ISA GLOBAL CYBERSECURITY ALLIANCE

IIoT Component Certification Based on the 62443 Standard

Co-developed by:

ISASecure®

THE TIME IS NOW

Version 1.4
October 7 2021

www.isa.org/ISAGCA

Table of Contents

TABLE OF TABLES

TABLE OF FIGURES

Co-developed by:

ISASecurity Compliance Institute

IIoT Component Certification Based on the 62443 Standard

Version 1.4
October 7 2021

Executive Summary

The ISA Global Security Alliance and the ISA Security Compliance Institute that sponsored this study, see an urgent need for industry-vetted IIoT (Industrial Internet of Things) certification programs. To accelerate the development of such programs, they launched a joint IIoT Certification Study, for which Phase 1 results are reported in the present document. The goal for the overall study is to determine the applicability of IEC 62443 standards and certifications to IIoT components and systems. This includes examining whether existing 62443 requirements and methods for validating these requirements under existing certification programs, are necessary and sufficient for the IIoT environment. Phase 1 of the study addresses IIoT devices and IIoT gateways, where these components are physical devices and have a direct connection to an untrusted network, usually the Internet. Later phases of this project will consider overall IIoT systems and other types of IIoT components.

The study concluded that a certification that addresses such IIoT devices and gateways could be constructed based upon existing 62443-4-2 certification programs, by incorporating a manageable number of program enhancements. The delta defined in this paper to existing 62443 certification programs is offered to contribute to the dialog regarding application and revision of 62443 for IIoT, looking forward to future IIoT product certifications based solely on that standard. In the near term, it provides a proposal for standardization and therefore the possibility of comparison across IIoT certification offerings, where such certifications may be offered prior to availability of 62443 updates for IIoT. Certification enhancements described in this document add a small number of functional requirements to those in 62443-4-2, add process requirements to 62443-4-1, and identify IIoT-specific guidance for certifier validation of existing functional requirements and process requirements. Certifier validation enhancements include strengthening the validation that a product maintains its security posture over time in accordance with 62443-4-1. Future project phases are expected to examine other parts of 62443.

Given the current broad acceptance of known cryptographic and hardware mechanisms considered appropriate and commonly accepted for the IIoT environment, it is likely that a credible security certification program will need to acknowledge those mechanisms in some manner. The recommendation here is that for selected mechanism-agnostic 62443-4-2 requirements, implementations equivalent or better than commonly accepted IIoT practices be required for certification. References to such practices would be provided and vetted by certification scheme owners; any organization may participate in their development and maintenance.

Of the fifty-two program enhancements identified, thirty-two identify potential enhancements to the 62443 standards; the others address how certifiers validate existing 62443 requirements.

Ten of these fifty-two enhancements address internal compartmentalization of a component.

Beyond existing 62443-4-2 requirements, five functional requirements related to compartmentalization and eleven other functional requirements are recommended as criteria for certification of IIoT devices and/or gateways. These requirements are also recommended for consideration as modifications to 62443 for IIoT. For both IIoT devices and gateways, a direct Internet connection, potential remote/unprotected physical location, and low cost, require components to protect themselves. This drives requirements that specify controls on management/configuration interfaces, authentication of non-human users from untrusted networks, remote update/upgrade, enable/disable of update/upgrade, enable/disable Internet connection, monitoring for component presence, and reverse engineering mitigations. For IIoT devices, scaling to a large quantity of devices is an additional characteristic that drives requirements for unique initial passwords/keys per device, default secure configuration, and maintaining user settings on update/upgrade. The common use of platform-sharing technologies, and the degree of exposure of associated host devices to their adversaries, also drives adoption of requirements for secure compartmentalized architectures. These characteristics of IIoT were not commonplace for industrial automation and control systems (IACS) at the time of development of the current 62443 standard.

Two certification tiers are recommended; new functional requirements have been assigned to either the Core or Advanced tier. As detailed in 4.4.4, the Core tier also requires conformance to all existing 62443-4-2 capability security level 2 requirements with one exception for IIoT gateways, and two for IIoT devices, and adds a few requirements from levels 3 and 4 in acknowledgment of the threat posed by the component's Internet connection. The Advanced tier requires conformance to all capability security level 4 requirements with four exceptions.

This work was based upon an analysis of six industry/government sources on the topic of IoT/IIoT security, and the expertise of the ISAGCA/ISCI project team. Candidate IIoT device or gateway properties from these sources were mapped against 62443-4-2; a significant number of the IIoT properties were found there. Many of those found were at high capability security levels. Properties not found in 62443-4-2 were potential gaps, examined by the team to determine whether they should represent a property for IIoT component certification, and/or for an IIoT security standard.

The 62443 standards development organization ISA99 is investigating IIoT under Working Group 9. This ISAGCA/ISCI effort has closely followed that work, and will donate the results described here to WG9. These results are also offered as input for developers of 62443 certification programs.

Forward

This report was developed as a joint project of the ISA Global Security Alliance (ISAGCA) and the ISA Security Compliance Institute (ISCI). Further information about these organizations can be found on their web sites, respectively http://www.ISASecure.org and https://isaautomation.isa.org/cybersecurity-alliance/.

ISAGCA and ISCI gratefully acknowledge the participation of their members, and of other members of the 62443 community, in this effort.

1 Scope

1.1 Study scope

This document reports the results of the initial phase of a project to determine the applicability of the ANSI/ISA/IEC 62443 standards and corresponding certifications, to types of IIoT components and systems that have high priority for project sponsors. This initial report addresses two types of components: IIoT devices and IIoT gateways. Industry definitions for these terms are found in Section 3.1. Future phases of this effort will address certification of other IIoT component types, and IIoT systems. IIoT systems are industrial automation and control systems that may include IIoT devices and gateways, other component types, and cloud-based functionality.

Project sponsors are the ISA Security Compliance Institute (ISCI), which develops certification programs based on ANSI/ISA/IEC 62443, and the ISA Global Security Alliance (ISAGCA), which champions the adoption of that standard. These results describe potential gaps found in the existing standards and certification program approaches, and recommends next steps toward their resolution.

Whereas the industry definitions for IIoT device and IIoT gateway do not inherently imply a direct connection to the Internet or other untrusted network, the IIoT components for which certification is examined in this study, are assumed to have such a direct connection. It is assumed that existing 62443-4-2 conformance certification programs are appropriate for certifying IIoT components without such a direct connection, not requiring the certification program enhancements described in the present document. While the expression "Internet connection" may be used for brevity – it is understood to also include the case of a direct connection to other untrusted networks.
The report assesses applicability to these components of IEC 62443-4-2, of certification to IEC 62443-4-2 in general, and of ISASecure® CSA (Component Security Assurance) certification in particular.

These results would not apply as-is to software-only products (such as software-only gateways). This is because recommended certification criteria here incorporate 62443-4-2 requirements intended for physical devices. A future task could adjust these recommendations to cover the software-only case, by combining the 62443-4-2 approach for software applications, with 62443-4-2 function-specific requirements for the other 62443-4-2 component types. For example, 62443-4-2 requirements that apply to physical network devices for restricting data flow, would also need to be met by software-only gateways.

The 62443 standards development organization ISA99 is investigating IIoT under Working Group 9. This ISAGCA/ISCI effort has closely followed that work, and will donate the results described here to WG9. These results are also offered as input for all developers of 62443 certification programs.

1.2 Document overview

Section 2 *References* provides references for documents analyzed in the course of the study, which include 62443 standards as well as industry and government studies of IoT and IIoT security.

Section 3 *Definitions and abbreviations* provides terms, definitions, and abbreviations as used in this document.

Section 4 *Component analysis* contains the main body of results for this study.

The main body of the document is followed by supporting appendices as follows.

Appendix 1 – *Industry/government sources* describes the six industry/government source documents upon which this study is primarily based.

Appendix 2 – *Summary of detailed recommendations* lists all specific recommendations of this study, and indicates whether they are potential modifications to certification programs, potential modifications to 62443 standards, or both. References are provided to the body of the report where each recommendation is discussed.

Appendices 3 through 6 provide detailed data to which the body of the report refers, that further illustrates the study process and results.

2 References

2.1 62443 standards and technical reports

[ANSI/ISA-62443-1-1] ANSI/ISA 62443-1-1 (99.01.01) - 2007, *Security for industrial automation and control systems Part 1-1: Terminology, concepts and models*

[IEC 62443-1-1] IEC TS 62443-1-1:2009 I*ndustrial communication networks - Network and system security Part 1-1: Terminology, concepts and models*

[ANSI/ISA 62443-2-3] ANSI/ISA-TR62443-2-3-2015 *Security for industrial automation and control systems Part 2-3: Patch management In the IACS environment*

[IEC 62443-2-4] IEC 62443-2-4: 2015 *Security for industrial automation and control systems Part 2-4: Security program requirements for IACS service providers*

[ANSI/ISA-62443-3-2] ANSI/ISA-62443-3-2-2020 *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design*

[IEC 62443-3-2] IEC 62443-2: 2020 *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design*

[ANSI/ISA-62443-3-3] ANSI/ISA 62443-3-3 (99.03.03) - 2013, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

[IEC 62443-3-3] IEC 62443-3-3: 2013 *Industrial communication networks - Network and system security Part 3-3: System security requirements and security levels*

[ANSI/ISA-62443-4-1] ANSI/ISA-62443-4-1-2018 *Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements*

[IEC 62443-4-1] IEC 62443-4-1:2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[ANSI/ISA-62443-4-2] ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[IEC 62443-4-2] IEC 62443-4-2:2019 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

2.2 Other international standards

[ISO/IEC 11889] ISO/IEC 11889-1: 2015 *Information technology – Trusted platform module library – Part 1: Architecture*

[ISO/IEC 29115] ISO/IEC 29115: 2013 *Information technology – Security techniques - Entity authentication assurance framework*

2.3 ISA99 WG9 technical report drafts

Definitions from the first of these two drafts are included in this report.

[IIoT TR WG9 200806] Technical report – considerations and 62443 guidance for asset owners implementing IIoT, ISA99 WG9 working draft, filename: *WG9 IIoT WD1 draft August 6 2020.docx,* retrieved Aug 22, 2020, ISA99 WG9 Sharepoint site

[IIoT TR WG9 200525] Technical report – Application of the IEC 62443 standards to the Industrial Internet of Things, ISA99 WG9 working draft, filename: *WG9 TR May 25, 2021.docx,* retrieved July 21, 2021, ISA99 WG9 Sharepoint site

2.4 Industry and government resources

The topic of IoT security has been studied by many stakeholders. One effort analyzed roughly 100 relevant documents from 50 organizations. The resources enumerated in this section were judged as representative and particularly relevant to the goals of the present document. They are described in Section 5 – Appendix 1 and were analyzed in detail for this study.

2.4.1
IIoT resources

[IICRA] Industrial Internet Consortium Reference Architecture, available at https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[IICSF] Industrial Internet Consortium Security Framework, available at https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

2.4.2
IoT resources

[CTIA] CTIA Cybersecurity Test Plan for IoT Devices v1.2, available at https://www.ctia.org/certification-resources

[MS7] The Seven Properties of Highly Secure Devices, Galen Hunt, George Letey, and Edmund B. Nightingale, Microsoft Research NExT Operating Systems Technologies Group

[ENISA] ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (2017)

[NIST8259A] NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline

[NISTCAT] NIST catalog of IoT device cybersecurity capabilities available at https://pages.nist.gov/FederalProfile-8259A/

2.5 ISASecure certification specifications

[CSA-100] *ISCI Component Security Assurance – ISASecure Certification Scheme* v4.3, as specified at http://www.ISASecure.org

[CSA-300] *ISCI Component Security Assurance – ISASecure Certification Requirements* v4.2, as specified at http://www.ISASecure.org

[CSA-301] *ISCI Component Security Assurance – Maintenance of ISASecure Certification* v3.2, as specified at http://www.ISASecure.org

[CSA-311] *ISCI Component Security Assurance – Functional security assessment for components* v1.11, as specified at http://www.ISASecure.org

[CSA-312] *ISCI Component Security Assurance – Security development artifacts for components* v3.2, as specified at http://www.ISASecure.org

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme* v2.1, as specified at http://www.ISASecure.org

[SDLA-300] *ISCI Security Development Lifecycle Assurance – Requirements for ISASecure Certification and Maintenance of Certification* v1.9, as specified at http://www.ISASecure.org

[SDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment* v5.7, as specified at http://www.ISASecure.org

[SSA-100] *ISCI System Security Assurance – ISASecure certification scheme* v3.1, as specified at http://www.ISASecure.org

3 Definitions and abbreviations

3.1 Definitions

Where concepts are used in common with the draft WG9 technical report noted in the references section, these draft terms and definitions are noted below.

3.1.1
asset

physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization

[SOURCE 62443-1-1]

3.1.2
capability security level

security level that a component or system can provide when properly configured and integrated

NOTE This type of security level states that a particular component or system is capable of meeting a target security level natively without additional compensating countermeasures when properly configured and integrated.

[SOURCE text in 62443-3-3 A.2.2]

3.1.3
certification scheme

certification system related to specified products, to which the same specified requirements, specific rules and procedures apply

NOTE 1 A “certification system” is a “conformity assessment system”, which is defined in ISO/IEC 17000:2020 as “demonstration that specified requirements are fulfilled.”

NOTE 2 The rules, procedures and management for implementing product, process and service certification are stipulated by the certification scheme.

[SOURCE ISO/IEC 17065, notes adapted]

3.1.4
certification scheme owner

person or organization responsible for developing and maintaining a specific certification scheme

[SOURCE ISO/IEC 17065]

3.1.5
certifier validation activity

method a certifier uses to validate that a product or process requirement is met during a certification evaluation

3.1.6
component

entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

[SOURCE 62443-4-2]

3.1.7
control system

hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

[SOURCE 62443-4-2, note from [SSA-100]]

3.1.8
compartmentalization

use of any method or technology to separate multiple functions during execution, where separation limits their interactions to those intended

NOTE Examples of compartmentalization methods are containerization, virtual machines, hardware separation (by chip or board), enforced memory allocation, software-based microsegmentation.

3.1.9
embedded device

special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

[SOURCE 62443-4-2]

3.1.10
essential function

function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential.

[SOURCE 62443-4-2]

3.1.11
foundational requirement

essential service, capability, feature, or activity that serves as a basis for derivation of detailed requirements

[SOURCE 62443-1-2 (Draft)]

3.1.12
functional security assessment

assessment of a defined list of security features for a control system, embedded device, or other control system component

[SOURCE [CSA-100]]

3.1.13
host device

general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

[SOURCE 62443-4-2]

3.1.14
IIoT (Industrial Internet of Things)

system that connects and integrates industrial control systems with enterprise systems, business processes and analytics

[SOURCE IIC The Industrial Internet of Things G8: Vocabulary V2.1]

3.1.15
IIoT device

entity of an IIoT system that interacts and communicates with the physical world through sensing or actuating

NOTE 1 An IIoT device may be a sensor or an actuator, or may communicate with sensors or actuators.

NOTE 2 Examples of IIoT devices that communicate with sensors or actuators are a PLC with an internet connection, and an IIoT integrated edge computing device.

NOTE 3 This industry definition does not imply that an IIoT device is always connected directly (or indirectly) to the Internet or other untrusted network. However, the recommendations in this paper apply specifically to IIoT devices with a direct connection to the Internet or other untrusted network.

NOTE 4 Alternative definitions have been proposed such that an IIoT device is by definition directly connected to an untrusted network. An example definition of IIoT device that assumes this, and also spells out the implications of "IIoT system" and "through sensing or actuating" from the above definition is:
"entity that is a sensor or actuator for a physical process, or communicates with sensors or actuators for a physical

process, that directly connects to an untrusted network to support and/or use data collection and analytic functions resident on that network."

[WG9 SOURCE ISO/IEC FDIS 20924, 3.2.4 (for IoT), NOTE 1 amended, NOTES 2-4 added]

3.1.16
IIoT gateway

entity of an IIoT system that connects one or more proximity networks and the IIoT devices on those networks to each other and to one or more access networks

NOTE 1 From [IICRA]: The proximity network connects the sensors, actuators, devices, control systems and assets, collectively called edge nodes.

NOTE 2 The access network may be the Internet or other untrusted network. Functions hosted on an IIoT gateway device may also include data translation, processing and control.

NOTE 3 An IIoT gateway device is a type of network device (see 3.1.21).

NOTE 4 This industry definition does not imply that an IIoT gateway is always connected directly (or indirectly) to the Internet or other untrusted network. However, the recommendations in this paper apply specifically to IIoT gateways with a direct connection to the Internet or other untrusted network.

[WG9 SOURCE ISO/IEC FDIS 20924, 3.2.6 (for IoT), notes added]

3.1.17
IIoT integrated edge computing device

IIoT device that communicates with other IIoT devices and includes either or both of: environment for hosting application software or pre-defined application software

NOTE 1 The reader is advised that terminology usage in the IoT arena is not standardized at this time, so that other sources may use other terms for this concept.

NOTE 2 Examples of application software are analytics and data filtering. Device may include IIoT gateway functionality to transmit sensor information or derivative information to the cloud, may provide instructions to sensors, actuators, controllers, or other IIoT integrated edge computing devices, application environment may consist of virtual machines and/or a container environment, may use wired communication, or cellular or other wireless communication.

NOTE 3 An IIoT integrated edge computing device may or may not be directly connected to an untrusted network. However, the recommendations in this paper apply specifically to IIoT integrated edge computing devices with a direct connection to the Internet or other untrusted network. A typical case includes sensor connections providing data for a "local" processing capability on the device, and a connection to the cloud for "remote" processing of some version of that data. In this example, the IIoT integrated edge computing device would meet 62443 definitions for network device and host (if it includes an environment for hosting application software) or software application (if it includes pre-defined applications).

3.1.18
IIoT system

system providing functionalities of Industrial Internet of Things

NOTE IIoT system is inclusive of IIoT devices, IIoT gateways, sensors, and actuators.

[WG9 SOURCE ISO/IEC FDIS 20924, 3.2.7 (for IoT)]

3.1.19
industrial automation and control system

collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation

[SOURCE 62443-4-2]

3.1.20
internal zone

security zone that exists within a single component

3.1.21
network device

device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

NOTE   Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

[SOURCE 62443-4-2]

3.1.22
proximity network

network that connects the sensors, actuators, devices, control systems and assets

[SOURCE text in [IICRA]]

3.1.23
security zone

grouping of logical or physical assets that share common security requirements

NOTE A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

[SOURCE 62443-3-3]

3.1.24
sensor and actuator

measuring or actuating elements connected to process equipment and to the control system

[SOURCE 62443-1-1]

3.1.25
software application
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

NOTE 1 Software applications typically execute on host devices or embedded devices.

NOTE 2 Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

[SOURCE 62443-4-2]

3.1.26
scheme owner
person or organization responsible for developing and maintaining a specific certification scheme

NOTE The scheme owner can be the certification body itself, a governmental authority, a trade association, a group of certification bodies or others.

[SOURCE ISO/IEC 17065]

3.1.27
supplier
manufacturer of hardware or software product used in an IACS

[SOURCE 62443-2-1]

3.1.28
trust
confidence that an operation, data transaction source, network or software process can be relied upon to behave as expected

NOTE 1 Generally, an entity can be said to 'trust' a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.

NOTE 2 This trust may apply only for some specific function.

NOTE 3 The only use in this document of the term "trust" that relies upon the above definition, is for the definition of the term "untrusted" in 3.1.31. All other appearances of the term "trust" in this document are in commonly used compound terms whose definitions do not rely on the definition of trust: TEE, TPM, TCB, trust boundary, and root of trust.

NOTE 4 ISA99 WG9 has discussed use of the alternative term "trustworthiness" from ISO/IEC 30145-2:2020, 3.9 with definition "ability to meet stakeholder expectations in a verifiable way."

[SOURCE 62443-4-2, NOTE 3 and NOTE 4 added]

3.1.29
trusted execution environment
area on the main processor of a device that is separated from the system's main operating system, with goal to ensure that data is stored, processed and protected in a secure environment

3.1.30
trusted platform module
tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of sensitive information, such as passwords and cryptographic keys

[SOURCE NIST SP 88-147]

3.1.31
untrusted
not meeting predefined requirements to be trusted

NOTE 1 An entity may simply be declared as untrusted.

NOTE 2 The use of this term in this document is limited to the phase "untrusted network" or "untrusted connection." Typically, this network will be the Internet, and this connection an Internet connection. The Internet is also "untrustworthy" per the definition of "trustworthiness" in NOTE 4 under 3.1.28.

[SOURCE 62443-4-2 NOTE 2 added]

3.1.32
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues

[SOURCE 62443-4-2]

3.1.33
upgrade
incremental hardware or software change in order to add new features

[SOURCE 62443-4-2]

3.1.34
version (of a product)
well defined release of a system, embedded device, or other control system component product, typically identified by a release number

3.1.35
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document.

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CCSC	common component security constraint
CPU	central processing unit
CR	component requirement
CSA	Component Security Assurance
CSRF	cross-site request forgery
CTest	certifier test
CTIA	Cellular Telecommunications Industry Association
CWE	Common Weakness Enumeration
D	IIoT device
Doc	documentation
DoS	denial of service
DM	security defect management
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	embedded device requirement
ENISA	European Network and Information Security Agency
EU	European Union
FDIS	Final Draft International Standard
FIPS	Federal Information Processing Standards
5G	Fifth Generation
FR	Foundational Requirement
G	IIoT gateway
GPS	Global Positioning System
HDR	host device requirement
HMI	human machine interface
HSM	Hardware Security Module
IAC	identification and authentication control
IACS	industrial automation and control system(s)
IACS-H	IACS with high capability security level
IEC	International Electrotechnical Commission
IIC	Industrial Internet Consortium
IoT	Internet of Things
IIoT	Industrial Internet of Things
IPsec	Internet Protocol Security
ISA	International Society of Automation
ISAGCA	ISA Global Security Alliance
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
LTE	Long Term Evolution
MoC	management of change
NA	not applicable
NDR	network device requirement
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OS	operating system
PEAP	Protected Extensible Authentication Protocol
PKCS1	Public Key Cryptography Standard 1
PKI	public key infrastructure
PLC	programmable logic controller
PtW	permit to work
RE	requirement enhancement
RSASSA	RSA Signature Scheme with Appendix
SD	secure by design
SDLA	Security Development Lifecycle Assurance
SDO	standards development organization
SG	security guidelines
SL-C	capability security level
SM	security management
SP	security program, Special Publication
SQL	Structured Query Language
SR	specification of security requirements, system requirement
SSA	System Security Assurance
SSH	Secure Shell
STest	supplier test
SUM	security update management
SVV	security verification and validation testing
TCB	trusted computing base
TEE	trusted execution environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UC	use control
US	United States
WG	working group
XSS	cross-site scripting
ZCR	zone and conduit requirement

4 Component Analysis

This section contains the main body of results for this study. It is organized as follows.

Section 4.1 *Overview of recommendations* briefly describes the study and highest-level recommendations for use of the study results.

Section 4.2 *Outline of enhanced certification criteria* enumerates and describes the types of enhancements recommended to existing 62443-4-2 certification programs, to certify IIoT devices and IIoT gateways.

Sections 4.3-4.7 describe these recommendations in detail, organized into sections by type of enhancement. For some enhancements, related modifications to 62443 are also recommended for consideration.

Section 4.8 describes the approach taken to arrive at the recommendations in this report, and alternative approaches considered.

4.1 Overview of recommendations

This effort analyzed a number of industry/government sources on the topics of IoT and IIoT security (described in Section 5 - Appendix 1). The security properties described in those sources were mapped to 62443-4-2 requirements, noting that 62443-4-2 incorporates 62443-4-1 requirements by reference. A large number of the properties described in the IoT/IIoT sources, are requirements found in 62443-4-2. Among those not found in 62443-4-2, a subset was judged by the project team to merit inclusion as security certification criteria for either IIoT devices, IIoT gateways, or both. The study also considered the question of how existing requirements in 62443-4-2 should be selected for certification of IIoT devices and gateways. For topics where differing points of view remained among the project team, a recommendation is made and alternative points of view also presented.

While the focus of the study was certification criteria, consideration was also given to whether any modifications are recommended for the 62443 standards in light of study results. Section 4.8 below further describes the study methodology.

The following are high-level recommendations from the study regarding development of certification programs for IIoT devices and gateways:

- **Scheme owners for 62443-4-2 certification schemes consider the enhanced certification criteria described in this report for certifying IIoT devices and IIoT gateways.** Owners of existing 62443 certification schemes that expect to be certifying IIoT devices or gateways, should consider developing certification schemes designed specifically for these products, as defined in this report. Such schemes would be based on existing 62443-4-2 certifications and include enhanced certification criteria as outlined in 4.2 below. One goal for the present effort is to encourage a common approach to certifying IIoT devices and gateways, where such certifications are offered prior to availability of 62443 updates for IIoT. Under the approach described in the present document, standard 62443 requirements are the basis for an IIoT certification program; unique characteristics of IIoT are addressed by a small number of well-defined functional and process requirement additions, together with guidance for certifiers regarding interpretation for IIoT of existing 62443 requirements. The program development effort for certification scheme owners would include consideration of the set of new certification criteria recommended in this document, and development of further requirement details and specifications for certifier validation of the new requirements.
- **Apply existing 62443-4-2 requirements by capability security level in accordance with the known IIoT threat environment.** Section 4.4.3 defines certification tiers Core and Advanced. Definition of the Core tier takes 62443-4-2 capability security level 2 as a starting point. The definition for Advanced tier starts with capability security level 4. Core tier defines minimum IIoT device or gateway certification criteria, which also

are required for Advanced tier. All existing 62443-4-2 functional requirements at all levels are applicable for IIoT device and gateway certification for the Advanced tier, with four exceptions as described in 4.4.4. All security capability level 2 requirements are required for Core certification, with two exceptions for IIoT devices and one for IIoT gateways, also as described in 4.4.4. In addition, specifically due to a direct interface to an untrusted network, a few level 3 and 4 requirements appear in the Core tier and therefore are mandatory certification criteria for an IIoT device or gateway.

- **SDO ISA99 consider 62443 modifications toward fully standards-based IIoT certifications.** In the course of this study, some criteria identified as certification requirements for IIoT devices or gateways, were felt to merit consideration as amendments to 62443-4-2 or 62443-4-1, and/or as additions to another new or existing part of the 62443 standard. Via the present report, these potential amendments are submitted to ISA99 WG9 as input to their efforts regarding the application of 62443 to IIoT. Some of these criteria are unique to IIoT environments; some may be applicable for all IACS components at high capability security levels. These criteria are mentioned in context throughout this report and summarized in Section 6 - Appendix 2. The consideration of how the 62443 series or its parts would be structured to incorporate these potential modifications for IIoT was not addressed by this effort. However, it is a goal for this effort to contribute to the dialog regarding application and revision of 62443 for IIoT, looking forward to future fully-standards-based IIoT product certifications.

4.2 Outline of enhanced certification criteria

This section enumerates and describes the types of enhancements recommended to existing 62443-4-2 certification programs, to certify IIoT devices and IIoT gateways that have a direct connection to an untrusted network. The security context for these components as described in 4.3.1, drives these recommendations.

The following figure illustrates recommended enhancements to existing 62443-4-2 certification programs for application to IIoT devices and gateways. The upper part of the figure shows the two major elements of existing certifications. These are verification of functional requirements in 62443-4-2, and of product development lifecycle requirements in 62443-4-1. 62443-4-2 requires conformance to 62443-4-1 for the product development lifecycle of a product. The lower part of the figure shows the types of enhancements that the present report recommends to existing 62443-4-2 certification programs, for application to IIoT devices and gateways.

Briefly, the certification program enhancements in Figure 1 are described as follows. These enhancements and related rationale, are

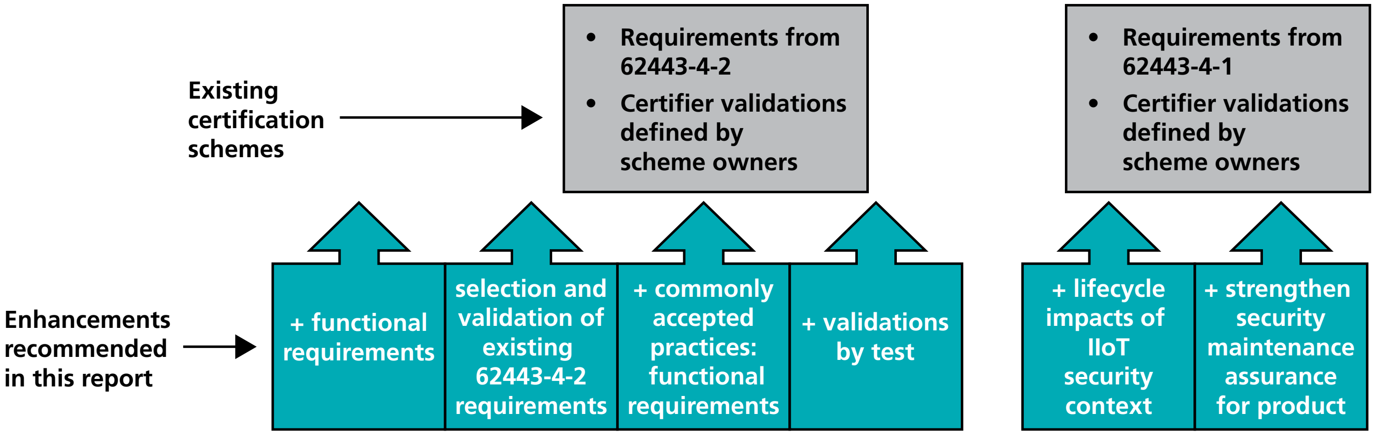
Existing certification schemes
Requirements from 62443-4-2
Certifier validations defined by scheme owners
Requirements from 62443-4-1
Certifier validations defined by scheme owners
Enhancements recommended in this report
+ functional requirements
selection and validation of existing 62443-4-2 requirements
+ commonly accepted practices: functional requirements
+ validations by test
+ lifecycle impacts of IIoT security context
+ strengthen security maintenance assurance for product

Figure 1. Certification enhancements for IIoT devices and gateways

further described in the remainder of Section 4 of this document in the sub sections noted in parentheses below. Section 6 – Appendix 2 a contains a consolidated reference list of all recommended certification program enhancements discussed in this document.

- *Additional functional requirements:* Add functional requirements not in 62443-4-2, as new certification criteria. Five sub-requirements for compartmentalization and eleven other functional requirements fall in this category. (4.3)
- *Selection and validation of 62443-4-2 requirements:* Define Core and Advanced certification tiers, where Core requires all capability security level 2 requirements in 62443-4-2 with a few exceptions, plus a few requirements from higher capability security levels. Advanced tier includes all 62443-4-2 requirements except four. IIoT-specific validation guidance for the certifier is identified for a few existing 62443-4-2 requirements, to specifically point out implications of a requirement for the IIoT environment, that may not be encountered in traditional IACS environments. This includes cases where existing 62443-4-2 zone/conduit and network segmentation requirements are interpreted to apply to compartmentalization within a component. (4.3.4.2.1, 4.3.4.2.2, 4.4)
- *Commonly accepted practices:* For selected mechanism-agnostic 62443-4-2 functional requirements, require that mechanisms used to conform to these requirements be consistent with commonly accepted industry practices for IIoT. (4.5)
- *Additional validations by test:* Identify selected functional requirements as requiring hands-on functional testing by the certifier, or review by the certifier of supplier test artifacts. Current certification schemes may permit validation of some of these requirements by other methods, such as user document review. (4.6)

Section 4.7 describes enhancements to certification criteria that address secure product development lifecycle process.

- *Lifecycle impacts of IIoT security context (before product release):* Add process requirement enhancements for: inclusion of device failures in the threat model, identifying IIoT-specific security context elements, product requirement selection, interactions with cloud development process, documentation requirements for cloud dependencies (4.7.1 - 4.7.4). Note lifecycle certification enhancements related to compartmentalization are recommended in 4.3.4.2.3 under the discussion of the compartmentalization topic.
- *Strengthen security maintenance assurance for product:* Add periodic audit of seven specified 62443-4-1 process requirements regarding maintenance of product security post-release, as applied to certified products, to maintain product certification. Require proactive notification of availability of updates/upgrades and advance notification of withdrawal of a product from the update process (4.7.5 - 4.7.7).

4.3 Functional requirements not in 62443-4-2

This section recommends functional requirements not found in 62443-4-2, as new certification criteria for IIoT devices and/or IIoT gateways. These ultimately could become additions to 62443-4-2, or to another part of the 62443 standard.

This section is organized as follows.

Section 4.3.1 describes the security context assumed for IIoT devices and IIoT gateways, which provides the general rationale for introducing new requirements.

Section 4.3.2 lists each new requirement, its source, and the specific rationale for including it.

Section 4.3.3 analyzes each requirement to support the conclusion that 62443-4-2 does not already include it.

Section 4.3.4 provides additional detail on the specific topic of compartmentalization, which is a multi-faceted new requirement introduced in 4.3.2 that includes a number of sub requirements.

Section 4.3.5 highlights requirements considered for addition as new requirements, but ultimately not selected.

Section 4.3.6 describes topic areas in which the study team felt new requirements may be needed. These are possible areas for future study.

4.3.1 Rationale

The security context for IIoT devices and gateways drives the need for additional functional requirements for IIoT devices and gateways beyond those found in 62443-4-2. The security context for these components includes:

- For IIoT devices and gateways, direct connection to the Internet or other untrusted network
- For IIoT devices and gateways, remote and/or unprotected location for component
- For IIoT devices, small physical size of the component
- For IIoT devices, low cost and wide availability of component
- For IIoT devices, large quantity of the same component
- For IIoT devices and gateways, use of platform-sharing technologies that place several functions co-resident on the same hardware.

While these security context elements for the IIoT environment were not ruled out for an IACS as envisioned during the development of the current 62443 standard, they were not commonplace.

At a high level, the first four elements imply that IIoT devices and gateways cannot rely upon other system components or physical security measures, but must protect themselves from network and physical attacks. Physical attacks include reverse engineering to enable other physical attacks on deployed systems, as well as supply chain attacks. For the fifth element, a few of the impacts on security of having a large quantity of the same component, are management of authentication credentials and security updates. The last element drives the need for compartmentalization of functions internal to a component. Functions now found on one device were previously implemented on separate devices, and typically separated into zones and conduits using network-level controls such as firewalls.

4.3.2 Functional requirements selected

Table 1 lists functional requirements recommended as certification criteria, beyond existing requirements in 62443-4-2. The following information is shown in the columns of Table 1.

- “Related FR” indicate the general topic under which the requirement would fall, if it were to be placed under the existing 62443-4-2 categorization of requirements by foundational requirement.
- “Requirement” gives a brief description of the recommended requirement. Further detail would be developed in the future to incorporate the requirement into a standard or certification program.
- “Applies to” shows a subset of the possible entries: <D, G, IACS-H>. “D” means the requirement applies for certification of IIoT devices; “G” means the requirement applies for certification of IIoT gateways, and IACS-H means consideration might be given to the requirement for all high capability security level IACS components, whether or not in an IIoT environment. The term “Core” or “Advanced” refers to the assignment of the requirement to one of two tiers possible for certification, defined further in 4.4.3.
- “Sources” lists the industry source documents analyzed for this study, where the requirement is discussed.

Results of the analysis of each of these requirements against 62443-4-2 follows the table in Section 4.3.3. For the purposes of this analysis, IIoT devices were assumed to be either embedded devices or host devices in 62443-4-2 terms. IIoT gateways were assumed to be network devices. IIoT devices and gateways may in addition satisfy the criteria for other 62443 component types. These assumptions are further explained in 4.8, which details study methodology.

Table 1. Proposed IIoT functional requirements not found in 62443-4-2

Related FR	Requirement	Applies to	IIoT security context/rationale	Sources
All	Compartmentalization –separation of execution environments for various functions within a component, for the purpose of limiting the effects of attacks or failures. Detailed sub requirements are found in 4.3.4.	D, G *IACS-H* Core	Attacks are expected against all systems, but with higher frequency for IIoT devices and gateways due to their connection to untrusted networks. In the case of successful attacks, separation of component elements limits the propagation of breaches between elements. Limiting the effect of breaches within compartments also supports secure recovery of the device.	[CTIA] 5.17 [MS7] [ENISA] GP-PS-05 [IICSF] 3.5, 8.12 [NISTCAT] Device security: secure execution
All	Security settings when device is initially placed in operational state after installation, default to supplier's recommended secure configuration ("Secure by default")	D, G *IACS-H* Core	More users will find this feature helpful in IIoT scenarios than in typical IACS scenarios, particularly for management at scale of large numbers of devices. Due to the known threat from connection to an untrusted network, fewer IIoT users are likely to authorize changes to a recommended secure configuration.	[ENISA] GP-TM-08 [IICSF] 7.9
FR 1	Authentication of non-human users from untrusted networks	D, G *IACS-H* Core	IIoT devices and gateways are directly connected to an untrusted network that hosts human and non-human users representing all skill levels and intentions, making it essential to confirm the entity with which the component is communicating.	[CTIA] 4.8 [MS7] [ENISA] GP-TM-42 [IICSF] 8.6.1 [NISTCAT] Device Identity: Device Authentication Support [NIST8259A] Logical access to interfaces: common elements
FR 1	Devices using passwords or keys, have unique initial passwords and keys per device. Initial passwords are generated according to internationally recognized and proven password guidelines OR require changing password on install	D *IACS-H* Core	Large quantity of components with the same password or key, exposed to an untrusted network, is high risk. Having pre-set unique initial passwords and keys assists with management at scale of large numbers of devices.	[CTIA] 3.2.1 [ENISA] GP-TM-09, GP-TM-22
FR 3	Protection of software and data in use	D, G *IACS-H* Core	Attacks against data in use are typically more advanced than those against data at rest and in transit, but may be expected from some adversaries resident on a directly connected untrusted network.	[ENISA] GP-TM-02 [IICSF] 7.6, 8.2.2, 8.7.2, 8.12.3, 11.7.2 [NISTCAT] Device Security: Secure Execution

Related FR	Requirement	Applies to	IIoT security context/rationale	Sources
FR 3	Device can be remotely updated and upgraded	D, G Core	Physical location and/or large quantity of components makes it impractical to require physical proximity to a component for update and upgrade.	[CTIA] 4.5 [ENISA] GP-TM-18 [IICSF] 11.5.1 [NIST8259A] Software update: common elements
FR 3	Enable/disable update/ upgrade	D, G Core	An inadvertent or automatic change to a software version that may have undesirable features, entails more risk when the component is connected to an untrusted network. This feature provides another layer of user control over software changes.	[ENISA] GP-TM-19, 20 [NIST8259A] Software update: common elements
FR 3	Update/upgrade maintains user security settings	D, G, *IACS-H* Core	Both direct connection to an untrusted network and large quantity of components will drive more update activity. It is impractical to require the user to reset security settings.	[CTIA] 3.5.4 [ENISA] GP-TM-20
FR 1, 2	For management and configuration interfaces from untrusted network, either authorize traffic by port, protocol, and application, OR do not accept incoming initiation of management/ configuration connections	D, G Core	Serves as built-in "firewall" function permitting required management and configuration communication with the untrusted network, but disallowing other traffic. Approach to not accept incoming connections is accomplished by the management/configuration entity using a separate existing operational channel, to request the device initiate a config/ management connection to that entity.	[IICSF] 8.6.2 [ENISA] GP-TM-43 (higher level principle) [NIST8259A] Logical access to interfaces [NISTCAT] Logical access to interfaces: Interface control
FR 3	Device itself does not provide printed design information useful to attackers	D *IACS-H* Advanced	Since an IIoT device may be stolen due to relatively unprotected physical location, or easily obtained due to low cost, this removes one barrier to reverse engineering. Reverse engineering in turn enables other physical or supply chain attacks. A common source of printed information that aids attackers is layout and other design information on a circuit board silk screen.	
FR 3	Presence/absence of component can be monitored	D, G Advanced	Component may be in a relatively unprotected physical location and may be relatively small. A component with this feature can be integrated into a system to detect its presence or absence.	[IICSF] 8.3
FR 6, 7	Turn off connection to untrusted network, maintain essential functions	D Core	Since IIoT devices discussed in this report by assumption have a direct connection to an untrusted network, turning off this connection will be a common response to a security threat or incident.	[ENISA] GP-TM-45 [NISTCAT] Device security: secure device operation [NIST8259A] Logical access to interfaces: common elements

4.3.3 Analysis against 62443-4-2

The requirements shown in Table 1 found in IoT/IIoT sources analyzed for this study, were not found in 62443-4-2. This section describes for each of these requirements, the analysis against 62443-4-2 that led to this conclusion.

- **Compartmentalization:** 62443-4-2 requires conformance with 62443-4-1 development processes, which require adherence to secure development practices in general, in requirement SD-4 *Secure design best practices*. The requirement SM-1 *Development process* in 62443-4-1 mentions modular design in the context of generally accepted product development processes, but not with specific goal to prevent attack propagation. Compartmentalization is a practice that could fall under SD-2 *Defense in depth design* or SD-4. However, compartmentalization to separate different functions executing within the same device is not explicitly required by SM-1, SD-2, or SD-4. The concepts of zones and conduits central to 62443 express the intent of compartmentalization, but are typically understood and applied to separate individual devices using network countermeasures, and not separate functions within a single device. Here, compartmentalization refers to separation between functions internal to an IIoT device or gateway. This may be viewed as the application of 62443-3-3 system-level requirements regarding zone partitioning, to the component level, so that a device may have internal zones. Here "internal zone" is not a new concept, but rather a phrase to refer to a zone in the usual 62443 meaning, that may exist within a single component. Section 4.3.4 details adjustments to existing 62443 requirements related to zones and conduits, to describe certification requirements for compartmentalization within a component.

  This topic was the most challenging aspect of the present study. Although the project team was in general agreement that compartmentalization requirements are needed, some members felt it would be more effective to replace "internal zone" by some other term not already used in 62443. In that case one would create new requirements, rather than attempt to reuse and adjust existing requirements, as has been done in the present report. These issues are further discussed in Section 4.3.4.

- **Secure by default:** 62443-4-2 does not require that a component be set to a secure configuration by default after installation and initial placement into operational status. A possible rationale for this is that IACS environments have varying risk profiles, so may not need to use all product security capabilities, and an IACS with a more secure configuration may require more time-consuming set-up to become operational. However, 62443-4-1 does require in SG-3 *Security hardening guidelines,* that supplier documentation instruct the user on how to set up a secure configuration and the effects of various security settings. In the case of IIoT, it is more likely that the user will wish to use the security capabilities provided by a product, so that it will be more helpful and convenient to deliver a hardened product as the default.

- **Authentication of non-human users from untrusted networks:** 62443-4-2 requirement CR 1.2 *Software process and device identification and authentication* states "Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA 62443 3 3 SR 1.2." However, 62443-4-2 does not require a component to have the capability to authenticate incoming access attempts *from* other components. It is understood that in the context of an overall system, other intervening components may provide satisfactory access protections on behalf of a component. Note that if an overall IIoT system were evaluated at the system level for conformance with 62443-3-3, then any device that is part of that system that had a direct Internet connection would need to authenticate non-human users of that connection, by 62443-3-3 SR 1.2 which states "The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures." However, the baseline set of IIoT device and gateway requirements assumed for this study is the component level requirements in 62443-4-2, not the 62443-3-3 requirements.

There is partial coverage of this incoming authentication requirement by 62443-4-2; in particular three 62443-4-2 requirements (shown below for reference) imply that a network device must authenticate wireless connections from an untrusted network. The argument is as follows: because of either NDR 1.13 OR NDR 5.2, a network device must support wireless access management if it has wireless access to an untrusted network. Then by NDR 1.6, it must authenticate everything on this interface. This argument covers the case of wireless communication from an untrusted network to a gateway (which is assumed to be a network device in 62443 terms), but not wireless communication to IIoT devices, nor wired communication.

- NDR 1.6 *Wireless access management* A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.
- NDR 1.13 *Access via untrusted networks* The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.
- NDR 5.2 *Zone boundary protection* A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

- **Unique initial passwords and keys per device. Passwords generated according to internationally recognized and proven password guidelines OR require changing password on install:** 62443-4-2 in CR 1.5 *Authenticator management* requires a component to "support the recognition of changes to default authenticators made at installation time." However, it does not state that a product must enforce that passwords be changed at installation time, nor that individual products as delivered must each have different passwords or keys.
- **Protection of software and data in use:** 62443-4-2 requires integrity protection of data in transit in CR 3.1 *Communication integrity*. CR 3.4 *Software and information integrity* requires "the capability to perform or support integrity checks on software, configuration and other information." Neither of these requirements explicitly calls out protection of software or data in use. This functionality is one aspect of the Trusted Execution Environment (TEE) concept, often mentioned in the context of IIoT. TEE in general is intended to ensure integrity of code and data at startup and runtime. Other existing 62443-4-2 requirements already cover startup requirements.
- **Device can be remotely updated and upgraded:** 62443-4-2 in EDR|HDR|NDR 3.10 requires a component support "the ability to be updated and upgraded." However, a component conforming to 62443-4-2 might require physical proximity to the component to perform updates or upgrades. It should be noted that "remote" update or upgrade (not requiring physical proximity to the component) is distinct from "automatic" (no human intervention). An asset owner's Management of Change (MoC) process for an IIoT deployment may require remote update or upgrade, however support for the capability would be required in the product being updated or upgraded, to achieve conformance with their process. 62443-2-4 requires in SP.01.02 RE(1) that a service provider "assigns only service provider, subcontractor or consultant personnel to Automation Solution related activities who have been informed of and comply with the asset owner's MoC and Permit to Work (PtW) processes for changes involving devices, workstations, and servers and connections between them." A service provider intending to meet SP.01.02 RE(1) in this case, would need product support of remote update and upgrade in order to do so.
- **Enable/disable update/upgrade:** As described for the previous feature, 62443-4-2 in EDR|HDR|NDR 3.10 requires a component support "the ability to be updated and upgraded." There is no 62443-4-2 requirement that a component be able to enable or disable this capability.

- **Update/upgrade maintains user security settings:** 62443-4-2 does not address the topic of security settings after update/ upgrade. 62443-2-4 points out under SP.11.06 RE(1) that "it is not uncommon for the installation of patches…to remove or degrade system hardening. Therefore, the service provider has to have a process that determines if this has happened and if it has, to restore the hardening." In the case of IIoT, it is recommended that such removal or degradation not take place.
- **For management and configuration interfaces from untrusted network, either authorize traffic by port, protocol, and application, OR do not accept incoming initiation of management/configuration connections:** For gateways, this is already addressed by 62443-4-2 NDR 1.13 *Access via untrusted networks,* although not as specifically as stated here. NDR 1.13 reads "The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks," However, this entry in Table 1 is not addressed in 62443-4-2 for IIoT devices, which as defined here are typically classified as embedded devices or host devices in 62443-4-2 terms. In general, 62443-4-2 allocates network level protections to network devices. As an alternative to adding this requirement for IIoT devices one might decide that any component with an Internet connection is to be considered a network device. However. it still remains unclear whether NDR 1.13 would apply to such a component, because it is unclear whether the IIoT device management/configuration interface is "supporting device access into a network." Designating an IIoT device with an Internet connection as a network device also would place other 62443-4-2 requirements upon it, which may not always be appropriate, such as NDR 5.3 *General purpose, person-to-person communication restrictions.*
- **Device itself does not provide printed design information useful to attackers:** 62443-4-2 provides protections against physical tampering with a device in EDR|HDR|NDR 3.11 *Physical tamper resistance and detection.* However, if an adversary has physical possession of the device, there are not further requirements for protection against reverse engineering to design future attacks.
- **Presence/absence of component can be monitored:** 62443-4-2 addresses tampering with devices in EDR|HDR|NDR 3.11 *Physical tamper resistance and detection,* but does not address the scenario in which an IIoT device has failed or is no longer physically present.
- **Turn off connection to untrusted network, maintain essential functions:** For gateways, this capability is likely intended by 62443-4-2 NDR 5.2 RE(2) *Island mode,* which reads: "The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode)." By 62443-4-2 CCSC 1 *Support for essential functions,* essential functions must be maintained in island mode per 62443-3-3 Clause 4. Therefore, this is a 62443-4-2 requirement "addition" for IIoT devices only. (A clarification of the requirement for the gateway case is discussed in 4.4.6.2.)

4.3.4 Compartmentalization

This section provides additional information about the requirement for compartmentalization introduced in 4.3.2. Subsections cover these topics:

- Approach to defining compartmentalization requirements by adapting existing requirements in 62443-3-3, 62443-3-2, and 62443-4-1 (4.3.4.1)
- Compartmentalization requirements (4.3.4.2)
- Certifier validation detail for compartmentalization requirements (4.3.4.3)
- Open issues regarding the "adaptation" approach taken to compartmentalization requirements (4.3.4.4)

4.3.4.1 Approach

It has been noted in discussions about applying 62443 for IIoT, that a complex IIoT component might be considered as a control system (thus subject to 62443-3-3), vs. as a component (subject to 62443-4-2). Under that approach, the concepts of zone and conduit in 62443-3-3 would apply internal to the component, and therefore one has compartmentalization requirements already defined by 62443. However, it was agreed impractical to impose all 62443-3-3 control system requirements on these IIoT components. A more practical approach would be to impose just those 62443-3-3 requirements that relate to zones and conduits. That is the approach taken here. It is presented as useful in the short term, to design an IIoT device and gateway certification that leverages existing 62443 concepts to the extent possible. Section 4.3.4.4 describes alternate viewpoints regarding whether and to what extent leveraging is appropriate, and longer term open issues regarding treatment by the 62443 standard of this topic for IIoT.

4.3.4.2 Compartmentalization requirements

Here we consider how to adapt for IIoT devices and gateways, 62443 requirements that specify how to create zones and conduits, and that specify their functional requirements. In existing 62443, these requirements apply to control systems (vs. components). Existing 62443 requirements related to zones and conduits are categorized as follows, and their adaptation for components is discussed in the subsections shown:

- 62443-3-3 requirements that use the term zone or conduit (4.3.4.2.1)
- 62443-3-2 requirements about zone separation (4.3.4.2.1)
- 62443-3-3 requirements about network segmentation (4.3.4.2.2)
- 62443-4-1 security development lifecycle requirements about security requirements and design (4.3.4.2.3).

The certification program enhancements in this section are labeled COMPART 1 through COMPART 10 for convenient reference. All of the new requirements and other certification criteria mentioned in this section could also be considered for non-IIoT high capability security level components.

4.3.4.2.1 Functional requirements adapted from 62443 zone requirements

The third column of Table 2 shows enhancements to 62443-4-2 functional requirements to address the topic of compartmentalization, proposed for both IIoT device and IIoT gateway certification.

These enhancements are “derived” from existing “parent” requirements related to zones and conduits, found in 62443-3-2 or 62443-3-3, shown in the first two columns of the table. A “parent requirement” here simply means a requirement that inspired the IIoT certification enhancement shown, and does not necessarily imply a particular structure for the future 62443 standard or its parts. It is not expected that 62443-4-2 requirements would be formally linked to 62443-3-2 requirements.

As shown in the third and fourth columns, in some cases a requirement in 62443-3-3 does not currently have a corresponding component-level requirement in 62443-4-2, and a new requirement is recommended. In other cases, there is an existing 62443-4-2 requirement, for which validation guidance for the certifier specific to IIoT is recommended.

The last column of Table 2 assigns certification enhancements to the Core or Advanced tier for IIoT certification. Section 4.4.3 describes these tiers.

Table 2. Certification functional requirements for compartmentalization

62443 Parent requirement ID	62443 Parent requirement	Certification enhancement (adapted for component)	Enhancement ID, type, tier
62443-3-3 SR 5.4 *Application partitioning* SL-C 1, 2, 3, 4	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.	The component ~~control system~~ shall provide the capability to support partitioning of data, applications and services internal to that component, based on criticality to facilitate implementing a zoning model. (adaptation in blue)	COMPART 1 New requirement Core tier
62443-3-2 ZCR 3.1, 3.2, 3.3 *Establish zones and conduits, separation of enterprise and safety assets*	The organization shall group IACS and related assets into zones or conduits as determined by risk. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization. IACS assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets. Safety related IACS assets shall be grouped into zones that are logically or physically separated from zones with non-safety related IACS assets. However, if they cannot be separated, the entire zone shall be identified as a safety related zone.	• A component that has internal or external interfaces that are trust boundaries in the threat model, shall have the capability to separate functions separated by these trust boundaries, in different zones. • A component that has safety-related functions shall have the capability to separate safety-related functions and non-safety-related functions in different zones. • A component that has business or enterprise functions, or to which the asset owner may add custom business or enterprise functions, shall have the capability to separate these from control system functions in different zones. Internal zones shall provide logical or physical separation in accordance with commonly accepted practices for IIoT.	COMPART 2 New requirement Core tier

62443 Parent requirement ID	62443 Parent requirement	Certification enhancement (adapted for component)	Enhancement ID, type, tier
62443-3-3 SR 5.2 *Zone boundary protection* SL-C 1, 2, 3, 4	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	Add certifier guidance for 62443-4-2 NDR 5.2 *Zone boundary protection* A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model. Guidance: Validation of this requirement will include cases where a zone boundary is internal to the network device. It will apply not only to network devices, but also to all types of devices with internal zones.	COMPART 3 Certifier guidance 62443-4-2 validation Core tier
62443-3-3 SR 4.1 RE(2) *Protection of confidentiality across zone boundaries* SL-C 4	The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary	Add certifier guidance for 62443-4-2 CR 4.1 *Information confidentiality* Components shall • provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and • support the protection of the confidentiality of information in transit as defined in ISA 62443-3-3 [11] SR 4.1. Guidance: Validation of this requirement will include cases where the zone boundary over which transit takes place (per SR 4.1 RE(2)) is internal to the component.	COMPART 4 Certifier guidance 62443-4-2 validation Advanced tier

62443 Parent requirement ID	62443 Parent requirement	Certification enhancement (adapted for component)	Enhancement ID, type, tier
62443-3-3 SR 2.3 RE(1) *Enforcement of security status of portable and mobile device* SL-C 3, 4	The control system shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.	The ~~control system~~ component shall provide the capability to verify that portable or mobile devices attempting to connect to a zone internal to that component comply with the security requirements of that zone. (adaptation in blue)	COMPART 5 New requirement Advanced tier

An example implementation of monitoring and control between compartments as described in COMPART 3 is "nanosegmentation" technology.

4.3.4.2.2 Functional requirements adapted from 62443 network segmentation requirements

Although 62443-3-3 requirements on the topic of network segmentation do not mention the term "zone," they provide support for meeting requirements about zoning found in 62443-3-2. For example, 62443-3-3 SR 5.1 RE(1) *Physical network segmentation* requires segmentation of control networks and non-control networks as well as critical from non-critical IACS networks; 62443-3-2 ZCR 3.2 *Separate business and IACS assets* and ZCR 3.3 *Separate safety-related assets* require separation of these types of zones. Network segmentation provides one possible approach for enforcing zone boundary requirements.   For that reason, we consider here whether and how the intent of the 62443-3-3 network segmentation requirements should be reflected at the component level for IIoT devices and gateways. All requirements and enhancements found under SR 5.1 are listed in Table 3 so that the reader may review this analysis, even though some did not appear to require analogs at the component level.

62443 does not include a definition for the term "network," however logical implementations of networking functionality have been commonly used to implement 62443 requirements about networks. Therefore, by extension, we could (for example) consider the virtual networks used for communication between internal zones of a device implemented using virtual machines or containers, a "network," and apply these requirements with adaptations shown in Table 3.

Table 3. Certification functional requirements for network segmentation

62443 Parent requirement ID	62443 Parent requirement	Certification enhancement (adapted for component)	Enhancement ID, type, tier
62443-3-3 SR 5.1 *Network segmentation* SL-C 1, 2, 3, 4	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	None, intent for control/non-control met by COMPART 2. Did not attempt to create analog for critical vs non-critical aspect of requirement at the internal component level.	
62443-3-3 SR 5.1 RE(1) *Physical Network segmentation* SL-C 2, 3, 4	The control system shall provide the capability to physically segment control system networks from non-control system networks and physically segment critical control system networks from non-critical control system networks.	A component that includes safety and non-safety functions, shall have no shared physical element of the component required by both functions. Describe in user documentation, component functions and physical elements of the component that they share. Component functions include those present upon initial installation or potentially added later. Functions added later may be provided by the component supplier, or other parties, supported by host functionality of the component. Other parties may include the asset owner or third parties. The certifier will also provide this information in certification documentation, so that that the supplier could if desired make it conveniently available to potential purchasers, typically under non-disclosure. NOTE: COMPART 6 implies for example that a certified IIoT device or gateway cannot use a hypervisor to separate safety functions from other functions. It could use a hypervisor to separate invoicing functions from sensors, all residing on guest operating systems on the same host device, as long as this was disclosed in the user guide and certification report. More broadly, safety functions cannot coexist in the same physical device as other functions, except to share a physical enclosure. COMPART 6 also may imply that the requirement under COMPART 2 to separate safety functions by internal zone, may not be needed. It seems likely that any implementation that met that requirement, would likely not meet COMPART 6.	COMPART 6 New requirement Core Tier COMPART 7 New requirement Core tier

62443 Parent requirement ID	62443 Parent requirement	Certification enhancement (adapted for component)	Enhancement ID, type, tier
62443-3-3 SR 5.1 RE(2) *Independence from non-control system networks* SL-C 3, 4	The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.	The component shall have the capability to support internal and external data flows as designed, required for internal or external control system functions, without providing internal or external connections for any non-control system functions.	COMPART 8 New requirement Advanced tier
62443-3-3 SR 5.1 RE(3) *Logical and physical isolation of critical networks* SL-C 4	The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.	None. Did not attempt to create analog for critical vs. non-critical at the internal component level.	

4.3.4.2.3
Security development lifecycle requirements for compartmentalization

The prior discussion has addressed functional requirements related to compartmentalization; this section discusses related security development lifecycle requirements.

There is difference in *who* applies system-level vs. internal component zoning. An *asset owner* ultimately defines zones for an overall control system using the risk-based process in 62443-3-2. That being said, if large integrated parts of the system are provided by a supplier (rather than a single component), the supplier has the role to anticipate the zoning capabilities that will ultimately be required by the asset owner. On the other hand, the *supplier* for a complex IIoT component defines the internal zoning capability for their product. It seems less likely that the asset owner typically makes decisions about component-internal zoning. These cases indicate the need for some supplier requirements in 62443-4-1 on the topic of zoning, at the component level, and for some situations, at the system level as well. The following certification enhancement is therefore proposed as a new 62443-4-1 requirement.

- Add design practice for zone partitioning to SD-4: Add to the lettered list of practices under 62443-4-1 SD-4 *Secure design best practices:* "h) partition critical from less critical functions to facilitate creating a zoning model for a system or internal to a component using commonly accepted practices" (COMPART 9 new requirement)

A second distinction between zones that separate individual devices using network countermeasures, and internal component zones, is that internal component zones share some hardware or software elements that are not intended to support interactions between those zones. Examples are a hypervisor, memory hardware, and processor. These shared resources may constitute a threat, distinct from specified, intentional interfaces between elements of the component. They might therefore be missed in the design information about internal interfaces and related threats, called for by 62443-4-1 SD-1 *Secure design* *principles* which states: “A process shall be employed for developing and documenting a secure design that identifies and characterizes each interface of the product, including physical and logical interfaces, to include a) an indication of whether the interface is externally accessible (by other products), or internally accessible…” Therefore, the following certification enhancement is recommended:

- *Include in certifier guidance for 62443-4-1 SR-2 Threat model:* Verify that the potential attack vectors in the threat model include resources shared across internal trust boundaries of a component. (COMPART 10)

4.3.4.3 Validation detail for compartmentalization requirements

The intent of the new requirements recommended for compartmentalization was to conform to the level of detail in the existing 62443 standard, stating the “what and not the “how.” It then becomes an important question, exactly how will a certifier determine whether more than one zone is needed for a component, whether “enough” compartmentalization has been done? Is the separation thereby achieved sufficient, using an appropriate compartmentalization technology and appropriately implemented?

It is expected that certifier expert judgment is relied upon to determine if a set of internal zones meets the intent of the requirement COMPART 1 and COMPART 2 in Table 2. Perhaps one zone is sufficient in some cases. It is not intended nor practical for an IIoT certification to require specific technologies for implementation of internal zones, nor to instruct on details of use of those technologies. It has been recommended above (COMPART 9) that the supplier maintain an internal best practice for component compartmentalization. This is further supported by certification scheme-identified commonly accepted practices to support validation of requirement COMPART 2 and as discussed in section 4.5.1.

4.3.4.4 Open issues: Using the unified zone concept

This section discusses open issues regarding the approach to defining compartmentalization requirements by adapting existing 62443 requirements regarding zones and conduits.

Recognizing that zones may exist within a single component, unifies the design of requirements for compartmentalization at the component level and at the system level, as shown in Table 2. However, some members of the project team felt that the use of the zone terminology would not be embraced by the larger community as applicable to new compartmentalization technologies. It would be viewed as backward-looking to traditional architectures where separation was normally achieved between devices, at the network level.

Further, there are conceptual issues that remain when unifying the concept of zone to apply at both the network level and internal to components.

In the overall 62443 model, one assigns a capability security level to a zone. Possible SL-C’s are 1-4. The purpose of assigning this level is so that security requirements can be selected for the zone based on the requirements in 62443-3-3. 62443-3-3 requirements have an associated SL-C. Assignment of an SL-C to a zone also allows an integrator to select components to use in that zone, that meet corresponding capability security level requirements found in 62443-4-2 for components. Component requirements in 62443-4-2 are derived from the system level requirements at the corresponding SL-C in 62443-3-3, so will need to be met by a zone’s components in order for the system zone to meet its intended SL-C.

This raises the question – do internal zones of a component have capability security levels? If so, how does one assign and make use of those levels? Is there a “component design” model (vs “system design” described in 62443-3-2) for selecting sub components of a component to be part of an internal zone? What types of entities are these sub components? Should standard requirements be developed for these types of entities?

If there is to be a “component design” process for selecting sub components to be used in internal zones, one would expect it to resemble 62443-3-2. However, 62443-3-2 is an asset owner process based on risk, which is not known to the supplier designing a component. However, the supplier will have the knowledge to apply some of the compartmentalization requirements in 4.3.4.2, such as whether or not the component supports both safety and non-safety functions, and whether it supports non-control-system functions. An example of the later is an invoicing interface integrated in the same device with sensors and valve control, such as for dispensing fuel.

A further question is introduced by the tier model proposed in the present document for certification of IIoT devices and IIoT gateways. Such a device or gateway can be certified at the Core tier or the Advanced tier, where these tiers are adaptations of capability security levels 2 and 4, respectively. Is this consistent with an approach that assigns SL-C's to internal zones of such a device? Does it make sense that a control system is *not* assigned an SL-C, but a component hosting many functions on the same hardware, is assigned a tier?

These issues do not necessarily need resolution to create a useful IIoT device and gateway certification program for the short term; however, they remain challenges for the IIoT conceptual and usage model for 62443 going forward.

4.3.5
Functional requirements not selected from sources studied

This section highlights requirements considered for addition to the set of new requirements identified in 4.3.2, but ultimately not selected.

The industry/government sources studied for this effort contain a large number of recommended practices which are not found in 62443-4-2. Although these are important for specific applications, they were not judged by the project team as critical or appropriate as IIoT certification criteria to be applied to all IIoT devices or gateways. The most notable among these are listed below.

Table 4. Requirements or practices not recommended as certification criteria

Requirement or practice	Source (example)	Comments
Small TCB (Trusted Computing Base)	[MS7]	Addressed more generally in 62443-4-1 SD-4 *Secure design best practices – attack surface reduction.*
Logging of anomalous or malicious activity based on configured polices and rules	[CTIA]	Simple devices may not require configurability.
Automatic installation of updates and/or upgrades	[CTIA]	[IICSF] 11.5.1 points out the risk of automatic updates. Some project team members felt it should be required to offer both automated and manual updates, with manual updates set as the default. Others did not see an automatic option as necessary or desirable in all cases.
Rollback an update or upgrade	[NIST8259A] Software update: common elements	62443-4-2 CR 7.4 *Control system recovery and reconstitution,* covers the case of an update or upgrade failure. In other cases, one may use the system level backup/restore process required by CR 7.3 *Control system backup* to revert to a prior version. Section 4.4.6.2 recommends that the certifier validations for these existing requirements be enhanced to verify these cases. It was noted that usual technique of having a second image on-board the device, that may be invoked whether or not a change to a new image was a "failure," isn't always feasible due to space. There are also risks involved in providing this functionality since it may be used as an attack vector to attempt to return a device to an insecure state.
Report device type so can determine functions of device	[CTIA]	
Severity-based event reporting deadline	[CTIA]	
Analytics that track security performance	[IICSF]	
Self-repair	[ENISA] GP-TM-16	
Accounts with time expiration	[NISTCAT]	
Out of band second authentication method	[CTIA] [NISTCAT]	

Requirement or practice	Source (example)	Comments
High granularity for control of access via untrusted networks for "operating" interfaces – meaning interfaces other than management and configuration interfaces	[IICSF] 8.6.2	62443-4-2 in CR 2.1 RE(1) *Authorization enforcement for all users (humans, software processes and devices)* requires controls on access by authenticated users for all component types. NDR 1.13 *Access via untrusted networks* quoted above in 4.3.3 requires control of all forms of access for network devices. Known characteristics of expected traffic and connection to untrusted network makes tight control feasible and desirable for IIoT. For example, specific requirements to control incoming traffic described in [IICSF] 8.6.2 authorize traffic by port, protocol, application, library and process. The project team did not universally agree on the filtering approach; other design approaches are available to control "operating" traffic such as a publish/subscribe model where entities on the untrusted network never initiate connections to the IIoT device or gateway. However, it was determined that to require such a model for management and configuration interfaces would be too restrictive. A less restrictive requirement, that applies to these interfaces appears above in Table 1: "For management and configuration interfaces…"
Self-integrity report – required to join network	[ENISA] GP-TM-42	
Explicitly authorize all new connections	[ENISA] GP-TM-44	
Ability to support various modes of IoT device operation with more restrictive operational states, such as travel mode, safe mode	[NISTCAT]	One capability that might be considered an example of this, was selected and is shown in Table 1, "Turn off connection to untrusted network, maintain essential functions."

4.3.6 Topics for future study

This section identifies two areas in which new certification criteria may be needed, but for which this report does not contain specific recommendations.

The project team discussed the emergence of two types of attacks to which IIoT components are particularly susceptible: supply chain attacks and hardware attacks.   These attacks continue to evolve; significant academic and industry effort is currently focused on these topics. Ultimately, it is expected that IIoT certifications will require additional countermeasures for these attacks well beyond those found in the recommendations of this report. The present study did not attempt a comprehensive investigation of ongoing industry efforts in these areas, to determine if existing results might contribute in the near term to IIoT product certifications. Such an investigation should be considered as an area for future work. Here, we briefly discuss these two types of attacks.

4.3.6.1 Supply chain attacks

There are certification criteria recommended in the present document that address some aspects of supply chain security. Two examples from 62443-4-1 are SM-9 *Security requirements for externally provided components* and SUM-4 *Security update delivery.* The industry overall has recognized the need for significant additional work in standardizing comprehensive requirements for supply chain security. The present study did not attempt an investigation of what is needed for supply chain security beyond existing 62443 requirements, for IIoT devices and gateways. A requirement for removing printed design information is recommended in Table 1, as it is a commonly practiced first step defense against reverse engineering, which enables supply chain attacks and others.

4.3.6.2 Hardware attacks

As more security is built into software targets, and hardware is used to protect data and software, the hardware itself becomes a more attractive attack vector. Another driver for increasing hardware attacks is the evolution of mobile devices to host an evolving set of attack tools. These attacks potentially affect any IACS device, so that countermeasures may be appropriate as future enhancements for 62443-4-1 and/or 62443-4-2. IIoT components are often not in a physically protected area and therefore are particularly vulnerable because the attacker may easily gain the close proximity required for many hardware attacks.

MITRE has created a Common Weakness Enumeration (CWE) categorization for hardware design weaknesses, which currently includes 95 weaknesses. It could serve as a starting point for investigating and prioritizing concerns in this area. There are academic papers, theses, and industry information on the specific topic of hardware attacks against IoT devices. There was little mention of hardware attacks among the resources used for this study. However, [MS7] did call for physical countermeasures against side-channel attacks, which is an example of a type of hardware attack that relies upon measurable characteristics of a device while in operation, such as power, electromagnetic waves, and timing. A typical goal for a side channel attack is to extract a key, using the fact that the value of the key affects contents of these information "side channels." Vulnerabilities that enable such attacks appear in the MITRE list as CWE 1300: *Improper Protection Against Physical Side Channels* and CWE-1255: *Comparison Logic is Vulnerable to Power Side-Channel Attacks.* The recently released United States cryptography standard FIPS 140-3 and associated international standard ISO/IEC 19790:2012 do not require countermeasures for these attacks, although they do require proof of effectiveness, if a cryptographic module claims to have such countermeasures.

As a second example, a group member raised the question of defenses against fault injection attacks, which are attacks on hardware or software, that introduce invalid conditions, internal states, or data. This may result in device failure or permit bypass of security functionality. Fault injection attacks on hardware are reported to be an increasing concern, for example as in "Fault Injection Attacks: A Growing Plague." Such attacks may be invasive or non-invasive. Examples of non-invasive fault injection attacks are clock glitching and voltage glitching, which attack clock timing and voltage input levels. Examples of invasive fault injection attacks on hardware are electromagnetic (EM) glitching, and optical injection, which require removing the chip's plastic package for effectiveness of the attack EM or light wave. In MITRE's CWE list, one finds CWE-1247: *Missing or Improperly Implemented Protection Against Voltage and Clock Glitches,* CWE-1319: *Improper Protection against Electromagnetic Fault Injection (EM-FI),* CWE-1332: *Insufficient Protection Against Instruction Skipping Via Fault Injection,* and CWE-1334: *Unauthorized Error Injection Can Degrade Hardware Redundancy.*

An example of a 62443-4-2 requirement recommended for IIoT gateways in this study, that requires a countermeasure to a specific type of fault injection attack is 62443-4-2 NDR 5.2 RE(3) *Fail close,* which reads "The network component shall provide the capability to protect against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close)."

4.4 Selection and application of existing 62443-4-2 requirements

Section 4.3 has recommended new functional requirements not found in 62443-4-2, as new certification criteria for IIoT device and/or IIoT gateways; this section describes how existing 62443-4-2 requirements would be used within these certifications.

This section is organized as follows:

As background, Section 4.4.1 reviews the structure of 62443-4-2 requirements and current certification programs.

Section 4.4.2 references an illustrative list of existing 62443-4-2 requirements which were called out in the IoT/IIoT sources analyzed for this study.

Section 4.4.3 introduces the concept of Core and Advanced tiers recommended for structuring IIoT device and IIoT gateway certifications.

Section 4.4.4 specifies the requirements in 62443-4-2 used in IIoT device and IIoT gateway Core and Advanced tier certifications.

Section 4.4.5 discusses how the recommendation in 4.4.4 was developed.

For a few 62443-4-2 requirements, additional IIoT-specific guidance for the certifier is recommended in 4.4.6.

4.4.1 Structure of 62443-4-2 and certifications

62443-4-2 determines applicability of requirements to an IACS component, based upon type of component and capability security level. The types of components defined by the standard are software application, embedded device, host device, and network device. The capability security levels defined are: 1, 2, 3, or 4. Thus for example, 62443-4-2 defines the subset of its requirements that would be needed for a component that is a network device, and is intended to meet capability security level 3. A component may meet the 62443 definition for more than one of the four types of components, in which case 62443-4-2 requires it to meet requirements for all applicable component types.

In 62443-4-2, common requirements for all types of components are labeled CR (Component Requirement). Requirements for software applications only, embedded devices only, host devices only, and network devices only, are labeled SAR, EDR, HDR, and NDR, respectively.

Requirements in 62443-4-2 are organized under seven foundational requirements (FR) such as FR 1 *Identification and authentication control*. 62443-4-2 defines the intent of capability security levels specifically for each foundational requirement, in terms of the type of adversary that would be prevented by the requirements under that FR, from achieving a violation of the security objective for that FR. For example, the following is a quote from 62443-4-2 11.1, which describes security levels related to FR 7 *Resource availability* and includes the following description for capability security level 4:

"SL 4 – Ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with extended resources, IACS specific skills and high motivation."

Product certifications to 62443-4-2 would typically select a capability security level and evaluate conformance to all requirements for that level, under all FR's, that are applicable to the component type(s) for the product. However, selection of the same capability security level across all FR's is not mandated by the standard.

4.4.2 62443-4-2 Intersection with industry/government IoT/IIoT sources

This section references an illustrative list of existing 62443-4-2 requirements which were called out in the IoT/IIoT sources analyzed for this study. This provides support for the applicability of 62443-4-2 requirements for IIoT device and gateway certifications.

This study analyzed six industry/government sources on the topics of IoT and IIoT security. Recommendations in these sources were compared to 62443-4-2 requirements. The comparison showed that a significant number of the recommendations found in common among many of the industry sources, are existing 62443-4-2 requirements. This was to be expected, since IIoT components are a particular class of IACS component, and 62443-4-2 is an international standard that applies to all IACS components.

Table 16 in Appendix 3 shows a sampling of 62443-4-2 functional requirements that were commonly seen in the IoT/IIoT sources, and also appear in 62443-4-2. Although this study concluded that additional functional security requirements beyond those in 62443-4-2 are recommended for IIoT component certification, it also confirmed that a component conforming to 62443-4-2 requirements has thereby already met a significant subset of functional security requirements deemed necessary for IIoT components.

The following sections propose how existing 62443-4-2 requirements would be applied for IIoT device and gateway certifications.

4.4.3 Core and Advanced tiers

For the purpose of structuring IIoT device and IIoT gateway certifications, two tiers have been identified, called Core and Advanced. The existing 62443-4-2 requirements that fall under these tiers are described in the following section; the tiers for new functional requirements are shown in Table 1.

The Core tier is intended to address adversaries as defined by 62443 capability security level 2. In addition, the Core tier incorporates selected level 3 and 4 requirements to specifically address the threat of more sophisticated attackers originating from the untrusted network. These higher level requirements (Table 6) strengthen identification/ authentication to narrow the field of successful attackers, and strengthen attack monitoring/ diagnosis/response capabilities beyond those required for capability security level 2. They were selected as fundamental to component security on an untrusted network in an unprotected physical location.

Advanced tier is intended to address adversaries as defined by 62443 capability security level 4.

4.4.4 Recommended existing 62443-4-2 requirements for IIoT devices and gateways

This section specifies the existing requirements in 62443-4-2 used in IIoT device and IIoT gateway Core and Advanced tier certifications.

In accordance with 62443 definitions (see 3.1), IIoT devices with embedded software are embedded devices (e.g. sensors, actuators, PLC's); IIoT devices with application software are host devices (e.g. IIoT integrated edge computing devices); IIoT gateways are network devices. IIoT devices and gateways may in some cases also meet the 62243 definitions for other 62443 component types. Once the 62443-component type or types for an IIoT device or gateway and the tier for the certification (Core or Advanced) are determined, one may then identify the set of existing 62443-4-2 requirements that will be applied for IIoT certification of the component.

The following outlines the approach proposed for IIoT devices and gateways, to identify this set of 62443-4-2 requirements.

- All 62443-4-2 requirements are among the criteria used in these IIoT certifications, with the exception of four requirements. Table 5 enumerates those exceptions and related rationale.
- An Advanced tier certification includes all Core tier certification criteria. For an IIoT gateway, the Core tier includes as certification criteria, all 62443-4-2 capability security level 2 requirements and requirement enhancements that are applicable to its device type(s) except CR 7.3 RE (1) *Backup integrity verification,* which is modified for the Core tier and is included without modification to its 62443-4-2 statement in the Advanced tier. Core also includes six requirements at capability security level 3, and one at level 4. Table 6 enumerates these level 3 and 4 requirements.

  For the Core tier, CR 7.3 RE(1) *Backup integrity verification* is modified by adding the conditional phrase in italics: "Components *that support restore via the untrusted network* shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information." This requirement implies that devices with memory space and processing power insufficient to perform such a validation may be restored locally.
- The Core tier for IIoT devices applies existing 62443-4-2 requirements with one difference from the Core tier for IIoT gateways. The difference is that the requirement CR 2.1 RE(2) Permission mapping to roles in the Core tier for gateways, is in the Advanced tier for IIoT devices.

  Permission mapping has been placed in the Advanced tier for IIoT devices as it may add unnecessary complexity for IIoT devices with very few user functions and therefore very few permissions.

- The Advanced tier for both IIoT devices and gateways includes as certification criteria all 62443-4-2 requirements, with exceptions as noted in the first bullet and listed in Table 5.

Section 4.4.5 describes the rationale for this structure.

If desired by a certification scheme owner, capability security level 2, 3, or 4 certifications as they are currently defined, could be made available for IIoT devices or gateways, obtained together with an IIoT certification. This would allow suppliers to demonstrate and declare the highest 62443-4-2 capability security level achieved by their product. An example declaration for a product could be "Certified to <Certification Brand Name> IIoT Gateway Requirements Core Tier and 62443-4-2 capability security level 3."

It is recommended that an asset owner for which the requirements in Table 5 were necessary, would request a 62443-4-2 certification to the capability security level at which the desired capabilities become requirements.

Table 5. All existing 62443-4-2 capability security level 1-4 requirements used for IIoT device and gateway certification with these exceptions

Capability security levels	Requirement not a criterion for IIoT device and gateway certification	Rationale for exception
3, 4	**CR 1.7 RE(1) Password generation and lifetime restrictions for human users** Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	Changing passwords often is no longer considered a best practice. See NIST SP800-63B, 5.1.1.2 which states "Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)."
3	**CR 2.1 RE(3) Supervisor override** Components shall support a supervisor manual override for a configurable time or sequence of events.	Used to elevate privileges to permit quick response in emergencies. Not included due to limited functionality of IIoT components for which this would be relevant, and added risk of providing this feature in an environment without physical protection.
4	**CR 2.1 RE(4) Dual approval** Components shall support dual approval when action can result in serious impact on the industrial process.	This organization of personnel responsibilities may not be practical or used in all cases. Other approaches such as safety systems may be used to mitigate the effects of such actions.

Capability security levels	Requirement not a criterion for IIoT device and gateway certification	Rationale for exception
4	**CR 3.9 RE(1) Audit records on write-once media** Components shall provide the capability to store audit records on hardware-enforced write-once media.	Requirement is intended to defend against attack on audit media, which is in many cases in a protected environment, and not exposed to the full set of adversaries on a connected untrusted network. Further, for IIoT devices, a typical architecture would not write audit records directly from such a device to removable media, as an IIoT device may hold only a few records at a time. Rather, the device would transmit records to a collection point (supported by CR 6.1 RE(1) *Programmatic access to audit records,* which falls under the Core tier per Table 6 below). Records could be written to write-once media from that collection point.

4.4.5 Rationale for recommended application of 62443-4-2 to IIoT devices and gateways

This section discusses how the recommendation in 4.4.4 was developed.

The study of the IoT/IIoT industry/government sources that yielded the additional functional requirements listed in 4.3.2, involved attempting to map the requirements in these sources to 62443-4-2. It was found that when such a mapping could be found (as shown in the examples in Section 7 – Appendix 3), the corresponding 62443-4-2 requirement was often identified in 62443-4-2 as required for level 2, 3, or 4. In other words, IIoT devices and gateways were judged by these sources to require some controls which 62443-4-2 had assigned to higher capability security levels. This is to be expected because:

- As defined in 62443-4-2, increasing capability security levels define the characteristics of the adversary against whom protection is desired. These characteristics are: context (casual/coincidental, or intentional), and for intentional attacks: means of attack (simple or sophisticated), skill (Generic or IACS specific), available resources (Low, Moderate, Extended) and motivation (Low, Moderate, High).
- Direct connection to the Internet provides exposure to all of these types of adversaries.

SL-C 2 is the lowest capability security level that considers intentional attacks, which are present in IIoT scenarios addressed here, due to the direct connection to an untrusted network. The capability security level 3 and 4 requirements added for Core tier are shown in Table 6 along with associated rationale for including them in Core.

Table 6. IIoT device or gateway Core tier requirements from 62443-4-2, with SL-C 3 or 4

62443-4-2 requirement ID and name	Rationale for placement in Core IIoT tier	62443-4-2 Capability Security Level
CR 2.12 RE(1) *Non-repudiation for all users*	Protect against and diagnose attacks via the untrusted network connection	4
CR 1.2 RE(1) *Unique identification and authentication*	Protect against and diagnose attacks via the untrusted network connection	3
CR 2.9 RE(1) *Warn when audit record storage capacity threshold reached*	Enable incident detection and investigation in a complex IIoT environment, with logs from a large set of devices and attackers that intentionally create large logs to obscure their activities	3
CR 6.1 RE(1) *Programmatic access to audit logs*	Enable incident detection and investigation in a complex IIoT environment, with logs from a large set of devices and attackers that intentionally create large logs to obscure their activities	3
CR 7.6 RE(1) *Machine-readable reporting of current security settings*	Enable practical monitoring of the status of large numbers of remote devices	3
EDR|HDR|NDR 2.13 RE(1) *Active Monitoring*	Refers to logging of attempts to access diagnostic and test interfaces, which otherwise will enable unseen and unrecorded attacks particularly for devices in unprotected physical locations	3
NDR 5.2 RE(2) *Island mode*	Supports shutting off the untrusted network connection to the component when under attack or in advance of an anticipated attack	3

4.4.5.1 Alternate approaches

The project team worked through the following approaches and concerns, to arrive at the two-tier approach for IIoT device and gateway certifications.

1. First proposed a mandatory capability security level, by foundational requirement. Found some exceptions desired to add and delete, for most of the FR's.

2. The lowest capability security level that included all needed requirements, was 4. However, that did not mean all capability security level 4 requirements were deemed mandatory for IIoT devices and gateways. Further, there are no existing 62443 components certified for SL-C 3 or 4.

3. It was also questioned whether the minimum IIoT requirements should not be static, but rather consider risk – at least to the extent that a supplier is able to do so. This means that there should be some choice of certification features corresponding to the level of risk which the certified product is expected to encounter. That is how 62443-4-2 uses capability security levels.

4. A 3-tier partition of 62443-4-2 requirements was proposed. The middle tier did not seem to have a driving rationale, and some middle tier items were moved up or down, leaving not much for the middle tier.

5. The two tier partition was proposed and refined.

4.4.6 Additional certifier guidance

While existing 62443-4-2 requirements are recommended as applicable for IIoT device and gateway certifications in 4.4.4, the implications of these requirements for the IIoT environment may not be fully apparent. For that reason, it is recommended that the guidance in this section on scope for certifier validation, be included in instructions for certifier evaluation of applicable 62443-4-2 requirements to IIoT devices and gateways. This guidance is judged to be within the requirement scope already intended by 62443-4-2. It serves to clarify this scope for the IIoT case, addressing aspects of these requirements called out separately in IoT/IIoT industry sources. This discussion covers topics that arose during the analysis of these sources; the present study did not undertake a 62443-4-2 requirement-by-requirement evaluation of additional guidance that may be helpful for certifiers of IIoT devices and gateways.

4.4.6.1 62443-4-2 Functions by integration into system

Ten requirements in 62443-4-2 state that a required function can be provided locally by a component, or by integration into a system that supports the function. These requirements (provided for reference in Section 10 - Appendix 6, Table 19) were examined to determine if this option should be permitted in the case of IIoT devices and gateways, particularly if the integration involves the component's connection to the Internet. The concern is the situation where the Internet connection or cloud based-functionality is not available, which is an expected occurrence. The conclusions from this investigation were that (1) no changes are recommended as necessary to the standard itself for these requirements and (2) some guidance for the certifier will be useful for four of the requirements, shown in Table 7 below:

- For the two requirements regarding the authentication event itself, if the authentication is gating access to an essential function, use of the connection to the Internet would not be permitted. This is due to 62443-4-2 CCSC 1, which requires (by reference to 62443-3-3 4.2) that "access controls (IAC and UC) shall not prevent the operation of essential functions..." The requirements in the standard stand as-is, but their implications in this case should be noted to the certifier.
- The two requirements CR 3.4 and CR 3.4 RE(1) which require reporting of the results of integrity and authenticity checks, do not explicitly require immediate reporting. Therefore, the Internet connection may be used for reporting in support of these requirements if there is an approach for preserving results until a lost Internet connection is restored. In this case, the usual strategy of preserving the newest results may not be appropriate. One might save the oldest results instead, since it may have been an integrity/authenticity attack which caused the Internet connection to fail.

Table 7. Selected 62443-4-2 functions that may be provided by integration into system

Requirement ID and Name	Requirement Statement	Topic
CR 1.1 *Human user identification and authentication*	Components shall provide the capability to identify and authenticate all human users according to ISA 62443-3-3 SR-1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.	Authentication event
CR 1.9 *Strength of public key-based authentication*	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device); and f) ensure that the algorithms and keys used for the public key authentication comply with 8.5 CR 4.3 - Use of cryptography.	Authentication event
CR 3.4 *Software and information integrity*	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Reporting
CR 3.4 RE(1) *Authenticity of software and information*	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	Reporting

4.4.6.2 Other 62443-4-2 requirements

This section provides IIoT-specific certifier guidance for validation of selected 62443-4-2 requirements in addition to that provided for the four requirements discussed in 4.4.6.1.

NDR 1.13 *Access via untrusted networks* reads: "The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks." The certifier should examine not only device access for normal component operations, but also access for component management and configuration via the interface with an untrusted network. For example, authorizing management and configuration traffic by port, protocol, and application would satisfy this requirement for "control," as would other approaches that the certifier judges as effective or better.

62443-4-2 CR 3.1 *Communication integrity* reads: “Components shall provide the capability to protect integrity of transmitted information.” The certifier should consider not only information transmitted to and from the component, but also information transmitted between zones internal to the component. Internal zones are discussed in Sections 4.3.4 that describes compartmentalization requirements.

62443-4-2 CR 3.1 RE(1) *Communication authentication* reads: “Components shall provide the capability to verify the authenticity of received information during communication.” The certifier should examine not only communication during component operations, but also communication for component management, in particular for configuration and remote delivery of software updates.

62443-4-2 EDR|HDR|NDR 3.14 *Integrity of the boot process* reads: “Embedded/host/network devices shall verify the integrity of the firmware, software, and configuration data needed for the component’s boot and runtime processes prior to use.” The certifier should include verification that integrity is accurately checked even following attacks enabled by physical possession of the component, but limited to attacks where the attacker uses external interfaces and does not physically open the unit.

62443-4-2 EDR|HDR|NDR 3.14 RE(1) *Authenticity of the boot process* reads: “Embedded/host/network devices shall use the component’s product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component’s boot process prior to it being used in the boot process.” The certifier should include verification that integrity is accurately checked even following attacks enabled by physical possession of the component, but limited to attacks where the attacker uses external interfaces and does not physically open the unit.

62443-4-2 NDR 5.2 RE(2) *Island mode* reads: “The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode).” The certifier should verify that the component has the capability to disable the connection to the untrusted network. Although this connection is not normally the control system boundary, it is a zone boundary, and this is believed to be part of the intent of NDR 5.2 RE(2).

62443-4-2 CR 6.2 *Continuous monitoring* reads: “Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.” The certifier should include verification that events are reportable through interfaces commonly accepted by the industrial and security communities. This is in accordance with requirements EVENT 1.3 in 62443-2-1 and SP.08.01 RE(1) in 62443-2-4.

62443-4-2 CR 7.1 *Denial of service protection* reads: “Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.” The certifier should include for consideration under this requirement, DoS events against the IIoT component or against other parts of the IIoT system of which the component is a part, that disable cloud functionality or communication of the component with the cloud.

62443-4-2 CR 1.5D *Authenticator management* reads: “Components shall provide the capability to protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.” The certifier should include verification of protection from attackers who have physical access to the component.

62443-4-2 CR 7.4 *Control system recovery and reconstitution* reads: “Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.” The certifier should include verification that this requirement is met after failure of an update or upgrade.

4.5 Requirements for commonly accepted practices

This section recommends that IIoT device and IIoT gateway certifications incorporate certification criteria, that require the mechanisms used to conform to selected mechanism-agnostic

62443-4-2 requirements, be consistent with commonly accepted industry practices for IIoT.

4.5.1
Overview of recommendation for commonly accepted practices criteria

All industry/government sources reviewed for this study include discussion of the use of *cryptography* and *hardware-based* security protections in the IIoT environment. The study concluded that for an IIoT certification to achieve credibility in the industry, it would need to address these topics. Further, certification criteria related to these topics would necessarily extend beyond strictly verifying conformance with the existing 62443-4-2 requirements. This is because although 62443-4-2 requires that the objectives intended for these protections be met, it does not specify how they will be met.

In particular, it is recommended that certification criteria for a selected set of existing 62443-4-2 requirements (listed below in Table 8), be augmented for IIoT devices and gateways to require conformance with "commonly accepted practices for IIoT." These practices typically will involve cryptographic mechanisms. For this specification approach to be effective, certification scheme owners will maintain pointers to sources external to the certification specifications, that are to be considered as sources for such practices. Certification will require either meeting these selected 62443-4-2 requirements in a manner specified by one of the referenced sources, or using other mechanisms if equivalence or superiority to commonly accepted practice is demonstrated.

In addition, one requirement for hardware implementation is recommended for the Core tier, that is not currently required by 62443-4-2; this is hardware support for supplier root of trust.

The following sections provide further background, and expand upon these recommendations, related rationale, and possible alternative approaches for validation of the 62443-4-2 requirements in Table 8 for IIoT devices and gateways.

4.5.2
Background

The two general technology mechanisms cryptography and hardware-based protections, can be viewed as implementations of requirements stated more generally in 62443-4-2, in particular for the 62443-4-2 requirements shown in the first column of Table 8 below. IoT/IIoT sources reviewed for this study discuss the use of particular mechanisms to meet these requirements, shown in the second column of Table 8. (Specific references in these industry/government sources are provided in Section 8 - Appendix 4.) In some cases, the sources specify the use of cryptography without further elaboration; in other cases, they further specify particular cryptographic protocols or algorithms.

Table 8. Selected 62443-4-2 requirements with industry accepted technology approaches for IoT/IIoT

62443-4-2 Requirement	Technology Approaches from Industry Sources
CR 1.1 *Human user identification and authentication* Components shall provide the capability to identify and authenticate all human users according to ISA 62443-3-3 SR 1.1 on all interfaces capable of human user access....	two-factor authentication, multi-factor authentication, certificates (See Note 1 below table)
CR 1.2 *Software process and device identification and authentication* Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA 62443-3-3 SR 1.2.	certificate-based; strong cryptographic credentials; multi-factor
CR 3.1 *Communication integrity* Components shall provide the capability to protect integrity of transmitted information.	digital signatures; SSH; IPsec; TLS; DTLS with 128-bit AES; EAP/TLS; PEAP
CR 3.1 RE(1) *Communication authentication* Components shall provide the capability to verify the authenticity of received information during communication.	Certificate based
CR 3.4 *Software and information integrity* Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	digital signatures; signatures using RSASSA-PKCS1-v1_5; signatures using ECDSA with curve P-256; hashes (See Note 2 below table)
EDR|HDR|NDR 3.12 – *Provisioning product supplier roots of trust* [Embedded|Host|Network] devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Hardware root of trust
CR 4.1 – *Information confidentiality* Components shall a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and b) support the protection of the confidentiality of information in transit as defined in ISA 62443-3-3 SR 4.1.	Standardized cryptographic modules; 128-bit AES minimum for at rest SSH; IPsec; TLS; DTLS with 128-bit AES for in-transit

NOTE 1 Multi-factor capability is required by 62443-4-2 CR 1.1 RE(2) for capability security levels 3 and 4. This requirement would apply for IIoT devices or gateways at the Advanced tier, under the recommendations in Section 4.4.4 of the present document.

NOTE 2 In 62443-3-3, the corresponding system level requirement to CR 3.1 is SR 3.1. The requirement SR 3.1 *Communication integrity*, in RE(1) *Cryptographic integrity protection,* requires the use of cryptography for communication integrity at levels 3 and 4.

The following sections discuss the treatment of cryptography and hardware security mechanisms in 62443-4-2, and rationale for the recommendation in 4.5.1 for the certification of IIoT devices and gateways.

4.5.3 Certification requirements for cryptography

A general observation is that 62443-4-2 does not explicitly require the use of cryptography to *meet any requirement at any capability security level,* however it does place requirements on the use of cryptography *if* it is used (CR 4.2 *Use of cryptography,* CR 1.9 *Strength of public key-based authentication,* CR 1.14 *Strength of symmetric key-based authentication).* Nevertheless, a case might be made that in today's technology environment, there is no method other than use of cryptography to conform to some 62443-4-2 requirements such as protection of authenticators (CR 1.5d), confidentiality protection for data in transit (CR 4.1b), and verification of the authenticity and integrity of software and information (CR 3.1, CR 3.4 and their requirement enhancements).

Given the current broad acceptance of known cryptographic mechanisms considered appropriate and commonly accepted for the IIoT environment, it is likely that a security certification program that does not acknowledge those mechanisms in some manner, will have limited acceptance and value to the industry.

As an example, an existing IoT device certification developed by CTIA [CTIA], explicitly enumerates permitted cryptographic algorithms and key sizes for device store encryption (62443-4-2 CR 4.1). As a second example, an asset owner in the ISAGCA/ISCI project team, keeps an internal list that ranks identification/authentication technologies (62443-4-2 CR 1.1, 1.2) by strength, and also maintains policies about where these technologies may be applied.

For this reason, the approach described in 4.5.1 is recommended to incorporate requirements for either the use of cryptographic methods, or the use of cryptography with specified characteristics in IIoT devices and gateways, in support of the related 62443-4-2 requirements listed in Table 8.

The corresponding cryptographic technologies listed in Table 8 are offered as examples, and are not specific recommendations from this study. The formal vetting and balloting processes, and resources available to certification scheme owners for development of certification criteria, are felt appropriate for identifying acceptable technologies.

4.5.4 Certification requirements for use of hardware security mechanisms

Normative language in 62443-4-2 does require hardware mechanisms in four requirements: CR 1.5 RE(1) *Hardware security for authenticators,* CR 1.9 RE(1) *Hardware security for public key-based authentication,* CR 1.14 RE(1) *Hardware security for symmetric key-based authentication,* and CR 3.9 RE(1) *Audit records on write-once media.* The first three of these hardware requirements are required at capability security levels 3 and 4; the fourth at level 4. All of these requirements with the exception of CR 3.9 RE(1) would apply for IIoT device and gateway certifications at the Advanced tier, under the recommendations in Section 4.4.4. The hardware security requirements CR 1.9 RE(1) and CR 1.14 RE(1) would apply, respectively, *if* the component used either public key-based authentication or symmetric key-based authentication.

The view presented in the IoT/IIoT security sources reviewed for this study is that further use of hardware protections is appropriate for IIoT.

Specific uses of hardware-based security seen in IoT/IIoT industry sources, and not required by 62443-4-2, are limited to (1) supplier root of trust (as noted above), and (2) hardware support of other security properties where neither the property nor hardware support for it are addressed in 62443-4-2. These properties are compartmentalization and trusted execution environment (TEE). For the purposes of this study, we have translated TEE into the functional requirement to ensure integrity of code and data at startup and runtime. Hardware is typically used specifically for protection of code and data for cryptographic or other security-sensitive operations. Compartmentalization and protection for code and data in use have been added to recommended certification criteria for IIoT devices and gateways as described in Section

4.3.2, but hardware implementations of them are not mentioned in those descriptions.

Recommendations for hardware-based security certification requirements are:

- Supplier root of trust in hardware for Core tier. A requirement for use of hardware for supplier root of trust is also recommended for level 3 or higher in 62443-4-2. This is consistent with the other requirements for hardware protections in the standard.
- Hardware compartmentalization of security functions, for Advanced tier
- Hardware-based protections for code and data in use, for Advanced tier.

A number of IoT/IIoT sources specifically recommended use of a TPM (Trusted Platform Module, specified in [ISO/IEC 11889]), which is a hardware component that performs cryptographic operations independent of the CPU. TPM provides an approach to implementing security of cryptographic information and TEE for some cryptographic operations. It may be used to meet a number of requirements in the present document that are recommended for IIoT components. Some members of the project team felt a TPM should be required for IIoT device or gateway certification; others felt that that the requirements themselves were sufficient and specification of their implementation via TPM is not necessary. However, it is recommended as a requirement for both Core and Advanced tier certifications, that mechanisms for protections for code and data in use, be in accordance with commonly accepted practices for IIoT. Certification scheme owners will identify such practices as described in 4.5.1.

4.5.5 Possible related modifications to 62443-4-2

Here the question is considered, whether requirements for specific cryptographic mechanisms, or use of cryptography in general, should be contemplated in the 62443 standard, for the IIoT environment. An alternative view is that addressing these kinds of implementation concerns should be in the scope of certification programs only.

Most IEC standards (such as 62443) would neither be expected nor permitted to specify the use of a particular technology mechanism. Such a specification would be considered a prescriptive standard, which by IEC directives, is not preferred under most circumstances. A performance-based standard is preferred, as it is felt to support and not limit innovation. Therefore, if there is a need to specify general or particular security mechanisms in the IIoT component certification program, this does not necessarily imply that one would ultimately include such requirements in the 62443 standard or other future IEC standard addressing IIoT.

It should be noted, however, that there is precedent for normative text in 62443 to refer to “commonly accepted standards and recommendations,” and “internationally recognized and proven [guidelines/practices/recommendations],” as these phrases appear in eight requirements in 62443-4-2. Further, there is one system requirement in 62443-3-3, that explicitly requires cryptographic methods (but is not more specific). This is for communication integrity protection at levels 3 and 4 (requirement SR 3.1 RE(1) *Cryptographic integrity protection).* The standard does not specify mechanisms to be used to meet SR 3.1 *Communication integrity* for levels 1 and 2. These approaches to requirements for IIoT could be considered for future modifications to 62443-4-2. One might also augment the phrase “commonly accepted standards and recommendations” to say “commonly accepted standards and recommendations for IIoT.”

4.5.6 Alternative approaches

Formulating requirements that will be judged by the marketplace as sufficient to serve the IIoT environment, is difficult to achieve without naming specific technologies. This is neither a new issue nor unique to this domain of study. It is a well-known challenge to avoid using the undefined term “sufficient” and avoid naming specific technologies in standards so as not to slow innovation. At the same time, one must effectively describe the performance expected for conformance with the standard.

Based upon the above discussion, it is assumed (1) that specific cryptographic technologies will not be named in 62443, now or in the future and

(2) nevertheless, IIoT certification criteria should address in some verifiable manner, the adequacy of security mechanisms used, specifically mandating use of cryptography, or something better, which will extend beyond 62443 requirements. The following are then alternative approaches for specifying such certification criteria for the 62443-4-2 requirements in Table 8, for certification of IIoT devices and gateways.

- **Silent on technologies:** Certifier validates conformance with these 62443-4-2 requirements as currently stated, agnostic to technology used. Adequacy of the mechanism used to meet a requirement is judged by the certifier, based on review of the product threat model and associated mitigations, as required for validation of 62443-4-1 conformance.
- **Specify acceptable technologies:** Identify as part of certification specifications, a list of acceptable technologies for meeting these requirements, certifying only products that use these technologies.
- **Specify examples of acceptable technologies:** Identify as part of certification specifications, a list of acceptable technologies for meeting these requirements, and also permit other technologies to be used if equivalence or superiority to a listed technology is demonstrated.
- **Refer to external sources for acceptable technologies:** Require in certification specifications, use of "commonly accepted practices." Maintain outside of the certification specifications, pointers to such practices. Certification will require meeting these requirements in a manner specified by one of these sources, and also permit other technologies to be used if equivalence or superiority to current acceptable practice is demonstrated.

The following paragraphs discuss the pros and cons of these approaches and expand upon the recommendation in 4.5.1.

An IIoT certification program *silent on technologies* is burdensome for certifiers, and may be viewed as too subjective. It is unlikely to provide sufficient value to asset owners, who would like an authoritative resource for navigating an evolving field. *Specify acceptable technologies* discourages supplier innovation. *Specify examples of acceptable technologies* will still limit supplier innovation to some extent, and also will require ongoing changes to the certification specifications themselves as the field evolves.

Therefore, in 4.5.1 it has been recommended that an IIoT certification program use the fourth approach, in which the certification program specifications would *refer to external sources for acceptable technologies.* The certification scheme owner or partner organizations may themselves provide pointers to practices documents and/or develop such documents. It will be important for scheme owners to ensure that these resources are kept up-to-date. However, if an innovation is ahead of these documents, certifications taking advantage of that innovation can still proceed. These external resources will be of value for the IIoT industry beyond their use in the certification program, and can be modified with less formal process and time delay than certification specifications (or standards).

The major reasons for this recommendation are to achieve credibility in the industry, and value for the certification, from the point of view of asset owners, while retaining flexibility for suppliers. It is understood that while flexibility for suppliers is retained "on paper," that most suppliers interested in certification will nevertheless opt for known accepted "certifiable" technologies, rather than risk being unable to make the case for a new technology solution. For this reason, if approaches can be developed to specify performance-based criteria for any of the requirements in Table 8, then at that time it will be preferred to integrate those performance-based criteria into the IIoT certification criteria and ultimately into the 62443 standard. An example would be to explore whether specifying levels of assurance as defined in [ISO/IEC 29115] *Entity authentication assurance framework* could be used as performance-based criteria for IIoT authentication.

It is possible that the IIoT certification program could benefit by treating other requirements in 62443-4-2 in this same manner. An example for which this is recommended is:

CR 6.2 *Continuous monitoring* Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

An industry practices document for IIoT that describes specific events to be considered for detecting breaches would be very valuable. [IICSF] under 7.3 *Endpoint Monitoring and Analysis* mentions integrity checking, detecting malicious usage patterns, denial of service activities, enforcement of security policies, and analytics that track security performance indicators. In 10.5.1 the document refers to a model of expected state and interactions, allowing deviations from that model to be detected; in 5.5 it describes analytics such as number of detected attack attempts, and the breakdown of those attempts, as well as characterizing successful attacks, incidents, close calls, policy violations and anomalies that have merited investigation. Many of these analyses would be done external to the component but most would require some support from the component itself. Some examples of detected events from [CTIA] are CPU activity spikes, event log activity spikes, loss of communication, loss of GPS signal. 62443-4-2 already includes a list of required audit log categories in CR 2.8 *Auditable events.* 62443-4-2 includes requirements for response in the face of DoS attacks, but does not explicitly mention detection of these types of attacks.

A second aspect of commonly accepted practices for CR 6.2 was introduced as certifier guidance in 4.4.6.2, which is that events are to be reportable through interfaces commonly accepted by the industrial and security communities. For example, it is expected that in the current environment, support for syslog would be documented among these practices, and therefore required for certification.

4.6 Validations by certifier or supplier test

For IIoT device and IIoT gateway certification, this section recommends validation methods for some functional requirements more rigorous than the methods used in some existing 62443-4-2 certification schemes. Specifically, certifier hands-on test or detailed audit of supplier test artifacts will be applied for some functional requirements. Section 4.6.1 describes the rationale for this recommendation.

4.6.1 Rationale for certifier testing

To validate conformance with functional requirements for 62443-4-2 certification, a certifier will typically either perform a "paper" assessment of design or user documentation, and/or perform functional hands-on testing of the requirement on the product under evaluation. An intermediate approach also used, is certifier review of artifacts from testing performed by the product supplier. A certification program may require the certifier to use a specific method or combination of methods to verify conformance with a requirement. A program may specify that the certifier is to select an appropriate validation approach. This section recommends functional requirements for which either certifier hands-on testing, or certifier review of supplier test artifacts, would be required for IIoT device or IIoT gateway certification.

Selection of certifier validation methods is important for the design of a certification program, because it drives both confidence in the program and program cost. It is expected that an IIoT certification program will incorporate new validation requirements; the incremental cost for doing so should be considered carefully. In particular, certifier hands-on testing is ideally applied selectively, taking into account its advantages and disadvantages. The primary benefit of certifier testing is that for some security requirements, independent testing is the most convincing method of validation. Asset owners that rely on the certification have an expectation that the certifier has some hands-on experience with the certified product. Valuable tests for a certification program are in high risk areas, for which documentation review will be unconvincing, and where supplier testing outcome may be particularly influenced by variations inherent in test approach, environment, configuration, or assumptions.

On the other hand, certifier testing is costly, and the logistics to achieve it extend the certification evaluation schedule. Certifier testing is (in the ideal case) redundant with tests already performed by the supplier in following 62443-4-1 processes. Conformance with these processes is required by 62443-4-2 and therefore will itself be verified under the certification process. Further, in some cases, audit of a thorough ongoing program of supplier tests is more convincing than a necessarily limited test by the certifier (testing of the upgrade process is an example). Therefore, tests valuable for the reasons noted here, with clear pass/fail criteria, and for which a relatively short duration test is convincing, have the highest benefit/cost ratio for a certification program. The overall amount of testing is also balanced to achieve a cost and duration for certification evaluations that is practical in the marketplace.

As an example of existing certification practices, under the ISASecure Component Security Assurance program (ISASecure CSA [CSA-311]), 22 functional requirements in 62443-4-2 for embedded devices require certifier hands-on testing, among the requirements applicable at capability security level 4. Other requirements are either verified by user and/or design documentation review, and a few by review of supplier tests. For those remaining, the certifier determines how they are to be verified.

For ISASecure CSA, the type of validation activity is specified per requirement, and does not change based upon the capability security level of the certification. For example, 7 of the 22 functional requirements with mandatory hands-on certifier testing for level 4, are also functional requirements for capability security level 1, and would also be subject to certifier hands-on testing under an ISASecure CSA certification to level 1. Some cybersecurity certification programs in the industry increase the amount of testing required, in some cases for the same requirements, at higher security levels; such an approach is not proposed here. For example, the highest evaluation assurance level under the Common Criteria standard, requires the certifier replicate all supplier testing of security functionality for the target of evaluation.

4.6.2
Requirements validated by certifier test or supplier test artifacts

Recommendations described in 4.6.2.1 and 4.6.2.2 below identify eight additional functional requirements for certifier hands-on test, and eight for certifier examination of supplier test artifacts, in addition to the requirements for which these methods are currently used under the ISASecure CSA program. Additional requirements subject to these validation activities are selected from among both new IIoT requirements presented in Table 1, and existing requirements in 62443-4-2. The selection recommended here is based upon the rationale described in 4.6.1.

4.6.2.1
Validation activity for new IIoT requirements

Among the new IIoT device or gateway requirements presented in Table 1, seven are identified for either certifier hands-on testing or examination of supplier test artifacts for IIoT devices, and seven for IIoT gateways, as shown in Table 9 below. Four of these requirements are identified for certifier hands-on test. These recommendations are considered a minimum validation approach for each requirement, acceptable to support certification.

Table 9. Validation activities for additional IIoT requirements, IIoT device and gateway certification

CTest = certifier hands-on-test; STest = supplier test artifacts; Doc = User or design documentation; NA = not applicable

Additional IIoT Requirement (not in 62443-4-2)	Requirement applies to IIoT devices (D), IIoT gateways (G), other high SL-C IACS components *(IACS-H)*	Validation activity for IIoT devices	Validation activity for IIoT gateways
Compartmentalization	D, G, *IACS-H*	Doc	Doc
Secure by default	D, G, *IACS-H*	STest	STest
Authentication of non-human users from untrusted networks	D, G, *IACS-H*	STest	STest
Devices using passwords or keys, have unique initial passwords and keys per device. Initial passwords are generated according to internationally recognized and proven password guidelines OR require changing password on install	D, *IACS-H*	Doc	NA
Protection of software and data in use	D, G, *IACS-H*	Doc	Doc
Device can be remotely updated and upgraded	D, G	Doc	Doc
Enable/disable update/upgrade	D, G	Doc	Doc
Update/upgrade maintains user security settings	D, G, *IACS-H*	CTest	CTest
For management and configuration interfaces from untrusted network, authorize traffic by port, protocol, and application OR do not accept incoming initiation of management/ configuration connections	D, G	CTest	CTest
Device itself does not provide printed design information useful to attackers	D, *IACS-H*	STest	STest
Presence/absence of component can be monitored	D, G	CTest	CTest
Turn off connection to untrusted network, maintain essential functions (test for IIoT gateways also appears under NDR 1.13 in Table 10)	D	CTest	CTest

4.6.2.2 Validation activity for existing 62443-4-2 requirements

Among the existing requirements in 62443-4-2 proposed in 4.4.4 of this report as applicable for IIoT device or gateway certification, 33 requirements are recommended for either certifier hands-on testing, or for audit of supplier test artifacts, as shown below in Table 10. The table also shows that 22 of these requirements currently require hands-on testing by the certifier under the existing ISASecure CSA certification program. All of the current ISASecure certifier hands-on test requirements have been retained in this recommendation.

Of the six requirements added for certifier hands-on testing, five apply to both IIoT devices and gateways. These address turning off the untrusted network connection, software and information integrity (CR 3.4, RE(1), RE(2)), and provisioning asset owner roots of trust inside the security zone (EDR|HDR|NDR 3.13B). For IIoT gateways, hands-on certifier test is also required for a one-way traffic feature for zone boundary protection (if present, under NDR 5.2).

Table 10. Validation activities for existing 62443-4-2 requirements, IIoT device and gateway certification

CTest = certifier hands-on-test; STest = supplier test artifacts; Doc = User or design documentation; NA = not applicable

Functional requirement in 62443-4-2	Validation activity for IIoT devices	Validation activity for IIoT gateways	Existing ISASecure CSA certifier test required for this level and higher
CR 1.9A Strength of public key-based authentication - check validity of signature of a given certificate	CTest	CTest	2
CR 1.9C Strength of public key-based authentication - check certificate's revocation status	CTest	CTest	2
NDR 1.13 Access via untrusted networks (partial test for turning off untrusted connection, test for IIoT devices appears in Table 9)	NA	CTest	—
NDR 1.13 RE(1) Explicit access request approval	NA	CTest	2
CR 2.7 Concurrent session control	CTest	CTest	3
CR 2.8 Auditable events	CTest	CTest	1
CR 2.10(b) Response to audit processing failures - actions taken	CTest	CTest	1
CR 2.11 RE(1) Time synchronization	CTest	CTest	2
EDR|HDR|NDR 2.13 Use of physical diagnostic and test interfaces	STest	STest	—
EDR|HDR|NDR 2.13 RE(1) Active monitoring	CTest	CTest	3
HDR RE(1) Report version of code protection	CTest	CTest	2
CR 3.4 Software and information integrity	CTest	CTest	—
CR 3.4 RE(1) Authenticity of software and information	CTest	CTest	—
CR 3.4 RE(2) Automated notification of integrity violations	CTest	CTest	—
CR 3.9 Protection of audit information	CTest	CTest	2
EDR|HDR|NDR 3.10 RE(1) Update authenticity and integrity	CTest	CTest	2
EDR|HDR|NDR 3.11 Physical tamper resistance and detection	STest	STest	—
EDR|HDR|NDR 3.11 RE(1) Notification of a tampering attempt	STest	STest	—
EDR|HDR|NDR 3.13B Provisioning asset owner roots of trust - inside zone	CTest	CTest	—
EDR|HDR|NDR 3.14 Integrity of the boot process	CTest	CTest	1
EDR|HDR|NDR 3.14 RE(1) Authenticity of the boot process	CTest	CTest	2
CR 4.1A Information confidentiality - at rest	CTest	CTest	1
CR 4.1B Information confidentiality - in transit	CTest	CTest	1
CR 4.2 Erase verification	CTest	CTest	3
NDR 5.2 Zone boundary protection (testing limited to one-way feature, if present as configurable feature, see NOTE following table)	NA	CTest	—
NDR 5.2 RE(1) Deny all, permit by exception	NA	STest	—
NDR 5.2 RE(2) Island mode	NA	CTest	3
NDR 5.2 RE(3) Fail close	NA	CTest	3
NDR 5.3 General purpose, person-to-person communication restrictions	NA	STest	—

Functional requirement in 62443-4-2	Validation activity for IIoT devices	Validation activity for IIoT gateways	Existing ISASecure CSA certifier test required for this level and higher
CR 7.3 RE(1) Backup integrity verification	CTest	CTest	2
CR 7.4 Control system recovery and reconstitution	CTest	CTest	1
CR 7.6 Network and security configuration settings	CTest	CTest	1
CR 7.6 RE(1) Machine-readable reporting of current security settings	CTest	CTest	3

NOTE: Project team members expressed particular concern about gateway testing for the one-way feature when it is a configurable option. This is due to situations in which compliance with configuration guidelines provided by the supplier to achieve the one-way configuration, fails to achieve it.

4.7 Component secure product development lifecycle

Prior sections have focused on component functional requirements for IIoT device and gateway certifications. This section describes enhancements to certification criteria that address secure product development lifecycle process.

Under the approach described in this report to apply 62443-4-2 for IIoT device and gateway certifications, 62443-4-1 also applies to these components (per 62443-4-2 CCSC 4). This section recommends certification program enhancements related to selected 62443-4-1 secure product development lifecycle requirements, in addition to the compartmentalization-related lifecycle enhancements described previously: COMPART 7 in 4.3.4.2.2, and COMPART 9 and COMPART 10 in Section 4.3.4.2.3. The following enhancements include both recommendations for how existing 62443-4-1 requirements are validated by certification programs, and IIoT specific enhancements for existing requirements. Briefly, these are:

- Selection of 62443-4-2 requirements for a component (4.7.1)
- Identify IIoT security context elements (4.7.2)
- Include device failures in threat model (4.7.3)
- Lifecycle impact of cloud dependencies (4.7.4)
- Periodic certifier audit of maintenance of security (4.7.5)
- Proactive notification of update/upgrade availability (4.7.6)
- Advance notification for products to be withdrawn from security update management (4.7.7).

The first four in the above list are pre-release practices in the product lifecycle, and the last three fall under security update management.

It may be useful to add IIoT specific enhancements to the 62443-4-1 standard or to certifier guidance for additional 62443-4-1 requirements. The present study identified topics suggested by industry/government IoT and IIoT sources and project group discussions, but did not review all 62443-4-1 requirements to identify possibilities for other useful IIoT guidance.

4.7.1 Selection of 62443-4-2 requirements

The 62443-4-1 requirement SR-4 *Product security requirements content* (quoted below) states that a supplier shall indicate the required 62443-4-2 capability security level for a product. If the recommendation in 4.4.3 of the present report is accepted, security requirements for IIoT devices and gateways are not cleanly described by a single capability security level, but are described by a tier (Core or Advanced). Hence an adjustment to this 62443-4-1 requirement for selection of security requirements for IIoT devices or gateways is recommended.

62443-4-1 SR-4 *Product security requirements content* A process shall be employed for ensuring that security requirements include the following information:
a) the scope and boundaries of the component or system, in general terms in both a physical and a logical way; and

b) the required capability security level (SL-C) of the product.

4.7.2
Identify IIoT security context elements

The 62443-4-1 requirement SR-1 requires that the intended security context for a product be documented. Under validation of the requirement for a product, it is recommended for IIoT devices and gateways, that the certifier verify that applicable IIoT security context elements such as those described in 4.3.1 are incorporated in this documentation.

4.7.3
Include device failures in threat model

The 62443-4-1 requirement SR-2 requires that a product have a threat model. Under validation of this requirement for a product, it is recommended for IIoT devices and gateways, that the certifier verify that hardware and software failures are identified as threats, where such failures could impact product security. In an IIoT system with many remote components, it may not be feasible to address a failed device quickly. In the meantime, an adversary may take advantage of this state of the device, and may in some cases have caused the failure in order to do so. For example, a hardware or software failure could permit bypass of authentication or authorization, or open additional ports. Reliability can minimize but not prevent failure; since failures will occur, additional layers should provide security protections.

4.7.4
Lifecycle impact of cloud dependencies

Three areas were noted in which known cloud dependencies for IIoT devices or gateways impact the requirements in 62443-4-1 due to required coordination with the cloud developer:

- Security requirements review (4.7.4.1)
- Supplier receiving notifications of security-related issues (4.7.4.2)
- User documentation (4.7.4.3)

4.7.4.1
Security requirements review

The 62443-4-1 requirement SR-5 *Security requirements review* (quoted below), describes representatives that should be part of the requirements review process. It is recommended that a representative knowledgeable in the cloud aspects of the architecture in which an IIoT component is to be deployed, also participate.

SR-5 *Security requirements review* A process shall be employed to ensure that security requirements are reviewed, …Each of the following representative disciplines shall participate in this process. …
a) Architects/developers (those who will implement the requirements);

b) testers (those who will validate that the requirements have been met);

c) customer advocate (such as sales, marketing, product management or customer support); and

d) Security Advisor.

4.7.4.2
Supplier receiving notifications of security-related issues

The 62443-4-1 requirement DM-1 *Receiving notifications of security related issues* (quoted below) enumerates sources that a supplier monitors for notifications of security-related issues for a product. It is recommended that for the case of IIoT devices or gateways, the development organization for cloud-based functionality upon which the product depends, be added as a required source.

DM-1 *Receiving notifications of security related issues* A process shall exist for receiving and tracking to closure security-related issues in the product reported by internal and external sources including at a minimum:
a) security verification and validation testers;

b) suppliers of third-party components used in the product;

c) product developers and testers; and

d) product users including integrators, asset owners, and maintenance personnel

4.7.4.3
User documentation

This section describes the recommendation that for IIoT device or IIoT gateway certifications, user documentation on cloud dependencies be required, and that conformance to a process for the maintenance of that documentation be verified. This documentation includes any ongoing required or optional network communications of the component with the supplier or for purposes of the supplier, and domain names for the destinations of those communications.

A component user may elect to turn off optional communications of this type if judged to pose a risk. If they are unaware that a communication is intended, it may be mistaken as evidence of an intrusion.

Existing requirements under the 62443-4-1 Practice 8 Security Guidelines (SG), remain applicable to user documentation for IIoT devices and gateways. The new user documentation topic referred to here as *cloud dependencies* is recommended as an addition to the existing topics in the SG requirements. The practice of documenting cloud dependencies is described in the two IoT sources as shown in Table 11.

Table 11. Industry/government recommendations for documentation of cloud dependencies

Source	Reference	Practice
[NISTCAT] NIST catalog of IoT device cybersecurity capabilities	Non-technical capabilities: Logical access to interfaces	Provide the IoT device customers with documentation detailing all the cloud services used to support the use of the IoT device
[CTIA] CTIA Cybersecurity Test Plan for IoT Devices Version 1.2	Test case 3.1.4 Terms of service and privacy policy test	Try to obtain the list of cloud services that the device requires access to for normal operation [of the] device...

In addition, it is recommended that certification criteria incorporate verification over time that cloud dependencies information is kept up to date. Maintenance of user documentation is not explicitly mentioned in normative requirements text in 62443-4-1, although informative text in 62443-4-1 12.1 reads "The remainder of Clause 12 defines requirements for development processes used to produce and maintain this documentation. Supporting these requirements means that the product supplier has identifiable processes for creating, maintaining and delivering documentation that describes how to harden the product." Typically, IACS product documentation will change driven by a new product release, and therefore such changes are naturally covered by existing 62443-4-1 requirements under the practice Security Guidelines (SG) which require creating documentation for a *product*. However, in the IIoT case, even though an IIoT device or gateway itself may not change, cloud-based functionality with which it interacts may change, in a way that alters IIoT device or gateway dependencies upon it.

Existing 62443-4-1 requirements under the SG practice already list integration information as a documentation topic, as shown below in Table 12. While this might in the ideal case include the cloud dependencies information described here, it is nevertheless recommended that IIoT certification requirements *explicitly* require that cloud dependencies be included in user documentation. The existing SG requirements are usually applied in a context where the asset owner or integrator is able to adjust the integration scenario in accordance with security guidelines provided by the supplier. In the IIoT case, the asset owner may have less control over how the component integration scenario is defined, due to fixed dependencies on cloud capabilities, that evolve separately from an asset owner's IIoT devices or gateways.

Table 12. Existing 62443-4-1 requirements for secure integration guidelines

62443-4-1 requirement number	Requirement name	Documentation topic related to integration
SG-2	Defence in depth measures expected in the environment	A process shall be employed to create product user documentation that describes the security defence in depth measures expected to be provided by the external environment in which the product is to be used (see Clause 6, Practice 2 – Specification of security requirements).
SG-3	Security hardening	Guidelines, instructions, rationale and recommendations for ...integration of the product, including third-party components, with its product security context

4.7.5 Periodic certifier audit of maintenance of security

This section recommends strengthening existing validation of supplier security maintenance practices, by adding a periodic audit of these practices for IIoT devices and gateway products after initial product certification.

One of the more challenging aspects in the design of a product certification program, is maintenance of the certification over the lifecycle of the certified product, as the product and its environment change over time. In the context of IACS components, this includes defining how certification can be maintained through updates and upgrades of these products, as well as changes to the threat environment. Because IIoT devices and gateways are directly connected to the Internet and may reside in remote physical locations, threats and their realizations are expected to evolve rapidly. Ideally a certification can continue to provide assurance to asset owners over time under these conditions.

62443-4-1 addresses these topics under requirement SR-2 Threat Model (see Table 13), and under requirements for the practices *Security Defect Management* (requirements DM-1 though DM-6) and *Security Update Management* (SUM-1 through SUM-5). The challenge in addressing DM and SUM requirements in a product certification program, is that at the time of product certification, the application of these practices to the product at hand cannot be verified - *as they will occur in the future*. For example, these practices require that suppliers actively track threats related to their products, determine responses appropriate to the severity of security-related issues, and carry them out in a timely fashion.

Table 13. 62443-4-1 requirement for updates to threat model

SR-2 (excerpt)	Updates to threat model	The threat model shall be reviewed periodically (at least once a year) for released products and updated if required in response to the emergence of new threats to the product even if the design does not change

IIoT devices and gateways exist in a dynamic threat environment, where a timely response to known defects and adversaries is critical. For this reason, it is recommended that a scheme owner for an IIoT device or IIoT gateway product certification program, offer a program where on a periodic basis, the certifier:

- Verifies conformance for a certified product, with the requirement for periodic update of the product threat model (part of 62443-4-1 SR-2); and
- Verifies conformance with 62443-4-1 requirements under DM (DM1-DM6), and with SUM-5, *Timely delivery of security patches,* as applied to a certified product.

A certification scheme owner might define this periodic review either as a requirement specifically for maintaining certification for IIoT components, for maintaining any IACS component certification, or as an optional offering to augment any product certification, as the market dictates. An appropriate length period for this periodic review would be defined by the scheme owner.

While offering this verification for IIoT device and gateway product certifications is the basic recommendation here, the following sub sections describe how such a review might be implemented with minimum impact on suppliers.

4.7.5.1
Example application approach for ISASecure CSA maintenance of certification

The approach currently taken by ISASecure for maintenance of product certification over time, is that a supplier must maintain the 62443-4-1 development process certification ISASecure SDLA (Security Development Lifecycle Assurance), in order to maintain the validity of ISASecure product certifications for updates of certified products, and to obtain certification of upgrades *(update* and *upgrade* as defined in 3.1). Maintaining ISASecure SDLA certification requires a recertification audit of the supplier's development process every three years. An SDLA recertification audit entails a review based upon a sampling of products, for conformance with all 62443-4-1 requirements. However, the ISASecure specifications do not explicitly require review of processes related to certified products during an SDLA certification audit.

Following the recommendation above, the three-year audit "sample" used for SDLA recertification could be required to include review of the security maintenance process as executed in the past three years for certified products. This "enhanced" audit would be limited to the 62443-4-1 requirement SR-2 for periodic threat model updates, all requirements under the practice Defect Management, and requirement SUM-5 for timely delivery of security patches, as they relate to products holding ISASecure certifications at the time of the SDLA certification audit. A scheme owner might permit the certifier to select a sample of certified products in cases where a supplier has many.

As noted above, periodic threat model updates, DM requirements, and SUM requirements, are for the most part not verifiable at the time of initial product certification. Under ISASecure CSA, 8 of these 11 requirements are not addressed for the certified product under CSA assessments.

4.7.5.2
Audit the auditor implementation concept

Under any certification program, supplier effort to support certifier review of 62443-4-1 SR-2, DM, and SUM-5 requirements for certified products, could be minimized by leveraging already existing supplier processes for conformance with the requirements in 62443-4-1, using an "audit the auditor" approach. This means that the certifier audits the results of internal supplier audit programs that are already in place due to conformance with 62443-4-1.

In order to audit DM requirements for certified products, the certifier could examine the periodic review of these requirements already performed under DM-6 (shown in Table 14), specifically as these requirements relate to certified products. This certifier review could be streamlined using a version of the outputs of the supplier's own DM-6 periodic review, organized by product and release. In order to audit SUM-5, likewise the certifier could examine the outputs of the supplier process verification performed under SM-12 (shown in Table 14) for the SUM-5 requirement, for releases of certified products.

In the ISASecure example, the requirement for update of the product threat model which is part of SR-2, would also be covered by the SM-12 process verification if a product version has been released in the past three years.

Table 14. 62443-4-1 Supplier audit requirements leveraged for assuring maintenance of security

SM-12	Process verification	A process shall be employed for verifying that, prior to product release, all applicable security-related processes required by this specification (See SM-5: Process Scoping) have been completed with records documenting the completion of each process.
DM-6	Periodic review of security defect management practice	A process shall be employed for conducting periodic reviews of the security-related issue management process. Periodic reviews of the process shall, at a minimum, examine security-related issues managed through the process since the last periodic review to determine if the management process was complete, efficient, and led to the resolution of each security-related issue. Periodic reviews of the security-related issue management process shall be conducted at least annually.

4.7.6
Proactive notification of update/upgrade

One goal for the asset owner in an IIoT environment is to be able to respond as quickly as possible to secure their system against a known threat. In particular, if an IIoT supplier has a product update or upgrade available that protects against the threat, the asset owner would like to be aware of this as soon as possible.

Current requirements in 62443-4-1 on related topics include:

- DM-5 *Disclosing security-related issues,* which requires the supplier will inform product users about reportable security-related issues and a description of the resolution
- SUM-2 and SUM-3 regarding security update documentation, which require that documentation with specified minimum contents will be made available
- SUM-5 *Timely delivery of security patches,* which requires a supplier policy for the timeframe in which a security patch will be delivered.

In conformance with these requirements, a supplier could for example tell a product user that a patch was planned to address a particular issue, and later make the patch and required documentation available from a customer support website.

An additional requirement recommended for IIoT device and gateway certification is that a supplier offer a proactive method for notification of availability of an update or upgrade, to designated contacts for product users. This can be implemented for example, by offering a sign-up for an email list. The distinction from the existing 62443-4-1 requirements is that the product user does not need to continuously check in with the supplier to look for updates, but will be notified proactively by the supplier.

This method for identifying patches for installation is listed as an option in [ANSI/ISA 62443-2-3] *Patch Management in the IACS Environment* (B.5.2, option b). It is also listed as a Common Element for implementing software updates in [NIST8259A]:
6b) The ability to enable or disable notification when an update is available and specify who or what is to be notified

This requirement is of importance whether or not a product offers the capability for automatic updates and/or upgrades and whether or not the product user employs the automatic feature. If a product user receives an automatic update or upgrade, the update notification informs them to be alert for possible undesired effects. If the product user does not use automatic updates or upgrades, the update or upgrade notification alerts them to start their process for evaluating and installing it.

In addition to individual update notifications, it is recommended that a list of all available updates to a product release be published and available to all product users.

It is recommended that the process requirements for proactive update/upgrade notification and list of available updates and upgrades, be considered as additions to 62443-4-1.

4.7.7
Advance notification for products to be withdrawn from security update management

The 62443-4-1 requirement SUM-2 *Security update documentation* lists specific documented items about product security updates that shall be made available to product users, noting that documentation is not limited to the list provided. A recommended certification enhancement is that the certifier verifies that the supplier process in fulfillment of SUM-2 includes a process to notify users in advance when a product is planned to be withdrawn from support for security updates, where the time frame for notification takes into account user management of change processes for replacement of the product. A requirement addition to this effect may also be considered for 62443-4-1 for all IACS components. Such notification may be more critical in the IIoT environment since the lifecycle for many IIoT components is shorter than is generally the case for IACS components.

A version of this requirement is recommended in [ANSI/ISA 62443-2-3] Section 6 part e) “provide adequate warning (at least two years in advance) about the components reaching ‘end of life,’ or for which cyber security patches will no longer be made available.” This concept can be also found in requirement GP-OP-02 in [ENISA]: “Disclose the duration and end-of-life security and patch support (beyond product warranty).”

4.8 Component study methodology

This section details the approach taken to arrive at the recommendations in this report.

4.8.1 Necessity of 62443-4-2 requirements for IIoT devices and gateways

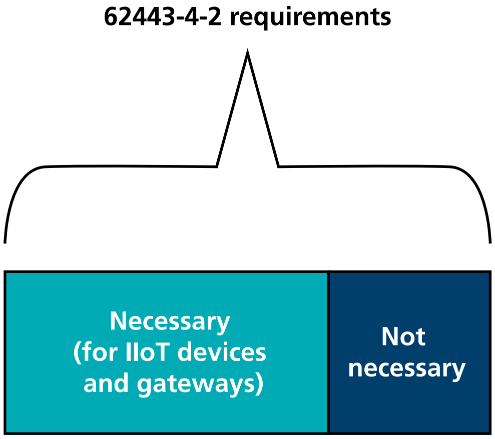

Figure 2. Classification of existing 62443-4-2 requirements

The current 62443-4-2 requirements were examined to identify any that would not be *necessary* requirements for an IIoT device or gateway. The meaning of *necessary* is that the requirement should be met by this type of IIoT component. The two statements in 4.8.1 that form the starting position which this analysis examines, state that *all 62443-4-2 requirements are necessary*.

Saying that a requirement is necessary in this context is not a judgment of whether or not that single 62443-4-2 requirement for a given topic, or the overall set of 62443-4-2 requirements, is *sufficient* for IIoT devices or gateways. Determining sufficiency is a separate step in the process, described next.

As discussed in 4.4.4, ultimately all 62443-4-2 requirements with a few exceptions were recommended as necessary.

4.8.2 Certification baseline

IIoT devices and gateways with a direct connection to a network considered untrusted (most often to the Internet) were the target and reason for this study. As noted in Section 1, we may use the expression “Internet connection” for brevity – it is understood to include the case of a direct connection to some untrusted network.

The following two statements were taken as a starting baseline for certification criteria for such IIoT devices and gateways. The study then proceeded to validate, change and enhance the following statements, potentially adding to the minimum set of criteria described:

- Certification of an IIoT device with direct Internet connection will at a minimum consist of validating 62443-4-2 requirements for the IIoT device considered as an embedded device, where it is assumed that the embedded device has a direct Internet connection.

  An IIoT device is an embedded device in 62443 terminology, since a sensor or actuator is an embedded device. (See definitions 3.1.9 and 3.1.15).
- Certification of an IIoT gateway will at a minimum consist of validating 62443-4-2 requirements for the IIoT gateway considered as a component, that is one or more of a network device, software application, or host device, where the component has a direct Internet connection. The selection of type of component(s) will depend upon the functionality of the particular IIoT gateway, OR (to be determined, if the gateway itself is considered as a system) will consist of validating 62443-3-3 system requirements, where the system has an Internet connection.

Ultimately, it was determined that an IIoT device might be a host device in 62443-4-2 terms, since the definition of IIoT device in 3.1.15 does not say that an IIoT device IS a sensor or an actuator, but rather that it “communicates with the physical world through sensing or actuating.” Therefore, an IIoT integrated edge computing device that communicates with an array of sensors, filters the data received, and sends it to the cloud would be consistent with the definition of IIoT device. That being said, note that 62443-4-2 requirements for embedded devices and host devices have very few differences (in EDR vs. HDR 3.2, 3.11, 3.14; and HDR 3.2 RE(1) is unique to hosts).

Also, as discussed in 4.8.4, gateways were ultimately considered to be (at least) a network device component (but not a system) and 62443-4-2 was used as the set of baseline IIoT gateway requirements. The process described in the next sections was used determine whether changes or enhancements are needed to the minimum criteria defined above, to certify IIoT devices and gateways.

4.8.3 Sufficiency of 62443-4-2 requirements and certification methods for application to IIoT devices and gateways

The approach to determine whether the requirements in 62443-4-2 and known certification methods are sufficient for IIoT devices and gateways, leverages numerous studies available that have proposed security and certification requirements for IoT and IIoT. IIoT device and gateway requirements were contributed by project team members and extracted from the set of industry and government resources listed in Section 2.4 and described in Section 5 – Appendix 1. These requirements were classified as one of the following, by mapping to 62443-4-2 (including 62443-4-1 by reference) and to existing 62443-4-2 certification program information:

1. **Covered** The requirement is in 62443, for some SL-C (capability security level). The methods being used by ISASecure and other certification programs to validate the requirement are considered sufficient.

2. **Covered, certification gap** The requirement is in 62443, at some SL-C. However, the methods being used by ISASecure and possibly other 62443-4-2 certification programs, are not considered sufficient to validate the requirement with the desired level of assurance.

3. **IIoT requirement gap** The requirement is not in 62443, but seems appropriate to add as a requirement in that standard if made specific to IIoT environments. It is not required for all IACS environments.

4. **IACS requirement gap** The requirement is not in 62443, and seems applicable not only for IIoT environments but for components in all IACS environments, particularly at high security levels.

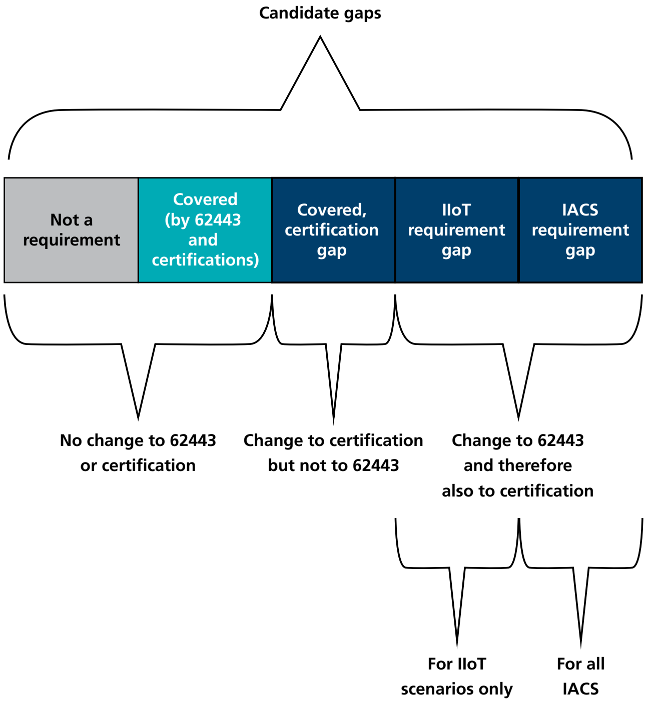
Candidate gaps
Not a requirement
Covered (by 62443 and certifications)
Covered, certification gap
IIoT requirement gap
IACS requirement gap
No change to 62443 or certification
Change to certification but not to 62443
Change to 62443 and therefore also to certification
For IIoT scenarios only
For all IACS

Figure 3. Classification of candidate gaps

Changes or enhancements to the starting minimum baseline sets of requirements described in 4.8.1 therefore come from:

- 62443-4-2 requirements judged as not necessary for IIoT devices or gateways; and
- Requirements from industry/government sources classified as either an IIoT requirement gap or IACS requirement gap.

Example functional requirements that are candidate gaps judged **Not a requirement,** are listed in 4.3.5. Example functional requirements that are candidate gaps classified as **Covered,** are listed in Section 7 – Appendix 3. Functional requirements that are in either category **IIoT requirement gap** or **IACS requirement gap,** are listed in 4.3.2. "Commonly accepted practice" requirements discussed in 4.5 were identified as a particular type of functional requirement falling under **IIoT requirement gap.** Supplier development process requirements that fall under IIoT requirement gap are identified in 4.3.4.2.3, 4.7.1, and 4.7.4.

The additional use of certifier test or supplier test artifacts, for validation of functional requirements in a few cases, is recommended in 4.6; this falls under **Covered, certification gap.** Likewise in this category is the identification of IIoT-specific security context in 4.7.2, recommended additional certifier guidance for reviewing threat models under 62443-4-1 (4.7.3), strengthening of certifier validation of maintenance of product security over time discussed in 4.7.5, and for validating selected existing 62443-4-2 requirements for IIoT devices or gateways, in 4.4.6.

For any IIoT or IACS requirement gap, there is by implication a certification gap – which is the validation of that "missing" requirement.

Some requirement classifications found broad agreement among the project team; others did not. These cases are noted in context within the report.

The overall gap analysis process described above for IIoT devices and gateways is shown in Figure 4. The analysis step is initially done against 62443-4-2. After a similar gap analysis is performed at the system level in future phases of this study, these system-level gaps will be further analyzed to determine if they imply additional gaps for IIoT devices and gateways, that were not already identified.

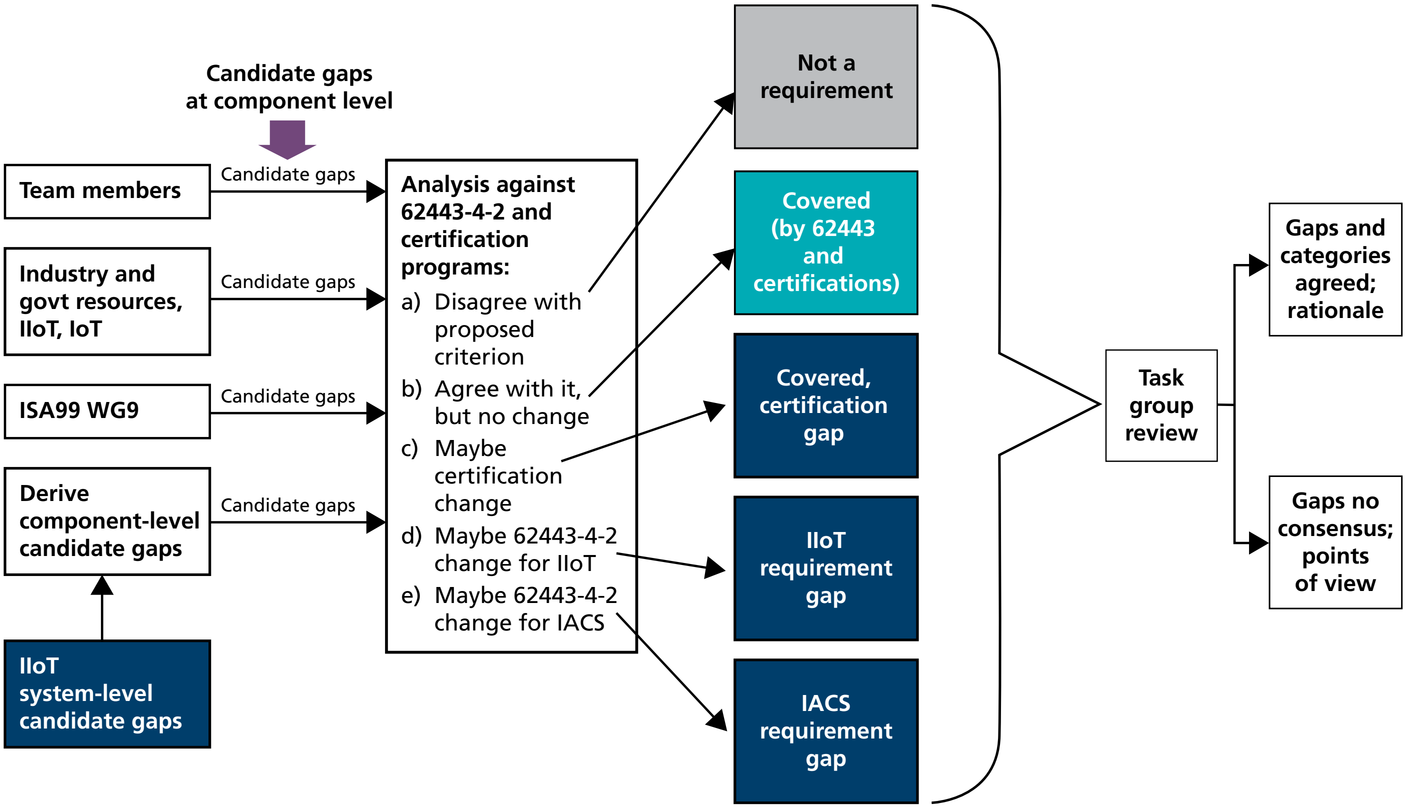
Candidate gaps at component level
Team members
Candidate gaps
Industry and govt resources, IIoT, IoT
Candidate gaps
ISA99 WG9
Candidate gaps
Derive component-level candidate gaps
Candidate gaps
IIoT system-level candidate gaps
Analysis against 62443-4-2 and certification programs:
a) Disagree with proposed criterion
b) Agree with it, but no change
c) Maybe certification change
d) Maybe 62443-4-2 change for IIoT
e) Maybe 62443-4-2 change for IACS
Not a requirement
Covered (by 62443 and certifications)
Covered, certification gap
IIoT requirement gap
IACS requirement gap
Task group review
Gaps and categories agreed; rationale
Gaps no consensus; points of view

Figure 4. Gap analysis process for IIoT devices and gateways

4.8.4 Alternative approaches

The following alternative approaches to analyzing IIoT requirements were discussed by the project team.

- **Component as a system:** Seeing the parallel between compartmentalization and zones/conduits as discussed in 4.3.4.1, the team discussed an alternative approach to applying 62443 to complex IIoT components, to that taken in the present document. This alternative was to consider such complex components as systems instead of as components, in 62443 terms. In this case, 62443-3-3 requirements would apply to the component, and internal compartmentalization of an IIoT device or gateway would become bona fide 62443 zones and conduits. This approach was considered in some detail. Challenges with that approach were:
  - If the entity is a system vs. a component, it would not be permitted to provide any required functions by "integration into a system." It was unclear if that is realistic or if one would need to change some of the system requirements for this type of system to permit this. (All requirements where 62443-4-2 permits a function to be provided by integration into a (larger) system are listed in Table 19.)
  - There are several 3-3 requirements that don't fit a device, even a complex one. Examples are SR 2.2 RE(1) *Identify and report unauthorized wireless devices,* SR 2.3 and RE(1) *Use control for portable and mobile devices,* SR 3.2 *Malicious code protection includes report,* SR 3.3 RE(1) *Automated mechanism for security functionality verification,* SR 7.3 RE(2) *Backup automation,* SR 7.5 *Emergency power.*

The approach taken here to treat IIoT devices and gateways as components rather than systems, stayed closer to the envisioned applications of the concepts of system and component when 62443-3-3 and 62443-4-2 were written. Ultimately, selected zone/conduit system requirements from 62443-3-3 and 62443-3-2 were adapted for components in Section 4.3.4.2.

- **Protection of functions:** It is understood that the concepts of virtualization and containerization are radically changing the nature of the entities that comprise an IACS architecture. This is true generally for IACS, and not only for the case of IIoT. A suggestion for how to structure a standard that can remain applicable under these and future paradigm shifts, is to fully abstract from the idea of physical devices, and write requirements in terms of the protection of functions. This approach is a significant change from current 62443-4-2 "component type" concepts. It was not attempted for the present effort focused on IIoT devices and gateways, which are products currently sold as physical devices. However, a "functional" approach may be required to address all aspects of the future IIoT environment for the longer term.

5 Appendix 1 – Industry/ government sources

Following are brief comments on the industry/ government sources consulted to identify potential IIoT requirements for the purposes of the present study.

- The Seven Properties of Highly Secure Devices [MS7]
  This document gives brief descriptions and rationale for seven capabilities needed by devices connecting to the Internet, and describes an example of a device that achieves these capabilities. The authors believe the capabilities can be implemented at any price point.
- Industrial Internet Consortium Reference Architecture and Security Framework [IICRA], [IICSF]
  Section 7.3 of the Security Framework lists security requirements for consideration on IIoT endpoints. Both IIoT devices and gateways are considered endpoints per the definition in this document. All of the topics in 7.3 have closely related requirements in 62443-4-2. Section 8 of the Security Framework walks through these requirements in more detail at the implementation level. The present study focused on these two sections of the Security Framework.
- ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (2017) [ENISA]
  This document is a discussion of IoT security including helpful background, "main threats, vulnerabilities, risks and the development of the main attack scenarios." ENISA is the organization charged with future certification harmonization for the EU. The document states: "the baseline security measures for IoT put forward in this report can serve as a springboard for further related efforts towards a harmonised EU approach, paving the way for a tacit adoption of the measures, and as criteria for other initiatives such as labelling or certification." The present study analyzed the list of security measures/good practices in Annex A against 62443-4-2. The Annex A list is available via spreadsheet download at https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool.
- An IoT Device Cybersecurity Certification Program was announced by CTIA, a US wireless industry association, in August 2018, see https://www.ctia.org/news/ctia-iot-cybersecurity-certification-program-certifies-first-device and https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program
  The test plan used for certification is found at https://www.ctia.org/certification-resources. [CTIA]

  CTIA's certification program consists for the most part of hands-on testing. The program applies to IoT devices that contain an IoT application layer that provides identity and authentication functionality and at least one communications module supporting either LTE, 5G or Wi-Fi®. CTIA defines IoT devices as: *connects to at least one network to exchange data with other devices, vehicles, appliances, infrastructure elements, etc. An IoT device might include hardware, software, sensors, actuators and network connectivity.* Although communication protocols assumed for this program are not the most common for IIoT, the features being examined under this program are familiar; they can be defined independent of protocol.

- NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline [NIST8259A]
  NIST states the purpose for this document as, to: "give all organizations a starting point for IoT device cybersecurity risk management, but the implementation of all capabilities is not considered mandatory." The document was "refined and validated using a collaborative public-private process to incorporate all viewpoints. Multiple requests for comment were issued, and multiple workshops and roundtables were held." The document lists six core baseline capabilities and common elements for each, where common elements are "elements an organization seeking to implement the core baseline often (but not always) would use in order to achieve the capability. (Note: the elements are not intended to be comprehensive…)." The present study reviewed both core capabilities and common elements against 62443-4-2.
- NIST catalog of IoT device cybersecurity capabilities [NISTCAT]
  This on-line catalog lists IoT security capabilities as one-line descriptions. The descriptions are technology agnostic. The lists include product features (called technical capabilities) as well as supplier responsibilities (called non-technical capabilities). A number of the IoT technical capabilities listed appear to be unique to specialized applications. From a NIST web site: "NIST leveraged the Core Baseline established in NISTIR 8259A and analyzed the controls found in NIST SP 800-53 to develop a catalog of key IoT device cybersecurity capabilities and supporting non-technical manufacturer capabilities and associated IoT device customer controls. This catalog is a critical building block for establishing a federal profile of the Core Baseline ("Federal Profile") to help government entities securely incorporate IoT devices into their systems and meet security requirements for federal information and systems."

6 Appendix 2 – Summary of detailed recommendations

The following table summarizes all detailed recommendations described in this report. Recommendation of a possible change to the 62443 standard, implies the resulting requirement is also recommended as a criterion for certification.

Table 15. Certification program enhancements

ID	Recommendation	Report reference	Possible change to requirements in this or related standard	Possible change to certification approach only
	Additional functional requirements			
1	COMPART 1 Compartmentalization – application partitioning	4.3.2, 4.3.4.2.1	62443-4-2	
2	COMPART 2 Compartmentalization – separating functions using commonly accepted practices	4.3.2, 4.3.4.2.1	62443-4-2	
3	COMPART 3 Compartmentalization - Certifier guidance – NDR 5.2 *Zone boundary protection* scope includes zones internal to component	4.3.2, 4.3.4.2.1		√
4	COMPART 4 Compartmentalization - Certifier guidance – CR 4.1 *Information confidentiality* scope includes protection of confidentiality across zone boundaries internal to component	4.3.2, 4.3.4.2.1		√
5	COMPART 5 Compartmentalization – Enforcement of security status of portable and mobile devices for internal zone connection	4.3.2, 4.3.4.2.1	62443-4-2	
6	COMPART 6 Compartmentalization – physical separation of safety functions internal to component	4.3.2, 4.3.4.2.2	62443-4-2	
7	COMPART 8 Compartmentalization – Independence from non-control system networks internal to component	4.3.2, 4.3.4.2.2	62443-4-2	
8	Secure by default	4.3.2	62443-4-2	
9	Authentication of non-human users from untrusted networks	4.3.2	62443-4-2	
10	Devices using passwords or keys, have unique initial passwords and keys per device. Initial passwords are generated according to internationally recognized and proven password guidelines OR require changing password on install	4.3.2	62443-4-2	
11	Protection of software and data in use, in accordance with commonly accepted practices	4.3.2, 4.5.4	62443-4-2	
12	Device can be remotely updated and upgraded	4.3.2	62443-4-2	
13	Enable/disable update/upgrade	4.3.2	62443-4-2	
14	Update/upgrade maintains user security settings	4.3.2	62443-4-2	

ID	Recommendation	Report reference	Possible change to requirements in this or related standard	Possible change to certification approach only
15	For management and configuration interfaces from untrusted network, either authorize traffic by port, protocol, and application, OR do not accept incoming initiation of management/configuration connections	4.3.2	62443-4-2	
16	Device itself does not provide printed design information useful to attackers	4.3.2	62443-4-2	
17	Presence/absence of component can be monitored	4.3.2	62443-4-2	
18	Turn off connection to untrusted network, maintain essential functions	4.3.2	62443-4-2	
	Selection of existing 62443-4-2 requirements			
19	Two certification tiers resembling capability security levels 2 and 4, incorporate all 62443-4-2 requirements except CR 1.7 RE(1), CR 2.1 RE(3), CR 2.1 RE(4), CR 3.9 RE(1)	4.4.3, 4.4.4	62443-4-2	
	Application of existing 62443-4-2 requirements			
20	Certifier guidance – CR 1.1, CR 1.9 authentication event functions gating essential functions cannot be provided solely via Internet due to CCSC 1	4.4.6.1		√
21	Certifier guidance – CR 3.4, CR 3.4 RE(1) considerations if reporting of integrity and authenticity checks uses Internet connection	4.4.6.1		√
22	Certifier guidance – NDR 1.13 *Access via untrusted networks* verify controls on management/configuration interface from untrusted network	4.4.6.2		√
23	Certifier guidance – CR 3.1 *Communication integrity* scope includes communication between zones internal to the component	4.4.6.2	62443-4-2	
24	Certifier guidance – CR 3.1 *Communication authentication* scope includes component management interface	4.4.6.2		√
25	Certifier guidance – EDR|HDR|NDR 3.14 *Integrity of boot process* under attacker physical possession of component	4.4.6.2		√
26	Certifier guidance – EDR|HDR|NDR 3.14 RE(1) *Authenticity of boot process* under attacker physical possession of component	4.4.6.2		√
27	Certifier guidance – NDR 5.2 RE(2) *Island mode* implies capability to disable connection to untrusted network	4.4.6.2	62443-4-2	
28	Certifier guidance CR 6.2 *Continuous monitoring* scope of commonly accepted practices includes commonly accepted reporting interfaces	4.4.6.2, 4.5.6		√
29	Certifier guidance – CR 7.1 Verify DoS protection addresses loss of Internet connection or cloud functionality	4.4.6.2		√

ID	Recommendation	Report reference	Possible change to requirements in this or related standard	Possible change to certification approach only
30	Certifier guidance – CR 1.5D Verify protection of authenticators under attacker physical possession of component	4.4.6.2		√
31	Certifier guidance – CR 7.4 Verify that capability to be recovered and reconstituted to a known secure state after a failure, includes failure of update or upgrade	4.4.6.2		√
	Commonly accepted practice requirements			
32	Require hardware protection for supplier root of trust for Core tier (EDR|HDR|NDR 3.12)	4.5.1, 4.5.4	62443-4-2	
33	Require hardware compartmentalization of security functions for Advanced tier	4.5.4	62443-4-2	
34	Require hardware-based protections of code and data in use, for Advanced tier	4.5.4	62443-4-2	
35	Modify 62443-4-2 to require use of cryptography to meet some of 62443-4-2 requirements in Table 8	4.5.5	62443-4-2	
36	Modify 62443-4-2 to require use of standards and recommendations commonly accepted for IIoT for some of 62443-4-2 requirements in Table 8	4.5.5	62443-4-2	
37	IIoT certification to require for meeting 62443-4-2 requirements in Table 8, use of recommendations commonly accepted for IIoT, as specifically referenced by certification specification, or use of demonstrably equivalent or better approach	4.5.1		√
38	IIoT certification to require for meeting CR 6.2 *Continuous monitoring*, use of recommendations commonly accepted for IIoT, as specifically referenced by certification specification, or use of demonstrably equivalent or better approach	4.5.6		√
	Validations by test			
39	Certifier hands-on testing for requirements #14, #15, #17, #18 listed under Additional Functional Requirements; verify supplier testing for #8, #9, #16, documentation evaluation for others	4.6.2.1		√
40	Certifier hands-on testing increases from 22 requirements to 28 requirements among existing 62443-4-2 requirements, and for 5 additional requirements currently evaluated by documentation review, change to review of supplier test artifacts, as shown in Table 10 (change is relative to ISASecure program [CSA-311])	4.6.2.2		√

ID	Recommendation	Report reference	Possible change to requirements in this or related standard	Possible change to certification approach only
	Strengthen security maintenance assurance for product			
41	Periodic certifier audit of maintenance of security	4.7.5		√
42	Supplier provide proactive notification to designated user contacts of available updates and upgrades, and passive publication of current list of these	4.7.6	62443-4-1	
43	Advance notification for products to be withdrawn from security update management	4.7.7	62443-4-1	
	Lifecycle impacts of compartmentalization			
44	COMPART 7 Describe shared physical elements of component in user and certification documentation	4.3.2, 4.3.4.2.2	62443-4-1	
45	COMPART 9 Compartmentalization – Add design practice for zone partitioning capability for system-level and internal component zones	4.3.2, 4.3.4.2.3	62443-4-1	
46	COMPART 10 Compartmentalization – certifier guidance to verify shared resources internal to component are included in threat model	4.3.2, 4.3.4.2.3		√
	Lifecycle impacts of IIoT security context			
47	In 62443-4-1 SR-4 *Product security requirements,* selection of 62443-4-2 requirements for a component, specified in manner other than specification of product capability security level	4.7.1	62443-4-1	
48	Certifier guidance to verify under 62443-4-1 SR-1 that applicable IIoT security context elements have been incorporated into documented security context	4.7.2		√
49	Certifier guidance to verify under 62443-4-1 SR-2 that threat model includes device failures	4.7.3		√
50	In 62443-4-1 SR-5 *Security requirements review,* reviewers to include cloud-based functionality dependencies expert	4.7.4.1	62443-4-1	
51	In 62443-4-1 DM-1 *Receiving notifications of security-related issues,* sources of notifications to include developer of cloud-based functionality related to product	4.7.4.2	62443-4-1	
52	Provide user documentation of cloud dependencies, including ongoing required or optional network communications of component with supplier or for supplier purposes	4.7.4.3	62443-4-1	

7 Appendix 3 – 62443-4-2 requirements in IoT/IIoT industry/ government documents

The purpose of the table below is to illustrate the intersection of 62443 requirements with industry/government compendiums of IoT/ IIoT requirements. It is expected that most requirements in 62443-4-2 could be mapped into some industry document on IoT or IIoT, because an IIoT component is an IACS component, and 62443-4-2 is an international standard for IACS components.

Table 16. Sample component properties from IoT/IIoT industry/government documents that appear in 62443-4-2

62443-4-2 Requirement number	62443-4-2 Requirement name	Capability security levels	Example Source
CR 1.2 RE(1)	Unique identification and authentication	3, 4	[NIST8259A] p5
CR 1.5 RE(1)	Hardware security for authenticators	3, 4	[MS7]
CR 1.11	Unsuccessful login attempts	1, 2, 3, 4	[ENISA] GP-TM-25
CR 3.1	Communication integrity	1, 2, 3, 4	[NIST8259A] p7
CR 3.1 RE(1)	Communication authentication	2, 3, 4	[ENISA] GP-TM-38
CR 3.4	Software and information integrity	1, 2, 3, 4	[IICSF] 8.8.2
CR 4.2	Information persistence [device erase]	2, 3, 4	[NIST8259A] p7
EDR|HDR|NDR 3.10	Support for updates	1, 2, 3, 4	[ENISA] GP-TM-18
EDR|HDR|NDR 3.10 RE(1)	Update authenticity and integrity	2, 3, 4	[NIST8259A] p9
EDR|HDR|NDR 3.11	Physical tamper resistance and detection	2, 3, 4	[IICSF] 8.3
EDR|HDR|NDR 3.11 RE (1)	Notification of a tampering attempt	3, 4	[CTIA] 5.16
EDR|HDR|NDR 3.14	Integrity of the boot process	1, 2, 3, 4	[CTIA] 4.11
EDR|HDR|NDR 3.14 RE(1)	Authenticity of the boot process	2, 3, 4	[IICSF] 8.7.1
EDR|HDR|NDR 3.12	Provisioning product supplier roots of trust	2, 3, 4	[MS7]
CR 4.1	Information confidentiality	1, 2, 3, 4	[IICSF] 8.8.1
NDR 5.2 RE(1)	Deny all, permit by exception	2, 3, 4	[IICSF] 8.2.3
CR 6.2	Continuous monitoring	2, 3, 4	[MS7]
CR 7.4	Control system recovery and reconstitution	1, 2, 3, 4	[ENISA] GP-TM-06
CCSC 4	(62443-4-1) SD-2 Defense in depth design	1, 2, 3, 4	[MS7]

8 Appendix 4 – Technology approaches for selected 62443-4-2 requirements

Table 17 lists selected 62443-4-2 requirements for which the industry sources reviewed for this study specified particular technology approaches. These are specific references in support of the summary in Table 8.

Table 17. Existing 62443-4-2 requirements with industry accepted technology approaches

62443-4-2 Requirement	Industry Source for Technology Approach	Comments
CR 1.1 *Human user identification and authentication* Components shall provide the capability to identify and authenticate all human users according to ISA 62443-3-3 SR 1.1 on all interfaces capable of human user access….	[CTIA] 4.9 multi-factor authentication for human users (at certification level 2) [ENISA] GP-TM-23 consider two-factor authentication, multi-factor authentication and certificates	Multi-factor capability required by 62443-4-2 CR 1.1 RE(2) for capability security levels 3 and 4. This requirement would apply for IIoT devices or gateways at the Advanced tier, under the recommendations in Section 4.4.4 of the present document.
CR 1.2 *Software process and device identification and authentication* Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA 62443-3-3 SR 1.2.	[MS7] IIoT device: certificate-based authentication [IICSF] 8.6.1 IIoT device or gateway: strong cryptographic credentials [ENISA] GP-TM-23 consider two-factor authentication, multi-factor authentication, and certificates	[CTIA], [NIST8259A], and [NISTCAT] specify a unique identity for IIoT devices but not technology for creating it.
CR 3.1 *Communication integrity* Components shall provide the capability to protect integrity of transmitted information.	[IICSF] 8.2.3 IIoT gateway: digital signature for communication integrity [CTIA] 4.8 IIoT device: SSH, IPsec, TLS, or DTLS with 128-bit AES for communication [ENISA] GP-TM-39: use standardized state-of-the-art protocols such as TLS [ENISA] GP-TM-52 web interfaces fully encrypt user session from device to backend services [NISTCAT] ability to establish and configure IoT device settings for communications technologies including authentication protocols (e.g., EAP/TLS, PEAP) [NISTCAT] Ability to support data encryption and signing to prevent data from being altered in transit	It should be noted that in 62443-3-3, the corresponding system level requirement SR 3.1 Communication integrity, in RE(1) Cryptographic integrity protection, requires the use of cryptography for communication integrity at levels 3 and 4. [NIST8259A] and [ENISA] agree: see notes below this table.

62443-4-2 Requirement	Industry Source for Technology Approach	Comments
CR 3.1 RE(1) *Communication authentication* Components shall provide the capability to verify the authenticity of received information during communication.	[ENISA] GP-TM-38 guarantee authenticity using data encryption methods	
CR 3.4 *Software and information integrity* Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	[IICSF] 8.8.2 IIoT device or gateway: digital signatures for integrity of executables, logs and config files [CTIA] 5.14 IIoT device: verify signatures using RSASSA-PKCS1-v1_5 or ECDSA with curve P-256 [ENISA] GP-TM-04 signatures for executables [ENISA] GP-TM-41 sign data wherever captured and stored [ENISA] GP-TM-52 web interfaces fully encrypt user session from device to backend services [NISTCAT] Protect audit information through use of signatures, cryptography [NISTCAT] Ability to verify software updates come from valid sources using an effective method (e.g., digital signatures, checksums, certificate validation, etc.) [NISTCAT] Ability to support data encryption and signing to prevent data from being altered in device storage [NIST8259A] Table 1: use standardized cryptographic modules (e.g., hashes, signatures) for integrity of stored and transmitted data	
EDR|HDR|NDR 3.12 – *Provisioning product supplier roots of trust* [Embedded|Host|Network] devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	[MS7] Hardware-based root of trust [ENISA] GP-TM-01 Hardware-based root of trust [IICSF] 8.4 Hardware based root of trust based on TPM or HSM platform	

62443-4-2 Requirement	Industry Source for Technology Approach	Comments
CR 4.1 – *Information confidentiality* Components shall a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and b) support the protection of the confidentiality of information in transit as defined in ISA 62443-3-3 SR 4.1.	[IICSF] 8.8.1 IIoT device or gateway: cryptography for confidentiality of data at rest [CTIA] 5.15 IIoT device: 128-bit AES minimum for data at rest [IICSF] 8.2.3 IIoT gateway: cryptography for communication confidentiality [CTIA] 4.8 IIoT device: SSH, IPsec, TLS, or DTLS with 128-bit AES for communication [ENISA] GP-TM-39: use standardized state-of-the-art protocols such as TLS [NIST8259A] Table 1: use standardized cryptographic modules for confidentiality of stored and transmitted data	[NIST8259A] and [ENISA] agree for both a) and b), see notes below this table.

NOTES:
In addition, [NIST8259A] identifies for IIoT devices a general requirement for Data Protection, and then in Table 1 row 3 in that document, under Common Elements associated with this requirement states: "The ability to use demonstrably secure cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised."
Similarly, the following security measure/good practices appear in [ENISA]:

- GP-TM-34: "Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest."
- GP-TM-38: "Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping."
- GP-TM-52: "Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc."

9 Appendix 5 – The Seven Properties of Highly Secure Devices and 62443-4-2

The following table provides an example of the analysis done for this study, mapping the industry source [MS7] to 62443-4-2. The gaps identified were ultimately dispositioned as follows, based on all sources and project team judgment:

- Hardware based supplier root of trust, compartmentalization (4.5.1, 4.3.2): Recommended additional functional requirements
- Small trusted computing base: not recommended as a requirement (4.3.5)
- Certificate based authentication: to be evaluated for status as commonly accepted industry practice (4.5.1, 4.5.2)
- Failure reporting: Although arguably covered by CR 6.2, development of industry practices and recommendations specific to IIoT that may be referenced by suppliers and certifiers is recommended (4.5.6)

Table 18. The Seven Properties of Highly Secure Devices and 62443-4-2

MS7 Property	62443 reference and comments
hardware-based root of trust	EDR|HDR|NDR 3.12 – *Provisioning product supplier roots of trust* Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device. This requirement applies for capability security level 2 and higher. It permits hardware or software implementations so does not imply the MS7 property at any capability security level.
small trusted computing base	This topic is addressed to some extent by 62443-4-1 SD-4 *Secure design best practices – attack surface reduction.* However, SD-4 does not fully imply the MS7 property.
defense in depth √	62443-4-1 SD-2 *Defense in depth design* A process shall be employed to implement multiple layers of defense using a risk based approach based on the threat model. This process shall be employed for assigning responsibilities to each layer of defense. 62443-4-2 implies the MS7 property.
compartmentalization	Although 62443 relies on a higher architectural level of compartmentalization using zones and conduits, and requires SD-2 *Defense in depth design* and SD-4 *Secure design best practices,* it does not explicitly address the topic of compartmentalization within 62443-4-2 components to prevent propagation of attacks and assist component recovery. 62443-4-2 does not imply the MS7 property.
certificate-based authentication	CR 1.9 *Strength of public key-based authentication* places requirements on the use of public key-based authentication, if it is used. However, 62443-4-2 does not require its use, for any purpose, at any capability security level. 62443-4-2 does not imply the MS7 property.

MS7 Property	62443 reference and comments
renewable security √	CR 7.4 – *Control system recovery and reconstitution* Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. This requirement applies at all capability security levels and implies the MS7 property.
failure reporting √	CR 6.2 – *Continuous monitoring* Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. This requirement applies for capability security levels 2 and higher, and implies the MS7 property for those levels.

10 Appendix 6 – Functions supportable by integration into system in 62443-4-2

The following table shows all 62443-4-2 requirements that describe functions that a component may locally support, or may provide by integration into a system that supports them. These requirements were analyzed for any specific IIoT implications of offering the "integration" option, in 4.4.6.1.

Table 19. All 62443-4-2 functions supportable by integration into system

Title	Statement	Topic
CR 1.1 *Human user identification and authentication*	Components shall provide the capability to identify and authenticate all human users according to ISA 62443-3-3 SR-1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.	Authentication event
CR 1.3 Account management	Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to ISA 62443-3-3 SR-1.3.	Management
CR 1.4 Identifier management	Components shall provide the capability to integrate into a system that supports the management of identifiers and/ or provide the capability to support the management of identifiers directly according to ISA 62443-3-3 SR 1.4.	Management

Title	Statement	Topic
CR 1.7 Strength of password-based authentication	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines.	Management
CR 1.7 RE(1) Password generation and lifetime restrictions for human users	Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	Management
CR 1.7 RE(2) Password lifetime restrictions for all users (human, software process, or device)	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	Management
CR 1.8 Public key infrastructure certificates	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with ISA 62443-3-3 SR 1.8.	Management
CR 1.9 *Strength of public key-based authentication*	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device); and f) ensure that the algorithms and keys used for the public key authentication comply with 8.5 CR 4.3 - Use of cryptography.	Authentication event

Title	Statement	Topic
CR 2.2 Wireless use control	If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.	A bit different case, since requires integration, not as an option. No recommendation in 4.4.6.1 related to permitting use of Internet interface at this time – investigation of "commonly accepted industry practices" is needed.
CR 3.4 *Software and information integrity*	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Reporting
CR 3.4 RE(1) *Authenticity of software and information*	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	Reporting

ISAGCA Member Companies

1898 & Co. (Burns McDonnell)
ACET Solutions
aeSolutions
BaseRock IT Solutions
Bayshore
Carrier Global
Claroty
ConsoleWorks
Coontec
CyberOwl
CyPhy Defense
Deloitte
Digital Immunity
Dragos
Eaton
exida
Ford Motor Company
Fortinet
Fortress Information Security
Honeywell
Idaho National Laboratory
Idaho State University
ISASecure
Johns Manville
Johnson Controls
KPMG
LOGIIC
Mission Secure
MT4 senhasegura
Munio Security
Nova Systems
Nozomi Networks
PAS
PETRONAS
Pfizer
Radiflow
Redacted
Red Trident
Rockwell Automation
Schneider Electric
Surge Engineering
TDI Technologies
Tenable
TI Safe
Tripwire
TXOne Networks
UL
Wallix
WisePlant
Xage Security
Xylem

ISA Security Compliance Institute Member Companies

Strategic Members

- Chevron
- ExxonMobil
- Honeywell
- Johnson Controls
- Schneider Electric (formally Invensys)
- Yokogawa
- Saudi Aramco

Technical Members

- Applied Risk
- HON Consulting S.r.l dba BYHON
- Control System Security Center
- DNV-GL
- FM Approvals
- exida
- Security Compass
- SGS ESPANOLA DE CONTROL
- Shell
- TUV Rheinland
- TUV SUD
- TrustCB

Supporter Members

- WisePlant HQ
- Tailyn Technologies, Inc.

Industry Participants

- ISA99 Standards Committee (includes representatives of NIST, DHS, National Labs, Chemical Sector and others)