WP513 (v1.0) May 22, 2019

Xilinx IEC 62443 Compliant Product Enablement

Xilinx® Zynq® UltraScale+™ MPSoCs provide a platform for accelerating the key requirements of cybersecurity standard IEC 62443, providing a secure, performant product solution for industrial and medical device designers.

ABSTRACT

Today's security experts are formalizing new approaches to protecting embedded systems. By establishing and formalizing security best practices, device manufacturers are supported in properly protecting against known threats. Among the leading initiatives is the international industrial-control system security standard IEC 62443.

Xilinx has participated actively and effectively in the authoring of IEC 62443 Part 4-2, which focuses on security requirements for hardware and software components in industrial and automation control systems (IACS).

In support of this key standard, Xilinx® Zynq® UltraScale+™ MPSoC devices embody a class-leading set of security capabilities providing silicon, software, and development tools that enable and/or accelerate many of the requirements outlined for developers working to the IEC 62443 Part 4-2 standard. This white paper provides a summary of mapping of Part 4-2 requirements to the features of Zynq UltraScale+ MPSoCs.

Introduction

Any asset connected to the industrial Internet of things (IIoT) without proper security is at risk of cyber-attack. In addition to causing inconvenience or financial loss, tampering with industrial systems can potentially cause injuries or even fatalities among workers or members of the public. Even a safety-critical system cannot be considered truly safe without adequate cyber protection.

Producers of connected cyber-physical systems are moving quickly to build robust protections into their products. While all would agree that cybersecurity cannot be left to chance, how can developers know how much security to provide? What proportion of the system's costs can be allocated to cybersecurity counter-measures? And how does one answer the question, "Is this device *secure enough?*"

Until recently, these questions have been difficult for security engineers to answer, especially when answers needed to be standard-justified. This has changed, however, since the publication of IEC 62443,(1) which provides:

- A spectrum of defined threat models
- Countermeasures for each standard-defined security level

This standard has allowed industrial security engineers to discuss a shared figure of merit that could be incorporated into an industry-standard certification. As a growing number of companies seek verifiably secure solutions, such certifications are becoming customer-defined requirements.

The IEC 62443 specification establishes a shared figure of merit and a set of recommendations for implementing cybersecurity solutions in the design and manufacture of industrial control equipment. Xilinx has been involved in the authoring of Part 4-2 of this specification, which governs industrial and automation control system (IACS) component-level security features, including those required by digital hardware and software. The Xilinx Zynq UltraScale+ MPSoC platform provides a differentiated foundation for building IEC 62443 compliant systems through its silicon, boot-time protection, and run-time software capabilities.

IEC 62443 Requirements

The IEC 62443 standard is a multi-part specification focused on industrial control systems, but it is also being adopted as a set of best practices in adjacent industries such as medical devices. The standard is presented in 13 parts, as shown in Figure 1.

- Part 1-1 through Part 1-4 establish general principles, taxonomy, and life cycle of an IACS.
- Part 2-1 through Part 2-4 establish requirements around the policies and procedures for implementing and maintaining an IACS through its life cycle.
- Part 3-1 through Part 3-3 describe high-level security technologies at the IACS system level.
- Part 4-1 and Part 4-2 describe specific IACS component-level security requirements.

1. For further information about IEC/ISA 62443 and certification, see ISA/IEC 62443 Cybersecurity Certificate Programs.

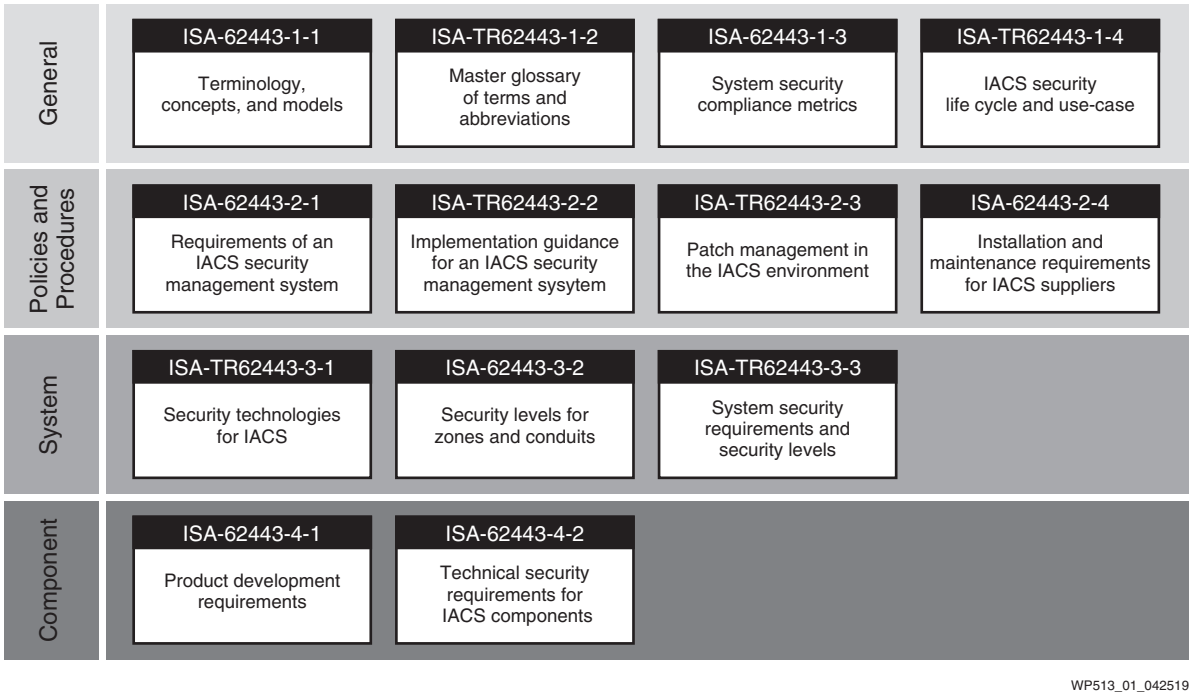

Figure 1: **IEC 62443 Specification Parts (Source: IACS)**

This white paper focuses on Part 4-2, which describes the technical security requirements for IACS components such as controllers and I/O modules. These components typically comprise digital electronics such as processors and FPGAs along with the software applications that run on top of them; they are coupled with mixed-signal electronics like analog-to-digital converters (ADC) and digital-to-analog converters (DAC).

The IEC 62443 Part 4-2 requirements are described and certified at the IACS component level, not at the integrated circuit device level. Thus, while a Zynq UltraScale+ MPSoC can help enable a customer to achieve IEC 62443 compliance, the Zynq device itself cannot be certified.

The IEC 62443 standard defines five security assurance levels (SL) based on the cybersecurity threats that a system can be expected to encounter, as well as on an associated definition of product counter-measures that should be included in a system that has been defined in a given SL. The SLs defined in IEC 62443-1-1, Section 10.4.3 are summarized in Table 1 and are defined by the following:

- **System Identification**: A device's ability to be found/identified through connected and unconnected scenarios.
- **Resources**: The amount of resources (time, financials, etc.) available to an attacker.
- **Skills**: The general skills of the person(s) mounting a cyber-attack.

Table 1: **IEC 62443 SL Ratings**

Security Level	System Identification	Resources	Skills	Motivations
0	No protections	-	-	-
1	Casual	**None**	None	None
2	Simple means	**Low**	Generic	Low
3	Sophisticated means	**Moderate**	System-specific	Moderate
4	Sophisticated means	**Extended**	System-specific	High

To reach Security Levels 3 and 4, the standard requires hardware-based security. This is because software, by definition, is malleable—and thus inherently more vulnerable to cyber-attack. Xilinx SoCs not only provide this fundamental hardware-based root of trust; they also expose many hardware features that can be used to accelerate security functions, such as encrypted communications. In the IEC 62443 Part 4-2 Mapping of Platform Requirements section, this white paper reviews the mapping of the Xilinx hardware and trusted boot-time software for meeting specific requirements within Part 4-2.

IEC 62443 Part 4-2 Mapping of Platform Requirements

The IEC 62443 Part 4-2 is linked to the IACS system-level requirements through matching the numerical identifiers of Part 3-3 System Requirement (SR) numbers and Requirement Enhancement (RE) numbers that correspond to Part 4-2 Component Requirement (CR) numbers. This white paper references Part 4-2 CR numbers and their associated RE.

For additional background on the specific Zynq UltraScale+ MPSoC features summarized in the tables of this document reference the detailed descriptions in these Xilinx technical publications:

- UG1085,* *Zynq UltraScale+ Device Technical Reference Manual*, Ch. 12: Security
- UG1137,* *Zynq UltraScale+ MPSoC Software Developers Guide*, Ch. 8: Security Features
- UG1209,* *Zynq UltraScale+ MPSoC Embedded Design Tutorial*
- XAPP1323,* *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices*
- XAPP1342, *Measured Boot of Zynq UltraScale+ Devices*
- XAPP1333,* *External Secure Storage Using the PUF*

* Also listed in Related Reading section.

A Xilinx Zynq UltraScale+ MPSoC "enabler" is defined as: Fundamental capability built into Xilinx silicon and implements or foundationally enables the requirement. A Xilinx Zynq UltraScale+ MPSoC "accelerator" is defined as: System owner or platform developer responsibility in which implementation is eased by Xilinx supporting technology.

IEC 62443 Component Requirements

Table 2 maps IEC 62443 component level requirement(s) in each row to Zynq UltraScale+ MPSoC security feature(s) that enable or accelerate that specific requirement.

Table 2: **IEC 62443 Part 4-2 Component Requirements to Xilinx Feature Map**

62443 ID	Requirement Summary	Xilinx Enable / Accelerate
CR1.1-RE1, RE2	Capability to identify and authenticate human users on all interfaces capable of human access.	***Enable***: Authentication of human users must be completed on a trusted platform. Xilinx provides a trusted platform through trusted silicon and boot-time software enforced by RSA-4096 authentication. The Zynq UltraScale+ MPSoC also provides user-accessible crypto accelerators in the CSU and Armv8 processors that can be used in accelerating the authentication of human users.
CR1.2-RE1	Capability for a component to uniquely identify itself.	***Enable***: Xilinx provides unique device identifier capabilities through a physically unclonable function (PUF) and/or device DNA that is unique at the silicon level. eFUSEs also provide user-programmable device ID capabilities. These can be accessed by application software for use in device enrollment or other system-level functions.
CR1.5	Authenticator management functions and protection of authentication information.	***Enable***: Authentication changes and management must only be completed on a trusted platform. Xilinx provides trusted platform through trusted silicon and boot-time software with encrypted and internal storage of the associated keys. The Zynq UltraScale+ MPSoC also provides user-accessible crypto accelerators in the CSU and Armv8 processors that can be used in accelerating authentication functions.
CR1.5-RE1	Hardware security functions for authenticators.	***Accelerate***: Xilinx provides the hardware capabilities for user application secure boot, data integrity, and protected memory. Xilinx also provides hardware mechanisms for asymmetric authentication including RSA-4096 with SHA3/384 hard block, Armv8 crypto functions, and FPGA-based custom authenticators. Xilinx provides secure storage of keys in eFUSEs, BBRAM, or encrypted memory. Keys can be stored in an obfuscated or encrypted (black) form.
CR1.8 CR1.9-RE1	Integration and strength of public key infrastructure (PKI) services when provided.	***Enable***: Xilinx has accelerators that support key exchange operations with internal and encrypted storage. Xilinx devices also provide key revocation and key agility capabilities. The CA interface must be implemented at the application level.
CR1.14	Symmetric key-based authentication and key management.	***Accelerate***: Xilinx provides options for AES boot time authentication. The hardware AES-GCM-256 accelerator is also exposed to user application functions needing to implement the same authentication functions at the application level.
CR1.14-RE1	Hardware security for symmetric key-based authentication.	***Accelerate***: The Zynq UltraScale+ MPSoC provides the hardware capabilities for user application secure boot, data integrity, and protected memory. Xilinx also provides hardware mechanisms for symmetric (AES-GCM-256) key-based authentication and secure storage of keys in eFUSEs, BBRAM, or encrypted memory. Keys can be stored in an obfuscated or encrypted (black) form.

Table 2: **IEC 62443 Part 4-2 Component Requirements to Xilinx Feature Map *(Cont'd)***

62443 ID	Requirement Summary	Xilinx Enable / Accelerate
CR2.8	Audit records for relevant security events.	***Enable***: Xilinx integrates device-level anti-tamper, access control, and security logging capabilities captured in device eFUSEs.
CR2.11	Timestamps for audit records.	***Accelerate***: Xilinx can create and maintain timestamps through PTP-enabled FPGA IP blocks.
CR2.13	Use of physical diagnostic and test interfaces.	***Enable***: Xilinx devices allow for the temporary and/or permanent disablement of test interfaces such as JTAG. Xilinx also allows for interfaces such as USB to be disabled by user configuration.
CR3.1	Protection of communications integrity.	***Accelerate***: Xilinx hardware supports the acceleration of authentication and encryption processes through cryptographic hardware blocks for AES-GCM-256 and RSA-4096 in addition to Armv8 accelerators. Additional application-specific cryptographic accelerators can also be built in the FPGA.
CR3.4	Software, configuration, and information integrity checks.	***Accelerate***: Xilinx provides the ability for boot-time software and FPGA configuration checks through Soft Error Mitigation (SEM), Security Monitor (SecMon), and FPGA-based independent software run-time memory monitors (e.g., MicroArx).
CR3.6	Deterministic output of physically or logically connected automation processes.	***Accelerate***: Xilinx driven I/O can be configured for a specific behavior in fault, power down, or security lock-down modes of operation.
CR3.11	Physical tamper resistance and detection.	***Enable***: Xilinx boot process provides several anti-tamper features including DPA resistance, SEU checking, temperature and voltage monitoring, tamper logging, JTAG monitoring, and JTAG block. Xilinx also enables various penalty enforcement actions including internal key clear and configuration memory clear.
CR3.12	Provisioning of product supplier roots of trust.	***Enable***: Xilinx provides root of trust mechanisms via integrated public key revocation, key agility, and obfuscated key loading features. Xilinx can also provide a secure key provisioning service for use at time of device manufacturing. See your Xilinx representative for details.
CR3.13	Provisioning of asset owner roots of trust.	***Accelerate***: Xilinx provides root of trust mechanisms via integrated public key revocation, key agility, and obfuscated key loading features.
CR3.14	Integrity of the devices boot process.	***Enable***: Xilinx provides two boot modes, *Hardware Root of Trust* and *Encrypt Only*, with secure internal key storage in BBRAM or eFUSEs.
CR4.1	Confidentiality of information at rest and in transit.	***Accelerate***: Xilinx provides mechanisms for AES-GCM-256 encryption of boot time software and configuration information. The same AES-256 cryptographic accelerator is also available to user application code; Xilinx software partners have implemented user libraries that exploit these HW accelerators (e.g., Mocana, WolfSSL). See XAPP1333 for additional details on protecting information at rest.

Table 2: **IEC 62443 Part 4-2 Component Requirements to Xilinx Feature Map *(Cont'd)***

62443 ID	Requirement Summary	Xilinx Enable / Accelerate
CR4.3	Support the use of cryptographic security mechanism.	***Accelerate***: Xilinx hardware supports the acceleration of authentication and encryption processes through cryptographic hardware blocks for AES-GCM-256, RSA-4096, and SHA3 in addition to Armv8 accelerators.
CR7.7	Restrict the use of unnecessary functions, ports, protocols, and services.	***Enable***: Xilinx provides JTAG disable/monitor and permanent JTAG disable via eFUSE. The Zynq UltraScale+ MPSoC provides mechanisms to disable all unused ports/interfaces via device configuration. It also provides run-time restriction mechanisms for memory and devices through the Xilinx Memory Protection Unit (XMPU), Xilinx Peripheral Protection Unit (XPPU), and the Xilinx Isolation Design Flow.

IEC 62443 Device Requirements

Xilinx devices are typically targeted at digital systems that IEC 62443 defines as embedded devices and network devices. Table 3 outlines a mapping of the Xilinx security features that enable or accelerate an embedded device requirements (EDR) and network device requirements (NDR). The IEC 62443 definition of a host device is a PC or workstation that Xilinx solutions are typically not used in and thus are excluded from this analysis.

Table 3: **IEC 62443 Part 4-2 Embedded and Network Device Requirements**

62443 ID	Requirement Summary	Xilinx Enabler / Acceleration
EDR2.13 NDR2.13	Protect against unauthorized use of physical diagnostic and test interfaces.	***Enable***: All diagnostic and test interfaces are protected when secure boot is enabled. Xilinx also provides JTAG disable and monitoring options and permanent JTAG disable via one-time programmable eFUSE.
EDR3.10 NDR3.10	Support for updates and upgrades.	***Enable***: Xilinx provides mechanisms for secure platform upgrades and associated keys via public key revocation, key agility, and obfuscated key loading.
EDR3.11 NDR3.11	Physical tamper resistance and detection capabilities.	***Enable***: Xilinx boot process provides several anti-tamper features including DPA resistance, SEU checking, temperature and voltage monitoring, and tamper logging. Xilinx also enables various penalty enforcement actions including internal key clear and configuration memory clear.
EDR3.12 NDR3.12	Support for provisioning of product supplier roots of trust.	***Enable***: Xilinx provides root of trust mechanisms via integrated public key revocation, key agility, and obfuscated key loading features. Xilinx can also provide a secure key provisioning service for use at time of device manufacturing. See your Xilinx representative for details.
EDR3.13 NDR3.13	Support for provisioning of asset owner roots of trust.	***Accelerate***: Xilinx provides root of trust mechanisms via integrated public key revocation, key agility, and obfuscated key loading features.
EDR3.14 NDR3.14	Integrity of the devices boot process including firmware, software, and configuration.	***Enable***: Xilinx provides secure boot and boot time encryption starting with immutable internal boot ROM, RSA-enforced authentication of FSBL, and subsequent software boot processes, with secure internal key storage in BBRAM or eFUSEs.

Summary

This white paper outlines how the Xilinx Zynq UltraScale+ MPSoC family provides a secure foundation for enabling and accelerating the embedded systems requirements defined by IEC 62443 Part 4-2. These features find applicability over a wide range of design needs: supply chain protections, device anti-tamper capabilities, boot time integrity, and user application security feature support.

As outlined in Table 4, Xilinx provides a strong foundation in device anti-tamper features that help an IACS component developer meet the challenging device-level protection requirements of IEC 62443. The Zynq UltraScale+ MPSoC also provides mechanisms for several user application run-time security features, outlined in Table 5, which can be used to implement and accelerate IEC 62443 requirements such as encrypted communications, and component life cycle events such as key rotation. For detailed explanations of the security features outlined in Table 5, please see XAPP1323.

Table 4: **Zynq UltraScale+ Anti-Tamper Features**

Built-in Silicon Features		Zynq UltraScale+
Passive	Confidentiality with AES-256 (BRAM/eFUSE)	☑ GCM
	Secure Configuration/Boot (PL/PS)	☑
	Hardened Readback Disable	☑
	Symmetric Key Authentication	☑
	Public Key (Asymmetric) Authentication	☑
	DPA Resistant	☑
	Obfuscated Key Storage Protection	☑
	Black (Encrypted) Key Storage Protection	☑
Active	SEU Checking	☑
	JTAG Disable/Monitor (BSCAN)	☑
	Internal Key Clear	☑ + Verify
	Internal Configuration Memory Access	☑
	Unique Identifier (Device DNA)	☑
	Unique Identifier (User eFUSE)	☑
	On-chip Temperature/Voltage Monitors	☑
	Key Agility	☑
	Tamper Logging	☑
	Permanent JTAG Disable	☑
	Permanent Decryptor Disable	☑
	Public Key Revocation	☑

Table 5: **Zynq UltraScale+ MPSoC Security Features**

Security Feature	Capability Description
Public Key Revocation	Hardware-based key storage support for key revocation and rotation required by good PKI practices.
Key Agility	Utilizing battery-backed RAM key storage. Keys can be securely updated in the field within the Zynq UltraScale+ MPSoC.
Permanent Decryptor Disable	Use eFUSE as a permanent tamper response/penalty against adversary probing of a device to disable and “brick” a system.
Tamper Logging	Tamper and maintenance events of a Zynq UltraScale+ MPSoC can be securely and permanently logged for forensic analysis.
DPA Resistance	AES bitstream decryption key is protected from differential power analysis via protocol methods.
Temp and Voltage Monitoring	Integrated ADC tracks device temperature and voltage rails, providing detection and security mitigation options when outside specified environmental conditions.
SecMon	MPSoC-based security monitoring solution can check the integrity of configuration memory, JTAG, and environmental conditions, and can implement system responses. See XAPP1323 for additional details.
Obfuscated Key Loading	AES secret key is never exposed outside trusted personnel or systems.
Key Readback Protections	Crypto key protections such that a key can never physically be read back or leave the device after it is loaded.
User Accessible HW Crypto Functions	AES-GCM, SHA-3/384, and RSA Montgomery multiplier hardware accelerators accessible to user application code. Any application-specific cryptographic accelerators can be built in FPGA fabric.

Overall, the Xilinx Zynq UltraScale+ MPSoC provides a strong security baseline for implementing IEC 62443 components that meet the requirements outlined in Part 4-2 of the standard. These silicon and boot-time software features help an IACS component developer meet the strict security standards required for SL3 and SL4 devices. The Zynq UltraScale+ MPSoC is a scalable and adaptable platform that can evolve with the changing security threats faced by industrial systems today and in the future.

In the Related Reading section, additional Xilinx documentation provides more detail on some of the Zynq UltraScale+ MPSoC security features highlighted in this paper.

Related Reading

1. Xilinx User Guide UG1085, *Zynq UltraScale+ Device Technical Reference Manual*
2. Xilinx User Guide UG1137, *Zynq UltraScale+ MPSoC: Software Developers Guide*
3. Xilinx User Guide UG1209, *Zynq UltraScale+ MPSoC: Embedded Design Tutorial*
4. Xilinx Application Note XAPP1267, *Using Encryption and Authentication to Secure an UltraScale+ FPGA Bitstream*
5. Xilinx Application Note XAPP1283, *Internal Programming of BBRAM and eFUSEs*
6. Xilinx Application Note XAPP1319, *Programming BBRAM and eFUSEs*
7. Xilinx Application Note XAPP1320, *Isolation Methods in Zynq UltraScale+ MPSoCs*
8. Xilinx Application Note XAPP1323, *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices*
9. Xilinx Application Note XAPP1333, *External Secure Storage Using the PUF*
10. Xilinx Application Note XAPP1335, *Isolation Design Flow for the Zynq UltraScale+ MPSoC*
11. Xilinx Application Note XAPP1336, *Isolation Design Example for the Zynq UltraScale+ MPSoC*
12. Xilinx Application Note XAPP1342, *Measured Boot of Zynq UltraScale+ Devices*
13. Xilinx User Guide UG580, *UltraScale Architecture System Monitor*
14. Xilinx White Paper WP493, *Key Attributes of an Intelligent IIoT Edge Platform*
15. Xilinx White Paper WP511, *Risk Management for Medical Device Embedded Systems*
16. Xilinx White Paper WP512, *Accelerating Cryptographic Performance on the Zynq UltraScale+ MPSoC*
17. Xilinx Website Isolation Design Flow

Third Party IP and Software Partners:

1. Mocana: IoT Software Security Platform
2. Mocana+Xilinx: Reference Design
3. wolfSSL: Software Crypto with Xilinx Acceleration
4. MicroArx: Hardware Monitor IP

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
05/22/2019	1.0	Initial Xilinx release.

Disclaimer

Automotive Applications Disclaimer