White Paper

Industrial Automation and Control Systems (IACS)
Hardware-Enabled Security Powered by Intel® Technology

Journey to ISA/IEC 62443 Readiness with Hardware-Enabled Security Powered by Intel® Technology

Cybersecurity is at the heart of every industry today, and Intel's longstanding commitment to security has never been stronger.

Authors

Hau, Tze-ming
tze-ming.hau@intel.com

Musti, Srinivas
srinivas.musti@intel.com

Tarkhanyan, Anahit
anahit.tarkhanyan@intel.com

Kwek,Ser Wee
ser.wee.kwek@intel.com

Upadhyay, Ajay Rajeshbhai
Ajay.Upadhyay@tuvsud.com

Müller, Markus
m.mueller@tuvsud.com

"With cybersecurity threats advancing rapidly against the industrial and critical infrastructure industry, the security of our product is top priority.

Industrial cybersecurity standards such as IEC 62443 series is crucial to help organization design and implement highly effective systems for industrial security that meet the requirements for certification.

Together with TÜV SÜD services, Intel customers can meet and implement the cybersecurity requirements of ISA/IEC 62443-4-2, within their OT (operational technology) and industrial control systems (ICS) environments." – ***Sunita Shenoy,*** *Senior Director of Technology Products, Federal and Industrial Solutions Division at Intel*

This white paper is intended to provide an overview of the ISA/IEC 62443 standard and how to use Intel hardware security technologies to meet the cybersecurity requirements of ISA/IEC 62443-4-2, while reducing the complexity of the implementation. The target audience of this white paper is the value chain of Industrial Automation and Control Systems (IACS), such as ODM, OEM, SI.

The desired outcome is to enable IACS systems stakeholders to produce products ready for ISA/IEC 62443 certification, help them to understand the certification process and documentation required, such as artifacts throughout the lifecycle of the product.

Introduction of IEC 62443

ISA/IEC 62443, Industrial Communication Networks – Network and System Security, is a series of internationally-accepted standards, technical reports and technical specifications that provide a systematic approach for assessing and mitigating current and future cybersecurity risks in each aspect of an industrial control system. Based in part on the principles found in several different national cybersecurity standards, the IEC 62443 series provides a clear yet flexible framework that is equally applicable in discrete and process-oriented manufacturing environments in a diverse range of industries.

Comprised of 14 separate parts (as of September 2020), the ISA/IEC 62443 series details specific cybersecurity responsibilities of individual participants ("roles") throughout the supply chain that are involved in the development, deployment, use or maintenance of industrial control systems and components.

These roles include:

Asset Owner — the individual or organization responsible for one or more IACSs.

Product Supplier — the manufacturer or developer of hardware or software components integrated into an IACS.

Service Provider — the individual or organization that provides support services or supplies to the asset owner for an industrial control system or component.

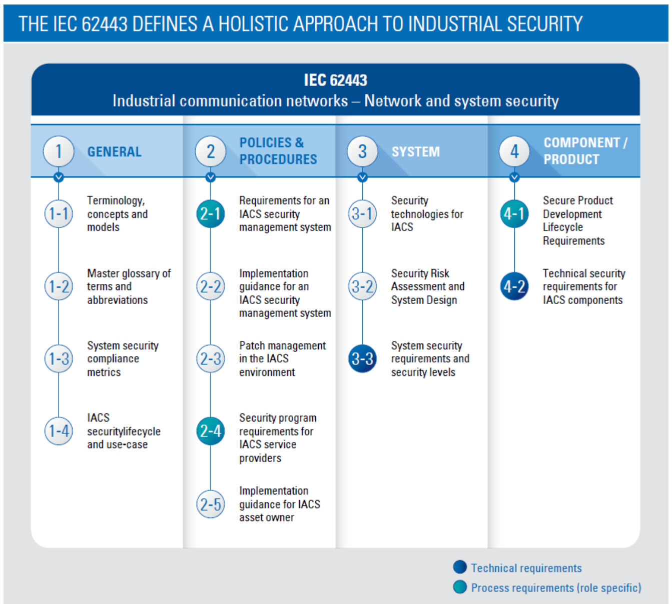
THE IEC 62443 DEFINES A HOLISTIC APPROACH TO INDUSTRIAL SECURITY
IEC 62443
Industrial communication networks – Network and system security
1 GENERAL
2 POLICIES & PROCEDURES
3 SYSTEM
4 COMPONENT / PRODUCT
1-1 Terminology, concepts and models
1-2 Master glossary of terms and abbreviations
1-3 System security compliance metrics
1-4 IACS securitylifecycle and use-case
2-1 Requirements for an IACS security management system
2-2 Implementation guidance for an IACS security management system
2-3 Patch management in the IACS environment
2-4 Security program requirements for IACS service providers
2-5 Implementation guidance for IACS asset owner
3-1 Security technologies for IACS
3-2 Security Risk Assessment and System Design
3-3 System security requirements and security levels
4-1 Secure Product Development Lifecycle Requirements
4-2 Technical security requirements for IACS components
● Technical requirements
● Process requirements (role specific)

Figure 1 . Categories of documentation

The specific requirements presented in the IEC 62443 series also give equal weight to the contributions of people, processes and technology in helping ensure cybersecurity in an industrial environment. Toward that end, individual documents in the series fall into one of the following four categories:

General — The parts comprising the "General" category (IEC 62443-1-x) include four individual documents that provide a general overview of the cybersecurity process and introduce key concepts, models, and definitions.

Policies & Procedures — The five documents in the "Policies & Procedures" category (IEC 62443-2-x) detail the requirements for a IACS security management system, along with security program (SP) requirements for asset owners and service providers, including system integrators and product suppliers.

System — The three documents in the "System" category (IEC 62443-3-x) of the series provide essential guidance of system security requirements, security levels and security risk management and system design.

Component — The last category, "Component" (IEC 62443-4-x), includes two documents, one that details technical security requirements for system components, and a second that presents secure product development lifecycle requirements.

Key Documents in the IEC 62443 Series

Of the 14 separate documents in the IEC 62443 series, the cybersecurity requirements in six represent a good starting point for industrial organizations seeking to secure their automation control systems from cyber threats. Here's a summary of the focus of each of these documents.

IEC 62443-2-1 Edition 2, Establishing an industrial automation and control system security program

IEC 62443-2-1 specifies requirements for asset owners of IACS. The security program has to define security capabilities that apply to the secure operation of an IACS. The implementation of these security capabilities often requires support from service providers and product suppliers, nevertheless the asset owner remains accountable for security.

IEC 62443-2-4, Security program requirements for IACS service providers

This IEC 62443 standard details a comprehensive set of security capability requirements for service providers of all types involved in the integration or maintenance of an IACS. As these requirements are mostly domain-independent, the standard provides for the development of "profiles", which can be used to address the unique characteristics of specific environments.

IEC 62443-3-2, Security risk assessment for system design

This standard establishes requirements for defining an IACS system, partitioning a system under consideration (SUC) into zones and conduits, assessing the risk for each zone and conduit and establishing their respective target security levels.

IEC 62443-3-3, System security requirements and security levels

IEC 62443-3-3 defines system security requirements applicable to automation systems and networks. Security requirements are based on the seven foundational requirements (FR 1-7) as defined in IEC 62443-1-1, and include:
1) identification and authentication control; 2) use control; 3) system integrity; 4) data confidentiality; 5) restricted data flow;
6) timely response to events; and 7) resource availability.

Security levels (SLs) referenced in IEC 62443-3-3 are based on those presented in IEC 62443-3-2 for the classification of risk of automation systems and networks.

IEC 62443-4-1 Secure product development lifecycle requirements

This IEC 62443 standard describes the product development life-cycle requirement related to the cybersecurity of products intended for use in the industrial automation and control systems environment. Specific aspects of the product lifecycle addressed in the standard include security requirements definition, more secure design, secure implementation, verification and validation, defect management, patch management and product end-of-life considerations.

IEC 62443-4-2 Technical security requirements for IACS components

IEC 62443-4-2 applies the security requirements and security levels to the components that constitute an IACS, such as:

Software applications: one or more software programs and their dependencies that are used to interface with the process or the control system itself (e.g., configuration software and historian).

Embedded devices: special purpose device designed to directly monitor or control an industrial process (e.g., PLC, intelligent electronic device).

Host devices: general purpose device running an operating system (e.g., Microsoft* Windows* OS or Linux*) capable of hosting one or more software applications, datastores or functions from one or more suppliers (e.g., operator workstation).

Network devices: device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process (e.g., switch, VPN terminator).

Security requirements are based on the seven Foundational Requirements (FR 1-7) as defined in IEC 62443-1-1, and include:

FR 1	Identification and Authentication Control (IAC)	Control access to selected devices, information, or both to protect against unauthorized interrogation of the device or information.
FR 2	Use Control (UC)*	Control use of selected devices, information, or both to protect against unauthorized operation of the device or use of information.
FR 3	Data Integrity (DI)	Help ensure the integrity of data on selected communication channels to protect against unauthorized changes.
FR 4	Data Confidentiality (DC)	Help ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
FR 5	Restrict Data Flow (RDF)	Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.
FR 6	Timely Response to Event (TRE)	Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission-critical or safety-critical situations.
FR 7	Resource Availability (RA)	Help ensure the availability of all network resources to protect against denial-of-service attacks.

The intent of the standard is to specify the component security capabilities required to mitigate threats for a given security level without compensating countermeasures.

Evaluation of Technology – Security Levels	
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
SL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation.
SL 1	Protection against casual or coincidental violation.

TÜV SÜD - Approach to the IEC 62443 Framework for Product Suppliers and Manufacturers

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions, specializing in testing, certification, auditing and training services. TÜV SÜD's experts have a wealth of experience working with clients on complying Operational Technology system with regulatory and industry best standards. Our experience with industrial processes, combined with profound expertise in industrial cybersecurity, makes us uniquely positioned to assess security processes and solutions. Based on our deep expertise on market-specific cybersecurity frameworks & industry standards and the cyberthreat landscape, TÜV SÜD partners with customers worldwide to release the full potential of their digital future.

Certification to one or more of the IEC 62443 standards can serve as an important step in an organization's overall strategy for minimizing the potential risks from cyber threats.

For suppliers, TÜV SÜD provides process certification in accordance with the requirements of IEC 62443- 4-1, which addresses the security of the product development lifecycle and is a prerequisite for certification to the product-specific standards in the IEC 62443 series. With this foundation, suppliers can then seek product certification to IEC 62443-4-2, which covers technical security requirements for IACS components.

TÜV SÜD's IEC 62443 certification is awarded only in cases where the product or process is subject to an evaluation covering all of the requirements detailed in the applicable standard. Our certification also includes annual monitoring of IEC 62443-certified processes and products. These additional aspects of our certification framework are intended to verify continuing compliance with the requirements of certification, as well as the uninterrupted security of certified IACS products and systems.

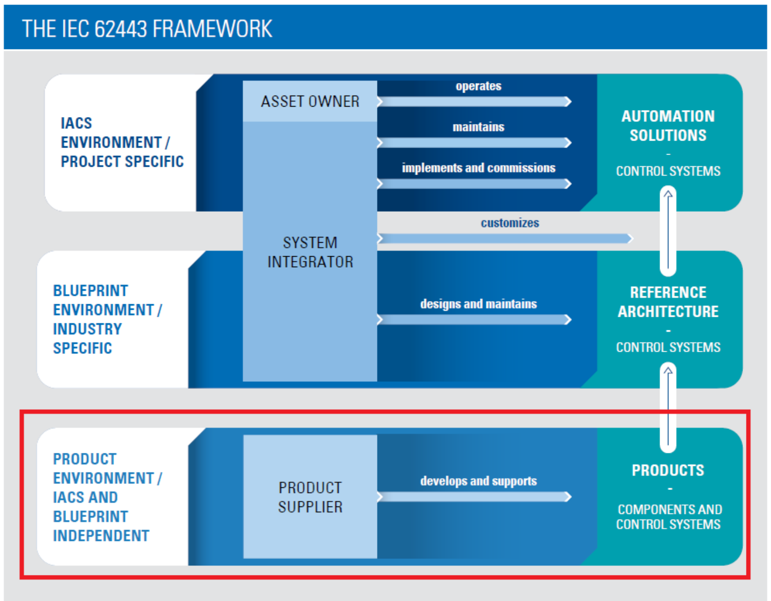

Figure 2 . IEC 62443 Framework

Roadmap to Certification - TÜV SÜD

1. Training, Preliminary Analysis
   - Awareness, basic understanding
   - Definition of project scope

2. Gap Analysis
   - Analysis of existing processes and technical security capabilities
   - Identification of security gaps
   - Definition of countermeasures
   - Test and evaluations

3. Certification
   - Validation of all countermeasures

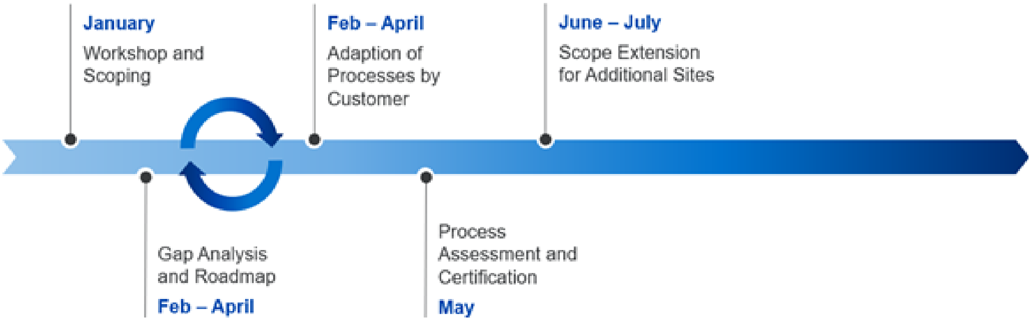
January
Workshop and Scoping
Feb – April
Adaption of Processes by Customer
June – July
Scope Extension for Additional Sites
Gap Analysis and Roadmap
Feb – April
Process Assessment and Certification
May

Figure 3 . Process Certification Timeline for IEC 62443-4-1 (sample)

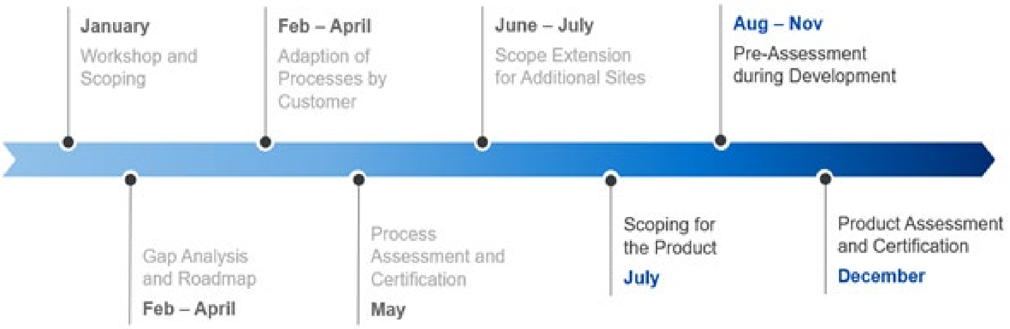
January
Workshop and Scoping
Feb – April
Adaption of Processes by Customer
June – July
Scope Extension for Additional Sites
Aug – Nov
Pre-Assessment during Development
Gap Analysis and Roadmap
Feb – April
Process Assessment and Certification
May
Scoping for the Product
July
Product Assessment and Certification
December

Figure 4 . Product Certification Timeline for IEC 62443-4-1 & 4-2 (sample)

Why is the IEC 62443 Process/Product Certification Required?

Aiming to mitigate risk for industrial communication networks, the international IEC 62443 standards provide a structured approach to cybersecurity for all types of plants, facilities and systems across industries. These standards apply to component suppliers, system integrators and asset owners.

Through a set of defined process requirements, these standards help ensure that all applicable security aspects are addressed in a structured manner throughout the stages of specification, integration, operation, maintenance and decommissioning. Furthermore, these standards help foresee that processes are established to facilitate all necessary technical security functions. Adapted to the relevant project scope, IEC 62443 standards lay the foundations for cybersecurity robustness throughout the product and system lifetime.

The implementation of IEC 62443 standards can also boost the competitiveness of the supplier and system integrator:

A third-party certification demonstrates to manufacturers, asset owners and operators that the component or system is in line with industry best practice for cybersecurity.

IEC 62443 certification provides assurances of compliance with industrial cybersecurity requirements and demonstrates an organization's commitment to the security and integrity of its products.

TÜV SÜD IEC 62443 Industrial Cybersecurity Certification Services

TÜV SÜD provides testing and evaluation to the IEC 62443 standards and certifies processes, products and systems under the following Certification Schemes:

1. TÜV SÜD Product Service certification mark for Industrial Cybersecurity

The IEC 62443 standards address security processes along the complete supply chain. TÜV SÜD mark provides certificates based on a set of security profiles from IEC 62443. Surveillance activities would be conducted to certificate owners to check if the compliance is maintained through the duration of certification.

For product suppliers, TÜV SÜD provides industrial cybersecurity certification services based on IEC 62443-4-1. The standard applies to the supplier's overall security programs, and to the security processes connected to the development of the relevant component or control system.

Corresponding certifications are available to system integrators based on IEC 62443-2-4. The compliance of generic processes and security processes for a reference architecture or blueprint can be verified by our experts. The conformity assessment can be based on document reviews, interviews, and on-site witness testing. A report and the TÜV SÜD Product Service certification are issued when found to be compliant with standard requirements. The validity of certification requires an annual surveillance audit.

Beside the generic process aspects during product development and system integration, the IEC 62443 standards specify technical security requirements to components and systems. These technical requirements are described in IEC 62443-4-2 and IEC 62443-3-3. To participate, the development teams would have to show a mature secure product development lifecycle process based on IEC 62433-4-1. They are the basis for the TÜV SÜD Product Service's certification of components and systems, respectively.

2. IECEE-CB Scheme for Cybersecurity (CYBR)

   IECEE Certificates of Conformity are issued for processes/products/systems based on a one-off evaluation in accordance with the rules of the IECEE-CB Scheme. No marks or logo of TÜV SÜD are allowed on a certified product.

   - Product Capability Assessment (IEC 62443-2-4/ IEC 62443-3-3/ IEC 62443-4-2)
   - Process Capability Assessment (IEC 62443-2-4/ IEC 62443-4-1)
   - Product Application of Capabilities Assessment (IEC 62443-4-1)
   - Solution Application of Capabilities Assessment (IEC 62443-2-4/ IEC 62443-3-3)

3. ISASecure IEC 62443 Conformance Certification

   The ISASecure Certification program is based on the Industrial Automation and Control security lifecycle as defined in IEC 62443 standards, with additional requirements published in the ISASecure Certification specifications. Depending on the type of certification, vulnerability assessment may have to be performed before certification is granted.

   TÜV SÜD PSB is an ISASecure Chartered Laboratory authorized by ISA Security Compliance Institute (ISCI), a not-for-profit automation controls industry consortium that manages the ISASecure conformance certification program.

   TÜV SÜD offers 3 types of certifications with four security assurance levels (SAL) in alignment with IEC 62443 standards.

   - ISASecure Component Security Assurance (CSA) Certification
   - ISASecure System Security Assurance (SSA) Certification
   - ISASecure Security Development Lifecycle Assurance (SDLA) Certification

   A company's development process, component, or system that passes evaluation according to the latest version of ISASecure specifications will be granted with ISASecure certification by TÜV SÜD. The ISASecure Mark may be affixed on certified products and systems.

ISA/IEC 62443 4-2 Requirements Mapping

This section introduces the requirements for ISA/IEC 62443 4-2, and how it can be mapped to the Intel hardware security technology. We will focus on the component requirements for host device components defined by ISA/IEC62443 standards, which cover industrial PCs or any form of derivative of industrial PCs such as operator workstations, HMI, robot controllers, and so on.

Security Objective	Component Requirement (Industrial PC)	Hardware-Enabled Security Powered by Intel® Technology
Identification and Authentical Control	CR1.2 Device Identification CR1.5 Authenticator Management CR1.8/1.9 PKI – RE(1) hardware security for public key base authentication CR1.14 (RE1) hardware security for symmetric key-base authentication	Intel® Converged Security and Management Engine (Intel® CSME) Intel® Crypto Acceleration Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) Intel® Secure Key Intel® Platform Trust Technology (Intel® PTT)
Use Control	CR2.4 Mobile Code HDR2.4 – Mobile Code execution control, authenticity check	Intel® TXT, Intel® Platform Trust Technology (Intel® PTT)

System Integrity	HDR3.2 – Protection from malicious code HDR3.10 – Support for update HDR3.11 – Physical tamper resistance and detection HDR3.12 – Provisioning product supplier root of trust HDR3.13 – Provisioning asset owner root of trust HDR3.14 – Integrity of boot process	Intel® TDT Intel® OS Guard MBEC (Mode-based execution control), UMIP (User-mode Instruction Prevention) Intel® CET, Intel® Key Locker Intel Platform Update (IPU), Intel Firmware Update Tools Serial Flash hardening through RPMC Intel® TME, Intel End of Manufacturing -> OEM Root Key Provisioning Intel® PTT Provisioning Intel® Boot Guard
Data Confidentiality	Use of cryptography	Intel® Crypto Acceleration Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) Intel® Platform Trust Technology (Intel® PTT) Intel® Secure Key
Restricted Data Flow	N/A (network device)	N/A
Timely Response to Events		Intel Firmware Restart / Recovery Intel® TDT
Resource Availability		Intel® Firmware Restart / Recovery

Note:

Each foundational requirement defines 4 Security Level (SL) targets. Each Security Level relates to the Component Requirements (CRs) to be met. The Highest Security Level (SL4) is needed to prevent more sophisticated means of attack with extended resources, IACS skills and high motivation. Software-based security measures are often not sufficient to reach SL4, while hardware-based security measures such as Intel® Hardware Shield technologies can help OEMs meet the higher security level's requirements. The Components Requirements are derived from System Requirements (SR).

Identification and Authentication Control, Data Confidentiality (FR1, FR4)

To achieve higher Security Levels, CR1.5 and CR1.9, under this Foundational Requirements (FR) mandate, hardware-based security engine for authentication control is used to achieve a higher level of security. A common usage of authentication control are passwords. Passwords should be stored safely or protected using secure hardware.

One of the recommendations is to use a TPM (Trusted Platform Module) to protect the password.

Authentication Management (CR1.5)

CR1.5 under FR 1 (Identification and Authentical Control) states the use of authentication mechanism for use control.

Intel® Platform Trust Technology (Intel® PTT) can be used to perform hardware-based authentication. Intel® PTT is an integrated on-chip hardware Trusted Platform Module (TPM) that supports Trusted Computing Group (TCG) TPM2.0 standards and FIPS 140-2 certification.

It can be enabled and used as a tamper-resistant location to store encryption keys. It allows establishment of hardware-based root-of-trust. For PKI authentication, the certification and private key can be provisioned and stored inside the PTT non-volatile storage.

Public Key Infrastructure Authentication (CR1.8), Strength of PKI Authentication (CR1.9)

Intel CPUs and SoCs include the ISA (Instruction Set Architecture) to support "big number" multiplication often found in public-key ciphers, such as the AVX512 Integer Fused Multiply-Add (AVX512_IFMA). The instructions multiply eight – 52-bit unsigned integers found in the wide 512-bit (ZMM) registers, to produce the high and low halves of the result and add to the eight 64-bit accumulators. Combined with software optimization techniques, such as multi-buffer processing, these instructions provide significant performance improvements for RSA and elliptic curve cryptography.

Recommended reading: https://newsroom.intel.com/articles/crypto-acceleration-enabling-path-future-computing/

The Hash function is heavily used to calculate the digest of a component, to support signature verification process of asymmetric cryptography. *Intel® Secure Hash Algorithm (Intel® SHA Extension)* is a family of instructions designed to accelerate the cryptographic Secure Hash Algorithms Extension.

Intel® PTT supports hardware-based PKI authentication and fulfills the requirement to provide capability to protect the sensitive private key of the PKI using the PTT.

Symmetric Key-based Authentication (CR1.14)

Hardware security for symmetric key-based authentication is recommended to support established symmetric cryptography algorithm such as AES (Advanced Encryption Standard), a symmetric key-base encryption standard adopted by the U.S. government starting in 2001.

Intel CPUs and SoCs include a set of instructions, *Intel® Advanced Encryption Standard (AES) New Instructions (AES-NI)*, designed to implement some of the complex and performance intensive steps of the AES algorithm using hardware, thus accelerating the execution of the AES algorithms. AES-NI can be used to accelerate the performance of an implementation of AES by 3x to 10x over a complete software implementation.

Recommended reading: https://www.intel.com/content/www/us/en/developer/articles/technical/advanced-encryption-standard-instructions-aes-ni.html

Data Confidentiality (FR4)

The objective is to prevent unauthorized disclosure of information. Disk encryption is a common approach to protect data confidentiality.

Information Confidentiality (CR4.1), Information Persistence (CR4.2)

It is recommended to encrypt the data on the non-volatile storage to prevent the data from being accessed by potential attackers. Full Disk Encryption (FDE) is a common feature of modern operating systems. Intel SoCs include AES-NI instructions to assess the hardware-accelerated cryptography engine for FDE operation. *Intel® Secure Key* is based on Digital Random Number Generator (DRNG) hardware implementation and can be used to generate high-quality keys for encryption purposes.

In addition to FDE, *Intel® Total Memory Encryption (Intel® TME)* helps protect platform memory (DRAM and NVRAM) on lost or stolen machines against physical attacks. *Intel® TME* encrypts all system memory and enables confidentiality of DRAM/NVRAM outside the SoC package. *Intel® TME* is an out-of-box capability that can be provided by OEMs for differentiation. It enhances memory data protection for end users to reduce concerns about sensitive and confidential data being stolen out of memory if their enabled devices are lost or stolen. *Intel® TME* is aimed at providing protection from tampering attacks such as 'Cold Boot' attacks.

Use of Cryptography (CR4.3)

IEC62443 recommends the use of established and tested encryption and hash algorithms such as the Advanced Encryption Standard (AES) and the secure hash algorithm (SHA) series. An effective random number generator is also needed to generate keys. *Intel® Secure Key* incorporates both *Intel® 64* and *IA-32* architectures' instructions RDRAND and RDSEED and the underlying Digital Random Number Generator (DRND) hardware implementation, which are useful in generating high-quality keys for cryptography usage. It is an SP800-90 compliant RNG solution that can be Cryptographic Algorithm Validation System (CAVS) certified, and thus permitted as a component of a FIPS-certified cryptographic module (such as FIPS-140-2 certification).

Recommended reading: https://www.intel.com/content/www/us/en/developer/articles/guide/intel-digital-random-number-generator-drng-software-implementation-guide.html

To support performance acceleration of Secure Hash Algorithm (SHA), Intel® architecture processors include SSE base instructions to support up to SHA-384, with reference to the FIPS Pub 180-2 Secure Hash Standard.

To support Public-key Infrastructure cryptography, "big-number" multiplication ISA was introduced in Intel® architecture processors (such as the AVX512), combined with software optimization techniques such as multi-buffer processing, to provide significant performance improvements in RSA and ECC cryptographic processing.

Use Control (FR2)

The objective is to protect against unauthorized actions on the components' resource, which includes enforcing security policy for usage of mobile code technologies such as control execution of the mobile code and integrity check prior to code execution.

Intel® SGX offers hardware-based memory encryption that isolates specific application code and data in memory. It allows user-level code that includes the allocation of private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels.

Mode-based execution control (MBEC) provides an extra layer of protection from malware attacks in virtualized environments. It enables hypervisors to more reliably and efficiently verify and enforce the integrity of kernel-level code.

Recommended reading: https://www.intel.com/content/dam/www/central-libraries/us/en/documents/intel-virtualization-technologies-white-paper.pdf

Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x) provides hardware-based supports for virtualization of platforms enabling the running of multiple OSes and applications in independent partitions. It enables simple, robust, and reliable virtual machine management (VMM) software.

Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) further helps enhance the security of virtualized environment with the ability to isolate and restrict device accesses to the resources owned by the partition management the device through I/O virtualization models.

System Integrity (FR3)

The objective is to protect the integrity of the IACS against manipulation.

Establishing a host intrusion detection system is critical to meet the requirement stated in SR3.2 RE 2 – Central Management and Reporting of Malicious Code Protection, and SR3.4 RE 1 – Automated Notification About Integrity Violation.

Intel® Trusted Edge Platform (Intel® TEP) reference software stack offers hardware-based remote attestation system that enables runtime detection and reporting of system integrity check on the host platform.

Protection from Malicious Code (CR3.2)

Intel® OS Guard, a.k.a. Supervisor-Mode Execution Prevention (SMEP), is a security technology that restricts the operating system from directly executing application code, even speculatively, thereby making branch target injection attacks on the OS substantially more difficult.

When UMIP is enabled, a general protection fault is issued if the SGDT, SLDT, SIDT, SMSW or STR instructions are executed in user mode. These instructions unnecessarily expose information about the hardware state.

To protect against common and emerging software attacks, Intel hardware security supports additional levels of verification of software while preserving the performance. *Intel® Threat Detection Technology (Intel® TDT)* provides hardware-based threat detection to help detect the latest threats such as crypto-mining and ransomware without an impact on performance.

Intel® Control-Flow Enforcement Technology (Intel® CET)[1], is designed to protect against the misuse of legitimate code through control-flow hijacking attacks – widely used techniques in large classes of malware. *Intel® CET* offers software developers two key capabilities to help defend against control-flow hijacking malware; indirect branch tracking and shadow stack.

Support for Update (CR3.10)

Host devices may require updates or upgraded software and firmware over the lifetime of its operation. To help ensure more secure and safe updating or upgrading operations, it is recommended that host devices validate the authenticity and integrity of the software update or upgrade prior to installation. *Intel Firmware Update/Recovery* provides the ability to update the firmware on a host device and also recover from a firmware failure. Firmware updates are deployed and signed by asset owners and applied in a fault tolerant manner. In case of power interruption or failure during the update, the system automatically boots to a last known 'good state' and restarts the firmware update process – all without human intervention.

Recommended reading: https://www.intel.com/content/dam/www/public/us/en/documents/guides/iot-security-capabilities-guide.pdf

Integrity of the Boot Process (CR3.13)

To help ensure that the host component's security functionality has not been compromised, it is necessary that the host component's software and firmware has not been tampered with. Verification must be performed to validate the integrity and authenticity of the firmware and/or software prior to the boot process. It is also recommended to use product supplier's Root of Trust to verify the authenticity of the firmware, software and configuration data needed for the boot process.

Intel® Boot Guard technology provides hardware-based boot integrity protection that prevents malicious firmware and software from taking over boot blocks. It cryptographically verifies the first portion of OEM pre-OS bootloader code executing out of reset. It detects unauthorized boot block and disallows it to execute. It also includes measured boot, which measures the initial boot block into platform's secure storage device, TPM. The measurement can be used for attestation at a later stage.

Restricted Data Flow (FR5)

This is related to network data flow.

Timely Response to Events (FR6)

The object is to monitor the operation of the components of the IACS, and respond to incidents such as security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective active when incidents are discovered.

Intel® Runtime BIOS Resilience and *Intel® System Resources Defense* aims to help reduce the risk of malware attacks on System Management Mode (SMM) environments at runtime and provides timely trusted audit reports of privileged system hardware resource accessed by the SMI handler. Using the *Intel® System Security Report* feature, the OS can enforce a more comprehensive security policy that includes hardware, firmware and software, including the SMM policy being enforced by *Intel® Runtime BIOS Resilience* and *Intel® System Resources Defense*. *Intel® System Security Report* provides visibility to the OS that the OS can use to make decisions on its security policy.

Resource Availability (FR7)

The objective is to ensure availability of components.

Control System Recovery and Reconstitution (CR7.4)

One of the components' requirements is to support failback recovery. "The IACS is recommended to have system failover and automatic fallback to previous working status when device fails to boot when critical changes are made to the system. *Intel Firmware Restart/Recovery,* which complies with NIST SP800-193 Platform Firmware Resiliency, provides the abilities to update the firmware on an IACS/OT system, and also recover from firmware failure.

Benefits of Working with TÜV SÜD

TÜV SÜD has been an active participant in the development of cybersecurity frameworks applicable to the deployment and use of IACSs. TÜV SÜD industrial cybersecurity experts have been involved in key standards development activities, including most of the individual standards in the IEC 62443 series, and remain engaged in ongoing regulatory and standards development activities related to industrial cybersecurity.

In addition to IEC 62443 certification, TÜV SÜD services also include the preparation of a comprehensive gap analysis that can serve as a roadmap for companies looking to implement the IEC 62443 framework. TÜV SÜD also offers industrial cybersecurity workshops for improved understanding of the standard, as well as customized trainings to further explore specific requirements or situations.

As a result, TÜV SÜD are well positioned to help organizations gain a thorough understanding of the IEC 62443 requirements as well as future regulatory developments. In turn, customers are able to design and implement highly effective systems for industrial security that meet the requirements for certification while also affirming the organization's strong commitment to security.

Intel would also like to acknowledge TÜV SÜD for the excellent contribution of content for this white paper.

Intel's Security-First Pledge: Strengthening Our Commitment

System trust is rooted in security – if the hardware isn't secure, then a system cannot be secure. Securing hardware is foundational to all security efforts.

At Intel, our goal is to build the most secure hardware on the planet, from world-class CPUs to XPUs and related technology, enabled by software. Plus, we have sophisticated systems to find and address security vulnerabilities in our products.

Intel's security solutions meet specific challenges centered around three key priorities:

Foundational Security, Workload and Data Protection, and Software Reliability.

Together, these innovations help drive our vision for a world where all data is encrypted.

[1] https://newsroom.intel.com/editorials/intel-cet-answers-call-protect-common-malware-threats.

Other references:

i. Intel's Security-First Pledge: Strengthening Our Commitment

ii. Hardware-enabled Security Technology

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

No product or component can be absolutely secure.

All product plans and roadmaps are subject to change without notice.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Document number: 732195, Revision 1.0.1, July 2022