Using 62443 Certification to Lower IIoT Cybersecurity Risk

October 27, 2021

ISASecure®

Speakers

Dan DesRuisseaux *possesses over 25 years of diverse experience in engineering, sales, and marketing roles in high tech companies. Mr. DesRuisseaux presently serves as the Cybersecurity Program Director for Schneider Electric's Industrial Division. In this role he works to insure the proper and consistent implementation of security features across SE's diverse product portfolio. He also identifies and fills security gaps by forging partnerships with best-in-class security appliance companies. Mr. DesRuisseaux is also the marketing Chairman of the ISA Security Compliance Institute - a non-profit organization seeking to improve ICS security through standards compliance.*

In over 25 years in the cyber security field, ***Carol Muehrcke*** *has led security assurance teams for high assurance products, software development teams for both commercial and government security products, research programs on assurance methods and security mechanisms, and industry working groups on cyber security. Starting in 2008 she has worked with the ISA Security Compliance Institute to manage, develop and roll out certification programs for control systems, control system components, and secure product development life cycle. Recently she has led ISA Global Cybersecurity Alliance teams to study Industrial Internet of Things product certifications and cross references of other standards with 62443. She was a contributing author to the process control cyber security standard ISA-62443-2-1-2009.*

Agenda

Problem – IIoT Cybersecurity Risk

Approach – IIoT Cybersecurity Certification

Recommendations

Next steps

Problem: IIoT Security Risk

Urgent need overcomes potential cybersecurity risk

Asset owners creating their own procurement criteria, would prefer standards-based certification

Agenda

Problem – IIoT Cybersecurity Risk

Approach – IIoT Cybersecurity Certification

Recommendations

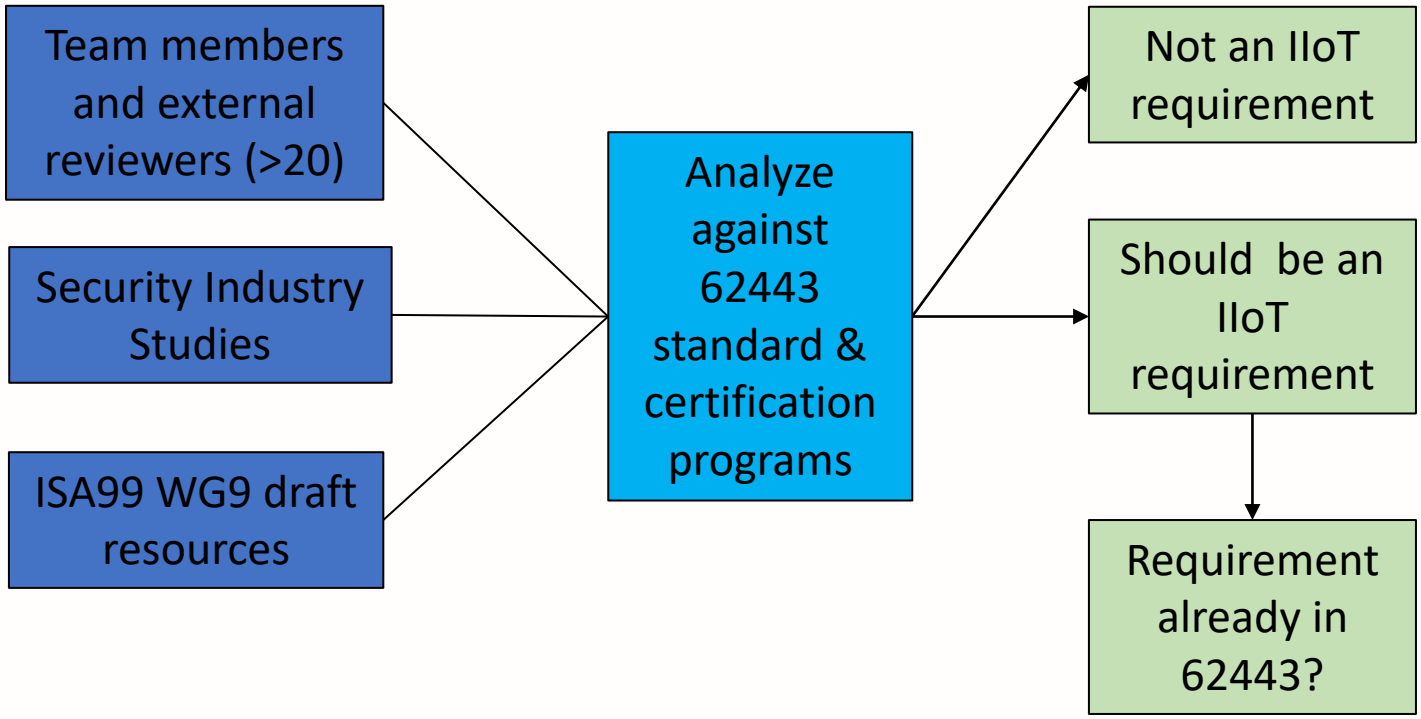
Next steps

Industry Driving IIoT Product Certification

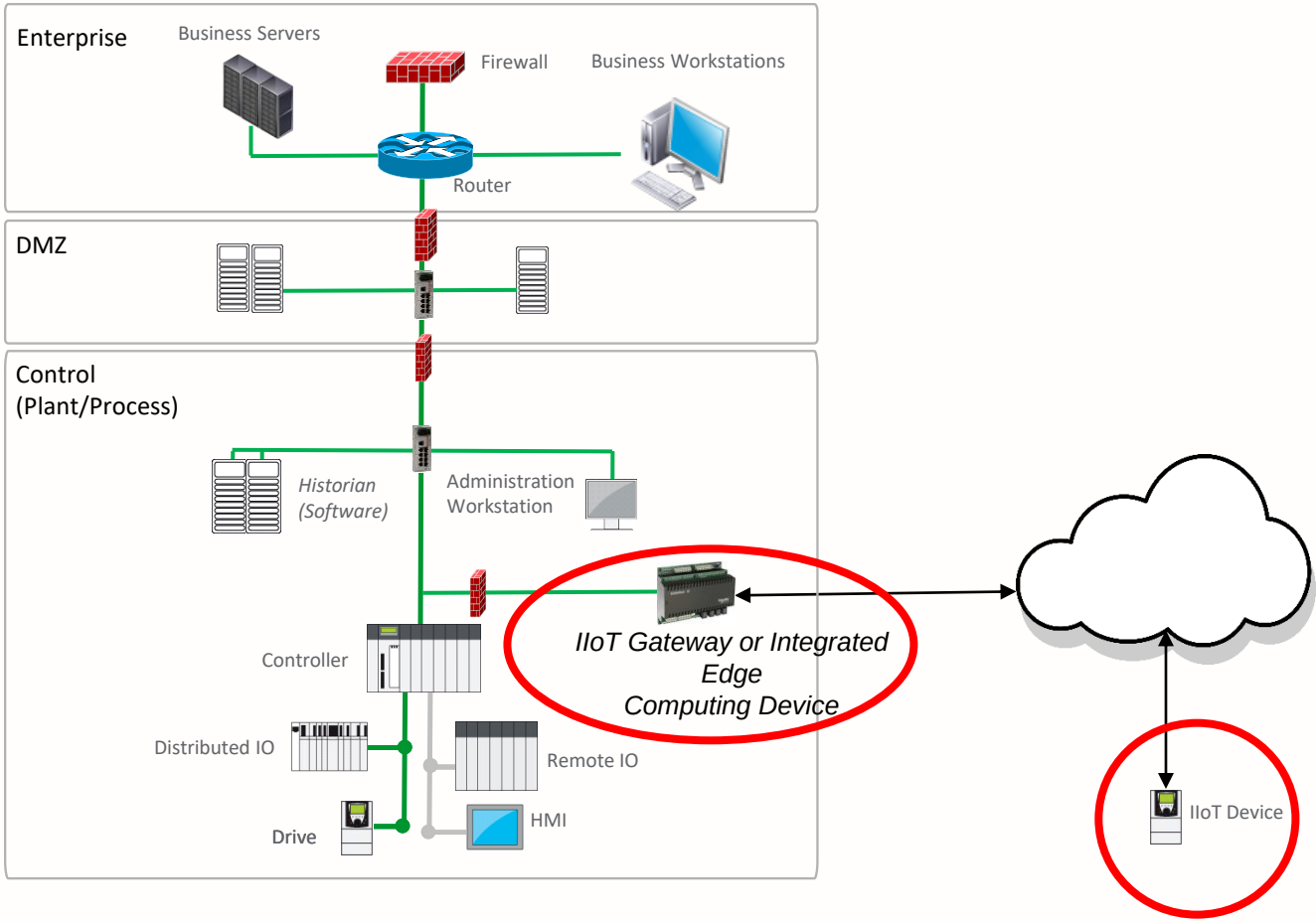
Study initiated to accelerate the availability of a vetted 62443 based IIoT product certification (**Link**)

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

Study Methodology



ISAGCA/ISCI Study Scope



Agenda

Problem – IIoT Cybersecurity Risk

Approach – IIoT Cybersecurity Certification

Recommendations

Next steps

Recommendation – Adjust 62443 Certification Criteria

Existing certifications cover ~90% of desired criteria for IIoT certification

To achieve the 10%:

- Add certification requirements
- Remove some existing requirements
- Refine evaluation methods for existing requirements
- Create two certification tiers instead of four security levels

The study makes recommendations; but does not itself constitute a certification program

Add Functional Requirements

Functional Requirement	Rationale
Compartmentalization (5 sub requirements)	Limit effect of breaches, more frequent from untrusted networks
Supplier root of trust in hardware	Commonly accepted to protect basis for component integrity
Secure by default	Address management and risk for at-scale deployments
Unique per device, initial passwords/keys (D*)	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 (D*)	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
No silk screen (D*) (Advanced Tier)	Basic countermeasure against reverse engineering
Presence of component can be monitored (Advanced Tier)	Damage, theft due to small size, unprotected location

**D = requirement for devices only, not gateways*

Remove Functional Requirements

62443-4-2 Reference	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

Refine Evaluation Methods - Functional Requirements

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

Unprotected Physical Location

http://energy-cg.com/EandP_pics/DeepWaterSemi-GulfOfMexico-BOEMOPA.jpg

Add Lifecycle Requirements

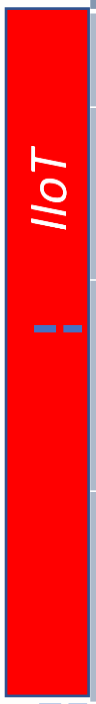
Lifecycle Requirement	Rationale
Add design practice for zone partitioning internal to components (compartmentalization)	Address threats previously addressed by network segmentation
Include related cloud supplier in security design review	Verify assumptions about system security
Receive security notifications 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

Refine Evaluation Methods - Lifecycle Requirements

62443-4-1 Reference	Lifecycle Requirement - 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
SUM-5	Periodic review of maintenance of security	Increase focus on lifecycle vs. point-in-time security

62443 Capability Security Levels to IIoT Tiers

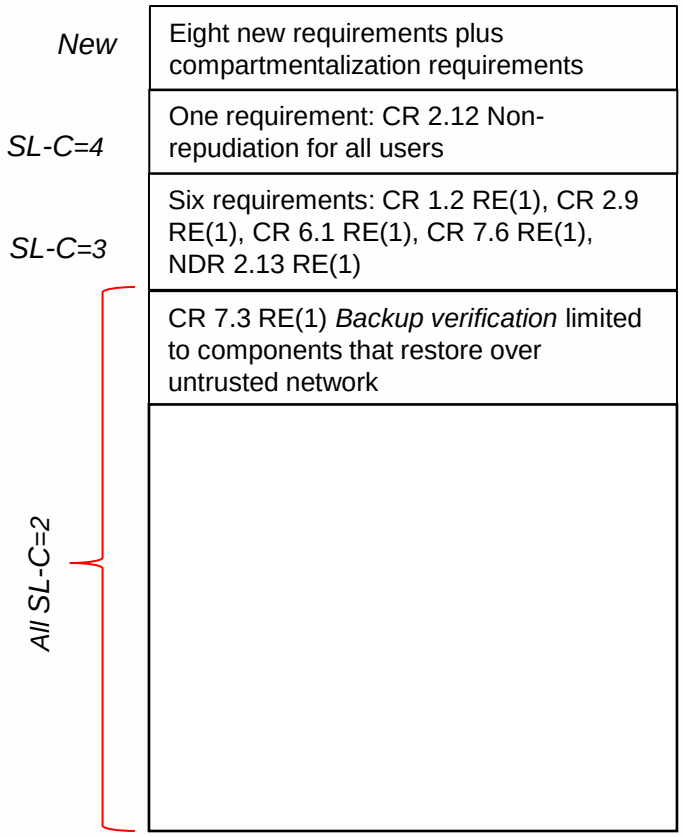
Security Level (SL-C)	Definition	Means	Resources	Skills	Motivation
1	Protection against casual or coincidental violation				
2	Protection against intentional violation using simple means with low resources, generic skills and low motivation	*simple*	*low*	*generic*	*low*
3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation	*sophisticated*	*moderate*	*IACS specific*	*moderate*
4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation	*sophisticated*	*extended*	*IACS specific*	*high*



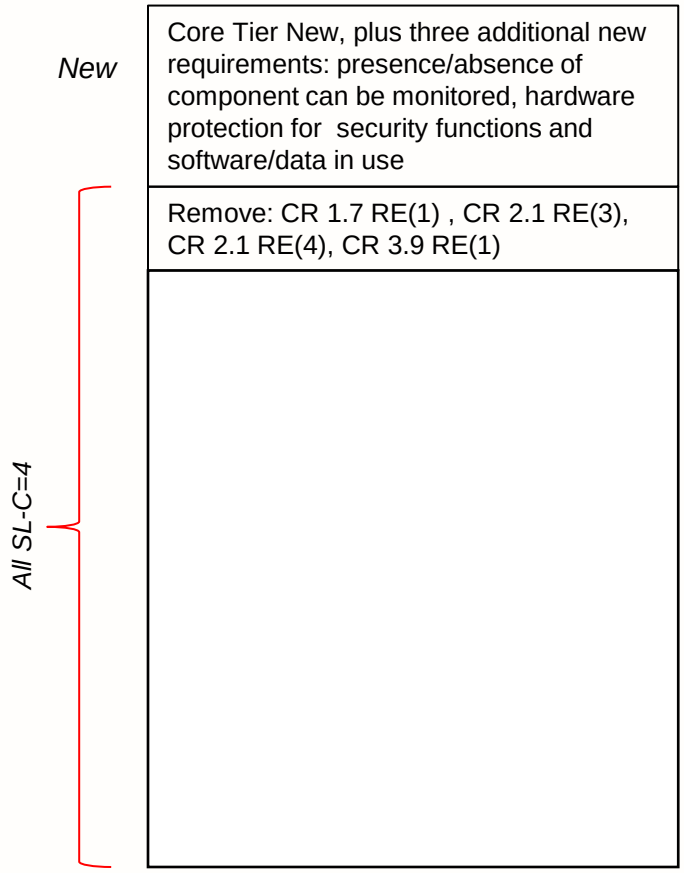
Core Tier

Advanced Tier

Functional Requirements by IIoT Tier



IIoT Gateway Core Tier Functional Requirements



IIoT Gateway Advanced Tier Functional Requirements

Agenda

Problem – IIoT Cybersecurity Risk

Approach – IIoT Cybersecurity Certification

Recommendations

Next steps

Next steps

Recommend consideration by

- 62443 standards organization ISA99
- 62443 certification scheme owners

Next phase of study targeting IIoT systems

- Cloud based functionality
- Edge functionality

Questions?

ISA Global CS Alliance

The objectives of the ISA Global Cybersecurity Alliance include the acceleration and expansion of standards, certification, education programs, advocacy efforts, and thought leadership. Members:

Schneider Electric
Rockwell Automation
Honeywell
Johnson Controls
Claroty
Nozomi Networks
PAS
txOne Networks
Xage Security
Wallix
Bayshore
Senhasegura

Radiflow
exida
Munio Security
Digital Immunity
Tripwire
Dragos
Idaho National Labs
TiSafe
ae Solutions
Mission Secure Inc
WisePlant
Tenable

Acet Solutions
1898 co
Cyberowl
Logiic
ISASecure
Nova Systems
Deloitte
Console Works
Eaton
KPMG
Surge Engineering
Petronas

UL
Idaho State University
Johns Manville
Red Trident Inc
Xylem
Baserock
Cyphy Defense
Coontec
Fortinet

ISASecure

ISASecure's mission is to decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders . Members:

Chevron
ExxonMobil
Saudi Aramco
Shell
Honeywell
Johnson Controls
Schneider Electric
Yokogawa
Applied Risk
CSA Group
DNV-GL
FM Approvals
exida
Bureau Veritas
Security Compass
SGS ESPANOLA DE CONTROL
Synopsys
TUV Rheinland
TUV SUD
TrustCB
YPF S. A.
HON Consulting S.r.l dba BYHON
Control System Security Center