Security portfolio gives protection from industrial and IoT threats

By Stefan Ingenhaag, Renesas Electronics Europe

The industrial and IoT markets present security considerations unlike anything embedded developers have ever faced. By offering a comprehensive and robust set of security features in both hardware and software, Renesas Synergy Platform delivers a sure path to long-term product integrity.

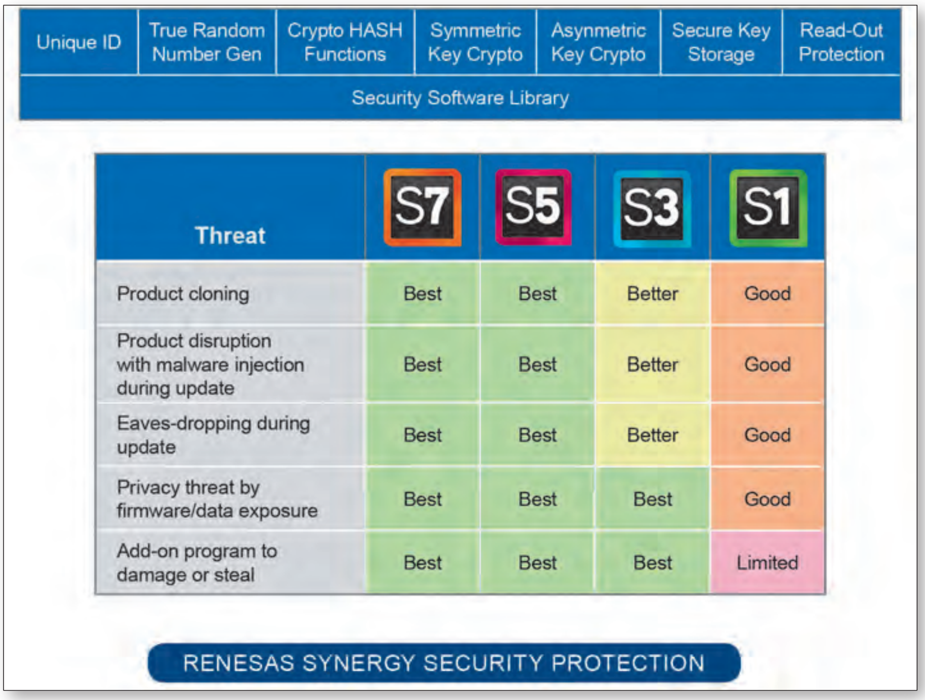
■ With an estimated 14 billion devices connected to the Internet today and that number expected to jump to 50 billion by 2020, the Internet of Things (IoT) offers a tremendous market opportunity. But it also presents a major security risk. Why? First and foremost, the vast majority of all connected devices in use today feature inadequate security. A recent report from the Open Web Security Application Project (OWSAP) gives some insight into the scope of the problem. According to the report: 60% of devices with user interfaces are vulnerable to issues such as weak credentials, 70% of devices use unencrypted network services, 70% of devices, along with cloud and mobile applications, enable an attacker to identify valid user accounts through account enumeration, and 80% of all devices, along with cloud and mobile applications, fail to enforce a policy requiring passwords of sufficient length and complexity.

As more devices and systems connect to the network, the potential risk and implications of a security breach continue to climb. A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack on an industrial plant could result in a system overload, leading to unavailability of important services and notifications at a critical time, for instance an industrial cooling system that provides critical temperature notifications could be severely compromised if the notifications to system operator or commands from the operator are blocked due to DoS/DDoS attack(s) on the connected temperature monitoring and control system. Similarly a DoS/DDoS attack can interfere with road traffic control systems resulting in massive gridlock in the area it serves. From a national security perspective the implications are even more frightening. The National Security Administration (NSA) admitted in 2014 that the US is in a de-facto state of cyber warfare and that hackers had already infiltrated systems in reconnaissance missions. And senior military officers reported that a number of countries now have the capability to shut down the US power and financial services industries.

From an individual user standpoint, consumers are becoming more vulnerable as they increasingly rely on connected devices. The use of connected healthcare devices such as baby monitors, glucose readers and pacemakers leaves the health and well-being of consumers exposed to malicious add-ons that could render those devices useless or worse administer incorrect does of medication. As consumers increase the intelligence and interconnectivity of their homes, the risk of hackers stealing personal data increases exponentially. To get a sense of the scope of the problem, Renesas recently asked its customers what they see as the most dangerous threats in the IoT marketplace. They identified the following six types of threats. 1) An untrusted contract manufacturer cloning software or firmware or the security configuration of an MCU or product. 2) Hackers disrupting a product by replacing a genuine firmware during the installation phase with malware. 3) A hacker mounting an eavesdropping attack during firmware installation especially if security parameters are exchanged in the clear. 4) Privacy threats when system firmware is not physically protected and an attacker can then extract security parameters. 5) Attackers using an add-on program to damage or steal information. 6) Hackers taking advantage of a simple software update session to replace firmware with malware.

For the designers of Renesas Synergy Platform, one thing was immediately clear. To ensure devices built around this platform were truly safe and secure, they had to address all these threats. They realized this meant they had to build into the platform security features that would provide protection at each stage of the product lifecycle.

To address potential threats in virtually any application, Renesas engineers developed an integrated hardware/software platform that offers an unprecedented line-up of security


Unique ID
True Random Number Gen
Crypto HASH Functions
Symmetric Key Crypto
Asymmetric Key Crypto
Secure Key Storage
Read-Out Protection
Security Software Library
RENESAS SYNERGY SECURITY PROTECTION

Threat	S7	S5	S3	S1
Product cloning	Best	Best	Better	Good
Product disruption with malware injection during update	Best	Best	Better	Good
Eaves-dropping during update	Best	Best	Better	Good
Privacy threat by firmware/data exposure	Best	Best	Best	Good
Add-on program to damage or steal	Best	Best	Best	Limited

Figure 1. Renesas Synergy Platform offers a broad range of security features.

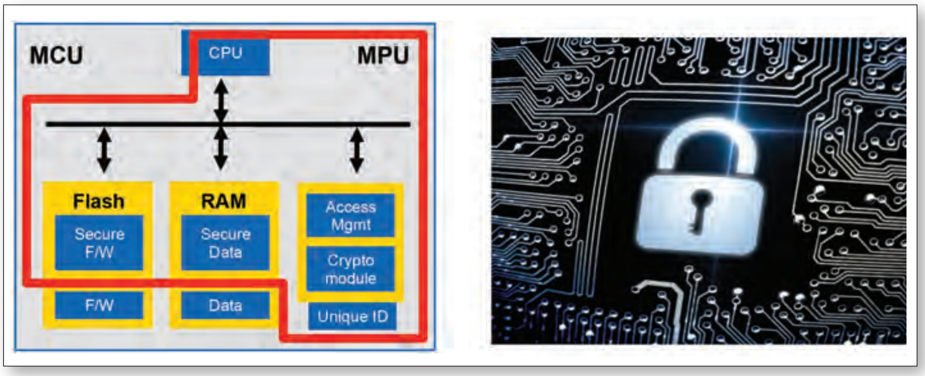


Figure 2. New features like key injection service and certifiable root of trust offer a solid defense against product cloning.

capabilities. Many of these new functions are implemented in hardware where they are less susceptible to attack. As an example, when each MCU in the Renesas Synergy family is manufactured, it is assigned a unique 128-bit ID which can be used to generate keys to protect applications and assist provisioning. Providing a significant improvement over pseudo-random generators, the Synergy random number generator meets the latest NIST SP 800-90 specifications and is tightly integrated into the cryptographic accelerators and key generator of the MCUs.

All MCUs in the Synergy product family, including the S1, S3, S5 and S7 Series controllers, feature accelerators for symmetric cryptography, HASH, a true random number generator and the ability to limit JTAG access. At the higher performance end of the product line, the S7 and S5 Series add accelerators for asymmetric cryptography, asymmetric key generation and key secure storage. To ensure that certain areas of memory can be accessed only by those with the right privileges, Secure Memory Protection Units (MPUs) in the MCUs are used. The platform plays a key role in ensuring the integrity and availability of systems. As an example, the separation of stakeholders is crucial to the integrity of many connected systems. By separating session keys and user data from equipment data and allowing the system to create a separate sandbox for configuration data, the Secure MPU, available on the Synergy MCUs, allows users to operate multiple stakeholders at the same time.

The risk of IP theft begins in the manufacturing phase as soon as the MCU leaves the hands of the design team. Say your design team is building a glucose reader. A less-than-honest contract manufacturer can reverse engineer a copyrighted algorithm to create counterfeit glucose reader MCUs to sell to competitors. Product cloning like this threatens to undermine sales revenue. It can also damage the original manufacturer reputation when lower quality devices hit the market and create support issues for partners who unknowingly purchased cloned parts. To protect against this threat, Synergy Platform developers integrated two innovative features into each MCU to help authenticate each device and minimize the threat of cloning. In the earliest stages of the manufacturing process, developers using the Synergy MCUs have the option of choosing Renesas or a third party key injection service. Key injection essentially assigns a unique identifier or birth certificate to each MCU. Early key injection allows code to be locked to a device. From that point forward a checksum of the code must achieve a known value to be accepted.

The earlier in the manufacturing process this unique identifier is assigned, the more difficult it is for anyone to steal the MCU identity. Today the Synergy S7 Series is one of a select few controllers offering key storage and generation on the MCU. The second feature Renesas is offering on the Synergy Platform to address product cloning is a certifiable root of trust. The root of trust serves as the basic foundation for security upon which other security components are built. It includes the key components in an embedded system that the operating system must trust and which must operate immediately out of reset including secure firmware, data, access management, the cryptography module, and the unique ID of the device.

The root of trust serves three key functions. First, it must measure and verify the software boot chain. This requires that it exist separately and underneath any system boot chain. Second, the root of trust must protect the cryptographic keys. This means that the root keys must be provisioned early and securely. The Synergy Platform early key injection, secure storage and limited JTAG access capabilities ensure it meets these requirements. Third, the root of trust must perform device authentication. The Synergy platform performs this task via asymmetric key generation, the asymmetric crypto-accelerator, the true random number generator, and the symmetric crypto engine.

Once an IoT device is deployed to the field, every remote patch, software update or lifecycle maintenance routine poses a potential threat. Each of these functions must be performed remotely and securely. To protect against malicious overwrites, the Synergy Platform offers an authenticated boot capability that places code and its key in a secured flash area in the on-chip memory of the MCU. In figure 3, the traditional MCU on the left has simply allocated the customer authentication code to user flash. The code is therefore

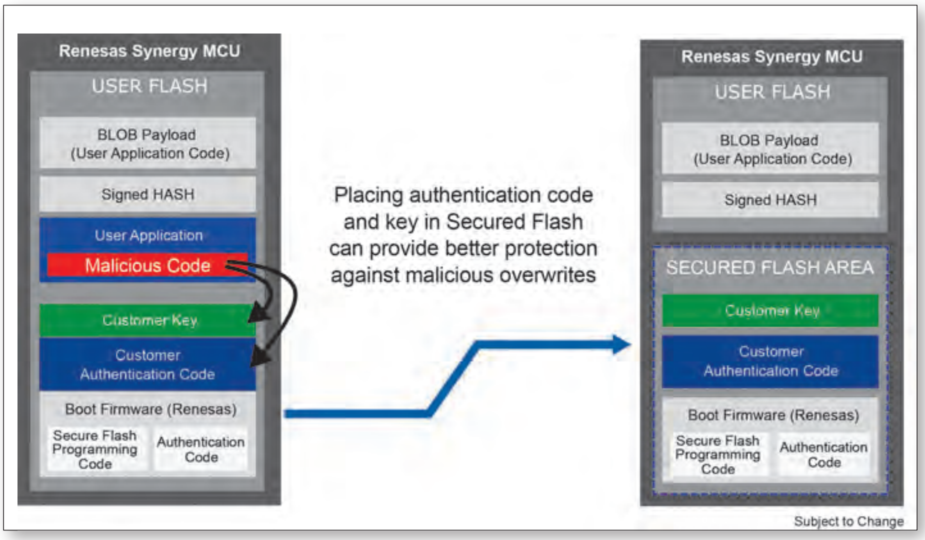


Figure 3. By placing authentication code and key in secured flash, Synergy's authenticated boot function extends product life.

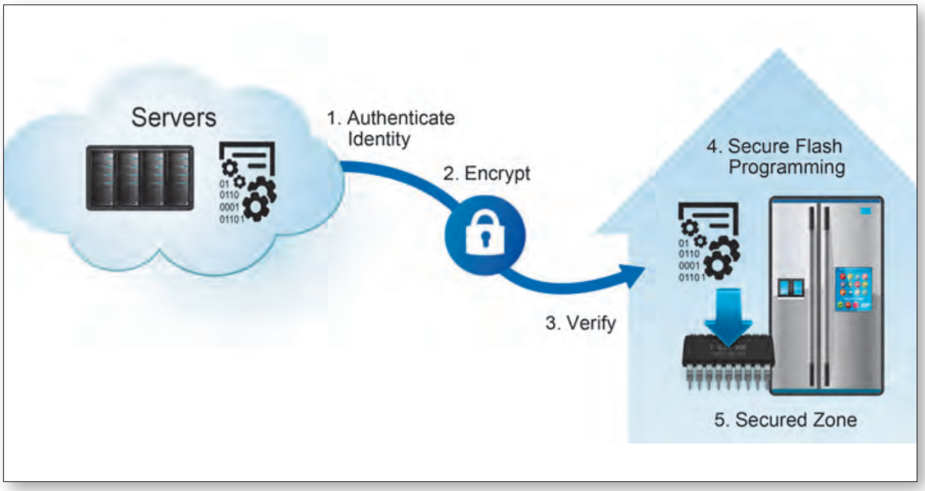


Figure 4. Synergy Platform offers a broad range of security features.

under threat of being overwritten. The Synergy Platform counter measure on the right side of the figure makes it far more difficult to hack by restricting JTAG access and protecting the authentication code in a secured flash zone of the Memory Protection Unit. The rest of the user flash security load remains unchanged. In this example, the BLOB payload would still likely be an update with the signed HASH authenticating that it comes from a trusted source and the expected size (HASH) to ensure nothing has been added.

Synergy authenticated boot feature can extend product life by ensuring a device continues to be protected in the event of a susceptibility. Once susceptibility is identified, authenticated boot will only allow the correctly identified owner to perform devices updates, it will only allow updates on signed and verified code from the server, and it will inhibit roll-backs of software to previous versions. In a post-deployment environment, users of connected devices or systems are constantly facing hacking threats. Hackers breaching networked smart homes can steal private data and undermine the operational capability of equipment on the network. Similarly, hackers attacking smart factories can slow or halt production or create a catastrophic failure.

To protect against device hacking, the Synergy Platform adds three key security features: trusted libraries of code, sandboxing and the ThreadX RTOS. Trusted libraries of code avoid buffer overflow and code injection by constraining inputs and communication. As an example, cryptography and secure boot components enable only a subset of inputs which helps create contagion control. Sandboxing is a feature which enables the Synergy Platform to maintain availability even while under attack. It allows the system to separate different aspects of the operating system and an application. Basically it functions by using an integrated MPU to segregate the on-chip memory into areas only accessible by privileged applications and areas which are open to communication. This segmentation allows users to create supervisory and user modes and ensures that any problems in user mode do not reach supervisory mode. In addition, with sandboxing users can create areas of memory as unreadable or unprintable. Once that division is set up, when an application goes out of bounds, as in a denial of service attack, the MCU will raise a flag in hardware to execute a handle to reset the system. That, in turn, will defend against the attack. Finally, the use of an industry-proven RTOS, Express Logic ThreadX, offers significant security advantages. As an operating system that has been used for years by tens of thousands of users, ThreadX offers users the reassurance that it has been developed, checked and certified to robust security standards.

At the development and manufacturing stages of the product lifecycle, embedded systems are particularly vulnerable through their firmware. One of the primary advantages of a connected device is the ability to update the firmware remotely. But this capability also creates vulnerabilities. In a typical example MCUs in a car assembly line programmed via firmware are injected with malware that undermines performance with potentially life-threatening consequences. Synergy Platform protects against this type of attack with a five-step authenticated firm-ware management program. This process begins by verifying the digital certificate and identity of the firmware update service. The Synergy Platform authenticates its communication channel by using several technologies including the unique ID, key secure storage, asymmetric cryptography, and the asymmetric key generator. Next, to protect the Binary from tampering and interception during the download, Synergy uses a Transport Layer Security (TLS) connection which employs the True Random Number generator and the Secure Crypto Engine with HASH.

Key to the platform ability to deliver high performance cryptography, the Secure Crypto Engine integrates a number of crucial functions including the True Random Number Generator, a symmetric cryptography accelerator, an asymmetric cryptography accelerator, a HASH accelerator, a stream cipher accelerator, and Secure Key Storage. Since the True Random Number Generator resides within the Secure Crypto Engine module close to the root of trust, is not software-enabled, and supports a smaller session key, it is less susceptible to attack. In step three the Synergy Platform verifies that the downloaded Binary is the same as the source Binary on the server by using its integrated HASH technology. Next, the platform only programs the authenticated Binary using the Secure Crypto Engine. Finally, to protect the binary on flash, the system creates a secured zone using the secure MPU and limited JTAG access. ■