

**SPECIAL REPORT**

# THE SMARTER SMART HOME



## Table of Contents

- CHAPTER 1  
**2 RF Reality in the Smart Home**
- CHAPTER 2  
**7 Smart Homes Enter the IoT 2.0 Era: Rethinking the Wireless Foundation**
- CHAPTER 3  
**11 Redefining Access Control for the Smart Home**
- CHAPTER 4  
**13 7 IoT Trends Shaping Smart Homes and Buildings in 2026**
- CHAPTER 5  
**16 Building Intelligent and Interoperable Smart Homes with Wi-Fi 7**

## Furnishing the Smart Home

*The smart home is an application space that's slowly maturing, with interesting devices and solutions addressing the needs of today's consumers.*



*By Alix Paultre, Editor-at-Large*

When it comes to developing application spaces, the smart home is one that has deep roots. However, it's essentially still in an evolutionary phase. Creating devices and systems to reduce the amount of work in a household goes as far back as the commercialization of electricity, yet the space has a long way to go. The smart home is much like the automotive world, as every technology currently under development is being ported to the home in one fashion or another.

From advanced power-management electronics to next-generation edge computing to robotics and automation, newer and better ways are being developed to make our lifestyles easier, more comfortable, and more productive. The latest solutions range from technologies that are empowering our appliances and devices, to in-wall systems to control our heating, lighting, convenience, and security.

This eBook collects together features that highlight various aspects of the smart home and its underlying infrastructures. We hope you find them useful and informative.

## CHAPTER 1

# RF Reality in the Smart Home

*This article explores the real-world RF challenges of coexistence, antenna integration, and enclosure interaction, and outlines a practical design approach for delivering reliable wireless performance in the connected home.*

BAHA BADRAN, Global Head of Engineering, *Taoglas*



dreamstime\_Vladimir Stanisc\_71562940.jpg

Smart-home products are rapidly evolving from single-radio nodes into dense, [multi-protocol systems](#) that must support Wi-Fi, Thread, Bluetooth Low Energy (BLE), and often sub-GHz or UWB within a single, highly constrained enclosure. While [Matter](#) has accelerated interoperability across ecosystems, it's also increased the number of active radios operating within the home (Fig. 1). The result is a growing disconnect between passing protocol tests and delivering reliable RF perfor-

mance in real houses.

Devices that function correctly in controlled lab environments can struggle once deployed into RF-dense homes. Interoperability may be addressed at the software layer, but reliability is still governed by physics. That constraint becomes more significant as wireless fragmentation converges within the home, with multiple protocols and spectrum bands now coexisting within the same device.

## Fragmentation Comes Home: Multi-Protocol by Default

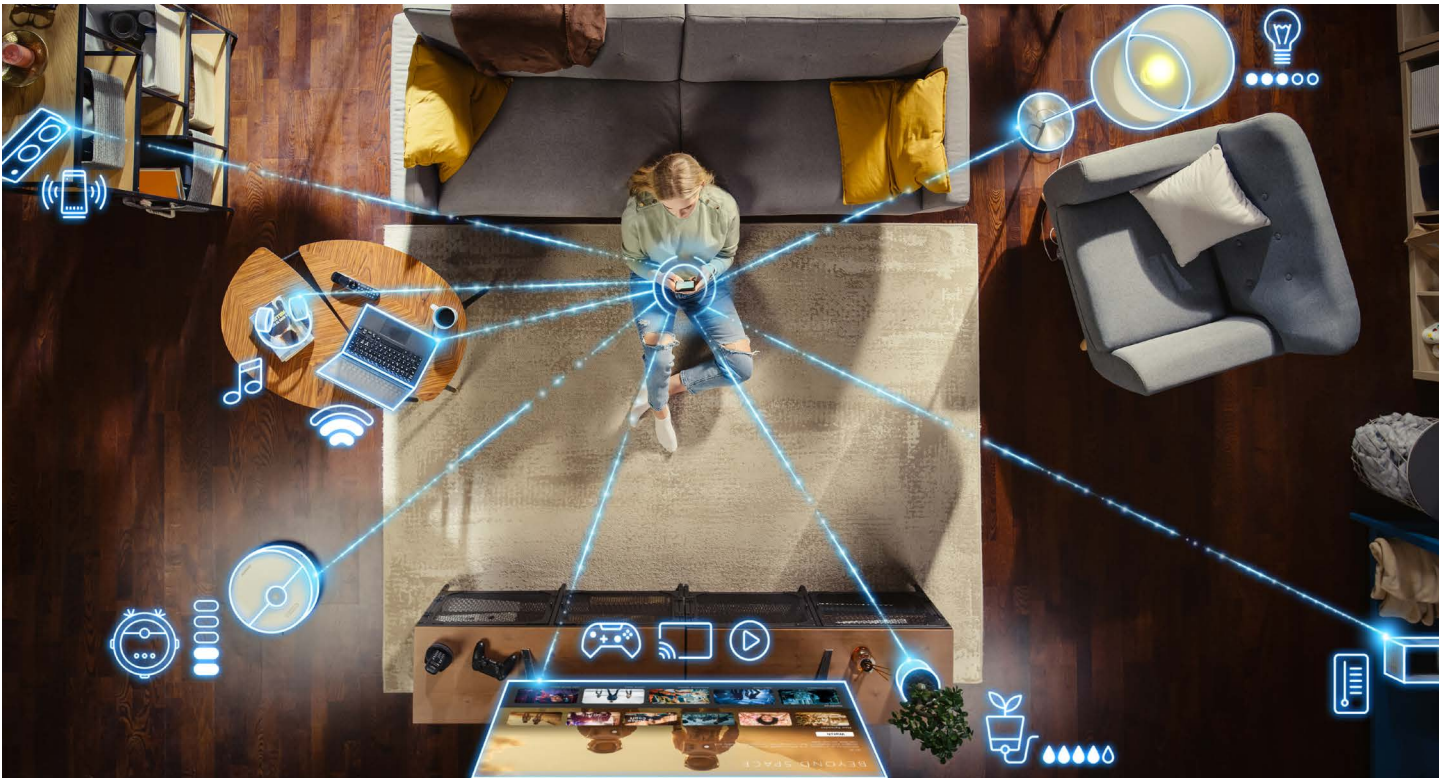
The typical smart-home device no longer supports a single connectivity option. Instead, it may combine Wi-Fi (2.4 GHz, 5 GHz, and increasingly [Wi-Fi 6](#)), Thread, BLE, and sometimes sub-GHz connectivity or UWB positioning within a single compact enclosure.

Much of this activity occurs in the unlicensed spectrum, particularly the crowded 2.4-GHz band. While protocol designers have developed coexistence strategies at the MAC layer, physical-layer coexistence remains a separate challenge.

In some multi-protocol modules, a single device may integrate three separate antennas within a confined footprint. Achieving sufficient isolation between these elements — while preserving radiation efficiency — becomes non-trivial. When multiple radios share common ground structures and confined enclosure volume, mutual coupling can quickly erode link margin.

These integration pressures are compounded by spectrum choices.

## CHAPTER 3: RF Reality in the Smart Home



1. Matter has increased the number of active radios operating within the home. (Credit: Adobe Stock)

Certain applications, including smart meters and heating systems in Europe, are increasingly moving toward sub-GHz bands such as 868 MHz.

Lower frequencies improve penetration through walls, but they require physically larger antenna structures, greater clearance from metal enclosures, and more substantial ground planes. The mechanical- and industrial-design implications can dominate enclosure and layout decisions.

### The Real RF Environment of a Matter-Enabled Home

Unlike anechoic chambers or simplified bench setups, real homes are electrically complex environments. Walls, reinforced concrete, appliances, and

metal fixtures introduce attenuation, reflection, and multipath propagation, causing fading that varies with small positional changes. At 2.4 GHz, congestion from neighboring networks, legacy routers, and consumer electronics further raises the noise floor.

Developers sometimes assume that limited coverage is acceptable in a domestic environment, and that a few meters of range will suffice. In practice, once installed in a real home, devices operate in electrically complex surroundings with multiple active transmitters and unpredictable interference. Marginal lab performance can quickly turn into practical problems — blinds that fail to respond, sensors that drop offline, or hubs that lose

connection stability.

In some applications, the consequences extend beyond inconvenience. EV chargers that rely on reliable smart-meter connectivity to access optimal tariffs can directly affect a homeowner's electricity costs. In these cases, unreliable RF performance could translate directly into lost tariff savings and frustrated customers.

### Why Smart-Home Designs Still Fail in the Field

Despite advances in chipsets and protocol stacks, many failures can be traced to basic RF integration issues.

A common issue is insufficient antenna-to-metal clearance. Enclosure

## CHAPTER 3: RF Reality in the Smart Home



## 2. Antenna topology is a key consideration. (Taoglas)

walls, internal shielding, mounting hardware, and even decorative metallic finishes can detune an antenna, reducing efficiency and shrinking effective range. The impact may not appear during early validation, but it often emerges during certification or field deployment.

Impedance mismatch is another overlooked factor, translating into increased current draw and shortened battery life in smart-home devices.

Time pressure often compounds these risks, with compressed testing cycles in fast-moving markets. Environmental validation and full coexistence evaluation can be deferred, only for customer complaints to surface later. Many late-stage redesigns originate from architectural RF decisions made early in the program, long

before performance problems become visible.

### Antenna and Front-End Strategies for Coexistence in Real Smart-Home Form Factors

Mitigating these risks requires deliberate antenna and front-end architectural decisions made with the final enclosure and operating environment in mind.

Antenna topology is a key consideration (*Fig. 2*).

Shared antenna approaches can reduce cost and conserve space, but they introduce additional filtering, switching complexity, and isolation challenges. Dedicated antennas per radio may improve robustness, although they demand careful spatial

planning within constrained enclosures and increase pressure on PCB real estate and mechanical design.

Physical integration is equally important. Adequate antenna-to-metal clearance, from enclosure walls and internal shields to battery cans and other conductive elements, is one of the most effective safeguards against performance degradation. These constraints become even more pronounced at lower frequencies, such as 868 MHz, where antenna size increases and interaction with ground structures becomes more significant.

When multiple radios coexist within a confined footprint, isolation must be designed in from the outset. Antenna spacing, orientation, ground strategy, and filtering all influence coexistence performance. In dense gateways or hubs operating simultaneous radios, unintended coupling can degrade receiver sensitivity or introduce desensitization risks if not carefully controlled.

Impedance matching is equally important to overall system performance. The effectiveness of the impedance match has a direct impact on radiation efficiency and the load presented to the RF front end.

Poor matching increases return loss, reducing effective radiated power and lowering received signal strength integration (RSSI) at the peer device. Reduced link margin drives retransmissions and higher transmit duty cycle. In battery-powered smart-home

## CHAPTER 3: RF Reality in the Smart Home



**3. In the smart-home enclosure materials, device placement, congestion, and multi-radio interaction all shape performance (Adobe Stock)**

devices, this translates directly into higher average current consumption and reduced operating life — a predictable consequence of suboptimal antenna integration.

Form factor further shapes these tradeoffs. Mains-powered devices may experience conducted noise and grounding interactions. Retrofit products, such as smart switches installed in metal backboxes, operate in RF-hostile environments with limited clearance. Gateways and hubs must balance antenna isolation against thermal constraints and compact industrial design requirements.

In practice, RF performance reflects how antenna choice, enclosure design, PCB layout, and power

architecture interact in the finished device. Addressing these constraints requires early coordination between RF, mechanical, and industrial design disciplines.

### **A Repeatable RF Design Flow for Smart-Home Products**

As smart-home devices grow more complex, reliable wireless performance requires a disciplined RF design process.

The process begins with early RF engagement, ideally before enclosure materials, PCB stackups, and industrial design are frozen. Antenna location, ground clearance, and proximity to noise sources should be treated as pri-

mary architectural decisions.

Next comes context-aware antenna selection. Designers must evaluate not only frequency band and efficiency targets, but also enclosure materials, device placement expectations, and multi-radio interaction within the final form factor (*Fig. 3*).

The next step is iterative validation, combining simulation with empirical measurement. Modelling tools support early exploration, but enclosure effects and coupling paths must be confirmed through representative measurement.

Final antenna tuning is carried out with the complete mechanical and electrical system in place, including cabling, power architecture, and sources of conducted or radiated noise. Tuning an isolated PCB rarely reflects the behavior of the finished product.

Pre-certification RF checks should then confirm link margin, coexistence robustness, and receiver sensitivity under realistic conditions before formal compliance testing gets underway. This reduces the risk of repeated certification cycles and costly redesigns.

Online integration and simulation tools can support this methodology. Manufacturers such as Taoglas provide cloud-based design platforms to guide antenna selection, placement, and optimization.

Taoglas' new AI-driven Antenna Product Recommendation Engine, for example, leverages application

## CHAPTER 3: RF Reality in the Smart Home

parameters to accelerate initial antenna selection, reducing iteration time while still requiring engineering validation. Embedded within a structured RF design flow, such tools reduce risk without sacrificing development speed.

### **Designing for Houses, Not Chambers**

Matter has simplified interoperability, but it hasn't simplified RF physics. The modern smart home is a dense and dynamic RF environment, where enclosure materials, device placement, congestion, and multi-radio interaction all shape performance.

Reliable smart-home products depend on early, disciplined RF architecture decisions. Late-stage tuning can't compensate for structural integration shortcomings. A well-executed RF design provides predictable performance in real deployment environments, giving developers, installers, and end users confidence that connected devices will operate as intended.

[view this article online](#)

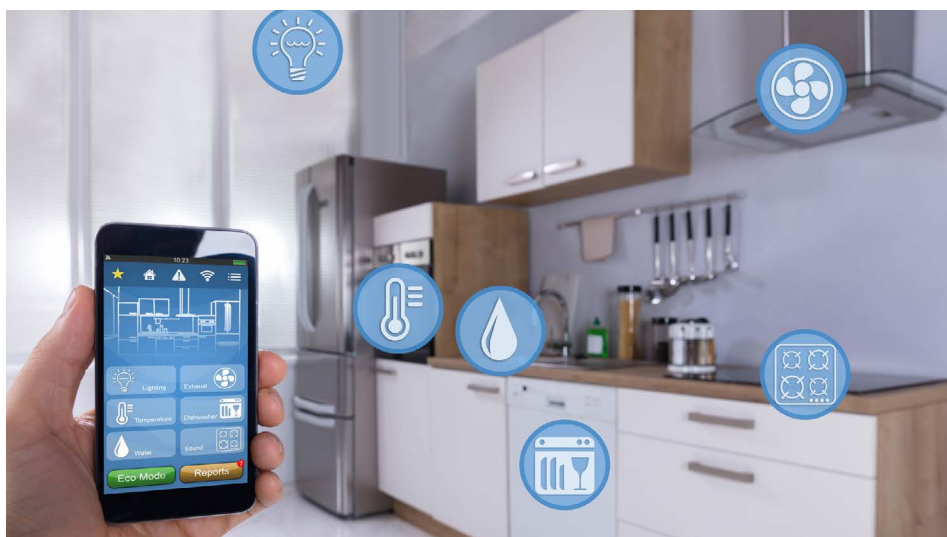
 **BACK TO TABLE OF CONTENTS**

## CHAPTER 2

## Smart Homes Enter the IoT 2.0 Era: Rethinking the Wireless Foundation

*As IoT 2.0 brings edge AI, real-time coordination, and constant data streams into residential environments, the challenge becomes the creation of a scalable, secure wireless foundation that can support truly intelligent homes.*

ANDY MCFARLANE, Vice President of Marketing, Morse Micro, [www.morsemicro.com](http://www.morsemicro.com)



dreamstime\_Andrey Popov\_126278521.jpg

For years, smart home innovation has focused on endpoints, cameras, locks, thermostats, lighting controls, and appliances. But as these systems evolve toward distributed intelligence, the constraint is no longer the device. It's the wireless layer.

We are now in what many describe as the IoT 2.0 phase: Systems that process data locally, perform AI inference at the edge, and coordinate in real-time. Unlike early IoT deployments that transmitted infrequent, low-bit-

rate telemetry, these new residential systems generate sustained data streams — video, audio, sensor fusion, and control feedback loops.

The architectural question is no longer “how do I connect a sensor?” Rather, it’s “how do I build a scalable, secure, property-wide wireless LAN that supports intelligence at the edge?”

### RF Physics Still Matters

Conventional Wi-Fi operates in 2.4-, 5-, and now 6-GHz bands. These

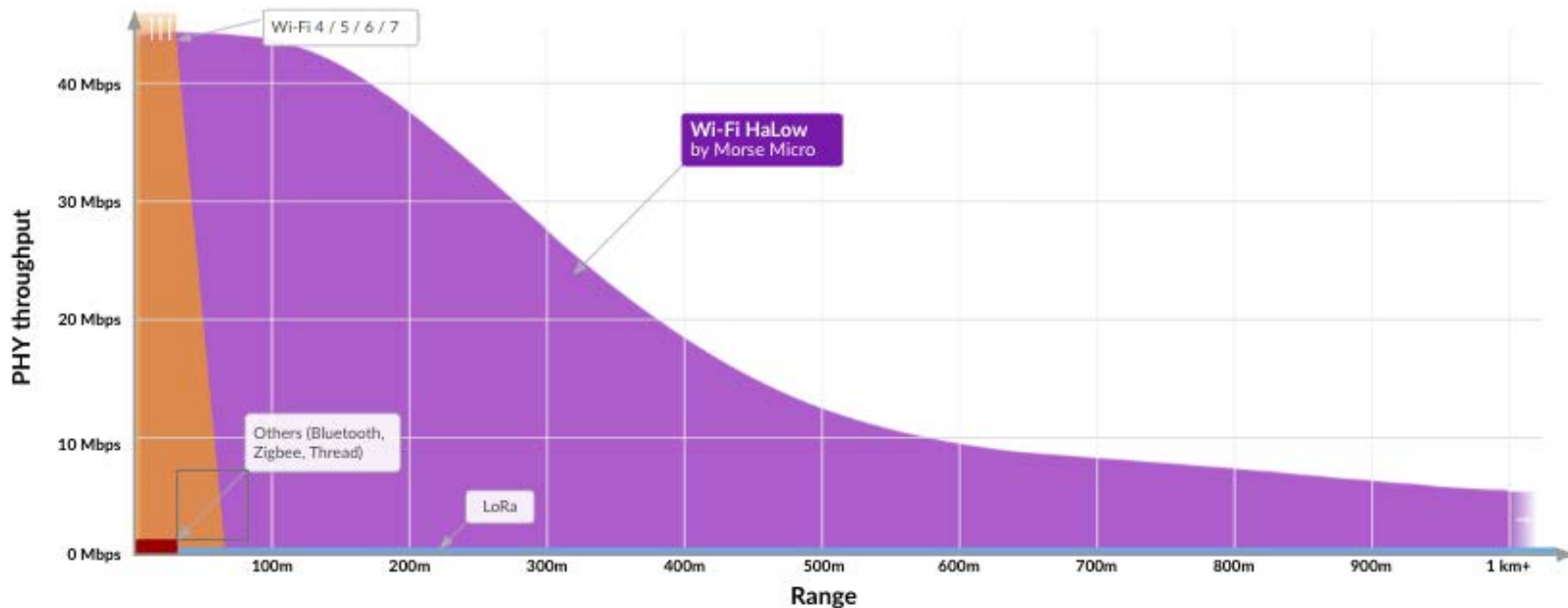
frequencies support high throughput via wide channel bandwidths (20/40/80/160 MHz), but they come with well-understood tradeoffs:

- Higher free-space path loss compared to sub-GHz
- Reduced diffraction around obstacles
- Greater attenuation through walls, concrete, insulation, and metal
- Dense access-point requirements in large properties

In residential deployments with detached garages, exterior cameras, multi-floor construction, and high device density, designers often compensate using mesh extenders and additional APs. This increases co-channel interference, airtime contention, and overall system complexity.

Sub-GHz operation fundamentally changes link budget dynamics. Path loss scales with frequency; moving from 2.4 GHz to ~900 MHz provides several dB of propagation advantage before accounting for improved diffraction and penetration charac-

## CHAPTER 2: Smart Homes Enter the IoT 2.0 Era: Rethinking the Wireless Foundation



1. Wi-Fi HaLow addresses the needs of modern smart home systems that increasingly require Mb/s-class throughput for compressed video or high-fidelity audio and property-wide IoT coverage.

teristics. In practice, this translates into more consistent received signal strength indication (RSSI) across property boundaries and fewer dead zones.

For distributed smart home systems, that RF advantage isn't incremental — it's architectural.

### Beyond “Pings”: Throughput and Latency Requirements

Early low-power wide-area-network (LPWAN) technologies such as LoRaWAN were optimized for narrowband, low-duty-cycle telemetry. Their link budgets are impressive, but their PHY layer data rates (sub-100 kb/s in many cases) and MAC-layer latency characteristics make them unsuitable for media-rich or interactive applications.

Modern smart home systems

increasingly require:

- Mb/s-class throughput for compressed video or high-fidelity audio
- Sub-second latency for door access control, alarm signaling, and energy automation
- Bidirectional firmware updates
- Secure IP connectivity

IEEE 802.11ah (Wi-Fi HaLow) was designed to address exactly this middle ground. Operating in unlicensed sub-GHz spectrum, it combines long-range propagation with orthogonal frequency-division multiplexing (OFDM)-based modulation, supporting channel bandwidths from 1 MHz upward and enabling multi-megabit throughput while maintaining lower power consumption.

Unlike LPWAN protocols that

require proprietary translation layers, 802.11ah remains fully IP-native. Devices integrate directly into standard TCP/IP stacks with WPA3 security. For system designers, this eliminates protocol bridging and reduces attack surfaces associated with multi-stack architectures.

### Device Density and Network Scaling

A critical engineering consideration in smart homes is not only coverage, but density. As the number of endpoints increases — security cameras, locks, occupancy sensors, lighting nodes, smart appliances — the medium-access-control (MAC) layer must scale efficiently.

802.11ah introduces mechanisms such as hierarchical AID (Association ID) structures and target wake time

## CHAPTER 2: Smart Homes Enter the IoT 2.0 Era: Rethinking the Wireless Foundation

(TWT) scheduling to support thousands of devices per access point. These features reduce contention and optimize airtime allocation, particularly for battery-operated endpoints.

This becomes especially relevant in multi-dwelling units and managed residential environments where device counts can exceed typical consumer Wi-Fi assumptions.

From a systems perspective, the ability to maintain a star topology across an entire property — without layering mesh protocols — simplifies RF planning and reduces failure points.

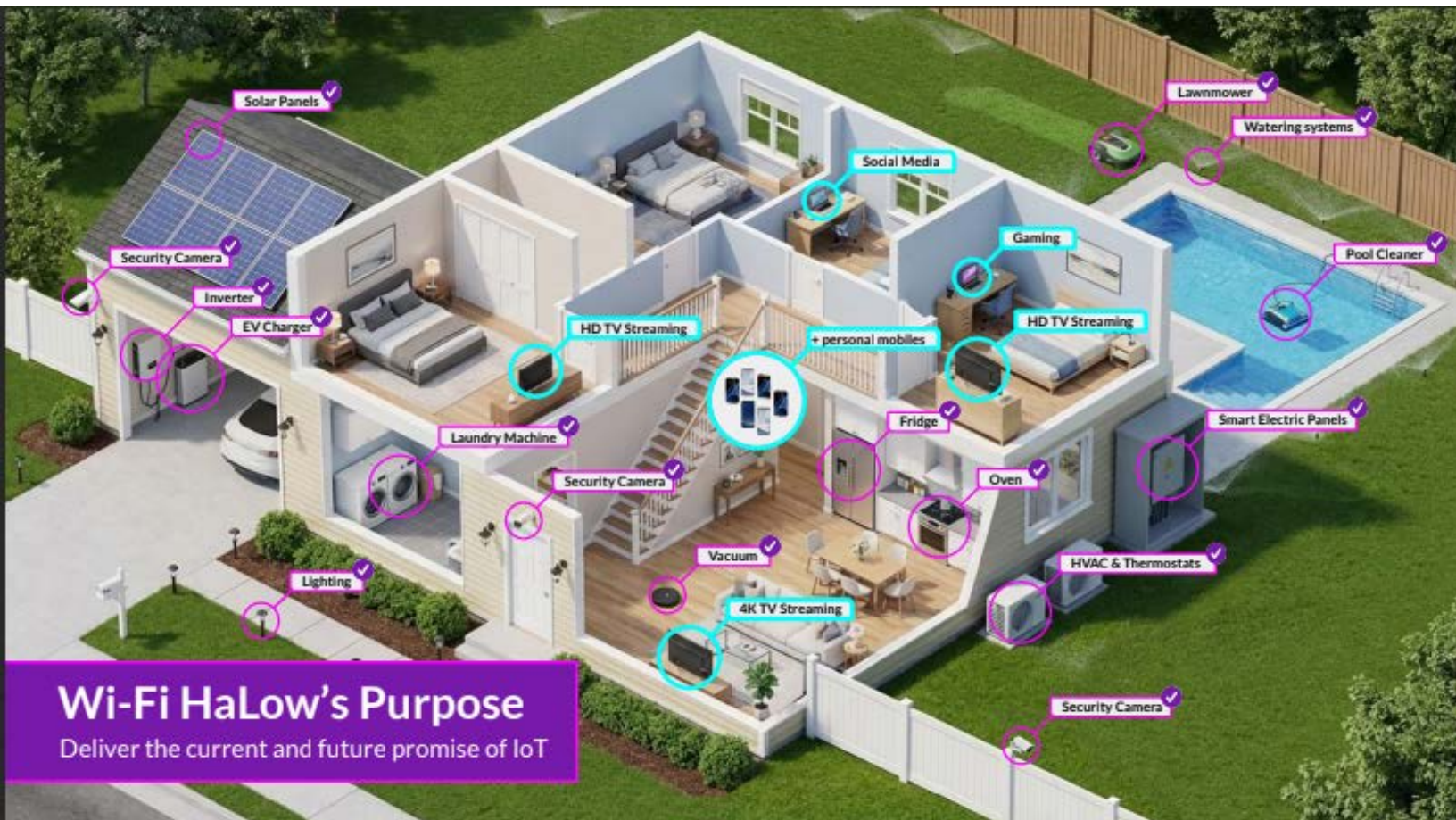
### Power Efficiency and Battery Longevity

Edge AI in smart homes doesn't eliminate the need for battery-powered devices. Door sensors, window monitors, environmental nodes, and perimeter detectors must operate for months or years without intervention.

Maintaining continuous connectivity over cellular links is power-prohibitive in most residential applications. Traditional Wi-Fi, while capable of power-save modes, wasn't architected primarily for ultra-low-duty-cycle endpoints.

802.11ah incorporates extended sleep intervals and optimized wake scheduling. Combined with narrower channel bandwidths and sub-GHz propagation advantages, this enables endpoints to achieve significantly improved energy efficiency while still supporting higher data rates when required.

The result is a practical balance: sufficient bandwidth for rich data exchange, without sacrificing battery longevity.



2. Edge AI devices such as cameras, locks, and sensors, connected via Wi-Fi HaLow as a LAN backbone, integrate into cloud services and existing Wi-Fi infrastructure.

## CHAPTER 2: Smart Homes Enter the IoT 2.0 Era: Rethinking the Wireless Foundation

## LAN, Not WAN: An Architectural Distinction

One of the most persistent misconceptions in long-range IoT connectivity is that range automatically implies WAN.

Smart homes are inherently LAN environments. Devices are fixed and local. They require robust intra-property connectivity first, with optional cloud backhaul.

Sub-GHz Wi-Fi extends the WLAN footprint rather than replacing it with a WAN service. This distinction matters:

- No recurring data fees
- No dependency on carrier availability
- Lower operational overhead
- Local intelligence remains local

Cloud integration remains straightforward via IP routing through a single broadband uplink, but device-to-device communication and AI-driven decision-making can occur entirely within the local domain.

For privacy-sensitive residential applications, such as video analytics and occupancy inference, this local-first architecture is increasingly important.

## Integration with Existing Infrastructure

Importantly, long-range sub-GHz Wi-Fi isn't positioned as a replacement for Wi-Fi 6 or Wi-Fi 7. High-bandwidth consumer traffic — AR/VR, gaming, 8K streaming — will

continue to rely on wider channels in higher bands.

Instead, sub-GHz Wi-Fi complements existing infrastructure:

- Traditional Wi-Fi handles high-throughput indoor traffic.
- Sub-GHz Wi-Fi provides property-wide IoT coverage.
- A unified IP framework ties both layers together.

From a design standpoint, this reduces the need for separate Zigbee/Thread gateways or cellular modules. The wireless stack becomes more coherent, security policies more uniform, and firmware management more centralized.

## Designing for the Next Decade

Smart homes are evolving into distributed computing environments. Devices no longer simply report state, they interpret context and take action. Cameras identify anomalies. Energy systems respond to grid conditions. Locks and access systems integrate with AI-based authentication.

This transition demands a wireless foundation capable of:

- Multi-megabit throughput
- Sub-second responsiveness
- Kilometer-scale coverage in residential environments
- Thousands of endpoints per AP
- Native IP interoperability
- Strong WPA3 security

For RF and system designers, the

takeaway is clear: As smart home intelligence scales, the PHY and MAC layers must scale with it. Sub-GHz Wi-Fi offers a path to extend the familiar WLAN model beyond the walls of a single room or building, without inheriting the cost and complexity of WAN-based alternatives.

The future of smart home infrastructure will not be defined solely by faster indoor Wi-Fi. It will be defined by smarter spectrum choices and architectures that align RF physics with the realities of distributed edge intelligence.

[view this article online](#)

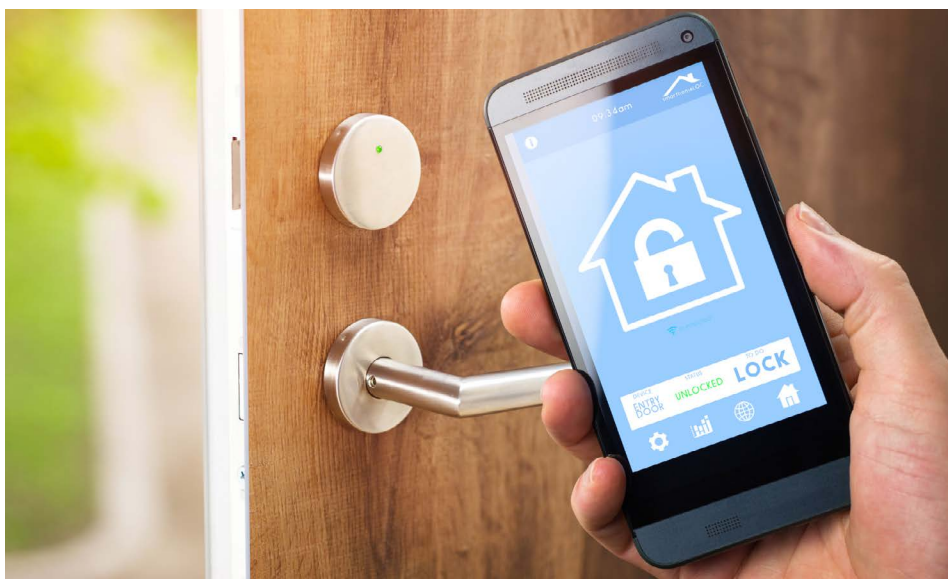
 [BACK TO TABLE OF CONTENTS](#)

## CHAPTER 3

# Redefining Access Control for the Smart Home

*Intelligent controllers are moving security and access decision-making from centralized servers to the edge of the network, right to the door.*

JEREMY FROMM, Evangelist, Mercury Security



dreamstime\_Audioundwerbung\_53546193.jpg

Access control has entered a new era. Intelligent controllers are moving decision-making from centralized servers to the edge of the network, bringing it right to the door. The result is faster performance, greater resilience, and new opportunities for customization that make access control more dynamic and adaptable than ever before.

## Why Edge Matters

Edge computing has already transformed fields such as industrial automation and automotive design. By

processing data closer to its source, engineers reduce latency, improve reliability, and enable real-time decision-making even when connectivity is unreliable. Physical access control is following the same path.

Traditionally, controllers enforced access rules locally, but their logic was limited to stored credentials and schedules. That's changing thanks to the newest generation of controllers. With modern processors and embedded software environments, these devices can execute sophisticated logic, analyze data, and interact direct-

ly with other building and IT systems without waiting on a head-end server.

## A Smarter Platform at the Door

Think of the modern access controller as a miniature application platform. Using standard SDKs and APIs, developers can deploy lightweight apps directly on the controller to perform specialized tasks. These could include:

- Monitoring network or device health in real-time
- Verifying configuration and certificate status
- Interfacing with building management or IoT systems
- Communicating with new types of access control hardware
- Running analytics on access patterns or door activity

By processing this information locally, systems respond instantly and continue operating smoothly even if network connectivity drops. This distributed approach also simplifies scaling because each controller becomes an autonomous node capable of managing its environment.

## CHAPTER 3: Redefining Access Control for the Smart Home

**From Integration to Innovation**

Edge-capable controllers don't just replicate server logic at the door. They enable entirely new functionality. For example, developers can build apps that adjust access rules based on occupancy data, trigger energy-saving modes after hours, or alert maintenance teams when a device exhibits abnormal behavior.

This flexibility transforms access control from a static system into an adaptive infrastructure component that can evolve in the smart home, much like industrial IoT has done for manufacturing. Instead of closed systems with proprietary logic that limit innovation, access control is shifting toward open architecture and standards-based platforms. Openness encourages collaboration, faster development, and long-term interoperability across technologies and vendors.

**Secure and Interoperable by Design**

As intelligence moves outward, trust must move with it. Modern controllers incorporate secure boot, encrypted communications, and signed firmware to protect local decision-making. They also encrypt all data at rest, ensuring that credentials, logs, and configuration files remain protected even if the device is physically accessed or removed from the network. Standardized interfaces such as OSDP Secure Channel and TLS

ensure that readers, controllers, and host systems communicate securely while remaining interoperable across vendors.

The emphasis on open architecture and shared APIs allows organizations to integrate edge controllers seamlessly into hybrid or cloud environments. This approach maintains central oversight while empowering distributed intelligence.

**Resilience at Scale**

Because each controller stores policies, credentials, and event data locally, it continues enforcing rules and logging events even during a network outage. When connectivity is restored, the controller automatically synchronizes updates and uploads its event history, preserving audit integrity. This architecture eliminates single points of failure and brings true operational resilience to large or remote sites.

**The Road Ahead**

Edge computing will continue to blur the line between physical access and IT infrastructure. As controllers gain more processing power and functionality through APIs, they will take on tasks such as local risk scoring, behavior analytics, or coordination with enterprise cybersecurity systems.

For integrators and end users, this shift represents more than faster performance. It's an entirely new development model. Instead of closed firmware updates, organizations can

deploy purpose-built apps that evolve with business needs. Access control becomes an extensible platform that's intelligent, secure, and open for innovation at the edge.

As access control becomes part of a unified digital ecosystem, its role within enterprise security expands. Controllers operating at the edge can participate directly in threat detection, data governance, and identity assurance — functions once reserved for centralized IT. This alignment transforms access control from a stand-alone physical safeguard into a critical layer of enterprise defense, one that strengthens resilience across both the physical and digital domains.

[view this article online](#)

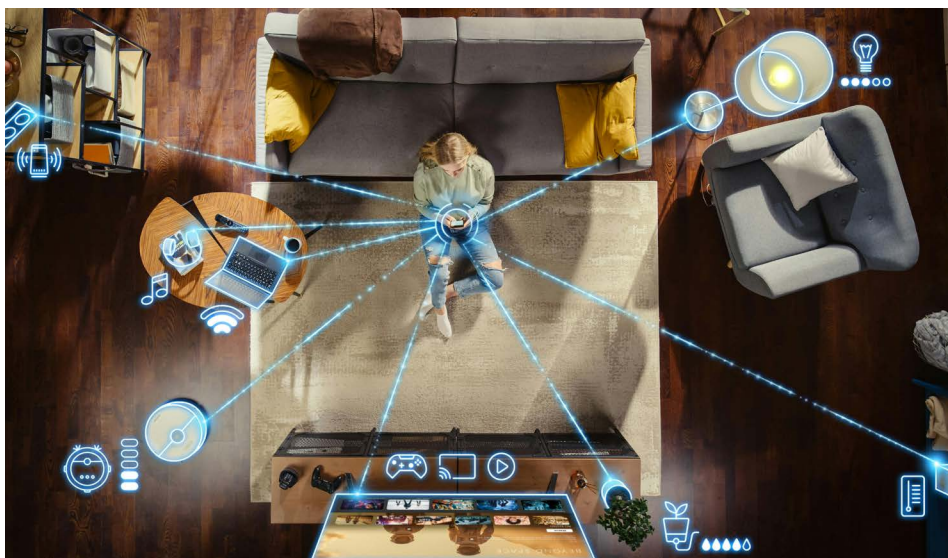
 **BACK TO TABLE OF CONTENTS**

## CHAPTER 4

# 7 IoT Trends Shaping Smart Homes and Buildings in 2026

*The Internet of Things has made our lives more connected and automated than ever before, with accelerated adoption across homes, buildings, and industrial environments.*

CHARLIE ICE, Wireless Connectivity Marketing, NXP Semiconductors



adobestock

Over the past years, the Internet of Things (IoT) has made our lives more connected and automated. Advances in connectivity, edge intelligence, and interoperability have all accelerated adoption across homes, buildings, and industrial environments, while evolving standards are helping to bring greater consistency and security to connected systems.

Looking ahead, the next wave of IoT

innovation will focus less on adding devices and more on making connected environments smarter, more autonomous, and easier to manage. Here are seven key trends expected to shape the IoT landscape in 2026.

## 1. Intelligent Energy Management in Homes and Offices

International regulations and efforts to reduce carbon footprints, along with

increases in energy costs, are driving homes and buildings to be more energy-efficient. This requires intelligent energy orchestration with the electric grid, home energy generators, storage systems, and major appliances all communicating using a common language and working seamlessly to optimize energy consumption.

For example, a tumble dryer may delay its cycle if the solar panels are struggling to generate energy and the grid is under heavy demand. The [Matter smart home protocol](#) is bringing this vision closer to reality by giving energy-management systems a secure, interoperable protocol that allows devices to intelligently and autonomously manage energy usage throughout the home.

While Matter is accelerating interoperability in residential environments, standards such as [KNX IoT](#) are playing a similarly important role in enabling interoperability across commercial building automation ecosystems.

## CHAPTER 4: 7 IoT Trends Shaping Smart Homes and Buildings in 2026

## 2. AI/ML Will Drive Increasingly Intelligent Smart Homes and Buildings

Smart homes and buildings are becoming increasingly efficient, driven by advances in AI and ML. This includes a shift to edge AI, where hardware and software innovations will increase efficiency for devices running AI/ML locally.

With edge AI, the AI model runs directly on a device, such as a camera, sensor, or gateway, instead of sending data to the cloud for processing. This, in turn, results in faster responses, lower bandwidth use, lower power consumption, and improved privacy as data stays local to the device.

The key to edge AI devices is reliable wireless connectivity. Wireless technologies such as Wi-Fi and Thread will enable cloud connectivity and device-to-device communication. Communication protocols such as Matter, KNX IoT, and Dali+ will bring improved compatibility and interoperability, enabling seamless edge AI device communication and integration within smart home and building ecosystems.

## 3. Thread Will Power More Reliable and Smarter Homes

Truly autonomous homes rely on devices such as sensors, buttons, and switches that need to last for years on a single battery. The [Thread networking protocol](#) brings low-power, mesh networking to Matter- and KNX

IoT-enabled devices. Using Thread, a smart sensor can last for years on a single coin-cell battery and have robust connectivity from Thread's self-healing mesh network.

Thread 1.4 delivers several enhancements, including a standardized way to share network credentials with new devices and border routers, allowing them to all join a single Thread network. It also supports extending Thread networks using Wi-Fi and Ethernet, making networks more robust. This flexibility will make Thread even more popular in 2026, allowing devices to benefit from multiple ecosystems and enabling smart homes to be more connected, automated, and energy-efficient.

## 4. Wireless Technologies Will Make Buildings Smarter, Greener, and Safer

Wireless connectivity will continue to bring new levels of intelligence and efficiency in 2026. Wirelessly connected sensors, thermostats, and other IoT devices, combined with edge intelligence, will allow existing buildings to be transformed into smart buildings that can efficiently optimize energy usage. This could include everything from closing window shades when a room is empty to automatically adjusting HVAC usage.

Technologies such as Thread with DALI+ are enabling building systems to work together more seamlessly, providing flexibility and efficien-

cy when it comes to features such as lighting. Building network security will also improve as new systems adopt IP-based networking and standardized protocols such as KNX IoT. These incorporate defined security mechanisms for devices, data, and network communications.

## 5. The Continued Rise of Smarter Buildings and Homes

Occupancy and spatial awareness technologies use location and presence information to enable a system to make intelligent, context-aware decisions that would otherwise be impossible. The ability to determine where a person or object is located within a home or building creates new opportunities for automation and efficiency.

For example, a smart door lock can automatically unlock when it detects the homeowner at the door. In a smart building, a conference room can automatically configure the lighting, HVAC, and IT equipment based on who enters and how many occupants are present.

Ranging and sensing technologies such as ultrawideband (UWB), Wi-Fi sensing, and Bluetooth channel sounding, combined with edge processing, will form the basis for occupancy and spatial awareness solutions. And emerging standards like Aliro, alongside Matter and KNX IoT, will translate these capabilities into interoperable products that can

## CHAPTER 4: 7 IoT Trends Shaping Smart Homes and Buildings in 2026

revolutionize how spaces in homes and buildings are actually used.

## 6. IoT Security Regulations Will Continue to Evolve

Recent years have seen new regulations around the world emerging to protect consumers through improved IoT security. The EU has enacted multiple pieces of legislation, including the [Cyber Resilience Act](#) and [Radio Equipment Directive \(RED\)](#) updates, to address cybersecurity threats. In parallel, the U.S. government has partnered with industry leaders to create the [U.S. Cyber Trust Mark](#), allowing consumers to quickly identify secure IoT products.

IoT devices for smart buildings will need to go beyond cryptography and implement system-level security, securing both the device, communications, and the network they operate on. Standards like Matter, Thread, KNX IoT, and Wi-Fi include multiple security requirements for the network and communications, while silicon security helps implement those requirements and secure the device itself.

As with previous years, the requirements for IoT device security will continue to grow, leading device manufacturers to adopt new standards and technologies.

## 7. More Devices, Less Complexity Through Interoperability

The total number of connected

IoT devices grew 13% year-over-year (YoY) in 2025 to 21.1Bn, according to IoT Analytics' State of Enterprise IoT 2026 report. This translates into smart homes and buildings having hundreds of connected devices, often from different manufacturers. These devices must work together to deliver an autonomous home or building.

Protocols such as Matter and KNX-IoT enable different ecosystems and devices to seamlessly interact. For example, with KNX, you can use any two certified devices from any vendor, and they will simply work together at an application level in a secure way.

As 2026 unfolds, semiconductor providers, such as [NXP](#), and groups like the [Connectivity Standards Alliance](#) and [KNX Association](#) will build upon these trends to bring innovations, security, and use cases to the IoT.

[view this article online](#)

 [BACK TO TABLE OF CONTENTS](#)

## CHAPTER 5

# Building Intelligent and Interoperable Smart Homes with Wi-Fi 7

*Many households now support more than 50 wireless devices, making it challenging to ensure a consistent user experience.*

KEVIN MUKAI, Director Product Marketing, Wireless, and  
CHING-LING HUANG, Principal Engineer Systems Architect, *Infinion Technologies*



dreamstime\_Haiyin\_56604947.jpg

Today's smart homes are more complex than ever before—many households now support more than 50 wireless devices. Thermostats, cameras, door locks, and appliances compete for airtime with smartphones, tablets, and gaming consoles across congested 2.4- and 5-GHz Wi-Fi bands. Overlapping networks from adjacent residences add interference and contention, reducing throughput, destabilizing connections, and increasing battery drain.

Setting up and managing smart-home devices can also be frustrating

for users. The average U.S. household has three users setting up, managing, and controlling their smart-home devices. A smart TV, dishwasher, and door lock may be controlled through separate manufacturer apps, often with different setup and control methods.

At the same time, smart-home devices are evolving beyond simple connectivity as AI transforms user experiences. Devices now incorporate voice, vision, and wireless sensing capabilities, placing new demands on wireless platforms. Cameras run AI-based object recognition, thermo-

stats adapt to occupancy patterns, and door locks authenticate entry using precise wireless ranging.

Beyond higher throughput, these systems require contextual sensing, coordinated power management, and interoperability across wireless protocols.

## Optimized for IoT Devices: Wi-Fi 7 for IoT

Wi-Fi standards have historically evolved to deliver higher peak throughput and greater network capacity. Wi-Fi 7 introduces several high-performance features, including 4096-QAM modulation, 320-MHz channels, and simultaneous multi-link operation across radios. These capabilities primarily target access points (APs) and high-throughput clients such as laptops, gaming consoles, and augmented- or virtual-reality devices.

IoT devices operate under different constraints than high-bandwidth clients. They typically use only a single antenna, must support multi-year battery life, and operate in 20-MHz-wide channels while transmitting and receiving small, intermittent payloads. The wide channel bandwidths of Wi-Fi 7 provide limited benefit for low-data-rate IoT traffic while increasing RF and baseband complexity, cost, and

## CHAPTER 5: Building Intelligent and Interoperable Smart Homes with Wi-Fi 7

power consumption.

To address these requirements, the Wi-Fi Alliance introduced Wi-Fi 7 certification for 20-MHz-only station devices in January 2026. This specification allows IoT devices to maintain narrowband operation while supporting Wi-Fi 7 MAC-layer innovations such as multi-link operation (MLO), multiple resource units (MRUs), and restricted target wake time (R-TWT).

For example, [Infineon's AIROC ACW741x](#), the first Wi-Fi 7 device designed for IoT applications, implements MLO using a multi-link single radio (MLSR) architecture with adaptive band switching. A single RF chain maintains logical associations across the 2.4-, 5-, and 6-GHz bands and transitions efficiently between them. When congestion or interference affects one band, the device automatically switches to a cleaner band.

Compared with fixed-band Wi-Fi 6 designs, this approach improves link reliability by up to 3X without additional hardware or power overhead.

### Low Power for IoT

In the smart home, low-power operation is essential for battery-powered accessories such as cameras and smart door locks. Wi-Fi sleep and standby power are critical for minimizing battery consumption when devices aren't actively transmitting or receiving data from a Wi-Fi access point.

The ACW741x family achieves 70- $\mu$ W Wi-Fi connected standby power at DTIM10, approximately 15X lower than comparable devices. Bluetooth-connected idle power measures 120  $\mu$ W, roughly 8X lower than competing devices, while active Wi-Fi receive power is 59 mW, about 3X lower. A smart door lock using the

ACW741x and four AA batteries, with 10 access events per day, can operate for more than three years, about two years longer than today's competing solutions.

Additional Wi-Fi 7 MAC-layer mechanisms implemented in the ACW741x further improve IoT traffic efficiency. For example, MRU extends orthogonal frequency-division multiple access (OFDMA) by allowing a device to occupy multiple non-contiguous resource units within a single transmission opportunity. For the short, burst-oriented packets typical of IoT traffic, this improves spectrum utilization and reduces latency, particularly when interference affects portions of the channel.

R-TWT, also implemented in the ACW741x, coordinates groups of IoT devices into shared, scheduled wake windows based on traffic characteristics and latency requirements. Instead of independently negotiated wake schedules that increase contention, the access point centrally schedules transmissions. Devices remain in deep sleep longer and wake during protected transmission windows, reducing collisions in dense networks.

### Interoperability: Matter, Thread, and Tri-Radio Smart-Home Platforms

AThread provides low-power wireless transport for many battery-operated Matter devices. Built on IEEE 802.15.4, it forms a self-healing mesh network that connects sensors, switches, and other constrained nodes while maintaining native IP connectivity. Multi-hop mesh routing extends coverage throughout the home without increasing device transmit power.

The Infineon ACW741x integrates

Wi-Fi 7, Bluetooth Low Energy, and IEEE 802.15.4/Thread in a tri-radio SoC with full Matter support. Wi-Fi brings high-throughput connectivity to the home network and cloud services, Thread connects low-power mesh nodes, and Bluetooth supports device onboarding and Wi-Fi provisioning.

Smart home appliances with Thread Border Router functionality connect Thread devices to the Wi-Fi network. Refrigerators, ovens, or washing machines equipped with the ACW741x can route Thread traffic from battery-powered sensors while maintaining Wi-Fi connectivity to cloud services and mobile applications. In this configuration, the appliance becomes part of the home's network infrastructure rather than simply another endpoint.

Tri-band Wi-Fi operation offers additional advantages for kitchen appliances that encounter interference from microwave ovens operating in the 2.4-GHz band. Adaptive band switching allows devices to migrate to 5- or 6-GHz channels when interference occurs, maintaining reliable connectivity. Low standby power during DTIM (delivery traffic indication map) sleep intervals also supports compliance with emerging EU regulations that impose near-zero standby power limits on connected appliances.

### Intelligence: Sensing the Environment Without Dedicated Hardware

Many smart-home devices monitor their physical surroundings and execute control decisions at the edge to reduce latency and enable real-time user experiences. Wi-Fi channel state information (CSI) can detect motion

## CHAPTER 5: Building Intelligent and Interoperable Smart Homes with Wi-Fi 7

in the environment by analyzing how Wi-Fi signals propagate within an environment.

CSI captures variations in signal propagation, making it possible for systems to infer presence, occupancy, and motion without specialized hardware or additional sensors. The ACW741x enables CSI exchange between Wi-Fi devices to support this sensing capability.

Smart thermostats use CSI measurements to detect room occupancy and adjust HVAC operation. They activate when people enter and suspend operation when the space is empty.

Unlike passive infrared sensors, which require line of sight and often fail to detect stationary occupants, CSI sensing operates through walls and, when combined with AI at the edge or in the cloud, can detect subtle motion patterns. The same sensing data can also trigger broader automation sequences, such as activating lights and audio when someone enters a room or alerting users when someone approaches the front door.

While Wi-Fi CSI enables environmental sensing, other smart-home applications require precise device-to-device ranging for proximity-based actions. Bluetooth channel sounding measures the phase and time of flight of Bluetooth signals with centimeter-level accuracy for device authentication and keyless entry.

Channel sounding significantly improves security compared with RSSI-based proximity detection used in legacy smart locks, where signal strength can be manipulated or spoofed. In door-lock applications, it enables keyless entry by activating only when an authenticated device is within a defined range, reducing the

risk of relay attacks. Between access events, Bluetooth LE remains in a low-power idle and advertising state, helping extend battery life.

By integrating Bluetooth channel sounding alongside Wi-Fi CSI, the ACW741x supports both ranging and environmental sensing. Together, these techniques enable local detection of presence, motion, and proximity without dedicated sensing hardware or cloud processing.

### Conclusion

Smart-home systems require wireless platforms that do more than connect devices. They must sense their physical environment, maintain low-power connectivity in congested deployments, and interoperate seamlessly across protocols and vendors.

Devices like the AIROC ACW741x address these requirements. The 20-MHz tri-radio system-on-chip (SoC) integrates Wi-Fi 7 (802.11be), Bluetooth Low Energy with Channel Sounding (Core spec 6.0), and IEEE 802.15.4/Thread with Matter support in a single chip. This architecture ushers in three key capabilities for modern smart-home systems: intelligence, efficiency, and interoperability.

[view this article online](#)

 [BACK TO TABLE OF CONTENTS](#)