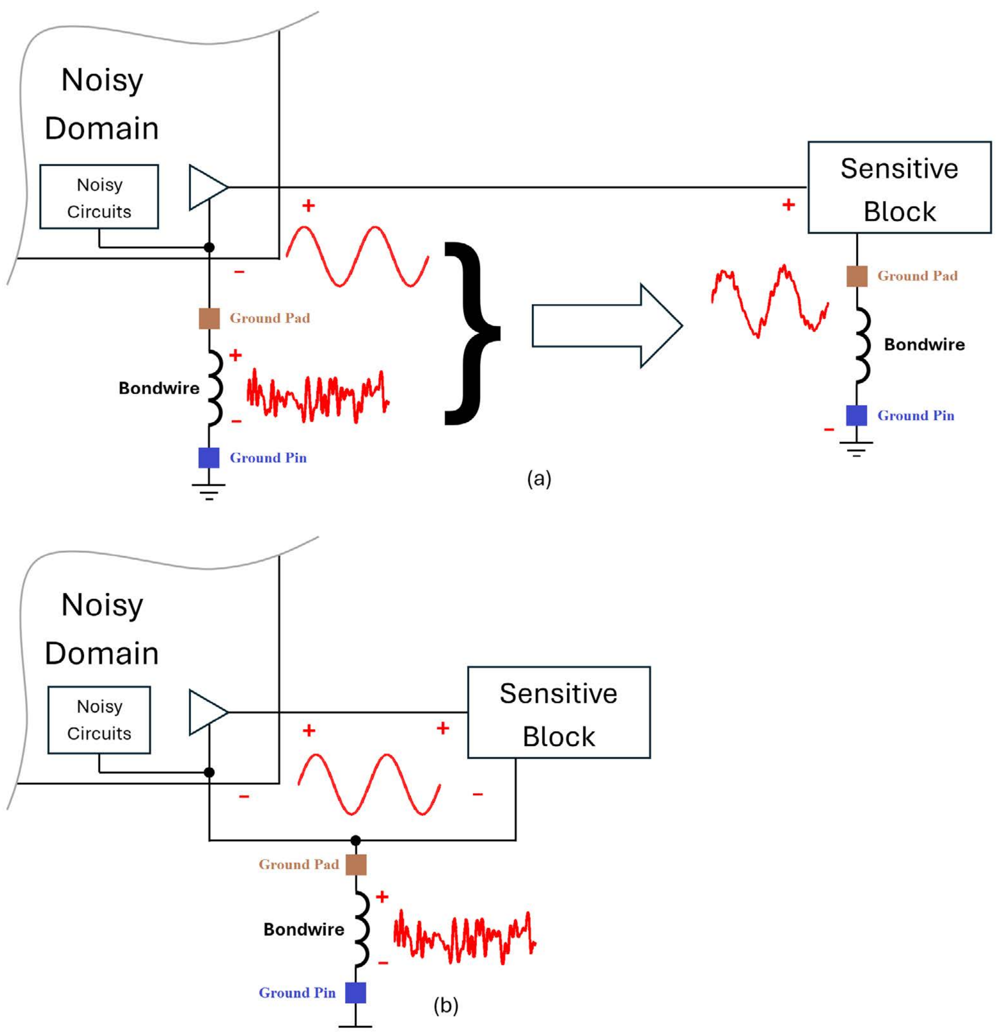


6. The filter capacitance can be greatly decreased in the active supply filter, which results in a compact design (Credit: Si-Vision).

realized by MOS devices, the length of the unit decoupling capacitors should be minimized to decrease its channel resistance.[2] Impedance of a capacitor in series with a parasitic resistor saturates at the parasitic resistance value at high frequencies (**Fig. 4**).

One infrequently used technique to mitigate supply network coupling is to add passive or active supply filters.[1] Design engineers may initially reject this idea as there's an associated loss of supply voltage headroom. However, consider a block that has a 1-V supply and consumes 0.5 mA (**Fig. 5**).

Insertion of a 100-Ω resistor decreases the supply headroom by just 50 mV. When the added filter capacitance is 16 pF, supply



7. The input signal to a sensitive block can be contaminated when the ground pads of the communicating domains are separated (a). The same signal is safely transferred when the ground pad is shared (b) (Credit: Si-Vision).

noise at 1 GHz gets attenuated by 20 dB. A similar argument can be made for the area-efficient active filter utilizing a native NMOS device (**Fig. 6**).

Finally, separating ground connections of different blocks and connecting them to different pads may lead to severe issues.[3] Separation can contaminate sensitive blocks instead of isolating them. This counterintuitive mechanism is illustrated in **Figure 7**.

Reduction of Parasitic Capacitive Coupling

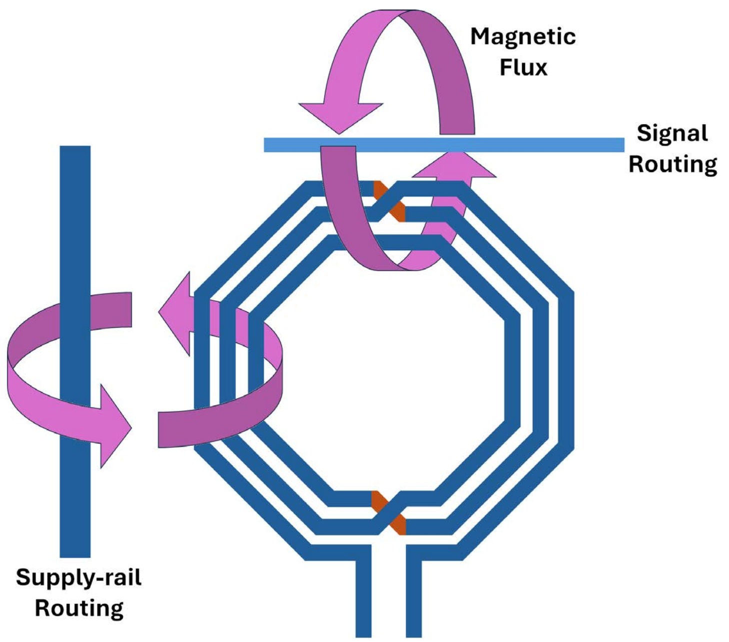
Parasitic capacitive coupling is handled on the layout level. Sensitive and noisy nodes should be shielded with their reference supply rails. Ground plane design can help as well.

Capacitance is inversely proportional to distance between conductors; therefore, increasing spacing between traces will help.

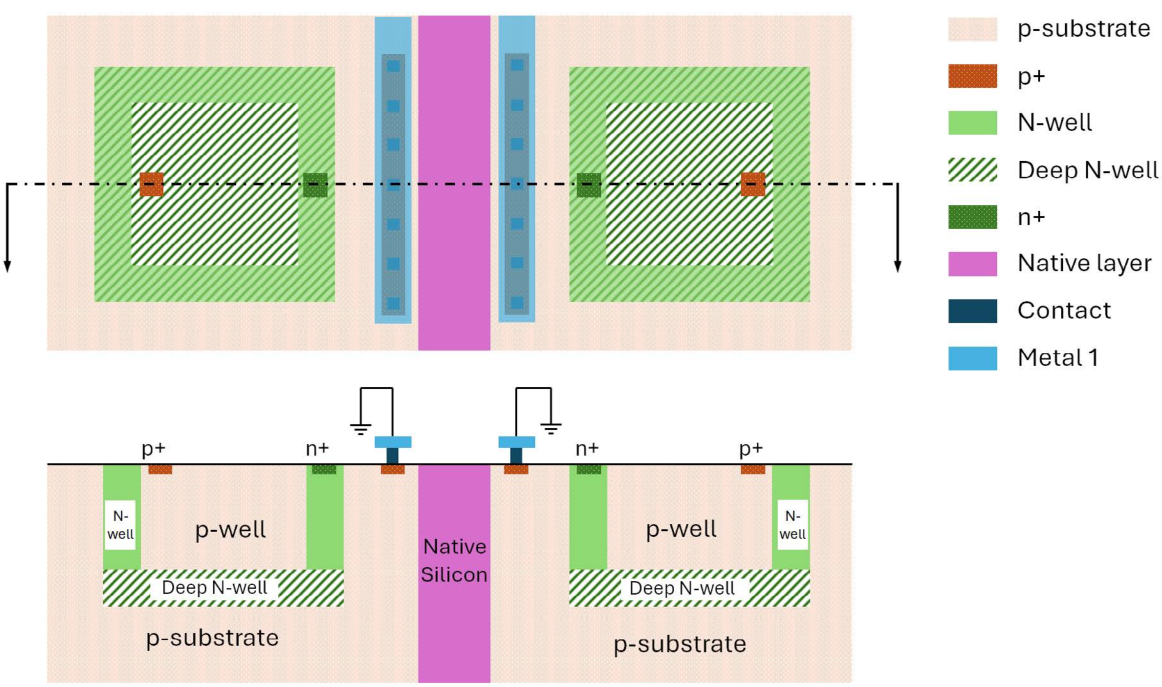
Reduction of Parasitic Magnetic Coupling

Long routes can be magnetically coupled to each other when they have the same orientation. This effect is more pronounced when coupling occurs between a long parallel route to one side of a spiral coil (**Fig. 8**). The situation worsens when the coil carries currents of both high frequencies and large magnitude, as in the case of power amplifiers.

To diminish this magnetic coupling, sensitive routes should be as far as possible from coils and other noisy



8. Magnetic coupling between a spiral coil and adjacent long routes is a serious concern (Credit: Si-Vision).



9. Isolation of domain substrates can be achieved in layout using deep N-well and native layers (Credit: Si-Vision).

routes. Also, when routes are orthogonal to each other, magnetic coupling decreases substantially.

Reduction of Substrate Coupling

Sometimes noise coupling can occur through the substrate. To overcome this, different circuits can be isolated into wells using the deep N-well layer. Moreover, the high-resistivity native layer should be added in between the isolated domains, with adjacent bulk ties that provide low-impedance paths to different ground pads.[4] This technique is illustrated in **Figure 9**.

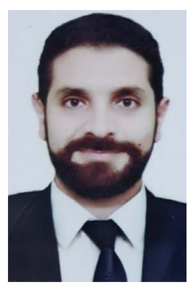
Finally, a couple of guidelines can be followed to further decrease noise transfer from one domain to another. Differential signaling should be used whenever possible for inter-domain connections. This minimizes transfer of the reference node noise. Also, the signal drivers at the boundary of one domain could be deliberately weakened to minimize the electrical transfer of all signals to other domains. This approach is very effective when handling CMOS logic signals, such as high-speed clocks and digital buses.

Don't Overlook Coupling Reduction Techniques

RF coupling in wireless SoC systems can be a real problem and could degrade overall performance. Special attention should be paid when designing the SoC floorplan and identifying aggressor and victim blocks. Coupling reduction techniques should be implemented to get the required high performance.

Karim Saleh *received B.Sc. and M.Sc. degrees in electronics and communication engineering from Ain Shams University, Cairo, Egypt in 2004 and 2011, respectively. From 2006 to 2011, he was an RFIC design engineer at SySDSoft Inc.; from 2011 to 2014, he worked at Intel Egypt IMC; from 2014 to 2022, he worked at ADI/Bosch Ireland; and since 2022 he's been Analog design manager at Si-Vision Egypt. His work involves circuit design of RF transceiver and analog/digital PLLs.*

Mohammed Tawfik AbdelHafez *joined Si-Vision in 2008. His work involves system design of RF transceiver subsystems, circuit design of RF and Analog/Mixed-Signal integrated circuits, plus testing and validation of fabricated chips. He holds a B.Sc. degree in Electronics and Electrical Communication Engineering from Ain Shams University, Cairo, Egypt.*



References

1. Maxim, A. "Noise and Spurious Tones Management Techniques for Multi-GHz RF-CMOS Frequency Synthesizers Operating in Large Mixed Analog-Digital SOCs." J Wireless Com Network 2006, 024853 (2006). https://doi.org/10.1155/WCN/2006/24853

2. Behzad Razavi. 2011. "Chapter 7 Passive Devices" in RF Microelectronics (2nd Edition) (Prentice Hall Communications Engineering and Emerging Technologies Series) (2nd. ed.), 487-491. Prentice Hall Press, USA.

3. M. T. AbdelHafez, "The ground illusion: Don't let it come back to get you." Accessed Oct. 27, 2024.

4. Durmaz, Faik M. "Layout Techniques For Analog Building Blocks And Application To An Adaptive Output Buck Converter," Istanbul Technical University, Sept. 19, 2016. Accessed Oct. 27, 2024.

view this article online

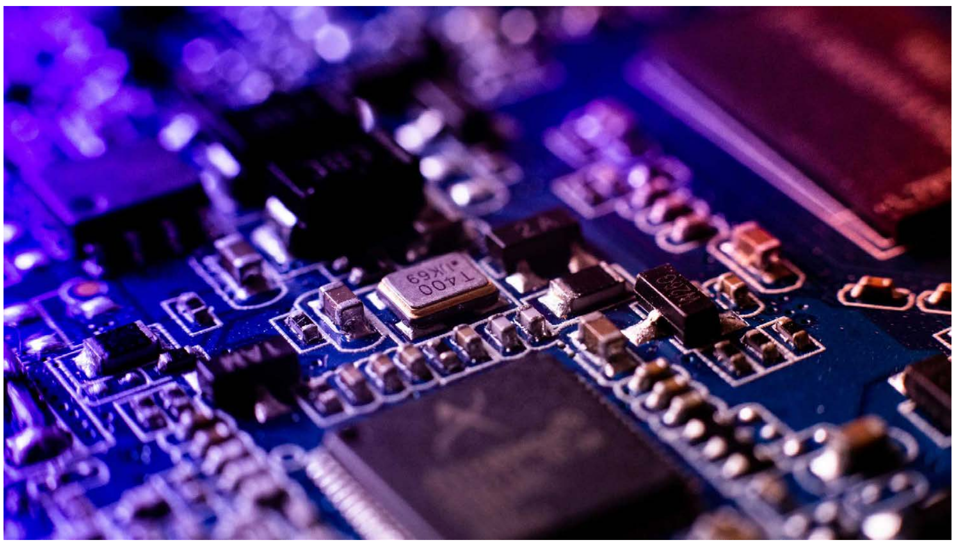
BACK TO TABLE OF CONTENTS

CHAPTER 4

Bringing Ultra-Low-Power Timing to Next-Gen IoT Devices

Understanding the ESR of timing devices is critical for curbing the power demands of wireless IoT devices.

JONNY LEE, Product Marketing Manager, *Epson*



dreamstime_Tiby Cherian_180163777.jpg

Timing devices supply the heartbeat for compact, wirelessly connected IoT devices that can sense, process, and communicate seamlessly with cloud and mobile platforms. These requirements place strict demands on these parts, which must come in a compact form factor and exhibit low power usage along with high accuracy. Failing to meet these requirements can take a toll on device performance, battery life, and overall reliability.

In IoT devices, timing components — including kHz and MHz crystals and oscillators — deliver highly stable reference clocks that help ensure reliable operation of the microcontrollers (MCUs) at the heart of most of them. In smartwatches and other wearables, for instance, accurate timing ensures that data is sampled and transmitted correctly, enabling precise monitoring and synchronization across the IoT ecosystem.

Precise timing also underpins robust wireless connectivity. Accurate timers play a critical role in minimizing data loss and errors as well as preventing desynchronization or signal drift, which is essential for consistent operation. They bolster connection stability and smooth out transitions between the many protocols used in IoT devices, such as Wi-Fi, Bluetooth, and Thread, while preventing data loss or link drops. Accurate timing is also vital for fast, stable reconnections during startup or wake cycles, when IoT devices must instantly rejoin the network.

However, robust timing requires careful engineering. For instance, as quartz-based resonators shrink, the equivalent series resistance (ESR) and other parameters can increase, impacting efficiency and stability. Selecting low-ESR, high-accuracy crystals with the right packaging can help balance power consumption, oscillation stability, and reliability — all of which are key factors in delivering high-performance, energy-efficient IoT designs.

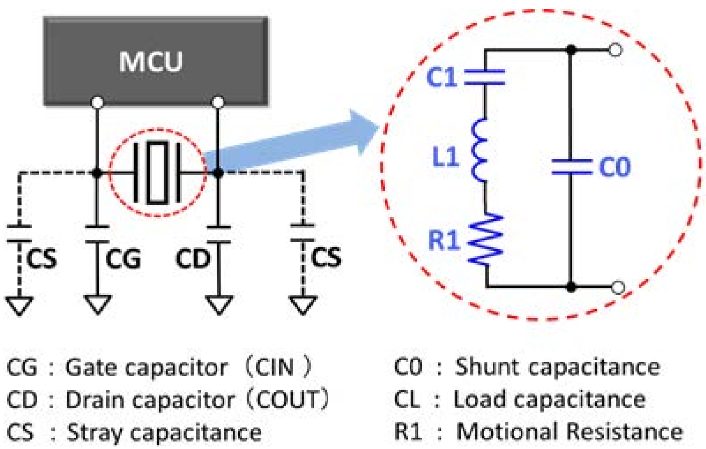
Understanding Equivalent Series Resistance

Crystals are essential in electronic devices, delivering precise timing signals for applications such as microprocessors and communication systems.

The performance of the resonator is a key requirement for these systems, as it enables efficient power consumption and enhances device reliability. The device must also ensure stable oscillation and precise synchronization of operations and be small enough to support the integration of multiple functions and components within compact devices.

A key parameter influencing performance is the equivalent series resistance, or ESR. ESR acts as an inherent resistance that opposes oscillation, causing part of the input energy to dissipate as heat. This loss reduces efficiency, which is particularly critical in low-power applications.

In a circuit, a crystal is represented with motional capacitance, motional inductance, motional resistance, and shunt capacitance (**Fig. 1**). ESR typically approximates the motional resistance, and a lower ESR value is highly desirable. Understanding ESR allows engineers to ensure reliable and efficient crystal operation.

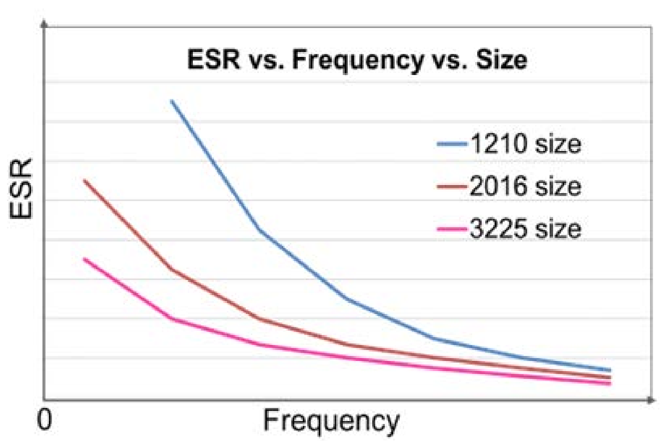


$$ESR = R1\left[1+\frac{C0}{CL}\right]^2 \qquad CL = \frac{CG \times CD}{CG + CD} + CS$$

1. The resonator is represented in a circuit by its motional capacitance, inductance, and resistance as well as its shunt capacitance. (Image credit: Epson)

The Tradeoffs Impacting ESR in Timing Devices

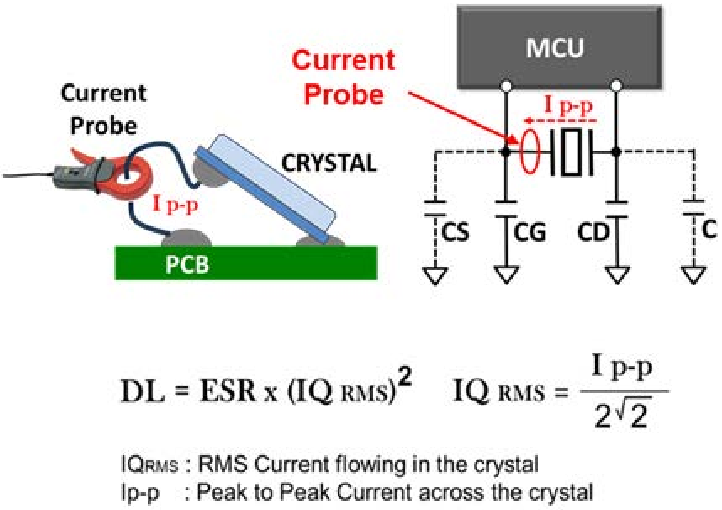
ESR is largely dependent on frequency and size. These timing devices are passive components that create a clock signal based on the vibrations of the resonator when it's run through with electric current. Smaller crystals and those operating at lower frequencies tend to have higher ESR values. This is primarily because smaller crystals possess a higher electrical resistance per unit area, and frequencies and resistance are inversely proportional (**Fig. 2**).



2. More compact crystals have a higher electrical resistance per unit area, and frequencies and resistance are inversely proportional. (Image credit: Epson)

The challenges of reducing ESR in smaller-size crystals come from inherent limitations imposed by size constraints and material properties. To achieve lower ESR values in these smaller timing devices, careful parameter optimization during the design phase is necessary to minimize resistive losses while maintaining desired electrical characteristics.

This is important because when ESR exceeds specified thresholds, issues can arise that degrade an electronic system's functionality and reliability. Maintaining ESR within specified limits is essential to ensure efficiency, stability, and reliability; excess ESR increases energy loss, reducing efficiency and shortening battery life. By carefully selecting low-ESR crystals, engineers can wring more perfor-



3. Lower ESR reduces the amount of power required to drive the resonator and maintain stable oscillation, boosting efficiency. (Image credit: Epson)

mance out of power-sensitive devices at the edge.

A higher ESR also means that crystals take longer to reach stable oscillation, delaying system functions, impairing performance, and increasing power even further. Moreover, the high ESR can block reliable startup, causing unstable oscillations, synchronization issues, and reduced system reliability.

How ESR Plays into Efficient Power Consumption

ESR directly impacts energy efficiency. By ensuring lower ESR, the resonator effectively reduces resistive losses during operation, leading to less power dissipated as heat. Optimizing ESR not only extends the battery life of electronic devices, but it also reduces the risk of performance degradation caused by excessive power dissipation.

The drive level (DL) primarily affects crystal power consumption. Lower ESR reduces DL, so the crystal uses less power to maintain oscillation, thus operating more efficiently. DL can be determined from the ESR and the peak-to-peak current (I p-p) across the crystal (**Fig. 3**).

The Influence of Low ESR on Fast Startup Times

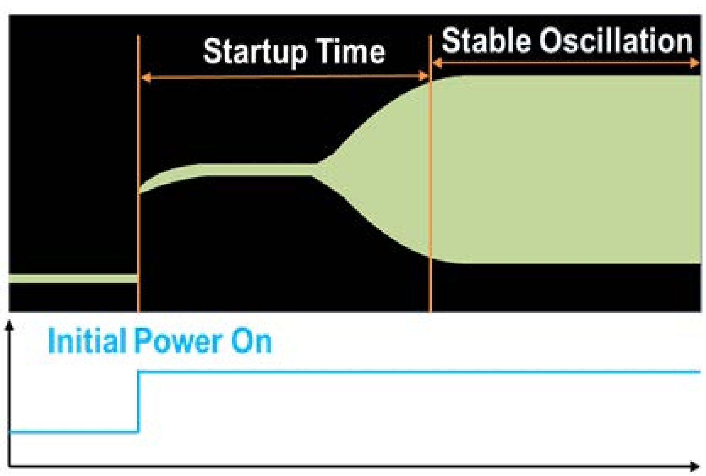
Maintaining low ESR in kHz crystals is crucial for fast startup times, ensuring a stable clock signal is provided to the microprocessor immediately after power-up (**Fig. 4**). Lower ESR reduces the time required for the crystal to stabilize, minimizing high current consumption during the startup period.

The startup times enabled by kHz resonators are inherently slower than in higher-frequency devices, making low ESR essential in applications that require immediate and reliable clock signals for MCUs and MPUs. As a result, minimal ESR helps enhance energy efficiency at a system level, making it a critical factor for power-sensitive electronic systems.

Low ESR Enables Stable Oscillation During Startup

Low ESR plays a key role in determining the “oscillation margin,” which ensures stable crystal oscillation during the startup period. The oscillation margin reflects the oscillator’s ability to start and sustain reliable oscillation under varying conditions during this period.

More specifically, it’s the ratio of the oscillator’s negative resistance to ESR and can be determined by measuring the maximum series resistance (RQ_{MAX}) that the crystal can tolerate

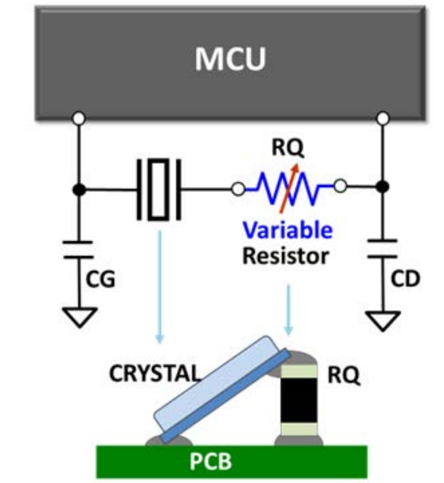


4. Maintaining low ESR in timing devices is crucial for supplying a stable clock signal during the startup of the microprocessor. (Image credit: Epson)

(**Fig. 5**). A higher margin indicates greater stability, and lower ESR improves it. RQ is adjusted until oscillation stops to determine RQ_{MAX}. A margin above 5 ensures reliable startup and stable operation.

Choosing Timing Devices to Deliver Reliability and Precision

Timing devices such as the FC1610BN that operate at 32.768 kHz can support a wide range of applications, providing designers with options to meet diverse requirements in modern portable and wearable IoT devices. A comprehensive crystal portfolio lets engineers select from a full range of packages, including industry "sweet spot" sizes, optimizing design flexibility. And the very low ESR ensures energy-efficient operation and reliable oscillation in IoT designs.



$$\text{Oscillation Margin} = \frac{RQ_{MAX.} + ESR}{ESR}$$

5. The oscillation margin reflects the oscillator's ability to start and sustain reliable oscillation under varying conditions. (Image credit: Epson)

Today's wireless IoT devices require compact size, low power, and high accuracy. The FC1610BN is a 32.768-kHz unit with ultra-low ESR that checks a lot of these boxes. The compact 1.6- × 1.0-mm package fits in space-constrained enclosures while the ESR extends battery life in energy-constrained wearable devices. The wide temperature range from −40 to +105°C ensures industrial-grade reliability in harsh conditions (**see table**).

Specifications (characteristics)

Item	Symbol	Specifications
Nominal frequency range	f_nom	32.768 kHz
Storage temperature range	T_stg	-55 °C to +125 °C
Operating temperature range	T_use	-40 °C to +85 °C -40 °C to +105 °C
Level of drive	DL	0.1 μW Typ. (0.5 μW Max.)
Frequency tolerance (standard)	f_tol	±20 x 10^{-6}
Turnover temperature	Ti	+25 °C ± 5 °C
Parabolic coefficient	B	-0.04 x 10^{-6} / °C^2 Max.
Load capacitance	CL	7 pF, 9 pF, 12.5 pF
Motional resistance (ESR)	R1	45 kΩ Typ. 60 kΩ Max. 70 kΩ Max.
Motional capacitance	C1	7.8 fF Typ.
Shunt capacitance	C0	1.5 pF Typ.
Frequency aging	f_age	±3 x 10^{-6} / year Max.

The specifications of the FC1610BN. (Image credit: Epson)

Selecting the right timing device is just the first step. Design evaluation services help engineers optimize performance and reliability in their devices. Early-stage support mitigates risks such as unstable oscillation, high power consumption, or inaccurate timing, leading to reliable, energy-efficient operation and faster time-to-market.

This support can help evaluate the ESR analysis and oscillation characteristics of a design as well as the oscillation margin and startup time. Measuring frequency accuracy and drift helps to verify timing reliability for the design.

Advancing the Clock with Vertical Integration

In kHz crystals, low ESR is essential for ensuring reliable operation. It supports energy-efficient performance, fast startup times, and consistent oscillation, all of which are particularly important for portable and wearable devices. Designers can use these timing solutions to ensure precise, stable timing and maximize energy efficiency in battery-powered systems.

Understanding ESR is critical for designers, as it affects power consumption, oscillation stability, and system reliability — but it's only part of a larger picture.

Another key factor in delivering the performance needed for IoT designs lies in working with suppliers that have a vertically integrated manufacturing process. Designing and producing both synthetic quartz crystals and semiconductor ICs in-house guarantees end-to-end control, making sure the timing solutions deliver the performance, reliability, and availability.

The vertically integrated process ensures that the timing solutions meet strict standards for uniform performance, and full control over production delivers a dependable supply chain. The integrated expertise helps in the rapid development of optimized and innovative solutions.

JONNY LEE is a Product Marketing Manager at Epson. Before joining Epson, he worked in the semiconductor industry, focusing on embedded system applications. With deep expertise in quartz-based timing devices and their diverse applications, Jonny has helped customers in optimizing their system designs and selecting the best crystal products for their needs.

view this article online

BACK TO TABLE OF CONTENTS

CHAPTER 5

Building the Bridge Between Smart Homes and EV Charging

From Wi-Fi to cellular IoT, explore the wireless technologies enabling secure, intelligent EV charging solutions for smart homes.

MARTIN LESUND, Technical Product Manager at *Nordic Semiconductor*

Nordic Semiconductor

Despite the steady growth of electric vehicles (EVs), charging infrastructure continues to lag behind, making reliable home charging essential.

While installing a charger is straightforward, optimizing its operation for both cost and convenience requires integration with a smart-home ecosystem. However, adding a high-power device like an EV charger to an already crowded home network presents unique connectivity challenges. Engineers must ensure secure, reliable, and scalable communication between chargers, home energy-management systems (HEMS), and other devices.

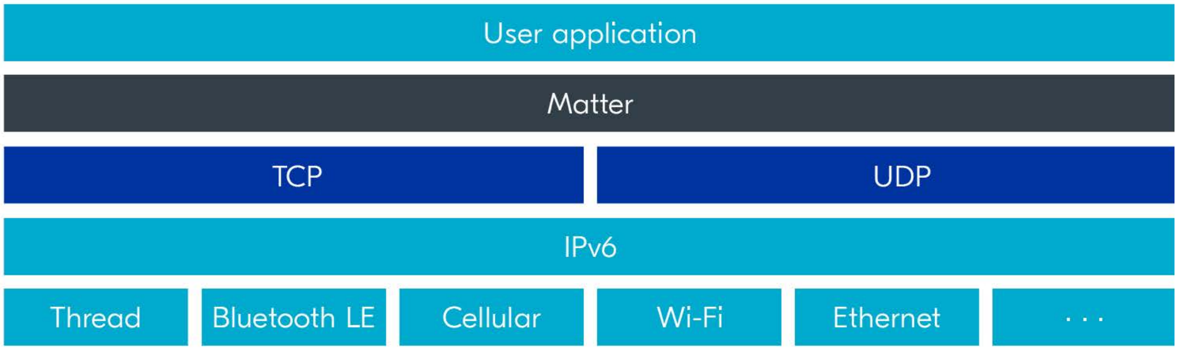
Advances in wireless connectivity, including Wi-Fi, Bluetooth, Thread, and the Matter standard, as well as alternatives such as cellular and non-cellular IoT technologies, are helping designers overcome the obstacles.

The Necessity of Smart At-Home Charging

As the world's major automakers channel R&D to an all-electric future, the need for intelligent, connected charging is rising, especially due to fluctuating energy costs and increasing demands on the electric grid. Smart-home integration allows users to schedule charging for off-peak hours, monitor charging status remotely, and even redirect excess solar power to the EV. This level of control requires secure and unfailingly reliable wireless connectivity, capable of relaying usage data, system health, and availability to a central platform.

For local user interaction and integration with other smart-home devices, the Matter standard is emerging as the key unifier. By building on top of proven IP-based protocols like Wi-Fi and Thread (with Bluetooth LE for commissioning), Matter aims to bring seamless interoperability to smart homes. In turn, the EV charger can communicate seamlessly with a HEMS or other devices like smart plugs, as well as solar inverters or energy storage, enabling flexible automation. But Matter can't do it all by itself.

The increasingly close ties between the smart home and the EV are creating a new frontier for innovation. However, the solution isn't a single wireless standard, but a combination of connectivity technologies — each chosen to meet specific performance, range, and reliability requirements.



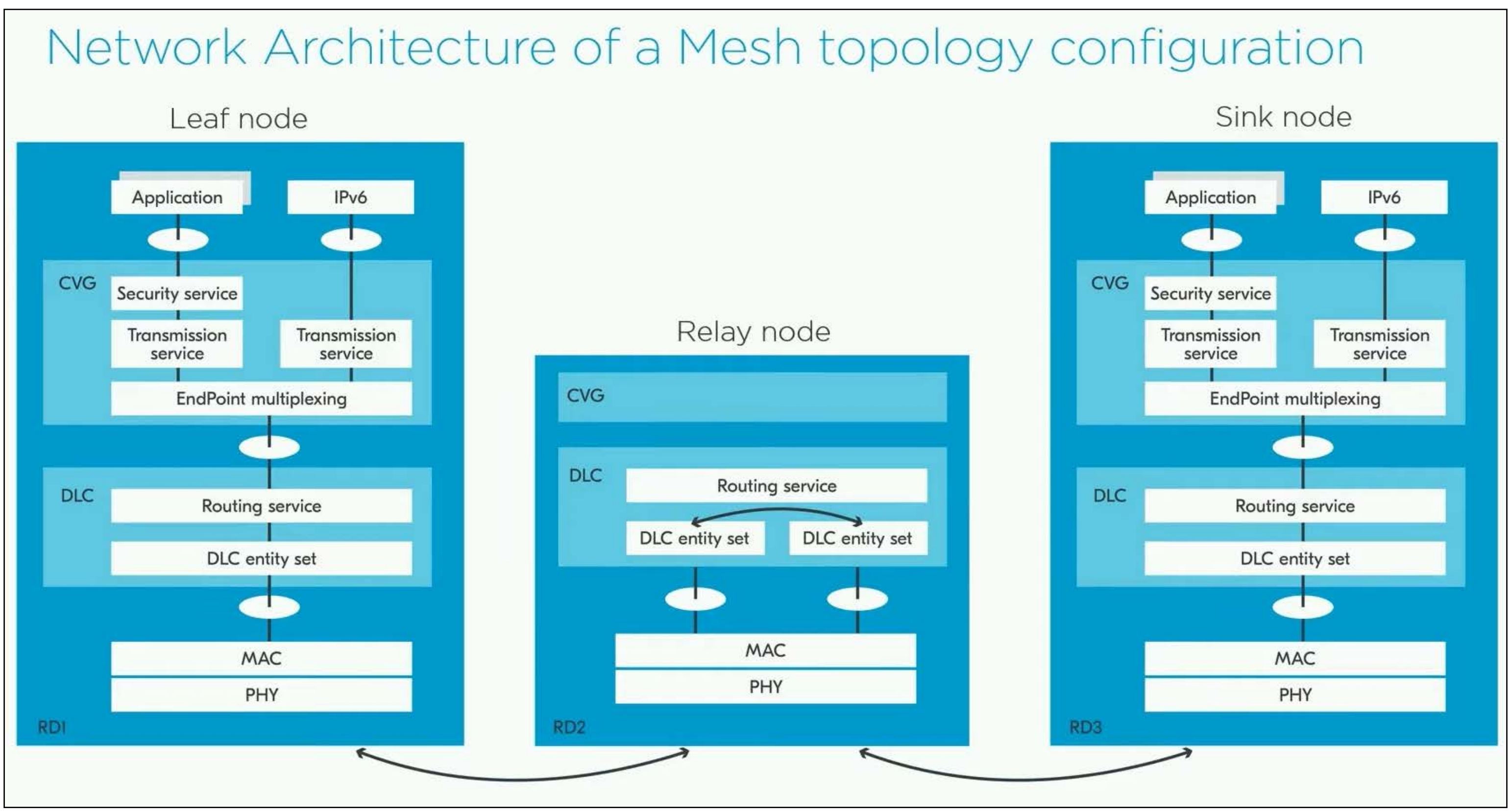
Matter runs on top of Thread and Wi-Fi and uses Bluetooth LE for commissioning, making it possible for IoT devices from different ecosystems and made by different companies to communicate.

Nordic Semiconductor

Combining Cellular and Non-Cellular IoT for Guaranteed Connectivity

While Wi-Fi is the default way to connect many smart-home devices to the cloud, it's not always the optimal solution for charging infrastructure. Today, EV chargers are often installed in locations with notoriously poor Wi-Fi coverage, such as concrete basements, underground parking facilities, or detached garages far from the home router. In these scenarios, relying on the local Wi-Fi network can be impractical — and unreliable. This is where cellular IoT technologies can come into play.

By embedding LTE-M or NB-IoT



A DECT NR+ network is comprised of a sink node that connects the wireless mesh network to other devices and the cloud.

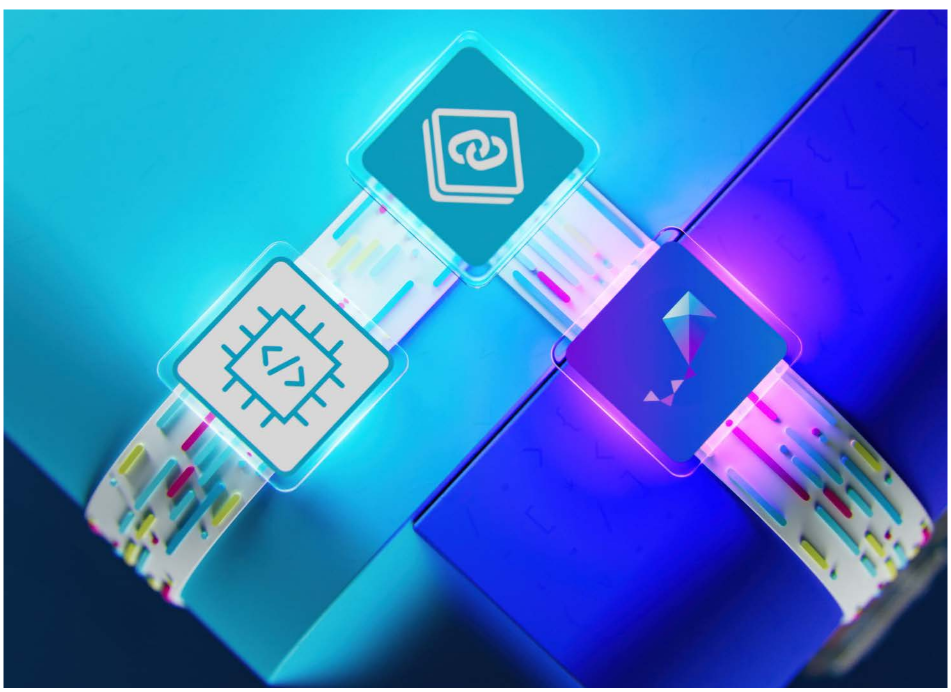
Nordic Semiconductor

connectivity directly into the charger, manufacturers can bypass the local network entirely. It creates a separate, secure, and professionally managed connection to the cloud, guaranteeing uptime regardless of the quality of the Wi-Fi network. This direct-to-cloud approach simplifies installation and provides a robust link for critical functions such as payment processing, over-the-air (OTA) firmware updates, and remote diagnostics.

The connectivity challenge evolves in multi-charger settings, such as apartment complexes, small businesses, or new housing developments. Equipping every charger with its own cellular or Wi-Fi connection could be costly and complex to manage.

In these situations, it can make sense to use mesh networking to connect all of the chargers to each other and a gateway that further connects them to the cloud. One potential solution is DECT NR+, a non-cellular 5G standard. Operating in a dedicated and license-free 1.9-GHz band, it allows you to create private, self-healing, and highly robust mesh network connecting dozens or even hundreds of chargers. This low-latency network is ideal for load balancing and coordinated charging across multiple vehicles.

In a DECT NR+ topology, one — or several — chargers can act as a sink node (or gateway). This sink node is the only unit that requires a backhaul connection to the internet, which is available via cellular IoT, Wi-Fi, or Ethernet. It then relays all data for the entire cluster of chargers, dramatically reducing infrastructure costs and simplifying network management.



The nRF Connect SDK from Nordic supports multiprotocol connectivity, enabling a single device to run a wide range of wireless standards, even cellular and non-cellular ones, at the same time. Nordic Semiconductor

The Keys to the Wireless IoT: Security and Connectivity

Bringing all of these wireless protocols into a single device is one of the main challenges for engineers.

For example, a modern connected EV charger may need to support Wi-Fi for its primary connection with cellular IoT as a fallback, DECT NR+ for local networking, and Bluetooth LE for initial setup. Supporting them requires wireless SoCs with multiprotocol radios as well as sufficient processing and memory to run multiple protocol stacks — or wireless modules bundling many of the same building blocks in a more plug-and-play package.

The growing complexity of the wireless IoT has pushed suppliers such as Nordic Semiconductor to develop SoCs that integrate more radios, more processors, and more memory to run multiple wireless protocols at the same time.

Beyond protocol support, one other issue involves implementing robust, hardware-based security. An EV charger isn't just another smart-home gadget; it's a high-power appliance connected to both the electrical grid and the cloud. The attack surface is significant, and the consequences of a breach are severe. A compromised charger could be used to disrupt the power grid, commit energy theft, expose sensitive user data and billing information, or even create a physical safety hazard.

Securing these devices requires a defense-in-depth strategy anchored in hardware. A software-only approach is insufficient, as it can be circumvented if an attacker gains initial access. The foundation of modern IoT security is a root of trust (RoT). This is an immutable, trusted system within the SoC or the system that serves as the anchor for all security operations. Building upon the RoT, a secure system must provide several key services:

- **Secure boot:** Every time the device powers on, the RoT verifies the cryptographic signature of the bootloader and application firmware. This ensures that the device only ever runs authentic, untampered-with software, preventing persistent malware infections.
- **Secure firmware updates:** OTA updates are essential for patching vulnerabilities and adding features. A secure update mechanism ensures that the device cryptographically verifies the authenticity and integrity of a new firmware image before installation, preventing attackers from loading malicious code.
- **Secure key storage:** The device needs to store cryptographic keys for encrypting communications and authenticating itself. These keys must be protected in a secure vault, isolated in hardware, to prevent them from being extracted even if an attacker has physical access to the device.
- **Hardware isolation:** Critical processes must be isolated from the main application. Technologies such as Arm TrustZone create a secure processing environment, where cryptographic functions and other sensitive operations can be executed separately from the less-trusted, internet-facing application code.

IoT solutions that are PSA Certified, such as those offered by Nordic Semiconductor, provide the highest level of security assurance. This third-party certification validates not just robust software protection, but also substantial resistance to sophisticated physical hardware attacks, giving designers and end-users confidence that the device's security foundation is sound.

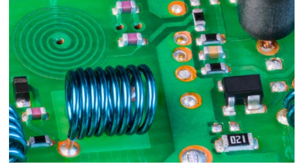
Multiprotocol Wireless Connectivity Covers All the Bases

By leveraging cellular IoT for guaranteed connectivity, Matter for smart-home interoperability, and DECT NR+ for scalable multi-charger networks, developers can create truly intelligent charging solutions. With advanced multiprotocol SoCs and unified software platforms like the nRF Connect SDK, companies are now equipped to bridge the gap, driving convenience, energy efficiency, and innovation in the future of residential EV charging.

view this article online

BACK TO TABLE OF CONTENTS



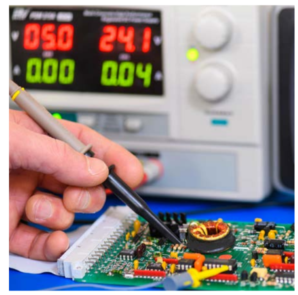




☞ ElectronicDesign

Electronic Design has a diverse array of content for your perusal. To explore what our site offers, check out these links:


☞ Special Reports

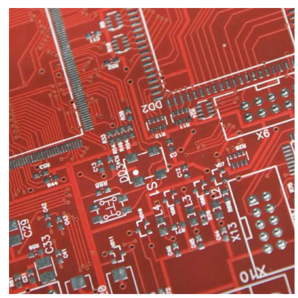
☞ Top Stories of the Week




☞ Inside Electronics

☞ TechXchanges

☞ Newsletters




☞ Blogs

☞ Become an Electronic Design Member