HOW TO SOLVE THE 6 TOP SECURITY CHALLENGES OF EMBEDDED IOT DESIGN

Ensuring security for embedded IoT designs can be challenging and time-consuming even for veteran developers. Explore these six common security challenges and discover how Renesas offers a number of approaches to help embedded developers ensure the security of their designs. Developers can choose from a fully integrated, platform-based approach to security that benefits from the latest advances in both hardware and software and delivers in-depth, comprehensive defenses with multiple layers of protection. Developers can also choose the flexibility of keeping (or creating) their own development platform and leveraging the vast, established Arm Cortex-M core ecosystem while still taking advantage of proven Renesas MCUs, peripherals, and functionalities.

COMMON SECURITY CHALLENGES FOR IOT

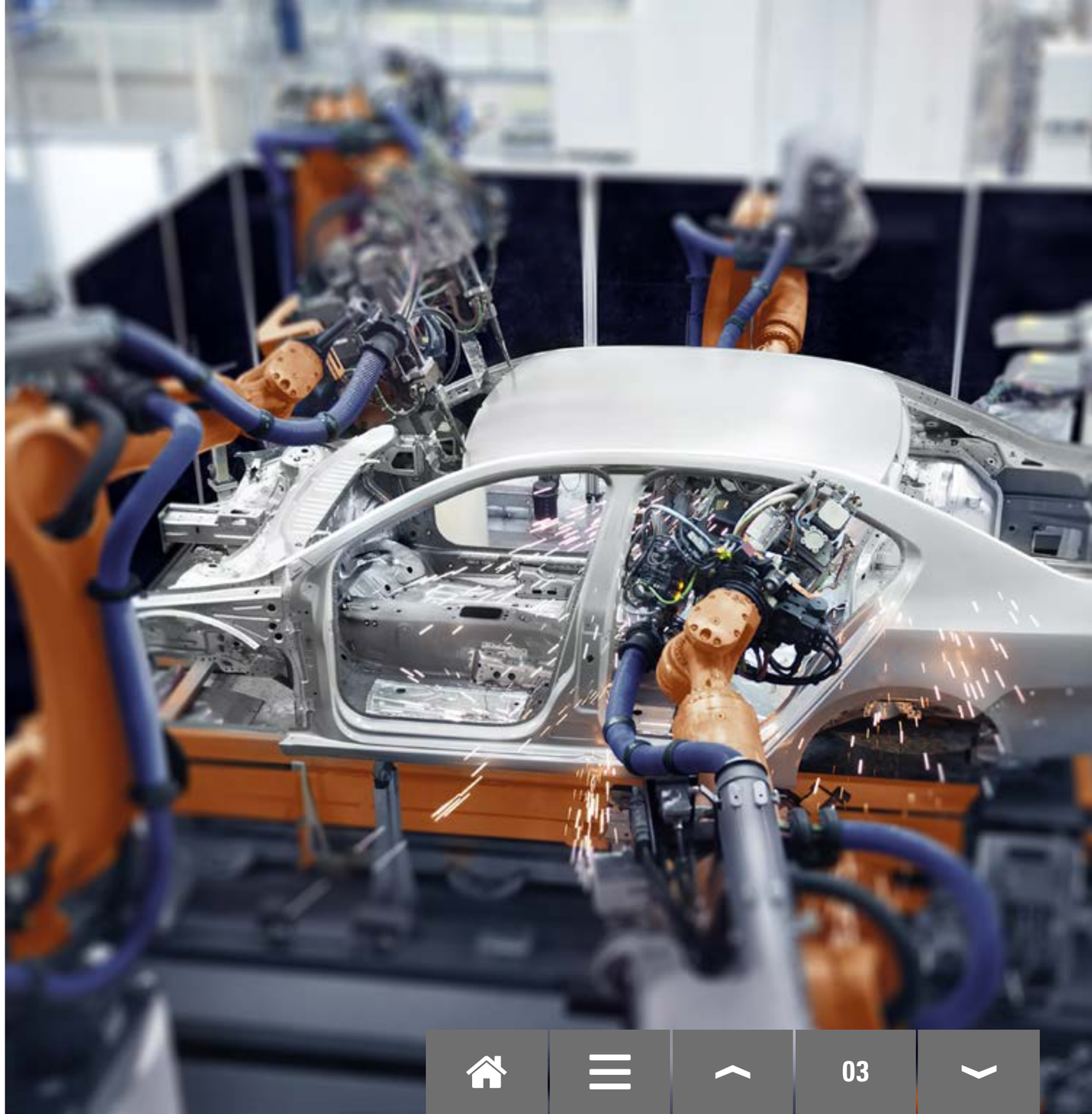
An estimated 31 billion IoT (Internet of Things) devices will be deployed by 2020, many with limited security controls that leave them ripe for hacking. Why are so many embedded systems designed with vulnerabilities? In large part, it's because developers face multiple challenges and complexities when securing embedded applications and devices. They must keep up with threat landscapes that morph daily and also meet always evolving security standards. Simultaneously, complex applications may require meeting multiple standards, which can inhibit device compatibility and flexibility. In many development scenarios, higher-level security features may also come with higher costs and higher power consumption, which can adversely impact the marketability of the end device.

> An estimated **31 billion IoT devices** will be deployed by 2020, many with limited security controls that leave them ripe for hacking.

In this eBook, we identify six of the most common security challenges that embedded developers face and provide insights and answers to help streamline the security design workflow to accelerate delivery of secure devices, services and systems to the market.

Here are the six security challenges for the embedded developer that we explore in this eBook:

1. How do I secure my device?
2. How do I secure my product so they are not replaced by unauthorized copies?
3. How can I manage security with less complexity?
4. How do I secure my device against multiple security threats?
5. I'm not a security expert, but I need a secure product. What do I need to know?
6. How can I get more standardization and support for security from vendors and put my own resources on the parts of the design that differentiate?



CHALLENGE 1: HOW DO I SECURE MY DEVICE?

A few years back, application developers didn't need to worry about securing their products because devices and applications were not connected like they are now.

Today, even the most basic items—from light bulbs to baby monitors and prescription drug containers—are connected through the IoT to the internet or the cloud. Too often, security is overlooked or only addressed when it is too late.

Securing IoT applications from cyber threats to protect data and functionality is a critical concern for developers and must be built into devices from the start. A security strategy that offers multiple layers of defense by taking advantage of the latest security advances in both hardware and software is necessary for implementing in-depth, comprehensive protections.

For the hardware side, effective security needs to include:

- **Secure key management,** to ensure that keys are not accessible in an unencrypted state. The device should be able to securely generate and store keys, including private keys, to enable truly secure device-unique identity and provisioning.
- **Hardware-accelerated encryption, hashing, and true random number generation,** which accelerates cryptographic operations on the device. This hardware support saves both time and power.
- **Secure memory access** to protect specific regions of RAM and Flash memory from unauthorized access. Separate memory domains isolate sensitive code and data from non-secure code and data, while write-once protected memory safeguards code and data from change or reprogramming.
- **Protected debugging and programming access,** which reduces the risk of hackers using debugger and programming interfaces as attack vectors.

The software side should include:

- **Driver level APIs** to provide an easy interface to hardware security features.
- **Cryptographic libraries** with a collection of APIs that provide a wide range of security features including macro-level security functions, root-of-trust, and the ability to recognize trusted sources and code.

- **Support for common communication protocols and transports,** such as Hypertext Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS), and other cloud-specific protocols.
- **Compatible and integrated stacks, libraries, HAL drivers, and potentially a real time operating system (RTOS),** forming a solid software platform upon which to build your application.

Renesas has been a leader in embedded security for decades and is well positioned to address the heightened need for security in today's connected products. Renesas offers multiple approaches to embedded security, providing a multi-tiered development infrastructure that provides in depth security protection for a wide variety of embedded products.

For instance, the Renesas Synergy™ Platform is a comprehensive, qualified development platform that includes production-grade software in the form of the Synergy Software Package (SSP), and a scalable family of pin-compatible MCUs, pre-integrated and pre-tested to provide security at multiple levels. The Synergy platform ensures that IoT applications are built on a secure, robust technology foundation.

In addition, the new Renesas RA Family of MCUs delivers an option with more platform flexibility, combining Arm Cortex-M cores and best-in-class embedded system peripheral IP from Renesas. The RA's Flexible Software Package (FSP) provides optimized HAL drivers as well as a baseline software platform built on FreeRTOS and associated middleware. Designed for flexibility, developers can easily incorporate their middleware and libraries of choice.

The Synergy platform and RA MCUs both contain an integrated crypto subsystem called the Secure Crypto Engine (SCE). The SCE provides hardware acceleration for the most prevalently used cryptographic algorithms (RSA/ECC/DSA/AES/SHA), as well as key generation and a True Random Number Generator (TRNG). Key binding can be performed by MCU-unique key wrapping, which encrypts keys specifically for each MCU, so keys are accessible only within the SCE module on the individual MCU that performed the wrapping. The SCE contains its own, dedicated RAM, ensuring that plaintext keys need never be exposed on a CPU-accessible bus. An access protection circuit will lock the SCE if the strict access control protocol is violated. The MCUs also incorporate a Secure Memory Protection Unit (SMPU) and Flash Access Window (FAW), which can be used for storing secure immutable boot code, certificates, and keys along with any other sensitive data. When used in conjunction with the MCU-unique key wrapping capability, the SCE can provide secure storage even in non-secure memory.

Developers also need to ensure that their development platform makes it safe and easy to connect to the cloud. As IoT applications grow more complex and safety-critical, they require ever-more data processing power. Secure connections to the cloud become essential as these systems increasingly depend on cloud computing to deliver hyper-scale compute and storage infrastructures for IoT data. The SSP delivers support for cloud connectivity with built-in MQTT and TLS modules, and the Synergy cloud connectivity applications provide secure, built-in connectivity to leading cloud environments, including Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. The RA FSP provides similar functionality, leveraging Arm ecosystem software.

CHALLENGE 2:
HOW DO I SECURE MY PRODUCTS SO THEY ARE NOT REPLACED BY UNAUTHORIZED COPIES?

Don’t want your products replaced by imitations? Then make sure your competitors can’t easily clone your device. To do this, you need to ensure that the products you sell contain proprietary features that only your organization can provide.

Global supply chains now require increased diligence and enhanced security to ensure product integrity and authenticity are maintained during manufacturing and production.

One way to do this is through secure manufacturing, which mitigates risk to intellectual property and maintains the integrity of production processes. In Renesas MCUs, a flexible boot manager provides a secure firmware flash programming solution that enables developers to dependably and securely program authorized firmware into approved-flash memory devices in remote manufacturing facilities. This protects the firmware from being pirated, modified, or installed on cloned hardware.

> Don’t want your products replaced by imitations? Then make sure your competitors can’t easily clone your device.

The boot manager also delivers a strong root-of-trust that provides unique identities, hardware protected keys, secure boot loader, secure flash update module, and cryptographic APIs to interface with the MCU hardware. Through a secure connection, the root-of-trust is pre-loaded into a high-volume programmer system designed for manufacturing and provisioning of processing units. The provisioned chip stores the data securely, and maintains tight control on how it is used.

Once products are in the field, the secure boot manager can securely update authorized firmware to the MCUs’ flash memory, with the on-chip root-of-trust validating and decrypting the firmware before flash programming – all securely provisioned via secure cloud infrastructure made more reliable and trustworthy with Renesas cloud connectivity solutions.

Or, if you prefer, select Renesas partners can assist with secure provisioning and programming of solutions and services, and are committed to providing manufacturing security at a reasonable cost.

CHALLENGE 3:
HOW CAN I MANAGE SECURITY WITH LESS COMPLEXITY?

Designing in-depth, layered security for embedded designs can be challenging and time-consuming, and one way to reduce the learning curve is to ensure that the latest security advances and protocols are already built in to multiple layers of the hardware and software.

With the Synergy platform, developers don't have to learn all new and relevant protocols and other security safeguards to produce a secure application. The Synergy Software Package simplifies complex functions encountered while developing secure connected embedded systems. The software secures areas of memory where developers can create and store portions of code that are Flash and SRAM read- and write-protected. Doing so allows developers to create customizable areas of memory that can be used to store temporal keys, private keys, and other sensitive data.

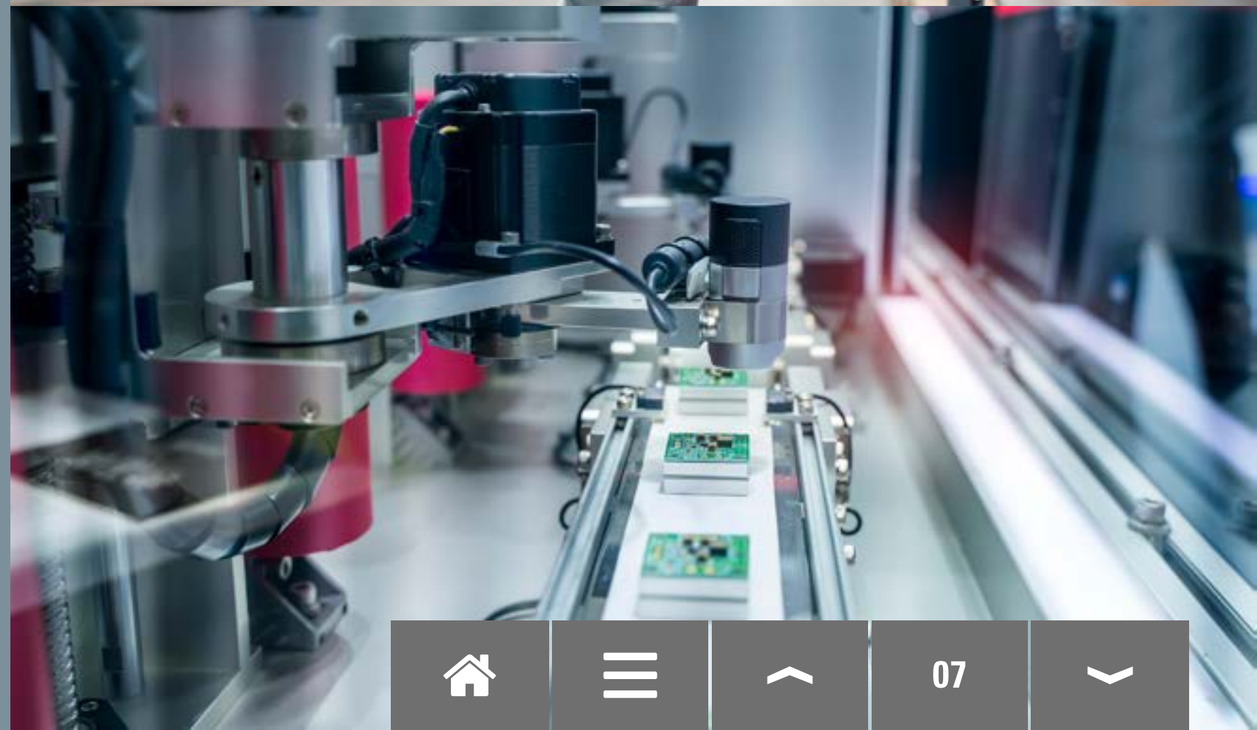
Both the Synergy platform and the RA FSP support both public key infrastructure (PKI), a cryptology methodology that offers authentication via digital certificates, and pre-shared key (PSK), an encryption model in which authentication is authorized when both peers in a digital connection specify the same key. PSK offers a simpler form of encryption and may provide appropriate levels of protection for situations such as access control for small numbers of users. Though more complex to initiate and manage, PKI is a form of asymmetric cryptography that can authenticate users, produce and distribute certificates, and maintain, manage and revoke certificates.

PKI, with public and private keys, is usually considered a more secure encryption model and is commonly used for authentication in large encryption systems.

> To manage security with less complexity, ensure that the latest security advances and protocols are already built in to multiple layers of the hardware and software.

The Synergy platform offers optimized commercial-grade software with standard APIs that simplify how interfaces are made with hardware security and encryption features. Application frameworks help streamline otherwise tricky wireless driver integration with a uniform interface between the application code and lower level drivers. This level of abstraction decreases complexity and makes it easier to integrate networking stacks, or to switch out or drop in drivers as needed.

The new Renesas RA Family of MCUs provides the flexibility to reuse and expand upon any existing infrastructure a customer might have, and enhance it efficiently, precisely as required for each application. Customers can build their own platform with scale to support various ranges of products while taking advantage of advanced security features in the SCE. RA developers can also easily incorporate Arm ecosystem software and solutions, leveraging the wealth of knowledge and experience of Arm developers world-wide.



CHALLENGE 4:
HOW DO I SECURE MY DEVICE AGAINST MULTIPLE SECURITY THREATS?

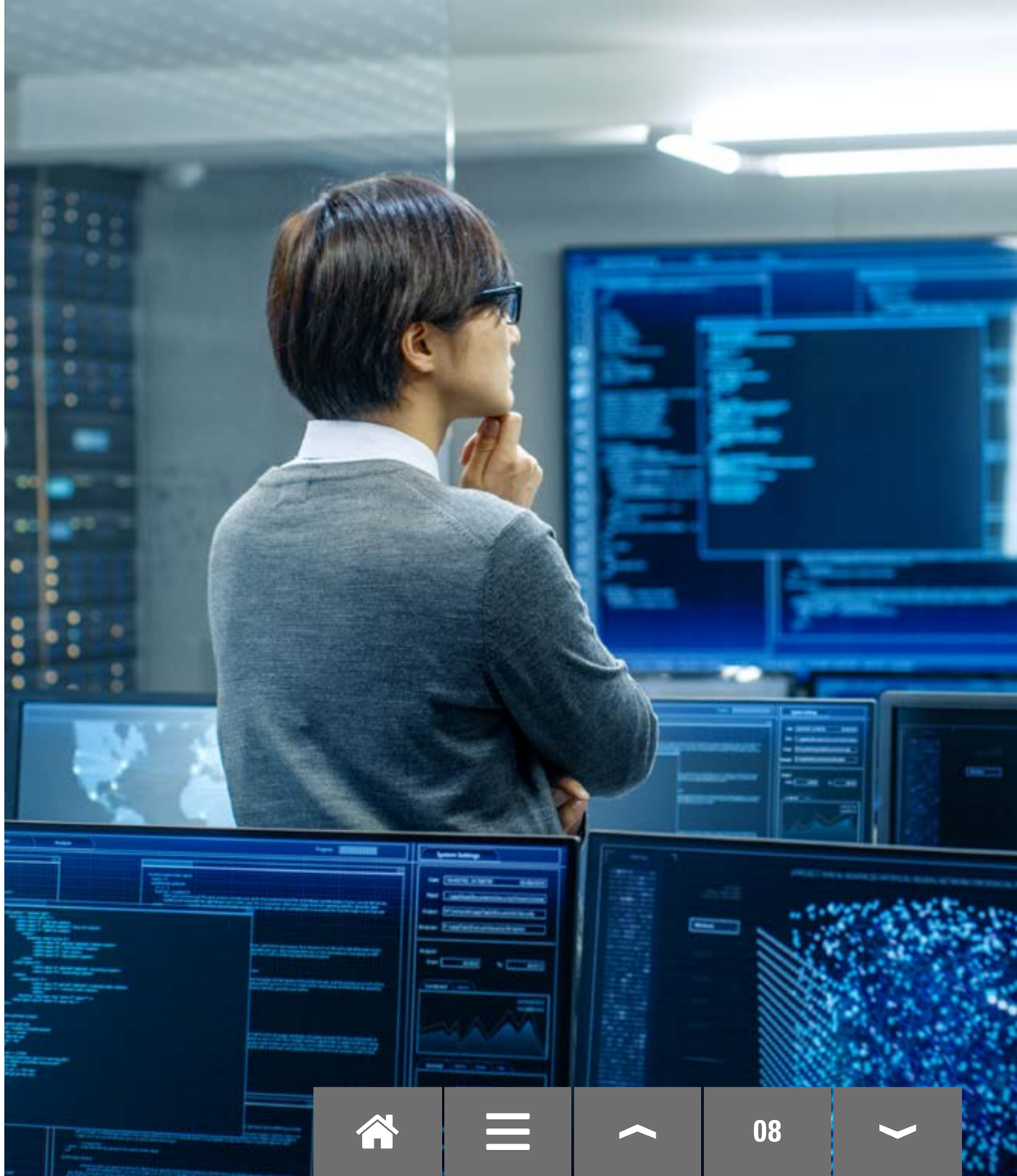
Today's cyberthreat landscape is filled with multiple bad actors and risks. Exploits and attack vectors await the unprepared and unprotected. To safeguard a device against multiple security threats requires securing the device's identity through hardware-based key generation. This identity can be securely stored in internal flash, leveraged to create trust, and provide privacy when added to designs and configured for target applications.

Establishing a strong device identity allows every IoT device to be singularly identified and authenticated as unique. This enables devices to be individually secured and to engage in encrypted communication with other secured devices and services. Both Synergy and RA MCUs provide strong device identity safeguards against multiple security threats through layered IoT security protections by providing the following features:

- **Trust.**
  Once connected to a network, the device must authenticate to create trust between other devices, services and users so that it can securely exchange encrypted data and information. Trust starts with properly authenticating the device to ensure it is a legitimate device and not a counterfeit.
- **Privacy.**
  The data and information captured and shared within IoT networks often include data that is sensitive, personal or financial, which must be kept private and secure to meet regulatory compliance. Secured device identity provides the keystone to ensure confidentiality when IoT devices and systems connect to share data.
- **Integrity.**
  Ensuring that data shared within networks has not been altered is a key element of layered security. Data integrity is an often-overlooked requirement, but connected devices and systems rely on the authenticity (trust), confidentiality (privacy) and integrity of the information being transmitted.

Digital data security is also a top priority for safeguarding against multiple security threats. Data at rest refers to data not actively in motion between devices or networks, usually parked in SRAM or non-volatile storage. To secure data at rest, both Synergy and RA MCUs offer data access controls, including read, write, read-write and write-once protections. Controlling access to stored data reduces the attack surface and increases system security.

In addition, Synergy and RA MCUs deployed in the field can be updated remotely to provide protection against the latest cyber threats.



CHALLENGE 5:
I'M NOT A SECURITY EXPERT, BUT I NEED A SECURE DEVICE. WHAT DO I NEED TO KNOW?

To deliver comprehensive, in-depth security protection for products based on embedded devices requires multiple protocols and safeguards that work together to provide security at many levels.

> Ensuring security for embedded IoT designs can be challenging and time-consuming. The Renesas network of trained and certified design service partners are available to support every stage in your design cycle.

The Renesas Synergy Platform offers developers a head start by delivering a complete development environment that provides a unique, built-in set of hardware and software security capabilities. These build on a shared root-of-trust that meets the requirements of securing embedded devices and IoT networks. The platform also extends the ability to ensure secure, scalable manufacturing and protection of intellectual property.

Developers can also take advantage of Renesas' online library of application projects for step-by-step instructions and guidance on building end-to-end security solutions.

Developers basing their designs on the new RA MCUs can take advantage of Renesas' expertise in security IP and other embedded peripherals while also benefiting from Arm's broad ecosystem to drive innovation, support, and choice.

In addition, basing your designs on the Renesas MCUs gives you the support of the large, robust Renesas community and ecosystem of alliance partners. The Renesas network of trained and certified design service partners are available to support every stage in your design cycle, working with you to achieve your design and business goals. Leveraging Renesas' partners can help speed development and extend deep expertise into your security solution development.

CHALLENGE 6: HOW CAN I GET MORE STANDARDIZATION AND SUPPORT FOR SECURITY FROM VENDORS AND PUT MY OWN RESOURCES ON THE PARTS OF THE DESIGN THAT DIFFERENTIATE?

Before you begin development, make sure to select an MCU solution that either provides a highly integrated platform, or that offers a flexible ecosystem of partners, resources and other building blocks to support secure design development.

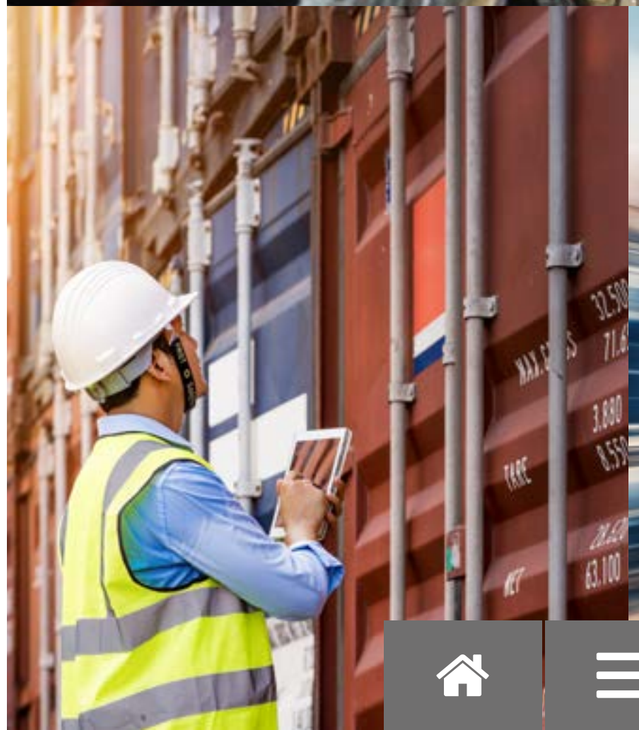
Platform-based approaches provide functionalities that work together to deliver security at multiple levels. This is important because malicious agents can take advantage of vulnerabilities in embedded designs when variations in design and security protocols create weak points that hackers can infiltrate. This is particularly a risk when MCU hardware, software, communication stacks and drivers have not been standardized into a fully integrated framework.

A comprehensive, fully integrated development platform with in-depth security protections makes securing your design as simple and painless as possible. Pick a framework that is pre-integrated with key software, functionalities, stacks and drivers already incorporated into the platform. This frees developers from dealing with lower-level integrations, allowing them to focus on designing the features and capabilities that will make your product stand out.

The Renesas Synergy Platform is a comprehensive, qualified development platform that includes production-grade software, a scalable family of pin-compatible MCUs, application frameworks, functional libraries, HAL drivers, and advanced software tools and kits. It ensures that applications are built on a secure, robust technology foundation. This allows designers to focus their time and skills on higher-level challenges and innovation that address fast-moving IoT market opportunities and consumer demands.

The Renesas RA Family of MCUs combines best-in-class security IP and peripherals from Renesas with Arm Cortex-M cores to provide a highly optimized feature set for holistic security protections. In addition, Arm's active ecosystem of partners and other resources provide the flexibility and expertise to deliver innovative designs with the multiple layers of defense that the market now requires.

Developers can also count on the expertise of Renesas' partners, who are available to step in and help with development of specific security features or functionalities. They can also support your existing team or add valuable skills and experience to your development processes. The option of outsourcing development of specific security features or functionalities to trusted experts can save time and strengthen your final product.



CONCLUSION

Renesas helps embedded developers meet the challenges of securing designs by offering numerous ways to take advantage of the latest breakthroughs in hardware and software security to deliver in-depth, comprehensive protections with layered security. Renesas MCUs build on a shared root-of-trust to secure IoT devices, services and networks at a deep level, extended to ensure secure and scalable manufacturing and protection of intellectual property across the product lifecycle.

CONTACT US

Web: renesas.com/support/contact