



WHITEPAPER

Elevate the Smart Camera Experience with Wi-Fi 6/6E

Learn how to overcome connection and power consumption challenges

Edition: v1.0
Date: 10/2023

www.infineon.com





Consumer Smart Camera Use is on the Rise

According to Strategy Analytics, IP camera shipments are slated to grow from 118 million units in 2023 to 210 million units in 2027, exhibiting a strong CAGR of 15.8%. Security cameras and video doorbells are growing fast because they are convenient, economical, and easy to install by consumers without professional help. Consumers also prefer always-connected cameras, which can be accessed remotely, notify users upon motion detection events, and store video to the cloud, all over a wireless connection.

Like many fast-growing applications, there are challenges with connection bandwidth and power consumption. New features, such as trainable image recognition, advanced object tracking, and simplified automated interaction, require more data to be sent to the cloud with low latency. A robust Wi-Fi connection is needed to meet these demanding performance requirements even in congested network environments such as offices, apartment buildings and remote locations.

So, how is this done? Read this whitepaper to understand these connectivity challenges for new and future smart cameras, and how Infineon's AIROC™ Wi-Fi 6/6E solution's enhanced features help to solve these challenges while providing other valuable benefits.



Figure 1. Modern-day security cameras and video doorbells come with many new features that must be powered by robust Wi-Fi connectivity to carry large amounts of data over already-congested networks.

Current IP Camera Challenges

While security cameras and video doorbells are designed for easy installation, there are pain points in using them. A smart connected camera needs:

- Long-range coverage
- Robust connectivity
- Low power consumption
- Increased security and protection

Wireless Cameras Struggle with Range

Wireless cameras can be prone to Wi-Fi range issues. Limited range can cause choppy video, slow response, and even disconnection from camera cloud services. This challenge can particularly affect outdoor cameras because they are typically placed by the front porch, garage, or back yard. Range issues also occur with indoor cameras and doorbells in large houses where the cameras are too far from the Wi-Fi access point. When wireless signals travel through physical barriers, their strength decreases, making them more susceptible to environmental noise and interference. Signal attenuation occurs through walls, ceilings, trees, large home appliances, metal objects (including doors), furniture, and other objects between the AP and the wireless camera.

Noisy Environments Affect Camera Connections

For smart cameras, low Wi-Fi signal strength caused by noisy environments leads to several negative consequences such as intermittent connections, cameras going offline and becoming unreachable by the cloud service or the consumer's mobile application. Low video/audio quality may be experienced when the Wi-Fi connection is impacted by poor signal quality, long delays, or lagging response. Sometimes, there is no video at all because the camera is offline.

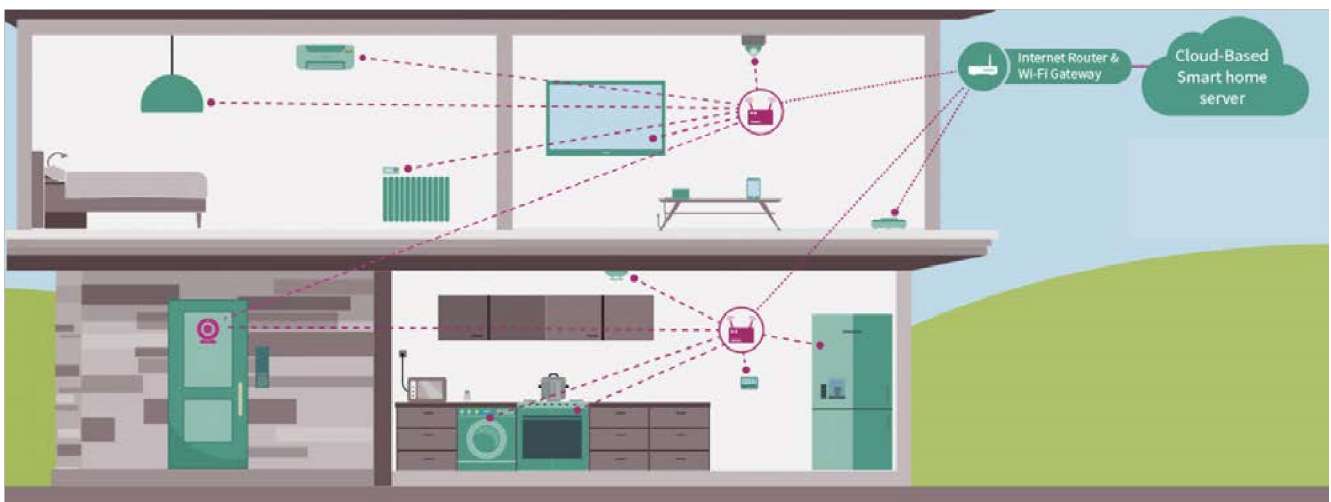


Figure 2 shows many devices may be connected in a home Wi-Fi network. The IP camera must compete with these devices for network bandwidth.

Battery Drainage Still Big Issue

While many smart camera vendors claim their battery-powered smart cameras last one year or more, they may struggle to keep this promise. Battery life may be shortened by unexpected Wi-Fi disconnections, which trigger scans and subsequent reconnections causing excessive current drain.

Cameras also are starting to implement artificial intelligence (AI) with facial recognition and other advanced capabilities. These features lead to increased power consumption for processing of video data inside the device or remotely on the cloud. This situation makes it more important for cameras to conserve power as much as possible in all modes.

Attacks are on the Rise

Attacks against security cameras are a growing concern for consumers and vendors. Many people now are looking for cameras that can protect themselves in addition to monitoring their environments. Unauthorized access to a smart camera could cause violations of privacy and compromise the security of the locations being monitored. Hackers may also try to disable cameras remotely or load malicious software onto these devices by exploiting weaknesses in the vendor’s firmware update mechanism. Smart camera vendors need to think ahead and protect their users’ devices in the field.

In summary, IP camera developers must deal with range, interference issues, power conservation and security threats. So, a state-of-the-art Wi-Fi solution must address these requirements now and in the future.

How the CYW5557x, a Highly Integrated SoC Wi-Fi 6/6E Solution, Helps Smart Cameras

The Wi-Fi 6/6E (802.11ax) specification includes new features that improve performance, latency, and power efficiency. While all of this helps, it’s only part of the solution for smart cameras. Choosing a Wi-Fi 6/6E + Bluetooth® 5.3 combo solution that goes beyond the standard adds advantages that boost performance, enable product differentiation, and speed your time to market. Infineon’s AIROC™ CYW5557x is an example. This highly integrated Wi-Fi 6/6E and Bluetooth® 5.3 SoC family includes special features addressing most critical connectivity issues for future surveillance cameras.

CYW5557x Extends Range and Performance Beyond Wi-Fi 6/6E

The AIROC CYW5557x SoC Wi-Fi 6/6E family not only meets the standard, but it also provides enhanced performance and range. For instance, the CYW5557x offers an innovative range boost feature that delivers double the communication range of Wi-Fi 5 devices and 74% more range than any other standard Wi-Fi 6 device in today’s market.

This solution also supports external power amplifier (ePA) for additional 5-6 dBm output power. A security camera using CYW5557x can reliably connect over Wi-Fi to cloud services--even through physical barriers inside the house or exterior walls when mounted outside. The range boost feature provides smooth and instant video streaming to cloud and to mobile phones.

An example of range extension capabilities with Wi-Fi 6 and AIROC™ CYW5557x family products is shown in Figure 3. Optimized for throughput and range, Infineon Wi-Fi 6 + Range boost results in:

- Over 2X range improvement vs. Wi-Fi 5
- Nearly 74% improvement vs. Wi-Fi 6

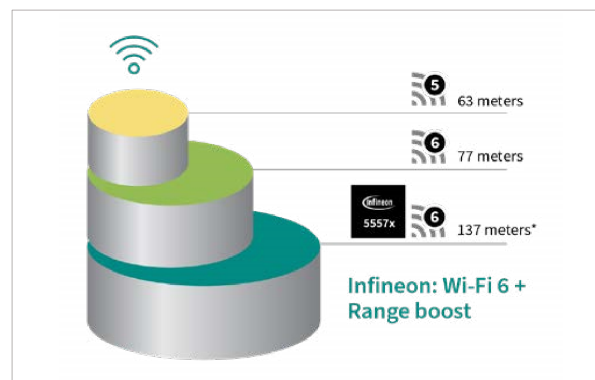


Figure 3. Long range enhancement of Wi-Fi 6 with range boost of AIROC™ CYW5557x family.

*Test case in ideal case space environment without multi-path effect and inference

CYW5557x Alleviates Network Interference for Smart Cameras

The AIROC™ CYW5557x improves network robustness for security cameras. This feature helps smart cameras because Wi-Fi signals can be susceptible to interference, jitter and other environmental effects. Most interference comes from the following categories:

- System noise possibly from HDMI, DDR, or host processor on the same board as the Wi-Fi chip
- Narrowband interference from clocks
- Wideband interference from microwave ovens or mobile phones
- Co-channel and adjacent channel interference from other wireless devices using the same or adjacent (overlapping) channels
- Neighboring Network interference happens when a camera is operating in a network area that overlaps with a neighboring network.

With CYW5557x SoC advanced wireless interference mitigation algorithms, a smart camera’s video quality is enhanced by eliminating system noise and interference from most of the categories.

When a security camera resides in a busy network environment, such as an apartment complex, many overlapping networks may cause delayed data streaming when other devices in the neighboring network are operating in the same channel. With CYW5557x SoC, a smart camera now can ignore signals from a neighboring network, while it continues the wireless data streaming in its own network. It leverages the latest Wi-Fi 6 features and extends the capability to legacy 11n and 11ac modes to enhance network connectivity.

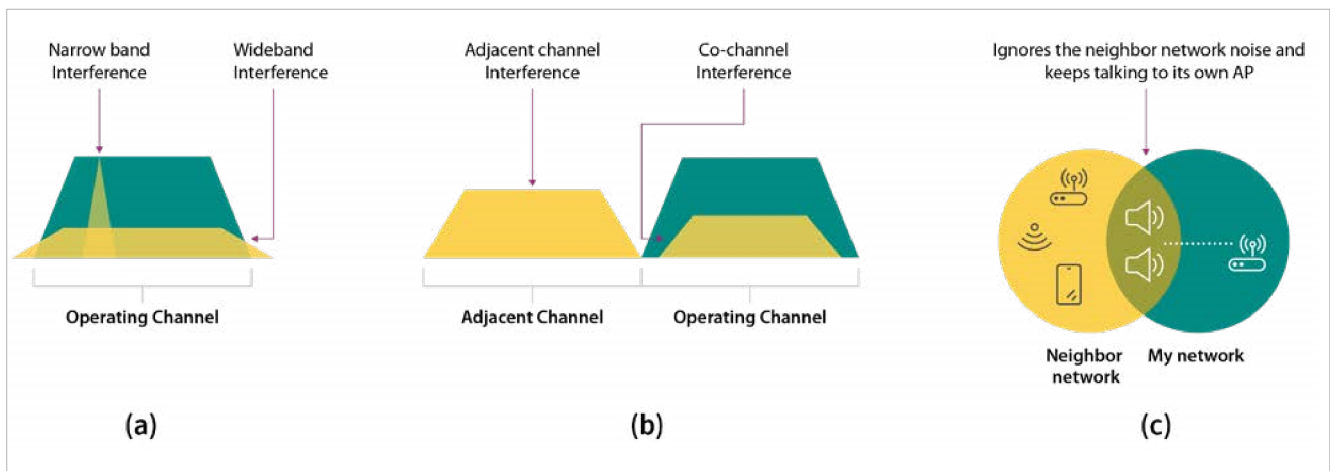


Figure 4. AIROC™ CYW5557x enhancements for network robustness and improved connectivity.

Saving Battery Life for Security Cameras

When it comes to battery life, Infineon goes beyond simply designing standard power saving features complying with Wi-Fi standards. CYW5557x comes with several new features that save chip-level and system-level power consumption. In battery-powered wireless cameras and doorbells, conserving battery life is critical. These devices remain in standby mode most of the time, waking up only when motion is detected or when a request is received via the cloud.

Camera power can be optimized for all stages of operation, from initialization to processing images, streaming video to the cloud, and sleep mode. Security cameras built with CYW5557x can save power by 30% during camera initialization via optimized radio calibration, and by 20% in active receive mode. The Wi-Fi radio also can filter out non-relevant traffic and optimize bandwidth on the fly to save power. With the implementation of more granular Target Wake Time features, cameras can remain in sleep mode longer than legacy Wi-Fi 4/5 devices, waking only at pre-determined times to receive targeted traffic.

Integrating AI for facial and object recognition capabilities increases system-level power consumption. To balance this increased current requirement, CYW5557x provides network offload features to manage the network connection autonomously, allowing the main host MPU to stay in sleep mode and save the overall system power consumption.

CYW5557x Improves Smart Camera Security

As discussed earlier, security is a growing concern for security camera owners. If not properly protected, security cameras are susceptible to man-in-the-middle attacks over the air, injection of unauthorized firmware into the system, or physical access to the Wi-Fi or Bluetooth® sub-system via debug interface. With the new Wi-Fi 6/6E architecture in the CYW5557x SoC, multi-layer security can now be implemented and enhanced.

If the Wi-Fi signal is intercepted over the air, encryption prevents a would-be attacker from decoding the video stream or other important data. Only a peer device with the right security key can decrypt the message.

With frequent discovery of security vulnerabilities, cameras often require field updates of patch software via Wi-Fi to keep security up to date. CYW5557x only allows firmware authenticated by a digital signature to be installed in the system, while also prohibiting “rollback” of previous firmware versions which may restore known vulnerabilities.

CYW5557x also disables the debug interface into the Wi-Fi chip, protecting firmware and data from attackers utilizing this interface. In addition, the CYW5557x’s Wi-Fi and Bluetooth® subsystems are isolated and individually protected.

Multi-layer Security Protections

The CYW5557 SoC’s secured boot, firmware authentication & encryption, and lifecycle management features enable a higher level of security for IoT applications. As shown in Figure 5, the CYW5557x family’s advanced multi-layer security features include:

- Crypto key establishment & management
- Multiple redundant levels of defense
- Crypto offloads
- Secured boot
- Firmware authentication
- Firmware encryption
- Anti-rollback prevention
- Lifecycle management

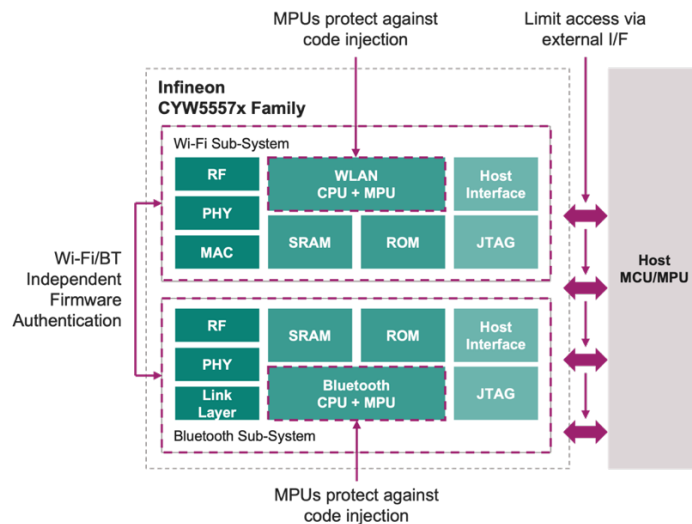


Figure 5. The AIROC™ CYW5557x family has advanced multi-layer security.

For any camera to be appropriately secure, it must be able to cope with different states that occur during its life cycle. The CYW5557x's lifecycle management enables four states of protection during process at chip manufacturer and camera OEMs for consumers and in the product return process, as shown in Figure 6.

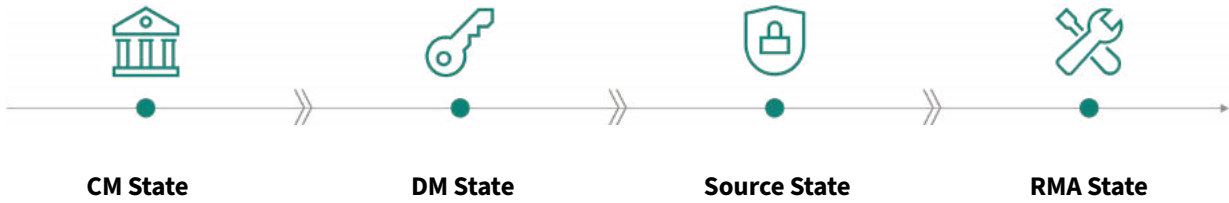


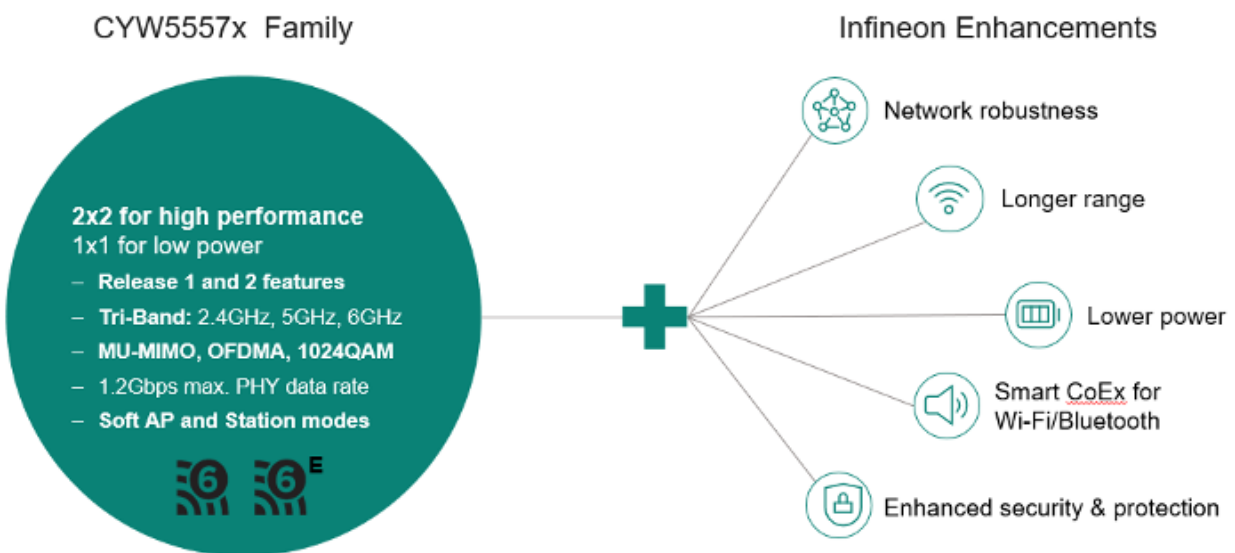
Figure 6. Multi-Layer Security from different states in Lifecycle Management.

The CM State is only available with Infineon internal development and provides a full debug JTAG. At Infineon customers, firmware and patches are authenticated/encrypted in the DM State, and most configurations and debug interfaces are disabled. For final products at end customers, Infineon provides a tool to transition to the Secured State, where all debug and programming interfaces are disabled to prevent attacks against the proprietary chip. In the event of a failure, the RMA State is implemented for units returned to Infineon for failure analysis where the debug and programming interfaces are available only after authentication by authorized Infineon quality personnel.

Conclusion

CYW5557x solutions based on the Wi-Fi 6/6E standards are game changers for smart camera consumers and manufacturers alike. Consumers enjoy an elevated smart camera experience which enables their products to do more. Manufacturers take advantage of improved security, bandwidth and power efficiency to extend smart camera capabilities without sacrificing battery life or being hampered by network interference or limited range.

The AIROC™ CYW5557x takes Wi-Fi 6/6E one step further by exceeding the standards, enabling developers to differentiate their products and deliver secured, innovative solutions to the market faster and with high quality.



References

- [1] Smart Home Camera and Doorbell Markets - Value Creation not Just Feature Updates
<https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/complimentary/report-detail/smart-home-camera-doorbell-value-creation-feature-updates>
- [2] IoT Product Manager's Guide to Wi-Fi 6/6E:
https://www.infineon.com/dgdl/Infineon-WiFi6-6E_Whitepaper-Whitepaper-v01_00-EN.pdf?fileId=8ac78c8c7cdc391c017cf08af0043c47&da=t
- [3] IEEE 802.11ax-2021
<https://standards.ieee.org/ieee/802.11ax/7180/>



www.infineon.com

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

© 2023 Infineon Technologies AG All
rights reserved.

Public

Date: 10/2023

Please note!

This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.