Featuring

Metasys by Johnson Controls

Helping Secure Building Automation Systems with the EmSPARK™ Security Suite

Johnson Controls is a leading provider of building technology and solutions, with a broad portfolio of products and services supporting a wide range of industries. The Johnson Controls Metasys Building Automation System creates intelligent environments by connecting HVAC, lighting, security and protection systems on a single platform to deliver the information building operators need to help ensure comfort, safety and security for building occupants.

Two critical components of the Metasys product line are the SNE Series Network Engine and SNC Series Network Control Engine. These SNE and SNC series network engines offer cost-effective solutions for providing supervisory control and coordination and control over subnetworks of equipment controllers. SNCs have the added capability of input/output (I/O) interfaces used for directly controlling central plants and large built-up air handlers.

THE PROBLEM—ROBUST SECURITY AT SCALE, THROUGHOUT THE PRODUCT LIFECYCLE

When installed in actual buildings, SNE/SNCs are often networked to each other, to third party devices, and to host client computing devices using an IoT or IP networking infrastructure, making them potential targets for cyberattacks. Johnson Controls required a solution with a high assurance of product security, spanning the development, manufacturing, and entire life cycle of the SNE/SNCs, including:

+ A mechanism to securely identify and protect firmware by verifying that the correct, authenticated firmware package is loaded at bootup.
+ The ability to provision software during the manufacturing process while maintaining IP confidentiality.
+ Support for a quick recovery in the event of a device failure by rapidly loading a backup software image.
+ A secure process for updating SNE/SNC software, by local installation or remote download.
+ Easy integration with Johnson Controls building control applications.
+ A best-practice solution that could be easily implemented across Johnson Controls product lines.

Photo by Zane Lee on Unsplash.
Printed in the U.S.A.

THE EmSPARK™ SOLUTION

Johnson Controls implemented the Sequitur Labs EmSPARK™ Security Suite to address the SNE/SNC requirements in a scalable, replicable manner.

+ The EmSPARK™ boot process was used to ensure software protection from ROM boot to critical application execution. This includes loading Linux files and device firmware followed by creating a secure memory partition for the EmSPARK™ CoreTEE™ Trusted Execution Environment. At bootup, the firmware is verified, secure applications are loaded in the CoreTEE™ environment, and known software such as Linux is booted and loaded into memory.
+ Johnson Controls created a diversified set of tools for device identification (IDs, keys) in the manufacturing process in order to ensure firmware protection.
+ Real-time integrity checking was implemented to monitor the integrity of firmware and the Linux kernel, with a quick remediation in the event of failure.
+ Key and certificate-based payload authentication mechanisms were enabled to ensure secure SNE/SNC updates.

Learn More

EVAL KIT Get Started with Free Evaluation Kit: EmSpark™ for Microchip SAMA5D2 Xplained Ultra & SAMA5D27 SOM1-EK1

Learn More: EmSPARK™ for NXP® Semiconductors Layerscape® and i.MX applications processors

Download: EmSPARK™ Whitepaper

Johnson Controls

METASYS®

At Johnson Controls, we transform the environments where people live, work, learn and play. From optimizing building performance to improving safety and enhancing comfort, we drive the outcomes that matter most. We deliver our promise in industries such as healthcare, education, data centers and manufacturing. With a global team of 105,000 experts in more than 150 countries and over 130 years of innovation, we are the power behind our customers' mission. For more information, visit www.johnsoncontrols.com or follow us @johnsoncontrols on Twitter.

SEQUITUR LABS

Sequitur Labs is developing seminal technologies to improve trust in a connected world, reducing the cost and complexity to build secure embedded and IoT devices. Sequitur's products span a range of disciplines required for trusted computing, from boot through the full device lifecycle. Sequitur's security solutions provide real business value to device makers, such as reducing BoM costs, protecting revenue by thwarting IP theft, improving product reliability and reducing liability, and improving device lifecycle management processes. To learn more about Sequitur's security platform, visit us at www.sequiturlabs.com or follow us at @SequiturLabs.

PO Box 1127
Issaquah, WA 98027

+1 425 654 2048
+44 20 3318 1171

info@sequiturlabs.com
www.sequiturlabs.com

Photo by Zane Lee on Unsplash.
Printed in the U.S.A.