White Paper

Security Technology Trends in Industrial Automation Equipment

— RA Family / RX Family / RZ Family and Security Software Stack Implementation Approach —

Takashi Kojo, Chief Manager of Engineering, wolfSSL Japan GK

Keisuke Koseki, Staff Engineer, Functional Safety & Security Core Tech/EP Core Technologies, Renesas Electronics Corporation

1. Introduction

The environment surrounding industrial automation equipment is undergoing significant changes. Previously, operation within closed networks was assumed; however, in recent years, the proliferation of cloud integration and remote monitoring has created demand for designs that assume external network connectivity.

Accordingly, the scope of security has expanded to encompass the entire product lifecycle, including communication, boot, updates, and key management. Furthermore, with the establishment of cybersecurity measures in various countries, such as Europe's Cyber Resilience Act (CRA), Japan's JC-STAR, and the U.S. Cyber Trust Mark, embedded devices are now required to address security from the design and development stages through market launch, and even up to End-of-Life.

Comprehensive security design considerations are now strongly required throughout the entire lifecycle. Additionally, the generational transition of cryptographic technology toward Post-Quantum Cryptography (PQC) is progressing. With industrial equipment requiring long-term operation of 10 to 20 years, development and design that anticipate future cryptographic risks is essential.

The following challenges have become apparent in many industrial devices:

- Difficulty in addressing vulnerabilities after shipment due to lack of software update capability
- Device authentication and certificate management prone to failure due to individual implementations
- Increasing costs for compliance with new regulations such as CRA
- Insufficient design for cryptographic updates assuming long-term operation

If these challenges become apparent after shipment, they can lead to significant business risks such as product recalls or service interruptions. This paper organizes the security requirements for industrial equipment such as PLCs, industrial robots, and gateways; and explains implementation approaches that

combine Renesas RA/RX/RZ Families with wolfSSL's security software stack, including wolfSSL/wolfBoot, focusing on risk reduction, certification cost reduction, and accelerating time-to-market.

2. Environment Surrounding Industrial Automation Equipment

2.1.Transition from Closed Network Assumptions

Traditionally, industrial equipment was generally operated within closed networks inside factories, and the risk of cyberattacks from outside was judged to be limited. However, in recent years, factors such as cloud connectivity, remote monitoring and maintenance, and distributed equipment deployment have fundamentally changed the assumptions about network environments. As a result, industrial equipment has become directly or indirectly connected to the Internet, increasing the likelihood of becoming a target for cyberattacks.

2.2.Extension to Intra-Device and Non-Connected Environments

Security measures are not only necessary for network communication. Intra-device communication between units, maintenance paths using USB or SD cards, and unauthorized firmware rewriting can also become important attack vectors. Therefore, designs that can ensure reliability of devices as standalone units are required, regardless of network connectivity.

2.3.Changes in Regulations, Certifications, and Procurement Requirements

In recent years, security regulations and security evaluation/labeling systems for embedded devices that connect directly or indirectly to the Internet have been advancing in various countries and regions. A characteristic feature of these measures and requirements is that they emphasize not only security at the time of shipment, but also continuous security assurance, including post-shipment updates and vulnerability response.

European CRA

The European CRA (Cyber Resilience Act) is a comprehensive cybersecurity regulation for products with digital elements. Its purpose is to enhance the security of digital products distributed in the European market, maintain security throughout the entire product lifecycle, and make it easier for users to understand the security characteristics of the products.

CRA imposes the following requirements on manufacturers based on risk assessment:

- Secure by design, secure by default
- Products released with no known vulnerabilities
- Vulnerability handling framework
- Secure security updates
- Technical documentation and conformity assessment
- Clear indication of support period
- Reporting of serious incidents and actively exploited vulnerabilities

As these requirements indicate, the CRA demands not only security at shipment, but also the ability to manage vulnerabilities throughout the expected product lifespan and to continue safe fixes and updates, affecting both product architecture and operational systems. Therefore, for industrial equipment as well, security design that considers the entire product lifecycle becomes important, including boot-time authenticity verification (secure boot, etc.), secure software updates (OTA, etc.), device authentication, access control, key/certificate management, and long-term vulnerability response.

These requirements are increasingly being reflected in customer procurement conditions, supply chain requirements, and security audits.

Japan JC-STAR

In Japan, JC-STAR (Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements) is operated as a labeling system that evaluates and visualizes the security functions of IoT products based on common criteria. This system aims to make it easier for procurers and users to understand the security level of products, targeting a wide range of IoT products capable of communicating with the Internet, while aligning with ETSI EN 303 645 and NISTIR 8425.
JC-STAR is not simply a system that evaluates the presence or absence of cryptographic functions. JC-STAR emphasizes security throughout the entire product lifecycle, including initial settings, updates, authentication/access control, vulnerability response, and considerations at disposal.

The conformance criteria consist of four levels from ★1 to ★4, where ★1 represents minimum common product requirements, and ★2 to ★4 represent higher requirements based on product type and usage. ★1 and ★2 are based on self-declaration of conformity, while ★3 and ★4 require third-party evaluation, and conforming products are given labels with QR codes.

Although JC-STAR is a domestic Japanese system, its concepts share many commonalities with the European CRA and U.S. Cyber Trust Mark. It also envisions utilization in government and private procurement and mutual recognition with overseas systems, potentially expanding its influence on domestic procurement requirements and supply chain demands in the future.

United States U.S. Cyber Trust Mark

In the United States, the U.S. Cyber Trust Mark is being developed as a cybersecurity labeling system targeting wireless-enabled consumer IoT products. Its purpose is to visualize product security functions and make it easier to identify secure IoT products in the market. A mechanism is also being considered where labels combined with QR codes allow verification of detailed information such as support period and availability of software updates and security patches.

The program's criteria are based on baseline requirements from NISTIR 8425, with emphasis on authentication, updates, data protection, secure communication, and vulnerability disclosure. The concept of continuously managing security throughout the entire product lifecycle is common with CRA and JC-STAR. While this system does not currently directly target industrial equipment, it holds important significance as a system that demonstrates to the entire market the direction that "embedded devices

connected directly or indirectly to the Internet require continuous security management," and may spread as future procurement requirements and market demands.

2.4.Implementation Requirements Demanded by Regulations

Although Europe's CRA, Japan's JC-STAR, and the U.S. Cyber Trust Mark differ in their systems and target markets, they all share common emphasis on security assurance throughout the entire product lifecycle, post-shipment vulnerability response, secure updates, device authentication/identification, and visibility of security information and accountability. The implementation requirements that are particularly important for industrial equipment are as follows:

- Boot-time authenticity verification (secure boot, etc.)
- Secure software updates (OTA, etc.) and rollback prevention
- Device authentication, access control, and key/certificate lifecycle management
- Vulnerability response framework, logging, and incident response
- Long-term support and management/presentation of security information

What is important is to design these not as individual functions, but as an architecture whereby all security features work together in harmony. Specifically, secure boot, TLS/DTLS, device authentication, OTA, and key management need to function as an integrated whole. Requirements related to design and procurement through post-shipment operation and maintenance are also strengthening, including SBOM, supply chain management, long-term vulnerability monitoring, and incident reporting obligations.

3. New Threats and Changes in Security Technology

3.1.Long-Term Operation and Cryptographic Lifespan

Since industrial equipment is operated over long periods of 10 to 20 years, even cryptographic methods currently considered secure may become unable to maintain their security in the future due to advances in computational power and analysis techniques. Therefore, in security design, it is important to have a structure that does not depend on specific cryptographic algorithms and allows for changing cryptographic methods in the future.

Security protocols such as TLS have considered algorithm flexibility (crypto-agility) from the design stage to address this challenge. For example, the following mechanisms enable migration to new cryptographic methods:

- Algorithm combination selection through cipher suites
- Switching of key exchange methods, signature methods, and hash functions
- Protocol version updates (migration from TLS 1.2 to TLS 1.3, etc.)

On the other hand, in industrial equipment, there are cases where this flexibility cannot be fully utilized due to fixed cipher suites, lack of implementation of key and certificate update functions, and constraints on firmware updates. With such designs, security risks may become apparent during long-term operation.

Therefore, it is important to incorporate the following elements in advance, considering long-term operation and cryptographic lifespan.

- Implementation of key rotation and certificate renewal mechanisms
- Functional expansion through secure firmware updates (OTA)
- Design that anticipates future updates to cryptographic algorithms
- Flexible selection of protocol versions and cipher suites

Furthermore, looking ahead to the development of quantum computers, migration to PQC (Post-Quantum Cryptography) is also an important consideration. This is not merely a replacement of cryptographic algorithms but involves a review of the entire system design considering the increase in key sizes and changes in computational characteristics.

Cryptographic technology must be designed with the assumption that it is not fixed but changes over time. Especially for industrial equipment operated over long periods, a design that can continuously respond to new threats becomes an important element of security.

3.2. PQC (Post-Quantum Cryptography)

PQC (Post-Quantum Cryptography) is a group of cryptographic schemes designed to maintain security against attacks by quantum computers. Traditional public key cryptographic algorithms (RSA and elliptic curve cryptography) have been identified as vulnerable to attack by algorithms such as Shor's algorithm, which can be highly accelerated by quantum computers. This makes the long-term security of these algorithms questionable. In contrast, PQC is designed based on mathematical problems such as lattice problems and hash-based signatures, which are currently considered difficult to solve efficiently even with quantum computers.

Standardization Trends of PQC Algorithms

PQC has already moved beyond the research stage and transitioned to the standardization and implementation phase. The National Institute of Standards and Technology (NIST) has established the following algorithms as standards through a multi-year selection process.

- ML-KEM (formerly Kyber): Key sharing and key encapsulation (KEM)
- ML-DSA (formerly Dilithium): Lattice-based digital signature
- SLH-DSA (formerly SPHINCS+): Stateless hierarchical hash-based digital signature

These have been standardized as NIST FIPS 203, 204, and 205 respectively, and implementation and evaluation are already underway. Further standardization efforts are also in progress.

Optimized implementations of those PQC algorithms are currently available in wolfSSL/wolfCrypt.

Application to Existing Protocols (TLS, etc.)

PQC is being integrated not only for standalone use but also into existing security protocols such as TLS. Rather than replacing conventional methods all at once, configurations are being adopted that gradually add quantum resistance while maintaining compatibility with existing systems by increasing key lengths of

conventional algorithms to reinforce security and introducing hybrid configurations that combine ECDHE with ML-KEM for key exchange and ECDSA with ML-DSA for signatures.

This concept is being deployed in the combination of multiple shared secrets in TLS, multiple signatures on certificates (hybrid certificates), and dual signatures in firmware signing, and is attracting attention as a mechanism that enables gradual introduction of PQC while maintaining compatibility with existing systems.

Certificate and PKI Support Status

The introduction of PQC affects not only communication protocols but also certificates and PKI infrastructure. Current X.509 certificates face challenges including OID definitions for new signature algorithms (such as ML-DSA), as well as increases in key sizes and overall certificate chain sizes. For this reason, efforts are underway to address these challenges through hybrid certificates that use both conventional and PQC signatures, gradual migration at the intermediate certificate level, and size optimization at the protocol level. For industrial equipment in particular, designs must consider the impact on communication bandwidth, flash capacity, and boot time.

3.3. Advanced Certificate and Key Management

Key management in traditional industrial equipment generally relied on relatively simple configurations dependent on a single shared key or fixed certificate. However, with current requirements for cloud connectivity, long-term operation, and regulatory compliance, such simple models have become difficult to address these demands. Therefore, advanced certificate and key management such as the following is required.

Trust Model Using Certificate Chains

Previously, configurations that relied on a single public key or self-signed certificate were common, but now hierarchical trust models consisting of root CA (Root of Trust), intermediate CA (separation of issuance and operation), and device certificates are beginning to be introduced. This structure enables long-term protection of root keys, rotation of intermediate keys, and revocation management on a per-device basis. For industrial equipment, it is particularly important to separately manage the root trust anchor written during manufacturing and certificates updated during operation.

Device Unique Key (Device Identity)

In recent years, it has become assumed that all devices have unique keys for cryptographic identity. This not only enables authentication on a per-device basis but also leads to the exclusion of unauthorized devices and ensures traceability. From an implementation perspective, it is important to have a configuration that generates and writes keys during manufacturing, or generates unique key values within the chip, stores them in the hardware Root of Trust, and can execute signing and decryption processes without exposing the keys externally.

Key Rotation and Lifecycle Management

Keys should not be set once and forgotten; they must be managed throughout their entire lifecycle. Specifically, in addition to regular certificate renewal, operations must anticipate rapid replacement in case of key compromise and algorithm updates from RSA to ECC and further to PQC. To achieve this, a mechanism combining certificate update mechanisms via OTA, key protection through secure storage, and rollback control in case of update failure becomes important.

4. Basic Security Requirements for Industrial Equipment

Security requirements for industrial equipment can be organized from five perspectives: communication protection, boot protection, update protection, key protection, and vulnerability response.

4.1.Communication Protection

- Encrypted communication using TLS/DTLS
- Ensuring authentication and integrity

Communication protection is the most fundamental requirement for industrial equipment connected to external networks.

TLS/DTLS ensures communication confidentiality (prevention of eavesdropping) and integrity (tampering detection), while server authentication and client authentication verify the legitimacy of communication partners. Particularly for industrial applications, mutual authentication between devices (mTLS) and certificate management assuming long-term operation are important. Additionally, designs that enable flexible updates to cipher suites and protocol versions (crypto-agility) are also required.

4.2.Boot Protection

- Secure boot
- Firmware authenticity verification

Boot protection is a mechanism that ensures the device starts operation in the correct state.

Secure boot verifies firmware signatures at startup and prevents execution of tampered code. It is important to retain the root key (Root of Trust) that serves as the starting point of trust within the hardware and separate the verification process from software. This prevents unauthorized boot even if an attacker rewrites the software.

4.3.Update Protection

- Secure OTA
- Rollback prevention

For industrial equipment, firmware updates are essential for vulnerability response and functional improvements.

Secure OTA (Over-The-Air) establishes a mechanism to safely distribute and apply updates remotely. By attaching signatures to update data and verifying before application, the introduction of tampered

firmware is prevented. Version control and counter-based control are also important to prevent rollback to older vulnerable versions.

4.4.Key Protection

- Secure key storage
- Lifecycle management

Keys are assets that form the foundation of security, and their protection is extremely important.

Device unique keys and certificate private keys are securely stored within hardware in a form that cannot be directly referenced by software and are protected from external leakage. Keys must be managed throughout their entire lifecycle, from generation and writing during manufacturing, through updates and revocation during operation, to disposal. For industrial equipment assuming long-term operation, support for key rotation and algorithm updates are also important design elements.

4.5.Vulnerability Response

- Update Framework
- Incident response

Recent regulations strongly require vulnerability response capabilities after product shipment. When vulnerabilities are discovered, a system is needed that can quickly provide correction patches and safely apply them.

When incidents occur, mechanisms for log acquisition, status confirmation, and identification of the scope of impact become important. Beyond simply having update functionality, the "operational capability to continuously maintain security" has become part of the security requirements.

It is important to design these not as individual functions but as an interconnected system. For example, security needs to function as a series of processes: starting trusted software with secure boot, communicating securely with TLS, updating securely with OTA, and supporting that foundation with key management.

Additionally, vulnerability response cannot be completed solely through the efforts of product manufacturers alone. Continuous support systems from suppliers of adopted software components are also important. For example, wolfSSL has announced a commitment to full compliance with CRA and has announced a policy to provide long-term vulnerability management, CVE response, structured vulnerability report reception, coordinated disclosure processes, and maintenance options for long-life products. This makes it easier for product manufacturers to achieve security maintenance throughout the entire lifecycle of their products by combining it with the support system for the software stack.

Security for industrial equipment should not be viewed as a single function, but rather as an architecture and framework that operates as a complete system.

5. Implementation Model

This chapter organizes future security implementation models for industrial automation equipment from the perspectives of hardware security functions and software stacks.

5.1.Hardware Implementation Model

Evolution of Implementation Models

In conventional embedded devices, hardware security functions have primarily been provided as hardware accelerators to speed up cryptographic processing. While this was effective in reducing processing load, mechanisms for consistently managing key generation, writing, and updating as a root of trust were limited.

The reliability of the entire system largely depends on how keys can be protected and controlled. Sufficient security cannot be ensured in secure boot, update validation, and device authentication if the underlying keys cannot be trusted. For this reason, in recent years, there has been a demand not only for faster cryptographic processing but also for establishing keys as a Root of Trust and working in conjunction with software to achieve system-wide security.

The security engines (RSIP/TSIP/SCE)* built into Renesas RA/RX/RZ Families are not simply cryptographic accelerators. They also provide secure key management capabilities that support secure key generation, injection, and update, as well as a foundation for Root of Trust, enabling the implementation of integrated security functions without adding external security components.

The Renesas security engine primarily provides the following functions.

- Root of Trust
- Secure key management (generation, injection, and update)
- Hardware cryptographic processing
- Foundation functions supporting lifecycle management

This enables efficient fulfillment of the advanced security requirements demanded by industrial equipment while reducing design workload, lowering BOM costs, and optimizing power consumption.
By combining these foundation functions with software, system-level security such as secure boot, authentication, communication protection, software updates, and key lifecycle management can be achieved. As a result, the coordination between hardware and software makes it possible to ensure consistent reliability across the entire product.

*RSIP: Renesas Secure IP, TSIP: Trusted Secure IP, SCE: Secure Crypto Engine

Establishing Root of Trust

The Renesas security engine provides a Root of Trust within the device. This protects device-specific keys and identification information and makes them available as a foundation of trust.

This Root of Trust establishes a foundation of trust for processes such as firmware verification at startup, authentication based on device-specific IDs and keys, and secure key derivation.

Secure Key Management

For secure key management, keys can be used without exposing plaintext keys externally. Keys are stored protected by hardware-unique keys, and cryptographic processing is completed within the security engine.

This mechanism provides benefits such as prevention of key extraction and copying, reduction of key exposure risk, limitation of impact scope during software compromise, and improved resistance to side-channel attacks.

Hardware cryptographic processing

For hardware cryptographic processing, supported algorithms such as AES, RSA, ECC, and hashing can be executed in hardware. This provides advantages compared to software-only cryptographic processing, including faster processing, reduced CPU load, lower power consumption, and improved resistance to side-channel and timing attacks.

Furthermore, by working with software stacks such as wolfSSL, key operations and cryptographic processing in TLS communications can be offloaded safely and efficiently.

Lifecycle Management Support

Across the product lifecycle, the security engine serves as a foundation for security operations from manufacturing through operation and disposal. By securely handling keys on the hardware side, it is possible to implement measures at the hardware level such as key injection and provisioning during manufacturing, key updates during operation, and erasure of confidential information at disposal.
In this way, it is positioned not as a mere cryptographic accelerator but as a foundation that supports continuous security throughout the entire product lifecycle with Root of Trust at its core.

5.2.Software Implementation Model

Hardware Root of Trust and cryptographic accelerators play an important role in enhancing key protection and the security of cryptographic processing. On the other hand, in actual products, communication protocols, certificate processing, firmware verification, and OTA update control need to be implemented as software.

In security implementation for industrial equipment, it is important to appropriately combine hardware security functions and software stacks.

wolfSSL Inc. and Product Overview

wolfSSL Inc. is a network security specialist vendor that provides security software for embedded devices and IoT. The company provides embedded security libraries that emphasize size, speed, portability, and standards compliance, and also offers technical support and consulting.

Representative products from wolfSSL Inc. include **wolfSSL**, which enables TLS/DTLS communication, and **wolfBoot**, which enables secure boot and firmware updates. Related products such as wolfSSH, wolfMQTT, wolfTPM, and wolfHSM are also available, complementing remote access, lightweight message communication, TPM integration, and key management infrastructure. By combining these components, it

becomes possible to build an integrated security architecture that includes communication, authentication, device management, secure storage, and lifecycle management.
These are designed for resource-constrained microcontroller environments and RTOS environments, and are used in fields requiring long-term operation such as industrial equipment, IoT devices, automotive, and medical devices.

In this document, wolfSSL/wolfBoot is positioned as a software stack for integrating communication, boot, update, and key management in conjunction with the security engine built into Renesas RA/RX/RZ Family.

wolfSSL: TLS/DTLS, Certificates, PQC, Security Engine Integration

wolfSSL is a lightweight SSL/TLS library designed for embedded systems. Implemented in C language, it targets embedded, RTOS, and resource-constrained environments, enabling secure communication via TLS/DTLS.

The primary role of wolfSSL in industrial equipment is to provide secure communication channels for external systems, cloud services, maintenance terminals, and inter-device communication. Specifically, it handles the following functions.

- Encrypted communication using TLS/DTLS
- Server/client authentication
- X.509 certificate verification
- Device-to-device and device-to-cloud authentication via mTLS
- Flexible selection of cipher suites and protocol versions
- Support for PQC and hybrid key exchange
- Integration with hardware cryptographic accelerators

Particularly in industrial equipment, communication partners are diverse, including not only cloud services but also maintenance terminals, gateways, and other control devices. Therefore, it is important not only to encrypt communications but also to verify communication partners using certificates and prevent connections with unauthorized devices or servers.

Additionally, in industrial equipment that operates long-term, cryptographic algorithms and certificates may need to be updated. By using a TLS stack like wolfSSL, protocol versions, cipher suites, and certificate verification methods can be updated and extended as software, making it easier to ensure crypto-agility.

Furthermore, when considering the transition to PQC, introducing hybrid key exchange and PQC signature algorithms in TLS becomes important. wolfSSL is advancing PQC support and serves as an option for extending future cryptographic methods for existing TLS/DTLS communication infrastructure.

In configurations that integrate with the Renesas security engine, private keys and cryptographic processing are delegated to hardware as much as possible, while wolfSSL handles TLS protocol processing, certificate processing, and session management. This configuration makes it possible to achieve TLS client authentication and encrypted communication while securely protecting keys at the hardware level.

wolfBoot: Secure Boot, Signature Verification, OTA, Rollback Prevention

wolfBoot is a secure bootloader for embedded systems, positioned as a portable secure bootloader that provides firmware authentication and firmware update mechanisms.
The main roles of wolfBoot in industrial equipment are as follows.

- Firmware signature verification at startup
- Prevention of execution of tampered firmware
- Application of signed firmware updates
- Support for updates via OTA or any communication channel
- Recovery control upon update failure
- Rollback prevention
- Verification configuration considering multiple keys and key updates

wolfBoot verifies signatures at startup and when receiving firmware updates, and only executes trusted firmware. Images that cannot be verified or authenticated will not boot.

Additionally, for industrial equipment, it is important to be able to securely update firmware even after shipment for vulnerability fixes and functional improvements. During updates, it is necessary to verify that the received firmware has a valid signature, has not been tampered with, and does not revert to an older version containing known vulnerabilities.

wolfBoot verifies the signature of firmware received through any transfer path including OTA, and also supports rollback prevention based on version information. This provides an implementation foundation that supports secure updates, vulnerability management, and post-shipment security maintenance as required by CRA, JC-STAR, and other standards.

Role Allocation with Renesas Security Engine

When combining Renesas security engines with wolfSSL / wolfBoot, the division of responsibilities between hardware and software is important. Specifically, the collaboration between the security engine (hardware) and software leads to practical solutions for long-term operational support and CRA compliance.
The security engine is primarily responsible for the following:

- Providing Root of Trust
- Protection of private keys and device-specific keys
- Hardware execution of cryptographic operations
- Control of key derivation and key usage
- Lifecycle Management Support

On the other hand, wolfSSL / wolfBoot is primarily responsible for the following:

- TLS/DTLS protocol processing
- Certificate verification and peer authentication
- Secure boot control
- Firmware signature verification
- OTA update flow control

- Rollback prevention
- Future updates of cryptographic algorithms and protocols

In this configuration, private keys are handled only within the security engine whenever possible, and wolfSSL / wolfBoot utilizes the necessary cryptographic operations as hardware functions. This enables a design where private keys are not handled directly by software. Specifically, during communication, wolfSSL handles TLS/DTLS and certificate verification, while during boot and update, wolfBoot controls signature verification, version checking, and rollback prevention. The Renesas security engine handles key protection and cryptographic processing in each scenario, serving as the trust foundation throughout the entire product lifecycle during operation.

In this way, the Renesas security engine protects keys and cryptographic processing as the foundation of trust, while wolfSSL / wolfBoot implements specific security functions for communication, boot, and updates on top of it. As a result, the communication, boot, update, key protection, and vulnerability management required for industrial equipment can be achieved as an integrated security architecture.

5.3.Operational and Compliance Support Model

Recent security regulations, including CRA, require not only implementing security features in products, but also continuously managing vulnerabilities after shipment, providing fixes as needed, and being able to explain the status of such responses. Therefore, for security implementation in industrial equipment, in addition to technical functions such as communication, boot, update, and key management, a compliance support framework including operation, maintenance, and documentation also becomes important.

Renesas is advancing initiatives to support customers ensure security throughout the entire product lifecycle and meeting regulatory compliance requirements through security features integrated into the RA/RX/RZ Families, related software, and compliance support frameworks.

wolfSSL announced full support for the European Cyber Resilience Act (CRA) in March 2026, indicating its policy to help meet CRA security requirements for connected devices and embedded equipment through its products. The announcement explains that wolfSSL's embedded security components and long-term support address the secure development processes, vulnerability management, and post-market maintenance responsibilities required by CRA.

Specifically, wolfSSL supports CRA compliance in the following areas:

Secure Communication and Data Protection

wolfSSL provides communication data encryption through TLS 1.3/DTLS 1.3, authenticated encryption, modern cipher suites, and configuration options suitable for resource-constrained environments.

Strong Cryptography and Secure Key Management

wolfSSL supports cryptographic primitives, including AES, RSA, ECC, EdDSA, and PQC algorithms, and facilitates integration with hardware-based key protection such as secure elements, TPMs, and HSMs. Additionally, FIPS 140-3 certified cryptographic modules are provided for regulated markets.

Firmware Integrity and Secure Boot

wolfBoot supports firmware verification at boot, authenticated firmware updates including OTA, and rollback protection. This provides a foundation for preventing the execution of unauthorized or vulnerable firmware.

Vulnerability Management and Coordinated Disclosure

Post-market maintenance is a key pillar of CRA. wolfSSL provides structured vulnerability report acceptance, coordinated disclosure processes, CVE tracking, rapid fix support, and maintenance options aligned with long-life product lifecycles.

Transparency and SBOM Support

CRA emphasizes maintaining Software Bill of Materials (SBOM) for supply chain transparency and vulnerability tracking. wolfSSL supports SBOM-based compliance through software components with minimal external dependencies, clear component traceability, and documentation that supports secure configuration and lifecycle maintenance.

In this way, wolfSSL / wolfBoot is positioned not only as a provider of individual functions such as encrypted communication and secure boot, but also as a software foundation that supports maintaining security throughout the entire product lifecycle as required by CRA. By combining with the Renesas security engine, it becomes easier to build an integrated security architecture that includes communication, boot, update, key management, vulnerability response, and documentation.

6. Future Trends and Summary

Security requirements for industrial automation equipment are expected to become more advanced and long-term in the future. Traditionally, the focus was on communication encryption, authentication using fixed keys, and ensuring security at shipment; but going forward, mechanisms to maintain security throughout the entire operational period, including long-term operation, cloud integration, OTA updates, and regulatory compliance, are being required. Technical trends that are expected to become important in the future include certificate chaining, remote attestation, and PQC support.

6.1.Certificate Chaining and Advanced Trust Models

In the future, hierarchical trust models using a root CA, an intermediate CA, and device certificates are expected to become as common as authentication models. This enables per-device authentication, certificate revocation management, key rotation, and supply chain-level management. Additionally, a configuration that separately manages the Root of Trust written during manufacturing and the certificates and keys updated during operation is also important. This trust model serves as a foundation supporting not only communication authentication but also OTA updates, device management, cloud integration, and remote maintenance.

6.2.Remote Attestation

Remote attestation is gaining attention as a mechanism for externally verifying not only that "it is the correct device" but also that "it is currently operating in the correct state." By presenting signed firmware information verified at boot, software configuration, and device identification information, the cloud side can perform health verification, exclude tampered devices, detect unauthorized firmware, and implement zero-trust access control. In recent years, technologies for lightweight devices such as DICE (Device Identifier Composition Engine) and EAT (Entity Attestation Token) have been advancing, and there is a growing trend of extending the trust chain built through secure boot to communication and cloud integration.

6.3.PQC Support and Cryptographic Migration

With the advancement of quantum computers, migration to PQC is also becoming an important issue. Currently, implementation and evaluation of hybrid key exchange in TLS, PQC signature algorithms, and hybrid certificates are underway.

On the other hand, PQC introduction involves not only algorithm replacement but also impacts key and certificate sizes, communication volume, and memory usage. Therefore, for industrial equipment, optimization including communication bandwidth, flash, RAM, boot time, and power consumption, as well as design that assumes crypto-agility, is important. While there is uncertainty about when quantum computers will become practical, the risk of so-called Harvest Now, Decrypt Later, where encrypted communications are captured now and decrypted in the future, has also been pointed out. Therefore, for industrial systems requiring long-term protection, design that assumes PQC migration (crypto-agility) is expected to become important in the future.

6.4.Evolution to Integrated Security Architecture

For future industrial equipment, it is important to design communication, boot, update, key management, device authentication, attestation, and vulnerability response as an integrated security architecture rather than implementing them individually. In particular, a configuration that links hardware Root of Trust, secure boot, TLS/DTLS, OTA, certificate management, attestation, PQC, and other elements is required to continuously maintain reliability throughout the entire product lifecycle. In this way, for future industrial automation equipment, integrated security architecture that achieves "continuously trustworthy throughout the operational period" rather than "safe at shipment" is expected to become increasingly important.

Renesas and wolfSSL provide reference implementations and evaluation kits that enable evaluation of the security architecture introduced in this article. For specific design and application inquiries, please contact your sales representative or use the web form.

About wolfSSL Inc.

wolfSSL Inc. is a network security specialist vendor that provides embedded security libraries focused on speed, size, portability, features, and standards compliance. In addition to providing security libraries as products, we also offer technical support and consulting services.

Our SSL/TLS products and cryptographic libraries, independently developed by our specialized engineers, support advanced security designs for government agencies, automotive, aerospace, and other sectors. We support RTCA DO-178C Level A certification for aerospace and MISRA-C for automotive applications, and have been adopted by over 2,000 customers worldwide since our founding in 2004.

In July 2024, the wolfCrypt cryptographic library became the world's first to obtain FIPS 140-3 certification compliant with SP800-140Br1. We also provide FIPS 140-3 certification acquisition agency services for customers, with 10 years of experience and numerous achievements.

wolfSSL Inc. is headquartered in Seattle, Washington, USA, with offices in Bozeman, Montana, Portland, Oregon, and other locations.

The technical support center of wolfSSL Japan GK provides support services and customization services by dedicated Japanese staff.

wolfSSL Company Information

wolfSSL Inc.	Headquarters: Edmonds Way, Suite C-300, Edmonds, WA 98020 USA CEO and Founder: Larry Stefonic Founded: 2004 https://wolfssl.com/
wolfSSL Japan GK	Headquarters: Level 28, Shinagawa Intercity A, 2-15-1 Konan, Minato-ku, Tokyo, Japan 108-6028 President: Yoko Suga Founded: 2018 https://wolfssl.jp
Business Description	Development, provision, and support of network security and related software technologies
characteristics	As a licensing model, we feature dual licensing with free open source and paid commercial licenses. While the open source version provides customers with ample opportunity for technical evaluation, the commercial license and support enable long-term stable technical development and continuity of product and technology development by highly specialized engineers.

Contact: facts@wolfssl.com

(Rev.1.0 Mar 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu, Koto-ku, Tokyo 135-0061, Japan
https://www.renesas.com

Trademarks

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
https://www.renesas.com/contact-us

Doc Number: R01WP0035EJ0100