WHITE PAPER

WINSYSTEMS®

# Securing a Reliable Future for the Industrial IoT

## Key Cybersecurity Elements to be Considered in the Design of an Industrial IoT System

October 15, 2021 (Revised)

George T. Hilliard
Director of Technical Sales
WINSYSTEMS, INC.

## SCOPE

**This white paper discusses key cybersecurity elements to be considered in the design of an industrial IoT system and how a strong, wide-ranging ecosystem can reduce development time while optimizing protection from cyber attacks.**

## OVERVIEW

Growth in IoT has been increasing consistently, with double digit growth resulting in billions of IoT devices being deployed every year. A mark of this growth was seen last year, when, for the first time, the number of IoT network connectors deployed exceeded the number of smartphones and PCs.

Concerningly, many of these IoT devices are shipping without the security features they need to operate safely. Cybersecurity risks can range from ransomware demands to a physical shutdown of both operations and critical infrastructure sites, to exposing chinks in the armour of many enterprises. There was a 500% year-on-year increase in cyber attacks according to IBM Security X-Force in 2019, principally driven by the Mozi Botnet which targets security cameras and routers. The Mozi Botnet network structure means that more than 400,000 devices are potentially under the control of this peer-to-peer botnet which can infect IoT devices and implement Distributed Denial of Service Attacks.

## LEARN FROM HISTORY

Cybersecurity incidents in the industrial sector can have far-reaching effects. This year alone has thrown up several examples, from cyber attacks and data breaches targeting Microsoft servers, and the ransomware attack on the Colonial Pipeline enterprise network. Without cybersecurity protection to isolate the attacks, or the awareness in the OT systems to be able to determine which systems were affected, the company initiated the shutdown of all its IoT devices.

Last year, a cyber attack on SolarWinds was undetected for months, exposing the data of government agencies and the IT firm's other clients to hackers.

For critical industrial IoT (IIoT) networks, cyber attacks, may pose a more damaging threat to breach data, compromise safety, halt production, corporate espionage and threaten the supply of services. Cybersecurity firm, Fire Eye reports that there were more than 15 low complexity cybersecurity attacks on industrial systems during a 15-month period (January 2020 and April 2021), placing equipment used in agriculture, water treatment, energy generation and distribution as well as building automation and factory networks at risk.

## STANDARDS AND REGULATIONS

The US Department of Commerce's National Institute of Standards and Technology (NIST) is working with government agencies, including the Department of Defense and the Department of Homeland Security to gather IoT cybersecurity vulnerabilities and to advise users about potential pitfalls.

Today, there are several standards and regulations as well as best practices which should be borne in mind when designing IoT systems. The IoT Cybersecurity Improvement Act and NIST 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers, apply to all markets. The latter defines core IoT device capabilities required to support common cybersecurity controls and form a sound base for a security architecture. *(Reference Figure 1: Six Core Baseline Cybersecurity Categories).*

### Figure 1: Six Core Baseline Cybersecurity Categories Defined in NIST 8259A

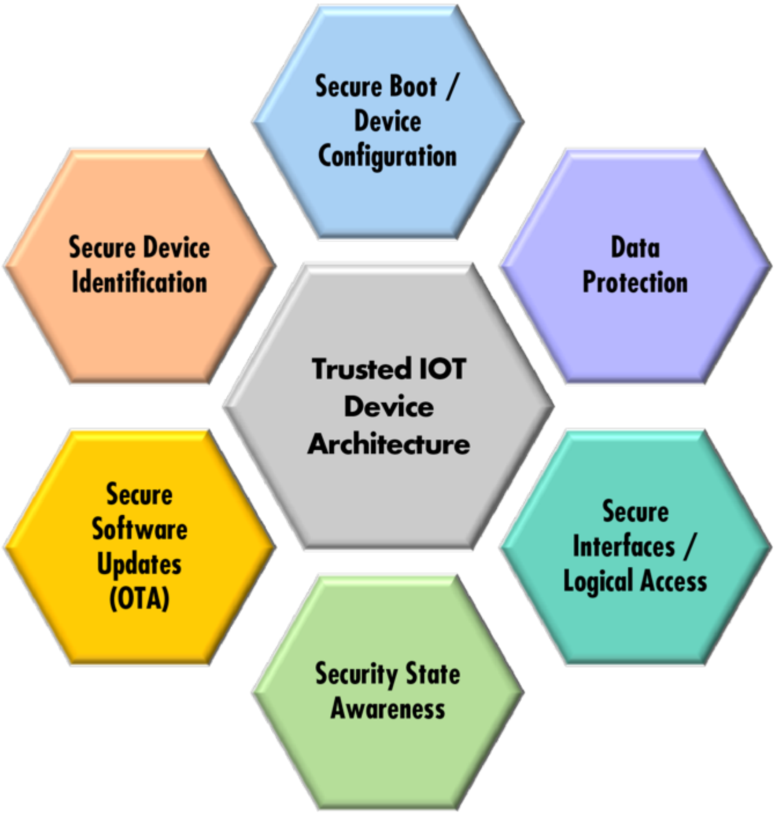
Secure Boot / Device Configuration
Secure Device Identification
Data Protection
Trusted IOT Device Architecture
Secure Software Updates (OTA)
Secure Interfaces / Logical Access
Security State Awareness

Illustration: BG Networks

*Reproduced from BG Networks & WINSYSTEMS joint webinar presentation "Implement IoT Security Features in Days Not Months."*

### The six baseline categories identified in NIST 8259A are:

- For device configuration: secure boot
- For data protection: encrypted data
- For securing interfaces: secure debug and I/O interfaces
- Security awareness: features such as secure non-volatile storage to detect anomalous secure boot or features to check if secure boot failed previously
- Secure over-the-air (OTA) software updates
- Secure device identification: The OTA software update server security tracks and authenticates the ID of the IoT devices / extension of the root of trust

The ubiquity of the IoT, however, means that different market segments have specific cybersecurity regulations. For example, automotive regulations, i.e. UNCEC WP.29 and ISO/SAE 21434, are strictly enforced because lives can be endangered if a vehicle's system is compromised. Consumer IoT devices such as smart speakers, typically adhere to IoXT (Internet of Secure Things) profiles, or the European ETSI 303 645 standard.

In the industrial sector, the Industrial Internet Consortium (IIC) provides many helpful resources, including test services and a cybersecurity framework. The ISA/IEC 62443 technical specification is used for automation and control systems.

## BEGIN WITH CYBERSECURITY IN MIND

Industrial system design should begin with the premise that a cyber attack will be attempted and that it is a case of when, not if, an attempt will take place.

Developers need to consider the hardware, software and future cybersecurity management of an embedded system as all three are required to work together to provide a device that can be initially secured and then maintained over the life of the product.

It is critical that the end customer and potential risk of cyber attack be evaluated during the planning stage of the design. The risk tolerance is very different for a weather station than a heavy vehicle. However, the complete end connectivity should be considered also. A vulnerable thermostat at your home is a different scenario than one connected to a network at an energy generation plant.

Deployment planning should also be taken into account during the definition stage. Too often, the pressure to get a product to market will lead to products being fielded without a proper security deployment strategy. Who, What, and Where will the security keys and identifiers be programmed and managed?

### HARDWARE SECURITY

Security should be addressed during the early hardware design stage, rather than an addition at the end of the design process. Treating security as an after-thought to the hardware design process can result in delays or risk deployment of ill-equipped products. Robust cybersecurity must start with the developer establishing the hardware Root of Trust

Following a risk analysis to establish the security profile required, the first decision is which CPU to use. Choose one with security features from a CPU supplier which supports the device with a comprehensive ecosystem of firmware and software, such as Intel, Arm, NXP, etc.

Next an engineer must decide if the RAM and Flash will need to be removable and also whether ECC protection, encryption, write protect and auto hardware erase are required. Physical tampering risks should also be assessed to make decisions about protecting the enclosure and limiting exposure of ports. Additional security hardware might include a TPM-2.0 module or proprietary hardware security modules.

The final product's operating environment may also warrant consideration in terms of temperature, shock and vibration, and ingress protection (IP rating). While not technically cybersecurity threats, fielding embedded computer hardware that is not rated for the environment might result in a device failure or malfunction so it is important to know if any security holes might be opened as a result.

A security stack with software and hardware elements can save development time and protect systems. *(Reference Figure 2: Hardware Security Stack).*

**Figure 2: Sample Security Stack**

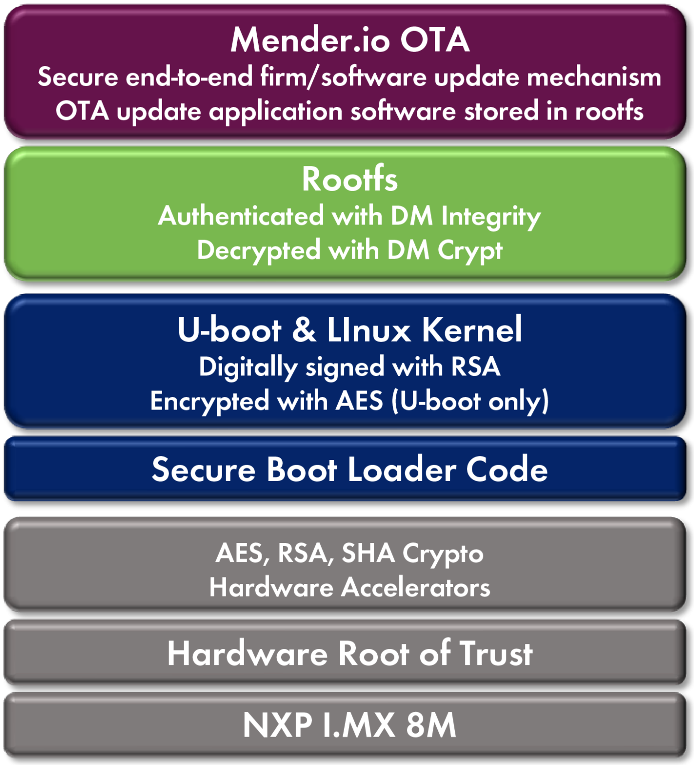
Mender.io OTA
Secure end-to-end firm/software update mechanism
OTA update application software stored in rootfs
Rootfs
Authenticated with DM Integrity
Decrypted with DM Crypt
U-boot & LInux Kernel
Digitally signed with RSA
Encrypted with AES (U-boot only)
Secure Boot Loader Code
AES, RSA, SHA Crypto
Hardware Accelerators
Hardware Root of Trust
NXP I.MX 8M

Illustration: BG Networks

*Reproduced from BG Networks & WINSYSTEMS joint webinar presentation "Implement IoT Security Features in Days Not Months."*

## SOFTWARE SECURITY

Software security goes hand-in-hand with the industrial system's hardware considerations. In an embedded Linux system, there are three major components that support cybersecurity.

The first is the bootloader which is authenticated to the hardware and which has its integrity checked as part of the secure boot process. The bootloader is used to authenticate the second component, the OS kernel. Once the integrity of the kernel has been verified, the signal of the third component, the root filesystem, is verified. Trust is then extended to update the kernel or root filesystem or the application, over-the-air (OTA) by verifying the authentication of the IoT server and any updates received.

This process, using a single component to validate the signature of the next element of the boot chain, is a chain-of-trust. It allows the security to be maintained in layers from the hardware to the cloud and back.

OTA updates authenticate the IoT device to the server, conduct an authentication and check the integrity of software updates to protect systems by preventing unverified or unauthenticated updates from being installed.

## WORKING IN PARTNERSHIP

It takes an ecosystem of partners that specialize in different segments to provide flexible solutions that are secure, maintain integrity even as the application evolves, and updates are required. Few hardware providers or OEMs have resources and expertise to provide all the layers of security required for a robust, secure, industrial IoT device. It is also true that different IIoT devices will have far different cybersecurity requirements, so a single company cannot provide a solution for every scenario. Look for edge computing and industrial IoT hardware platforms that provide an ecosystem of proven partners to provide a flexible solution to improve product time to market and security. We recognize this at WINSYSTEMS and continue to add to ecosystem partners for development and cybersecurity. After all, selecting an embedded computer with security features without the proper software and operations plan is like installing a lock on the front door and then leaving the door open.

*Selecting an embedded computer with security features without the proper software and operations plan is like installing a lock on the front door and then leaving the door open.*

The i.Mx 8MQ processor used on the WINSYSTEMS ITX-P-C444 single board computer has multiple and varied security functions, such as secure boot which uses HAB to establish root-of-trust, cryptographic accelerators, including AES and SHA-256, SNVS for cybersecurity state awareness as well as support for secure interfaces, such as JTAG, UART and USB.

*The WINSYSTEMS' ITX-P-C444 is a rugged industrial Pico-ITX form factor single board computer that uses the NXP i.Mx 8MQ processor.*

Within the WINSYSTEMS' ecosystem, partner Intel® is also the source of the Atom Apollo Lake-I E3900 processor which integrates with TPM 2.0 devices and is used in the SBC35-427. The SBC's BIOS is AMI-UEFI (Unified Extensible Firmware Interface) which supports secure boot. Another Intel E3900-based module is the COMeT10, an industrial COM Express Type 10 Mini which is Linux, Windows 10 and x86 OS-compatible and supports custom-configurable UEFI-based AMI BIOS.

Software partner, BG Networks' Security Automation Tool (BGN-SAT) presently supports NXP's i.MX8 and i.MX 6UL families, with processors due to be announced. The design tool supports secure boot, key generation, code signing and encryption, processor locking and download the sequence to Flash memory. Crucially, it is designed for use by those with little or no cybersecurity experience.

BGN-SAT can be integrated with the open source code BGN-ESSA (Embedded Software Security

Architecture) to extend a hardware root of trust to higher layers of the software stack and to integrate an OTA software update manager.

OTA updates are delivered via the open source Mender.io project's server with automated deployment across all connected Linux devices. The end-to-end open source architecture based on a permissive license model is available as on-site or as a service management server option. It is easy to use and, importantly for industrial operation, applications on the device continue to run while the device is being rebooted. Mender OTA has a breadth of security features. It supports secure TLS/HTTPS communications, software verification with signed images and elliptic curve cryptography. There is also the option for the edge device to verify the management server and for the server to verify the device, for end-to-end security checks.

Foundries.io is an IoT software platform and services company using open-source software to create high-value solutions for customers developing secure and Over-the-Air updatable IoT and Edge devices. Foundries.io helps its customers bring IoT and Edge devices to market faster, increasing their data security and substantially reducing the cost of developing, testing, and deploying devices across their entire installed lifetime.

## CONCLUSION

**Implementing a comprehensive security architecture requires careful planning in the face of time-constrained projects. The wide-reaching IoT and variety of cyber threats means that safeguarding an embedded industrial design requires many disciplines. Using security-enabled, off the shelf embedded computing hardware, open-source software and automation tools can reduce development time. Ensuring there is a reliable supply chain, innovative partners and a wide-ranging ecosystem to support development will ensure the deployment of IoT networks that are prepared to resist cyber attacks and continue the proliferation of the IIoT in new and emerging industrial applications.**

WINSYSTEMS®

This white paper has been made available through WINSYSTEMS, INC. and is offered as an educational resource. Please feel free to contact us if you have questions about what you have read or would like to speak with the author/s or one of our application engineers.

2021.1015

**WINSYSTEMS, INC.**
2890 112th Street, Grand Prairie, Texas 75050

**www.winsystems.com**

Telephone:  +1 817.274.7553

Email:  info@winsystems.com