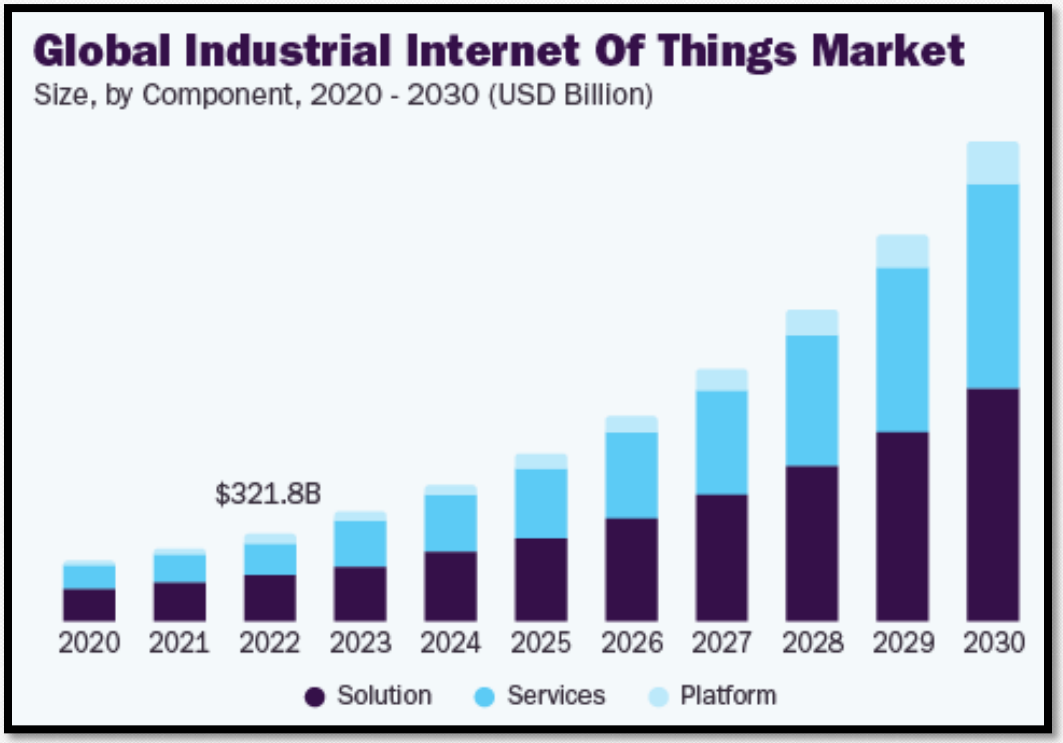
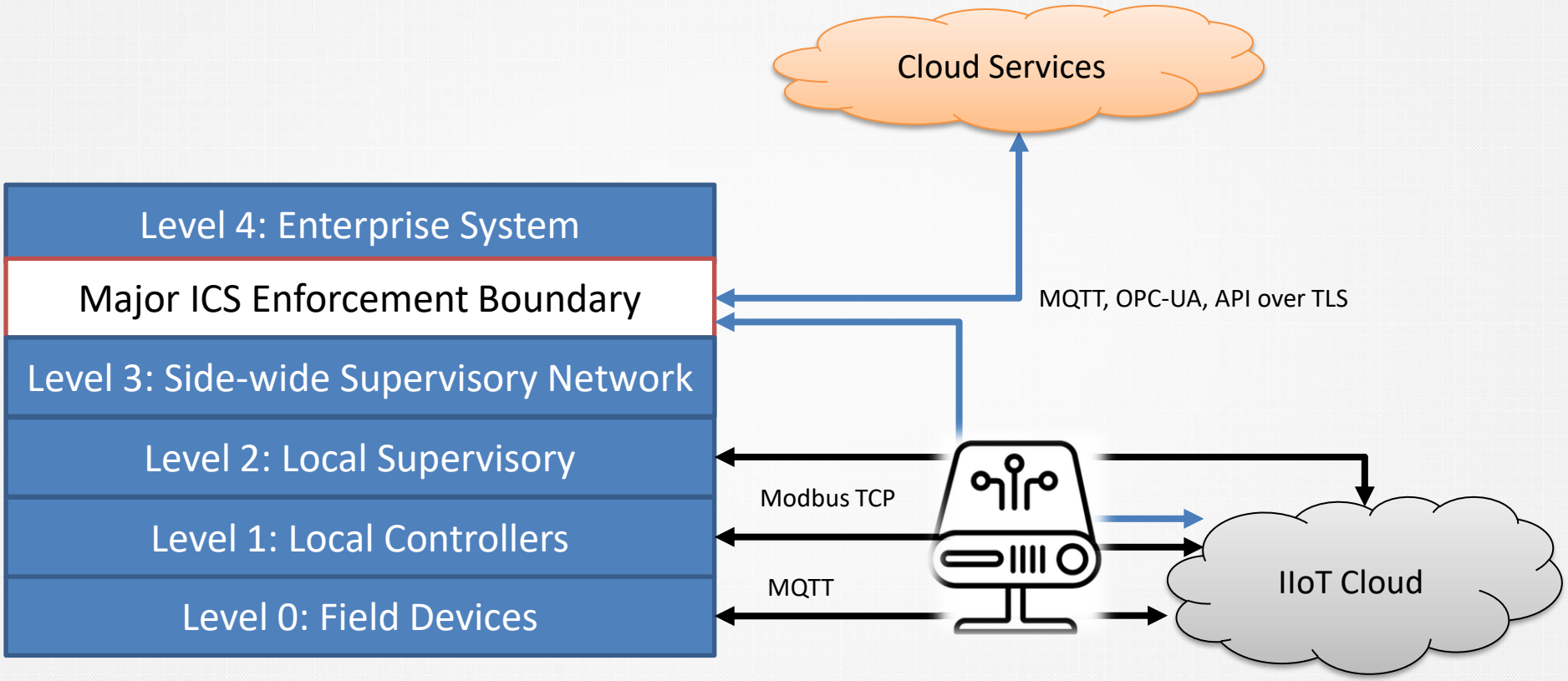
工業物聯網（IIoT）資安策略：從雲端系統到端點設備的全面防護

SZ Lin (林上智)

Date: 2024/05/14



src: https://www.grandviewresearch.com/static/img/research/us-industrial-internet-of-things-market.png


Cloud Services
Level 4: Enterprise System
Major ICS Enforcement Boundary
Level 3: Side-wide Supervisory Network
Level 2: Local Supervisory
Level 1: Local Controllers
Level 0: Field Devices
MQTT, OPC-UA, API over TLS
Modbus TCP
MQTT
IIoT Cloud

Asset Owner Perspective

Integrating IIoT Technology Into the Security Program

- Should the asset owner use a standardized risk approach and methodology, as part of their security program, to determine the risks of IIoT to their IACS and identify possible mitigations?
- Should the asset owner develop and provide training to their personnel on the cybersecurity aspects of IIoT?
- Should the asset owner consider the impact of IIoT on their business continuity and availability planning, and evaluate whether additional redundancies or activities are needed to ensure continuity and availability?
- Before implementing IIoT, should the asset owner determine if their security policies and procedures cover IIoT and consider revisions if the coverage is non-existent or inadequate?

- Should asset owners review and, if necessary, revise their policies and procedures around physical security and physical assets to include IIoT?
- Should asset owners carefully consider access policies, activities and authentication strategy around IIoT?
- Should asset owners review their authorization policies and procedures to determine the impact of IIoT?
- Should asset owners incorporate IIoT into security program maintenance activities, such as patch management?

Incident planning and response, DiD strategy, and more…

Risk Assessment

IEC 62443-3-2

Edition 1.0 2020-06

INTERNATIONAL STANDARD

colour inside

Security for industrial automation and control systems –
Part 3-2: Security risk assessment for system design

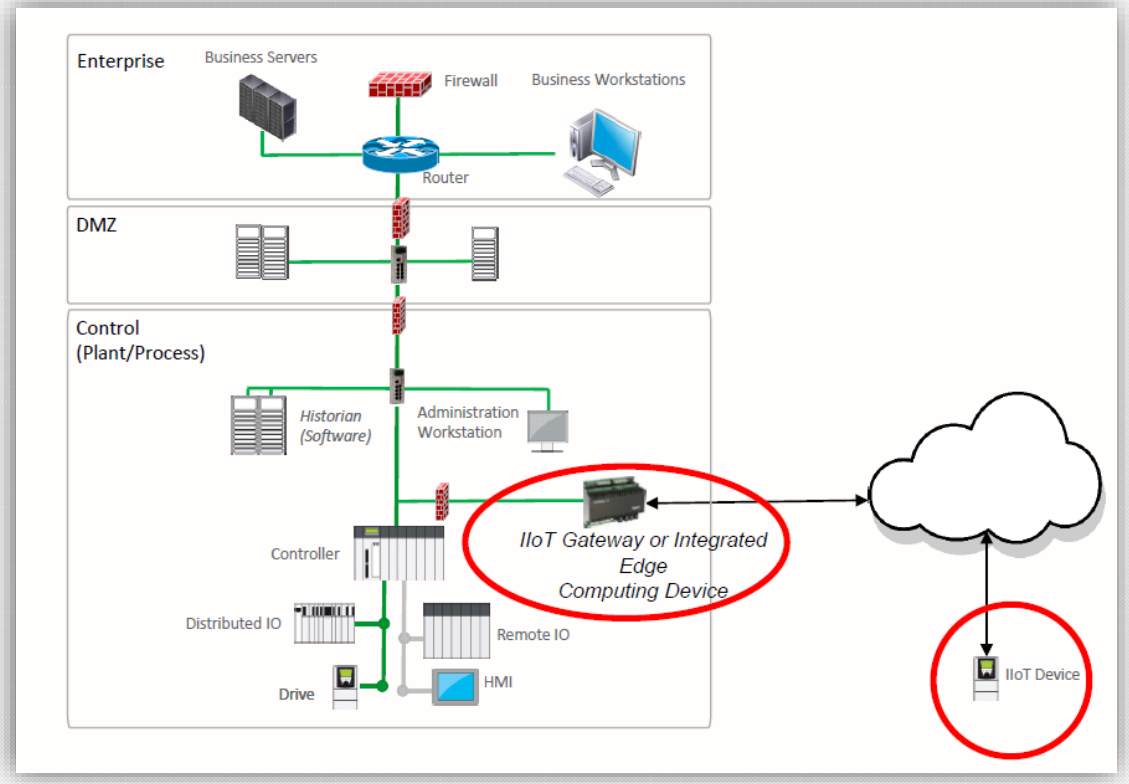
IIOT | Industry Driving IIoT Product Certification [3]

Study initiated to accelerate the availability of a vetted ISA/IEC 62443 based IIoT product certification

- ✓ Identify gaps in current 62443 certifications
- ✓ Recommend next steps for creation of IIoT product certification

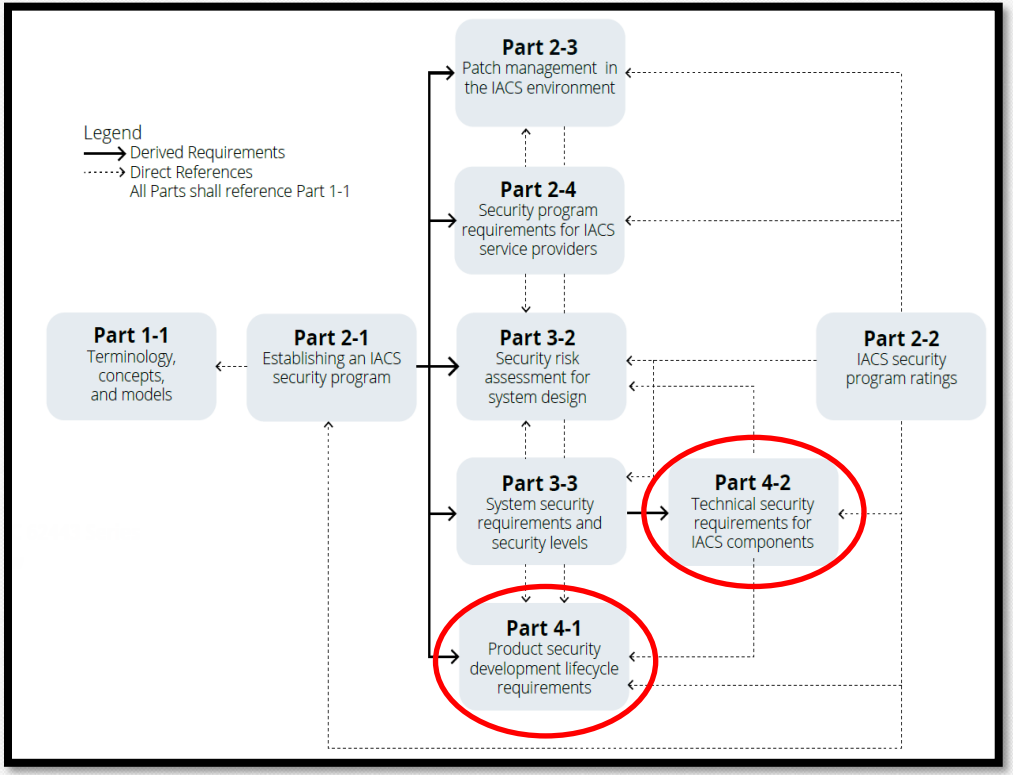
src: Using 62443 Certification to Lower IIoT Cybersecurity Risk

IIOT | Cybersecurity Risk



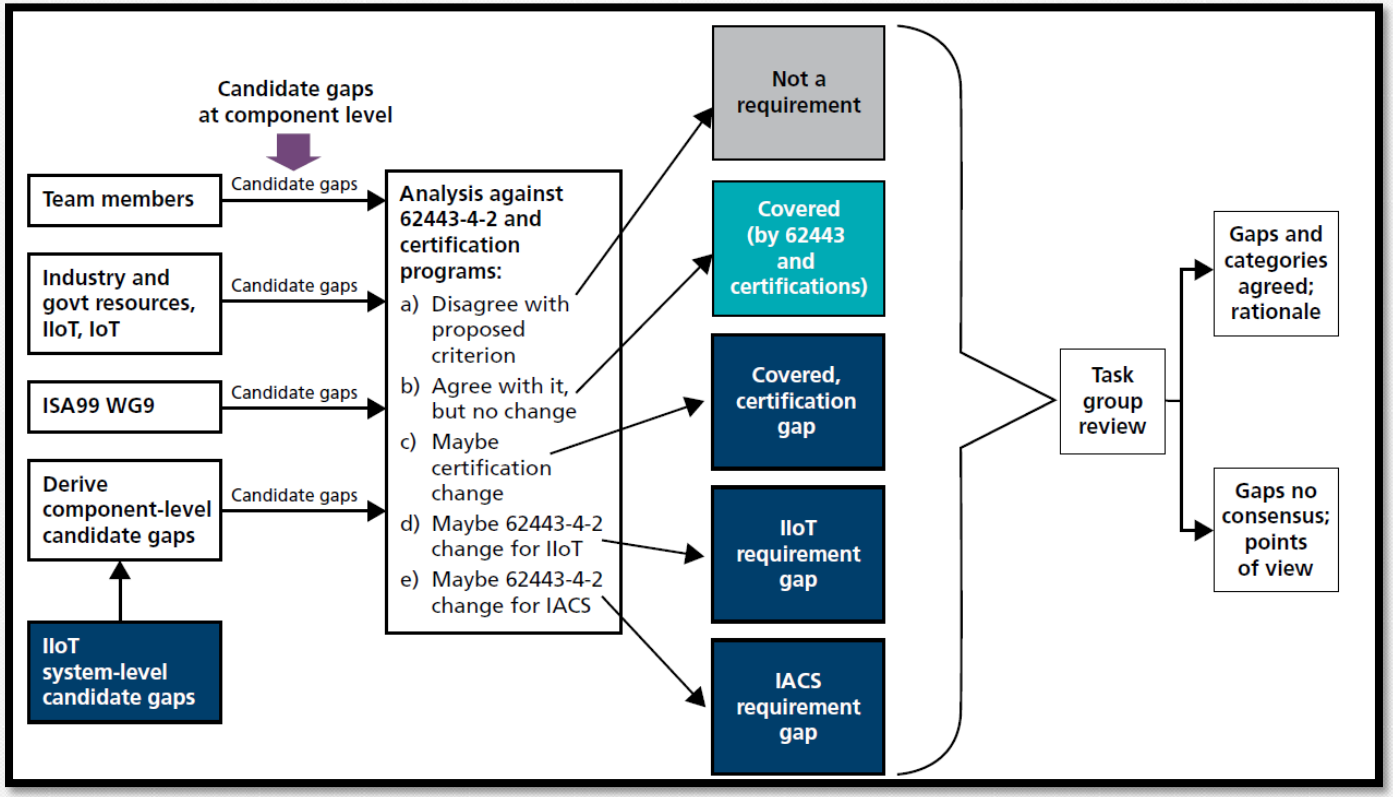
src: Using 62443 Certification to Lower IIoT Cybersecurity Risk

ISA/IEC 62443 | Series Hierarchical View



img src: https://www.isasecure.org/en-US/Documents/Articles-and-Technical-Papers/ISAGCA-Security-Lifecycles-whitepaper.pdf

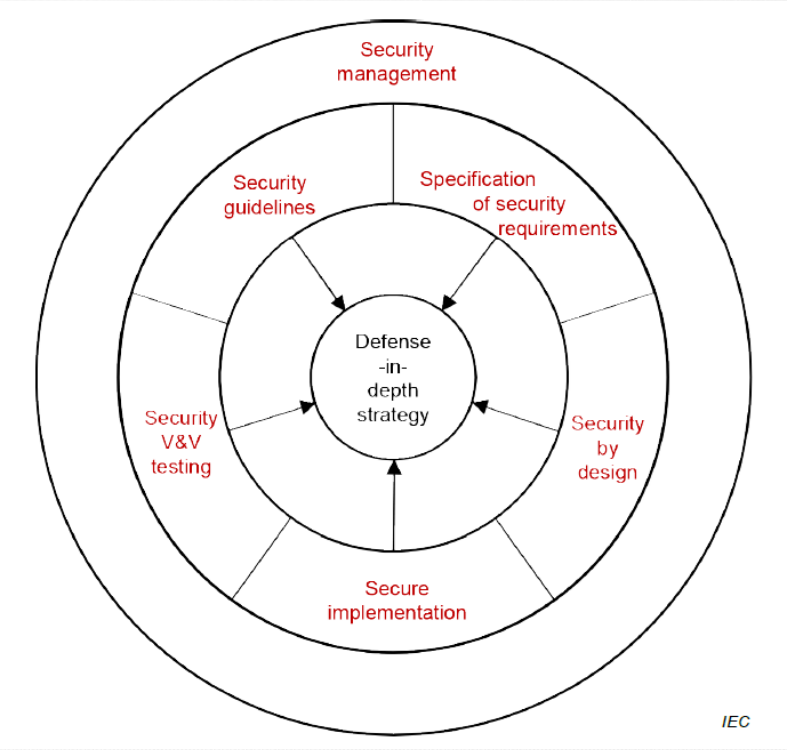
IIOT | Gap analysis process for IIoT devices and gateways [3]



src: IIoT Component Certification Based on the 62443 Standard

ISA/ IEC 62443-4-1 安全產品開發流程

- Security management
- Specification of security requirements
- Secure by design
- Secure implementation
- Security verification and validation testing
- Management of security-related issues
- Security update management
- Security guidelines



img src: IEC 62443-4-1:2018

ISA/IEC62443-4-1 | Maturity Levels

Practiced

Undocumented
(or not fully documented)

Continuous improvement

- Documented
- Policies
- Procedures
- Repeatable

Refined Evaluation Methods - Lifecycle Requirements [6]

62443-4-1 Reference	Evaluation Refinement	Rationale
SR-1	Security context incorporates IIoT elements	Recognize unique threats
SR-2	Threat model incorporates device failures	Small window before attackers locate opportunity
SR-2	Threat model incorporates shared resources between functions	Use of co-location architectures
SR-4	Required ICSA (ISA/IEC 62443-4-2) certification tier documentation in security requirements.	Required tier aligns with organization's security needs based on risk assessments.
SR-5	Cloud security expert review for cloud-based component verification.	Cloud components have unique risks.
SUM-5	Periodic review of maintenance of security	Increase focus on lifecycle vs. point-in-time security

New Lifecycle Requirements [6]

Lifecycle Requirement	Rationale
Add design practice for zone partitioning internal to components (compartmentalization)	Address threats previously addressed by network segmentation
Include related cloud supplier in security design review	Verify assumptions about system security
Receive security notifications from related cloud supplier	Enable related actions/mitigations for component user
Provide user documentation of cloud dependencies, including ongoing traffic over untrusted network	Distinguish attacks from normal operation; assess ongoing risk
User documentation describes physical elements shared among component functions	Assess risks of function co-location
Proactive notification of update/upgrade availability	Shorten vulnerability window
Advance notification of withdrawal from security update process	Shorter lifecycle for IIoT components than general control system components; greater exposure if unable to replace in time

img src: IEC 62443-4-2:2019

ISA/ IEC 62443-4-2 Component Type

Host device	Embedded device	Network device	Software application
● 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	● special purpose device designed to directly monitor or control an industrial process EXAMPLE PLCs, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, distributed control system (DCS) controllers.	● device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process	● 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)

src: IEC 62443-4-2:2019

IIoT Component Type [7]

IIoT device	IIoT gateway
● 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 accessible via that network	● entity of an IIoT system that connects one or more proximity networks and the IIoT devices on those networks to each other and directly connects to one or more untrusted access networks

ISA/IEC 62443-4-2 | Security Levels

Hacker

Actively searching for it using sophisticated means with moderate resource, IACS specific skills and moderate motivation

Staff

Via eavesdropping or casual exposure

Nation state hacker group

Actively searching for it using sophisticated means with extended resource, IACS specific skills and high motivation

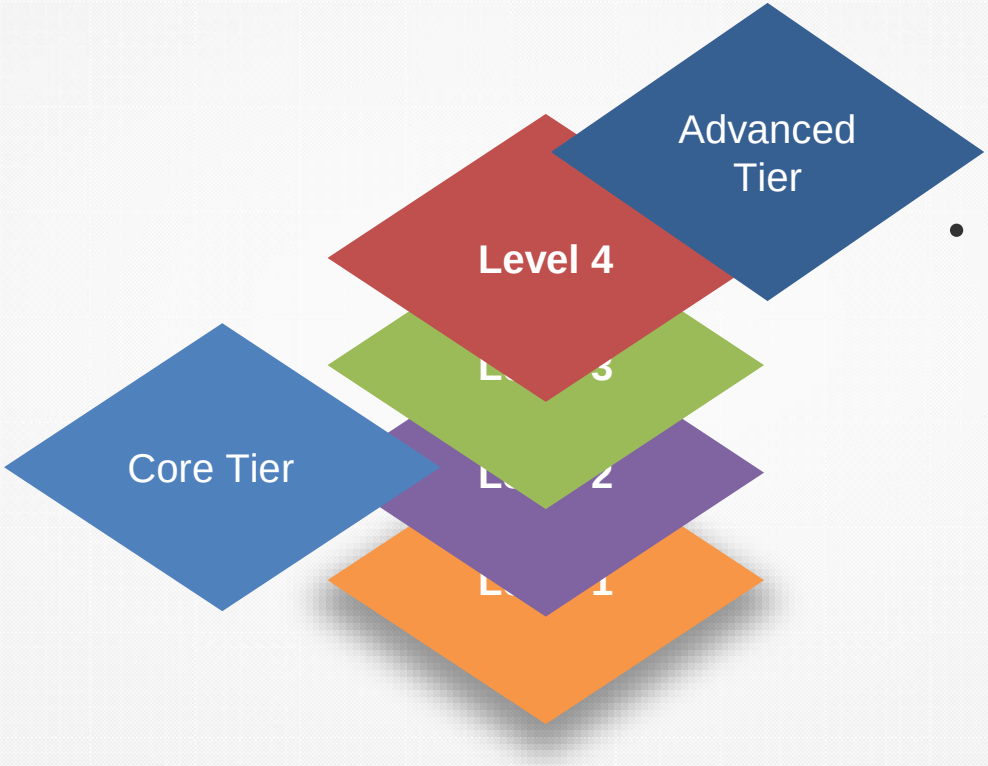
Script kid

Actively searching for it using simple means with low resource, generic skills and low motivation

62443 | Capability Security Levels to IIoT Tiers

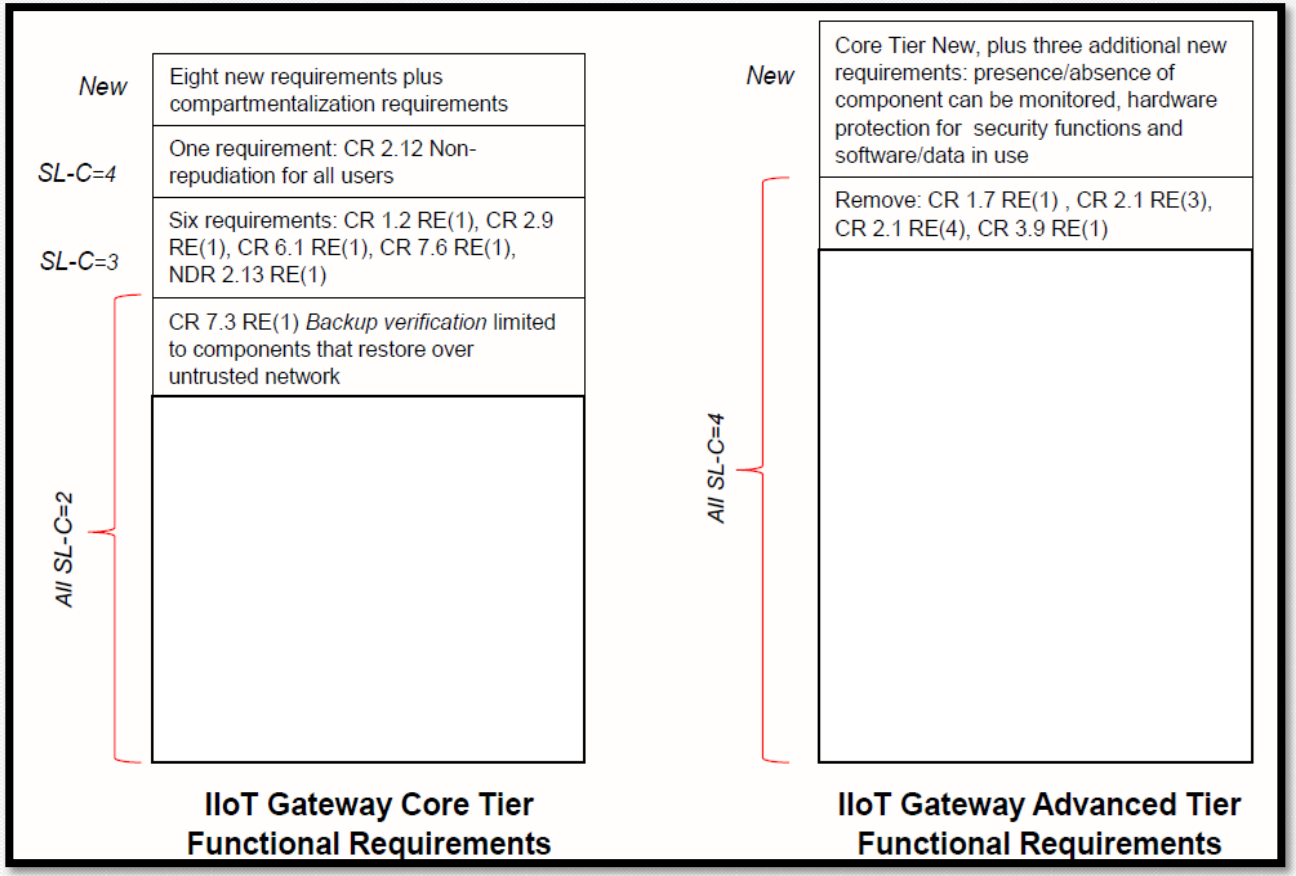
IIoT Core Tier

- Intend to address adversaries as defined by 62443 capability security level 2
- Incorporate selected level 3 and 4 requirements to specifically address the threat of more sophisticated attackers originating from the untrusted network.



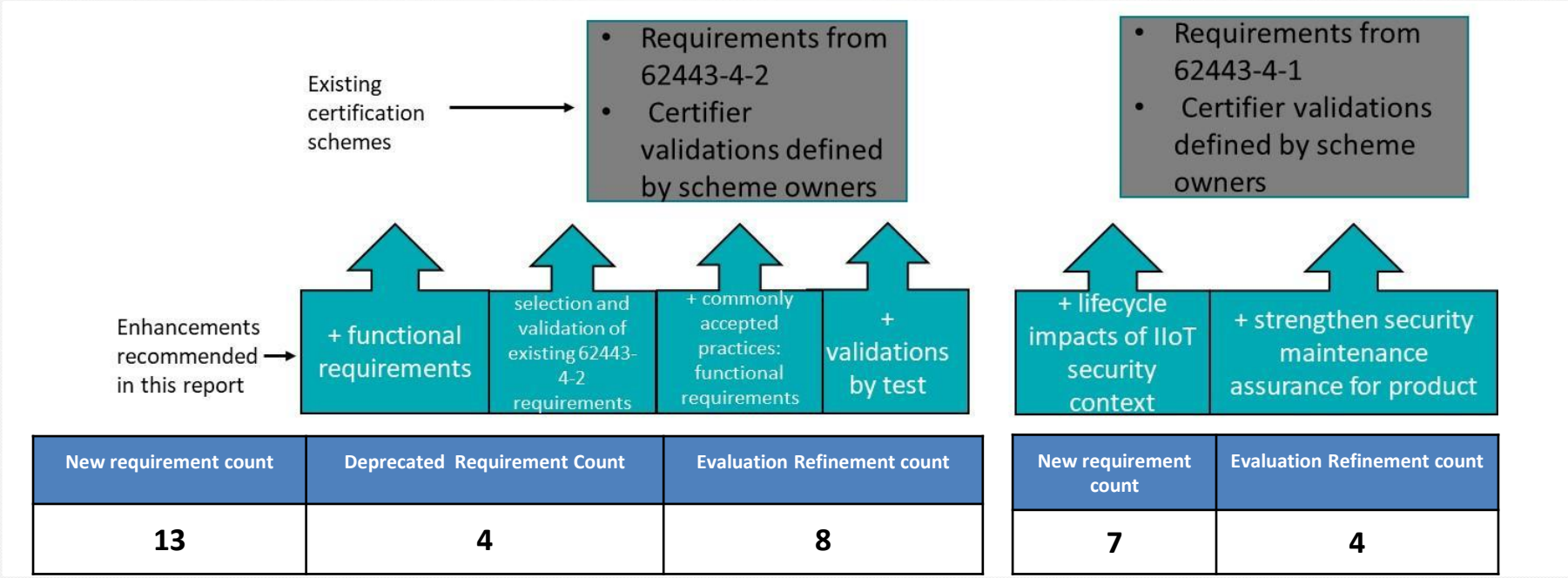
IIoT Advanced Tier

- Intend to address adversaries as defined by 62443 capability security level 4



img src: Using 62443 Certification to Lower IIoT Cybersecurity Risk

62443 Certification | Enhancements for IIoT devices and gateways [3]



New requirement count	Deprecated Requirement Count	Evaluation Refinement count
13	4	8

New requirement count	Evaluation Refinement count
7	4

IIoT Core Tier requirements from 62443-4-2, with SL-C 3 or 4 [3]

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 3.1 RE(1) Communication authentication	Protect against and diagnose attacks via the untrusted network connection	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

All Existing 62443-4-2 Capability Security Level 1-4 Requirements Used For IIoT Device And Gateway Certification With These Exceptions [3]

62443-4-2 Requirement ID	62443-4-2 Requirement	Rationale for not including
CR 1.7 RE(1)	Password generation and lifetime restrictions for human users	Periodic password change no longer considered best practice
CR 2.1 RE(3)	Supervisor override	Not useful for limited device functionality, introduces risk
CR 2.1 RE(4)	Dual approval	Not used in many cases
CR 3.9 RE(1)	Audit records on write once media	Records typically sent to other systems

New Proposed IIoT Requirements not found in 62443-4-2

Functional Requirement	Rationale
Compartmentalization (5 sub requirements)	Limit effect of breaches, more frequent from untrusted networks
Secure by default	Address management and risk for at scale deployments
Unique per device, initial passwords/keys	Address management and risk for at scale deployments
Authentication of non human users from untrusted networks	Connection to untrusted network, non human attackers of all intentions
Protection from untrusted management traffic	Management interface is lethal attack vector and often overlooked
Turn off untrusted network connection, maintain essential functions	Turning off this connection is common response to incident
Remote update and upgrade	Devices in remote physical locations, potentially at scale
Update/upgrade maintains security settings	Practical management at scale, given frequent updates/upgrades
Enable/disable update and upgrade	Enable asset owner management of change
Protect software and data in use (with hardware for Advanced Tier)	Sophistication of attackers increases attacks on data in use
Presence of component can be monitored (Advanced Tier)	Damage, theft due to small size, unprotected location
…	…

Refined Evaluation Methods in 62443-4-2 [3]

62443-4-2 Reference	Evaluation Refinement	Rationale
NDR 5.2, CR 4.1	Evaluate zone requirements internal to component	Use of co-location architectures
CR 1.1, 1.9, 3.4, 3.4 RE(1)	Acceptable use of untrusted network for security functions	Availability a concern
EDR|HDR|NDR 3.14, 3.14 RE(1)	Protect boot process given attacker physical possession of component	Unprotected physical location
CR 1.5D	Protect authenticators given attacker physical possession of component	Unprotected physical location
CR 6.2	Use commonly accepted interfaces for reporting continuous monitoring	Support use of best analysis tools
CR 7.1	DoS protection for loss of cloud functionality or untrusted connection	Common occurrence for IIoT
CR 7.4	Recovery after failed update/upgrade	Small window before attackers locate opportunity
CR 1.1, 1.2, 3.1, 3.1 RE(1), 3.4, 4.1	Identification, authentication, protection of confidentiality/integrity, use cryptographic methods commonly accepted for IIoT	Increase user confidence, drive definition of commonly accepted, move industry forward

IIOT | Certification Requirements for Use of Hardware Security Mechanisms

Advanced tier for IIoT gateway and device

- ✓ 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

~~CR 3.9 RE(1) Audit records on write-once media.~~

New requirements:

- ✓ Supplier root of trust in hardware for Core tier.
- ✓ Hardware compartmentalization of security functions, for Advanced tier.
- ✓ Hardware-based protections for code and data in use, for Advanced tier.

ICSA-500

ISA Security Compliance Institute — IIoT Component Security Assurance –

Selected commonly accepted security practices

Version 1.1

January 2023

4.1.1 Practices

IIoT PR 4.1.1-1 Cryptographic techniques

Cryptographic algorithms, including key lengths selected and random number generation methods used, conform to ISO/IEC 19790, or conform to an approved national or regional modification to Annex C of ISO/IEC 19790 (noting that such modifications are permitted by ISO/IEC 19790). There should be no reliance on proprietary or modified cryptographic algorithms. The following are examples of documents that provide conforming methods:

- For the United States, methods referenced in FIPS-14 Modules" fall under this practice. FIPS-140-3 referenc revision 1 "CMVP Validation Authority Updates to ISO/I in NIST SP 800-131A revision 2 "Transitioning the Use o
- For recommendations developed for the European Ur Parameters Report. 2014 Recommendations"
- From Germany Federal Office for Information Security, Recommendations and Key Lengths" Version: 2022-1

ICSA-311 FSA-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.*

4.5.3 External references

Example references that support above requirements as commonly accepted practices:

TCG Guidance for Securing Industrial Control Systems Using TCG Technology states in 4.2: "Secure and Measured Boot can be extended to run-time software through mechanisms such as the Linux Integrity Measurement Architecture."

Example references regarding implementation of these practices:

Linux Integrity Measurement Architecture (IMA) and Advanced Intrusion Detection Environment (AIDE) are examples of utilities that can be used to support the above practices.

Linux IMA is a kernel solution, described in the first four references below. Linux IMA natively provides automatic triggering of integrity checking for files as they are used. AIDE is a user space solution, described in the last reference. AIDE natively provides integrity checking triggered on-demand.

An Overview of The Linux Integrity Subsystem

https://www.kernel.org/doc/html/latest/security/IMA-templates.html

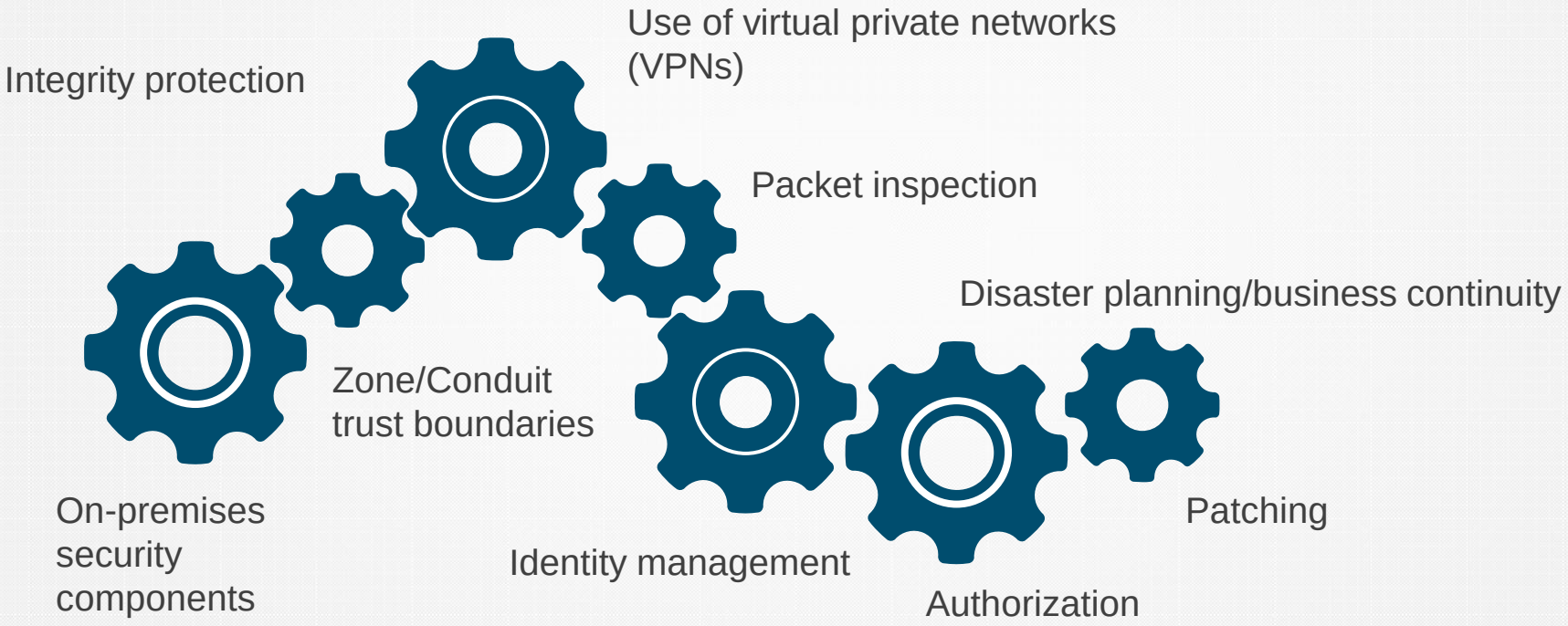
https://www.redhat.com/ja/blog/how-use-linux-kernels-integrity-measurement-architecture

TCG Guidance for Securing Industrial Control Systems Using TCG Technology discusses IMA in 6.12.1

https://aide.github.io/

Cloud Service Providers

Cloud Service Providers Security Controls [1]



Thank you

References

[1] ISA-TR62443-1-6 Security for industrial automation and control systems Application of the 62443 standards to the Industrial Internet of Things, Draft Technical Report
[2] IIoT System Certification Based on 62443 Standards, Final Draft Version 0.10
[3] IIoT Component Certification Based on the 62443 Standard, Version 1.4
[4] Using 62443 Certification to Lower IIoT Cybersecurity Risk, October 27, 2021
[5] ICSA-500 ISA Security Compliance Institute — IIoT Component Security Assurance – Selected commonly accepted security practices, Version 1.1
[6] ISDLA-312 ISA Security Compliance Institute —Security Development Lifecycle Assurance - Security Development Lifecycle Assessment for ICSA, Version 6.3
[7] ICSA-311 ISA Security Compliance Institute — IIoT Component Security Assurance Functional security assessment for IIoT components, Version 2.3