IIoT System Implementation and Certification for Cloud-based Functionality Based on ISA/IEC 62443 Standards

Johan Nye
ICS Guru LLC

ISA International Society of Automation
Setting the Standard for Automation™

ISA GLOBAL CYBERSECURITY ALLIANCE

ISASecure®

Bio

- Independent consultant specializing in ICS cybersecurity and ISA/IEC 62443
- Current Co-Chairman of ISA 99 Committee
- Retired from major petrochemical company
  - 38 years as Control System Engineer
  - Last 20 years focused on cybersecurity
  - Distinguished Engineering Advisor
- Founder and former Chairman of ISA Security Compliance Institute (ISASecure)
- linkedin.com/in/jbnye

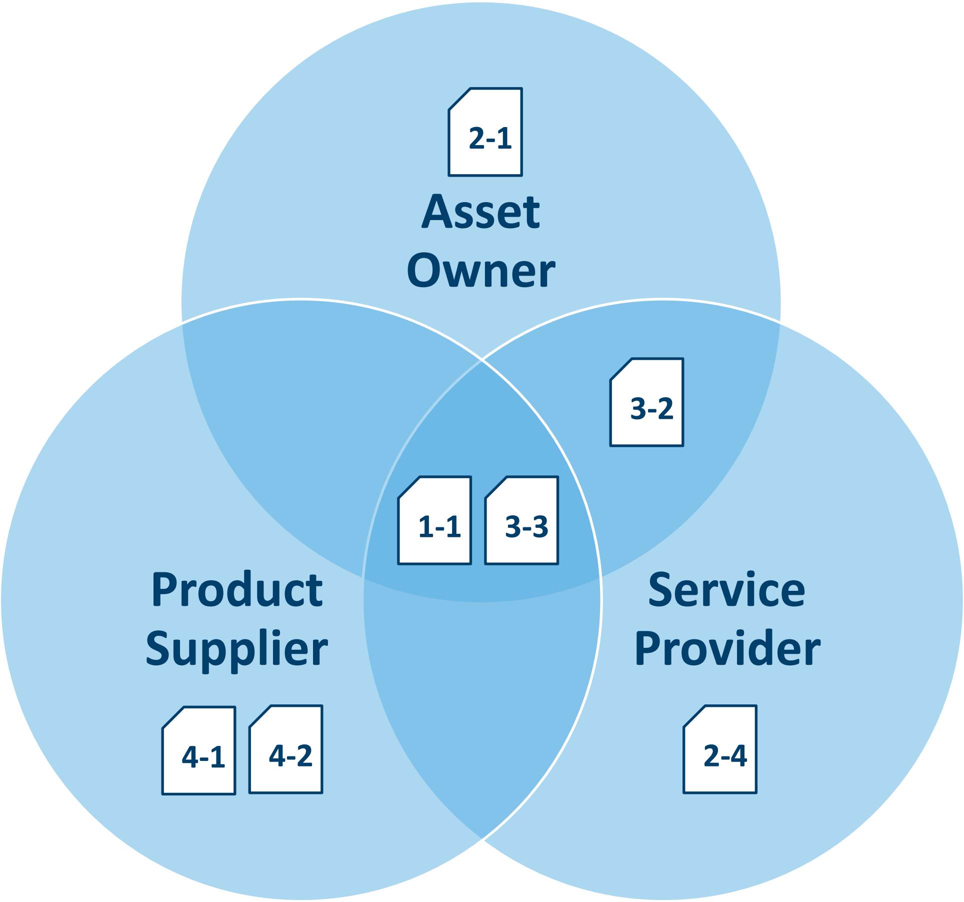
IIoT Systems Implementation and Certification Based on 62443 Standards

- Research on IIoT implementation and certification based on 62443 standards funded by:
  - ISA Global Cybersecurity Alliance (ISAGCA.org)
  - ISA Security Compliance Institute (ISASecure.org)
- Research published in two parts:
  - Part 1 – IIoT Component Certification Based on the 62443 Standard
  - Part 2 – IIoT System Implementation and Certification Based on ISA/IEC 62443 Standards
- Part 2 is the subject of this presentation and has three main parts:
  - Section 4 – Applying ISA/IEC 62443 Standards to IIoT Systems
  - Section 5 – Enhancing ISA/IEC 62443 Standards for IIoT Systems
  - Section 6 – Conformity Assessment of IIoT Systems using ISA/IEC 62443 Standards

Note

This report is not intended to encourage or dissuade the use of cloud-based functionality for Industrial Automation and Control Systems. The use of cloud-based functionality for IACS is a risk-based decision that is the responsibility of the Asset Owner.

ISA/IEC 62443 Overview



Core Parts of the 62443 series of standards

- Part 1-1 – Overview of the 62443 Series
- Part 2-1 – Security Program for Asset Owner
- Part 2-4 – Security Program for Service Provider
- Part 3-2 – Security Risk Assessment process
- Part 3-3 – System technical requirements
- Part 4-1 – Product security development lifecycle
- Part 4-2 – Component technical requirements

Key Concepts

- Security Program requirements (Part 2-1, 2-4, 4-1)
- System and component requirements (Part 3-3, 4-2)
- Security Risk Assessment process (Part 3-2)
- Essential Functions
- Security Zones and Conduits
- Security Levels (for technical requirements)
- Maturity Levels (for process requirements)

Terminology

cloud

- collection of networked remote servers

IIoT system

- system providing functionalities of Industrial Internet of Things
- includes: IIoT devices, IIoT gateways, sensors, actuators, cloud-based functionality

IIoT component

- component with the capability to communicate with cloud-based services over an untrusted network
- includes: embedded devices, host devices, network devices, software applications, IaaS, PaaS, SaaS

IIoT IACS

- industrial automation and control system that uses cloud-based functionality

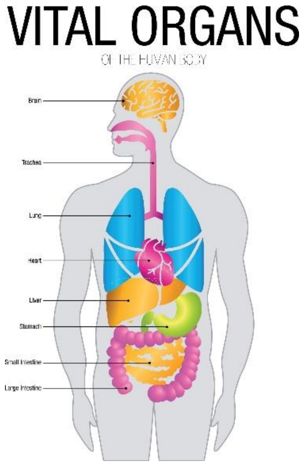
Applying ISA/IEC 62443 to IIoT Systems

- Questions…
  - Can Essential Functions implemented in the cloud meet 62443 requirements?
  - Can the 62443 risk assessment process be used for an IIoT System?
  - When do 62443 requirements apply to cloud-based functionality?
  - Can the cloud provider role be mapped to existing 62443 roles (AO, SP, PS)?
- Example Use Cases
  - Example Use Case #1 – Data analysis in the cloud – non-Operational use
  - Example Use Case #2 – Data analysis in the cloud – Operational use
  - Example Use Case #3 – Operator view and manipulation from the cloud
  - Example Use Case #4 – non-Essential Control in the cloud

Essential Functions

What are Essential Functions ?

- Safety functions to protect health, safety, the environment
- Control functions where high availability is required
- View and manipulate functions where high availability is required



ISA/IEC 62443-3-3, clause 5.2

- Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment
- Access controls shall not prevent the operation of essential functions
- Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode
- A Denial of Service (DoS) event on the control system or safety instrumented system network shall not prevent the SIF from acting

IIoT System implications when essential functions are implemented in the cloud

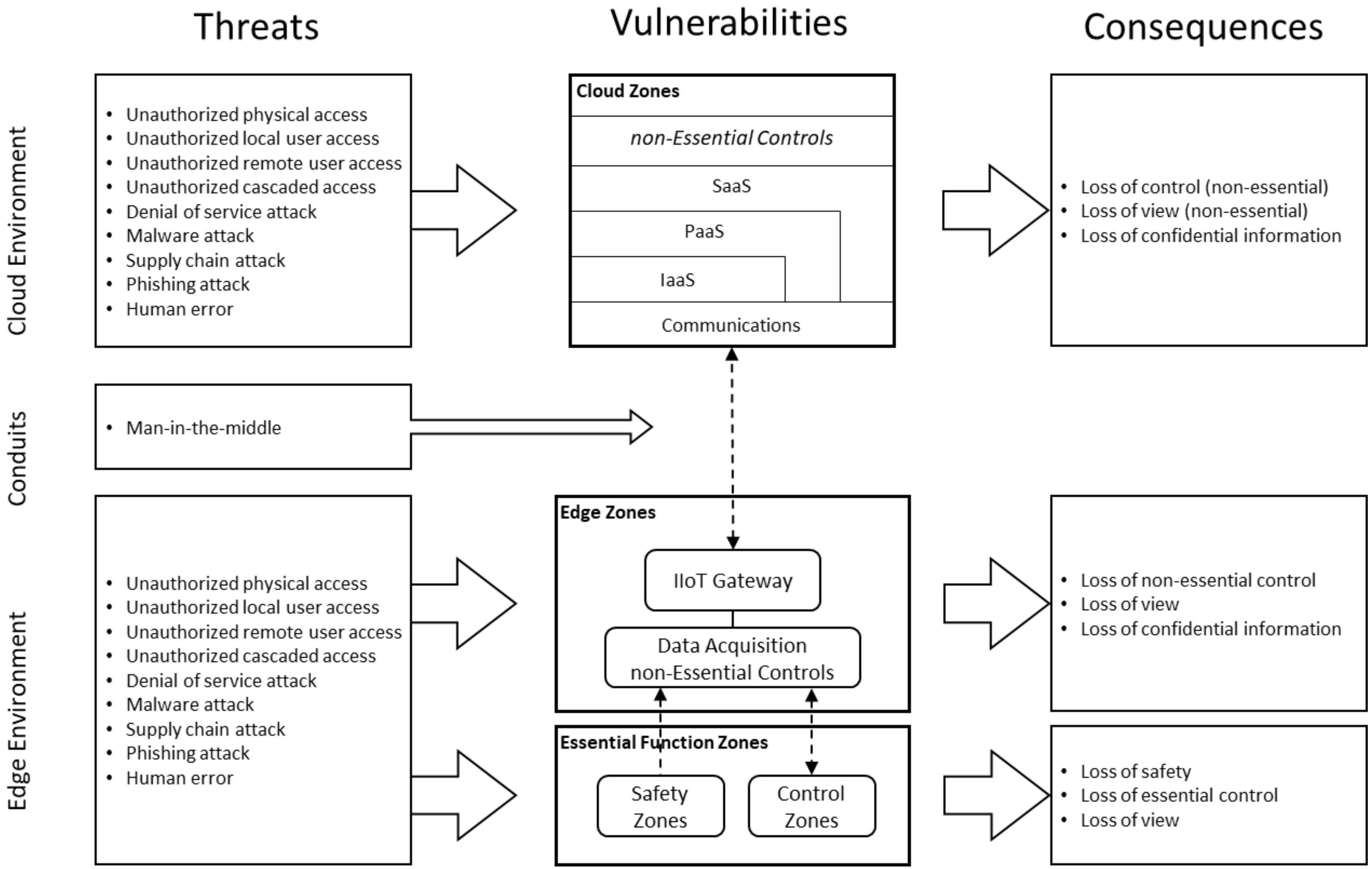
- If the edge zone boundary goes into fail close or island mode it would impact essential functions (#3)
- A denial-of-service event on the network between cloud zone and edge zone would impact essential functions (#4)

Implementation of essential functions in the cloud environment does not meet the requirements of ISA/IEC 62443 standards

Risk Assessment note

This is not an actual risk assessment. Generic consequences such as loss of protection, control or view have been substituted in place of actual consequences such as loss of health/safety, damage to environment, or loss of product integrity. It is intended to be used as an example of the risk assessment process and should not be used in place of an actual risk assessment. This particular risk assessment was performed by a small team comprised of asset owners, product suppliers and cybersecurity consultants familiar with ISA/IEC 62443

Example Risk Assessment Model



Threats

Vulnerabilities

Consequences

Cloud Environment

- Unauthorized physical access
- Unauthorized local user access
- Unauthorized remote user access
- Unauthorized cascaded access
- Denial of service attack
- Malware attack
- Supply chain attack
- Phishing attack
- Human error

Cloud Zones

non-Essential Controls

SaaS

PaaS

IaaS

Communications

- Loss of control (non-essential)
- Loss of view (non-essential)
- Loss of confidential information

Conduits

- Man-in-the-middle

Edge Environment

- Unauthorized physical access
- Unauthorized local user access
- Unauthorized remote user access
- Unauthorized cascaded access
- Denial of service attack
- Malware attack
- Supply chain attack
- Phishing attack
- Human error

Edge Zones

IIoT Gateway

Data Acquisition non-Essential Controls

- Loss of non-essential control
- Loss of view
- Loss of confidential information

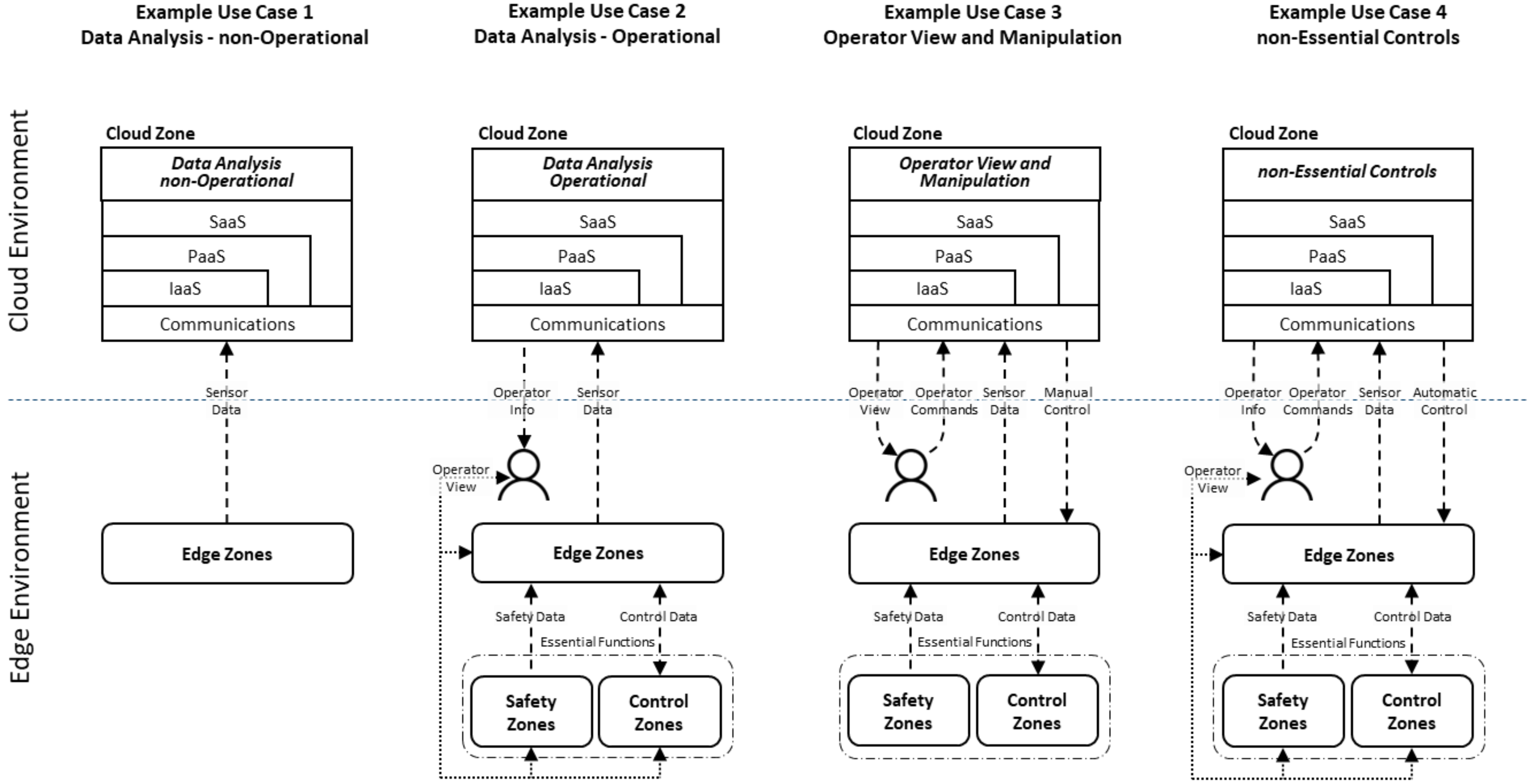
Essential Function Zones

Safety Zones

Control Zones

- Loss of safety
- Loss of essential control
- Loss of view

Example IIoT Use Cases – Zone and Conduit Partitioning



Example IIoT Use Cases – Impact Severity and Likelihood

Impact Severity

IACS Consequence Categories (unmitigated)	Use Case 1 Zones		Use Case 2 Zones				Use Case 3 Zones				Use Case 4 Zones			
	Data Analysis - non-operational		Data Analysis - Operational				Operator View (SCADA)				non-Essential Controls			
	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud
Loss of Safety function (Essential)	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a	n/a
Loss/compromise of Control function (Essential)	n/a	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a
Loss/compromise of View function (Essential)	n/a	n/a	High	High	n/a	n/a	High	High	n/a	n/a	High	High	n/a	n/a
Loss/compromise of Control function (non- Essential)	n/a	n/a	n/a	High	Low	n/a	n/a	High	Medium	Medium	n/a	High	Medium	Medium
Loss/compromise of View function (non-Essential)	Medium	n/a	Low	Low	Medium	n/a	Low	Low	Medium	Medium	Low	Low	Medium	Medium
Loss of Confidential Information	Medium	n/a	Low	Low	Medium	Medium	Low	Low	Medium	Medium	Low	Low	Medium	Medium

Likelihood

Threat/Vulnerability Likelihood (unmitigated)	Use Case 1 Zones		Use Case 2 Zones				Use Case 3 Zones				Use Case 4 Zones			
	Data Analysis - non-operational		Data Analysis - Operational				Data Analysis & Manipulation				non-Essential Controls			
	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud
Unauthorized physical access	Possible	Unlikely	Possible	Possible	Possible	Unlikely	Possible	Possible	Possible	Unlikely	Possible	Possible	Possible	Unlikely
Unauthorized local user access	Possible	Unlikely	Possible	Possible	Possible	Unlikely	Possible	Possible	Possible	Unlikely	Possible	Possible	Possible	Unlikely
Unauthorized remote user access	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely
Cascaded access (e.g. pivot from another zone)	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely
Denial of Service	Possible	Likely	Possible	Possible	Possible	Likely	Possible	Possible	Possible	Likely	Possible	Possible	Possible	Likely
Man-in-the-Middle	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely
Malware	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely
Supply chain (e.g. firmware update)	Possible	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely
Unpatched system or component	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible
Phishing attacks	Possible	Likely	Unlikely	Unlikely	Possible	Likely	Unlikely	Unlikely	Possible	Likely	Unlikely	Unlikely	Possible	Likely
Human error (design, implementation, operation, maintenance)	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely

Example IIoT Use Cases – Risk Assessment results

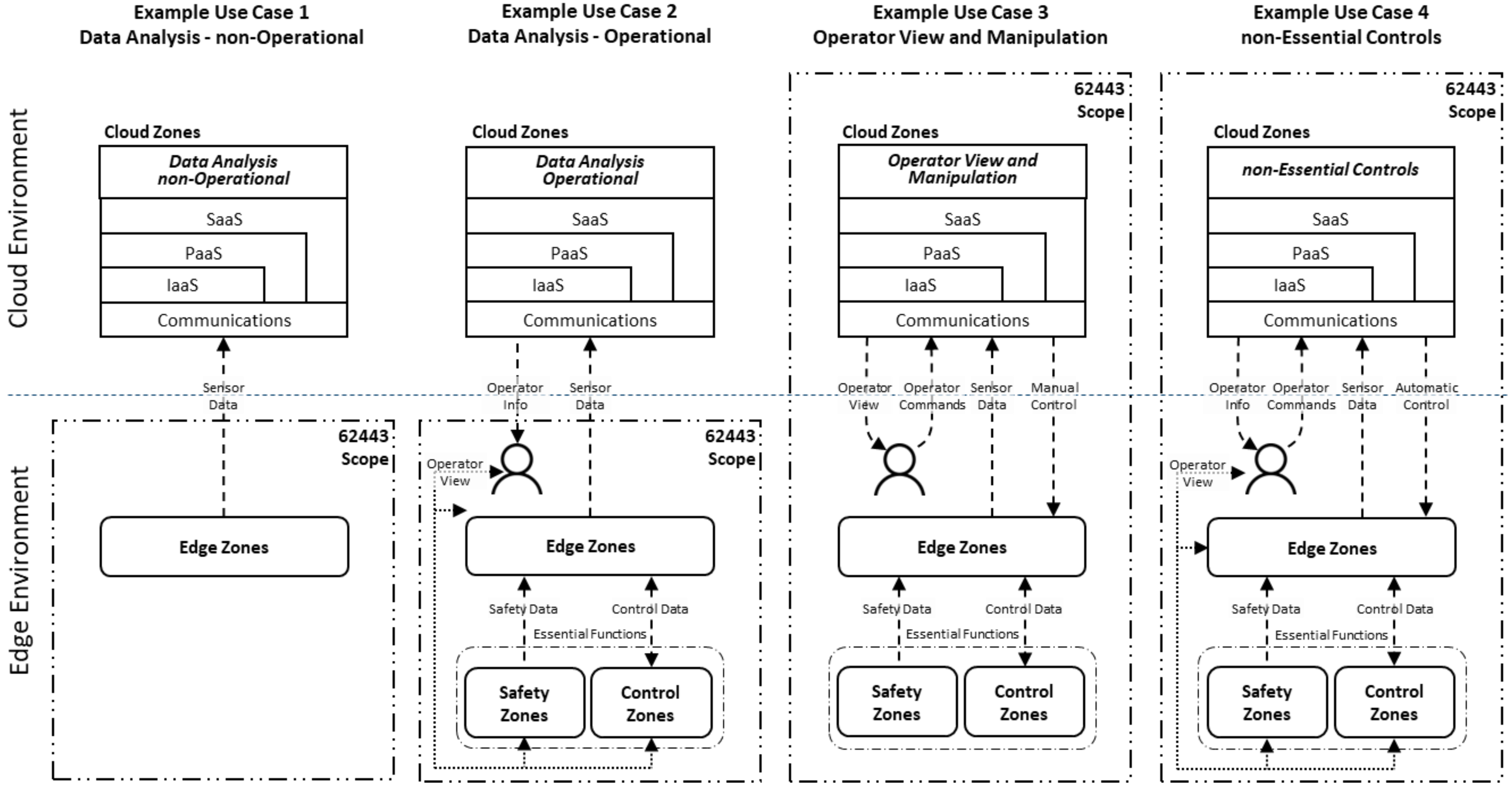
Initial Risk

Initial Risk	Use Case 1 Zones		Use Case 2 Zones				Use Case 3 Zones				Use Case 4 Zones			
	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud
Loss of Safety (Essential)	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a	n/a
Loss/manipulation of Control (Essential)	n/a	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a	n/a	High	n/a	n/a
Loss/manipulation of View (Essential)	n/a	n/a	High	High	n/a	n/a	High	High	n/a	n/a	High	High	n/a	n/a
Loss/manipulation of Control (non-Essential)	n/a	n/a	n/a	High	Medium	n/a	n/a	High	Med-High	Med-High	n/a	High	Med-High	Med-High
Loss/manipulation of View (non-Essential)	Med-High	n/a	Medium	Medium	Med-High	n/a	Medium	Medium	Med-High	Med-High	Medium	Medium	Med-High	Med-High
Loss of Confidential Information	Med-High	n/a	Medium	Medium	Med-High	Med-High	Medium	Medium	Med-High	Med-High	Medium	Medium	Med-High	Med-High

Target Security Level

Security Level - Target	Use Case 1 Zones		Use Case 2 Zones				Use Case 3 Zones				Use Case 4 Zones			
Consequence Type	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud	Safety	Control	Edge	Cloud
Loss of Safety (Essential)	n/a	n/a	SL 4	n/a	n/a	n/a	SL 4	n/a	n/a	n/a	SL 4	n/a	n/a	n/a
Loss/manipulation of Control (Essential)	n/a	n/a	n/a	SL 4	n/a	n/a	n/a	SL 4	n/a	n/a	n/a	SL 4	n/a	n/a
Loss/manipulation of Control (Non-Essential)	n/a	n/a	SL 4	SL 4	n/a	n/a	SL 4	SL 4	n/a	n/a	SL 4	SL 4	n/a	n/a
Loss/manipulation of View (Essential)	n/a	n/a	n/a	SL 4	SL 3	n/a	n/a	SL 4	SL 4	SL 4	n/a	SL 4	SL 4	SL 4
Loss/manipulation of View (Non-Essential)	SL 4	n/a	SL 3	SL 3	SL 4	n/a	SL 3	SL 3	SL 4	SL 4	SL 3	SL 3	SL 4	SL 4
Loss of Confidential Information	SL 4	n/a	SL 3	SL 3	SL 4	n/a	SL 3	SL 3	SL 4	SL 4	SL 3	SL 3	SL 4	SL 4

Example IIoT Use Cases – Scope of 62443



Cloud Environment

Edge Environment

Example Use Case 1
Data Analysis - non-Operational

Cloud Zones

Data Analysis non-Operational

SaaS

PaaS

IaaS

Communications

Sensor Data

62443 Scope

Edge Zones

Example Use Case 2
Data Analysis - Operational

Cloud Zones

Data Analysis Operational

SaaS

PaaS

IaaS

Communications

Operator Info

Sensor Data

62443 Scope

Operator View

Edge Zones

Safety Data

Control Data

Essential Functions

Safety Zones

Control Zones

Example Use Case 3
Operator View and Manipulation

62443 Scope

Cloud Zones

Operator View and Manipulation

SaaS

PaaS

IaaS

Communications

Operator View

Operator Commands

Sensor Data

Manual Control

Edge Zones

Safety Data

Control Data

Essential Functions

Safety Zones

Control Zones

Example Use Case 4
non-Essential Controls

62443 Scope

Cloud Zones

non-Essential Controls

SaaS

PaaS

IaaS

Communications

Operator Info

Operator Commands

Sensor Data

Automatic Control

Operator View

Edge Zones

Safety Data

Control Data

Essential Functions

Safety Zones

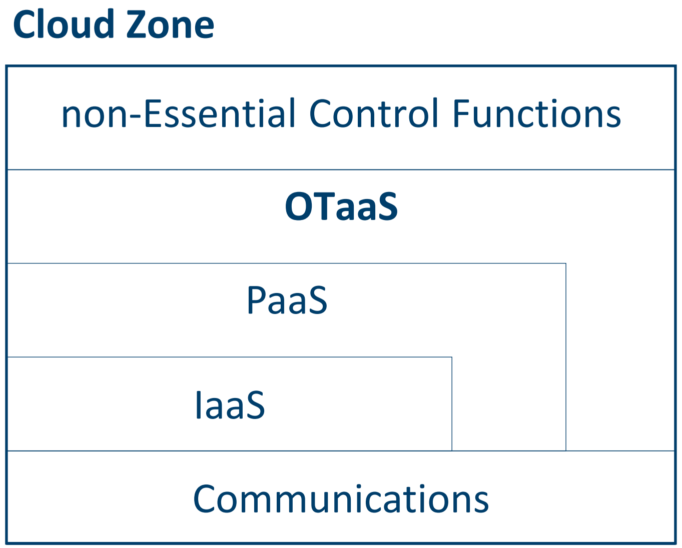
Control Zones

When does ISA/IEC 62443 apply to IIoT Systems?

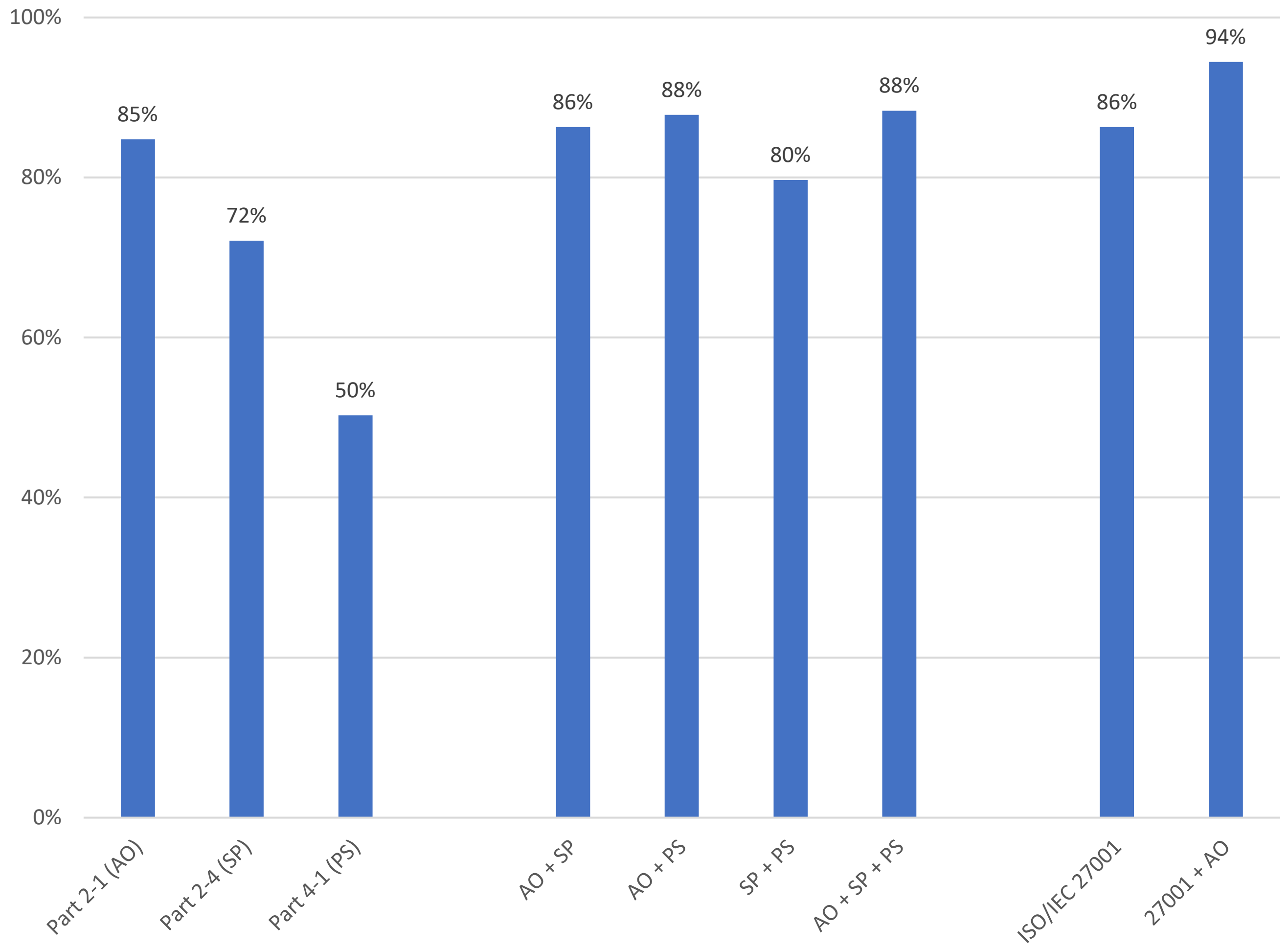
ISA/IEC 62443 requirements apply to the cloud environment when the cloud-based functionality has the capability to directly or indirectly change the physical state of the Equipment Under Control

Operational Technology as a Service (OTaaS)

- We need a mechanism to easily and transparently communicate when 62443 applies to the cloud (and when it does not)
- Adding a new cloud service category named Operational Technology as a Service (OTaaS) would meet this need
- OTaaS definition
  - cloud service category in which the cloud service customer can directly or indirectly control or manipulate physical devices or equipment that is located in the edge



CSA Cloud Control Matrix v4 Cross Reference



Cloud Security Alliance Cloud Control Matrix v4 cross reference to:

- Part 2-1 for Asset Owner (AO)
- Part 2-4 for Service Provider (SP)
- Part 4-1 for Product Supplier (PS)
- Part 3-3 for System technical requirements

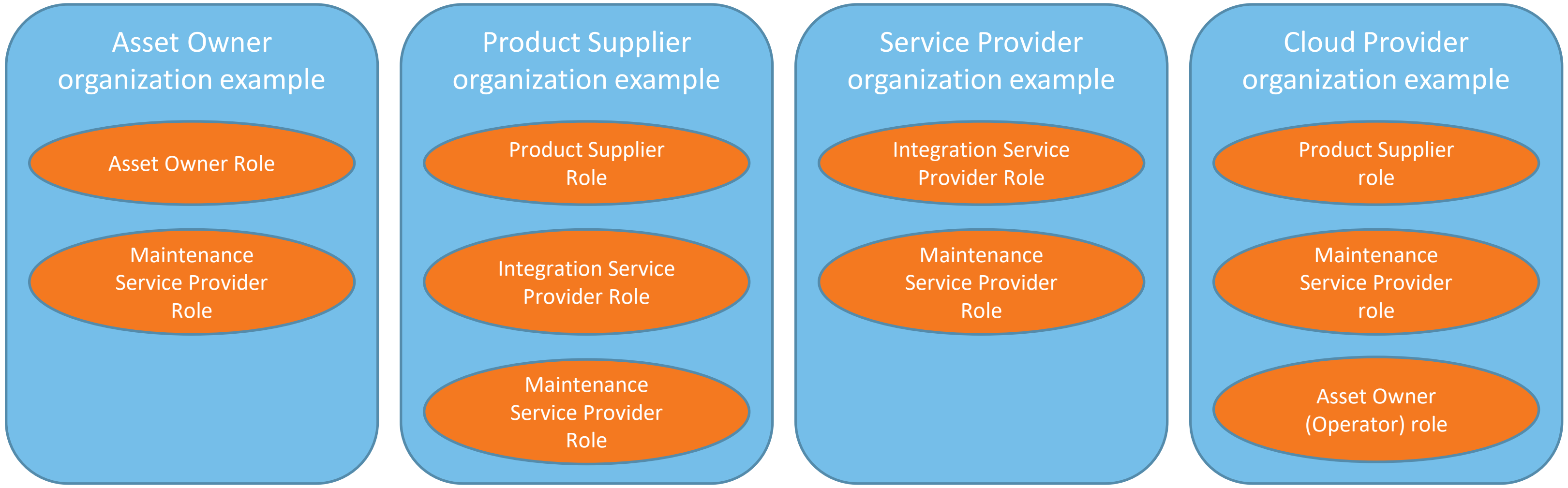
Examples of missing 62443 requirements

- multiple tenants on the same shared resources
- geolocation of data

Examples of missing CSA CCM requirements

- essential functions
- risk assessments include physical consequences

Cloud Provider Role

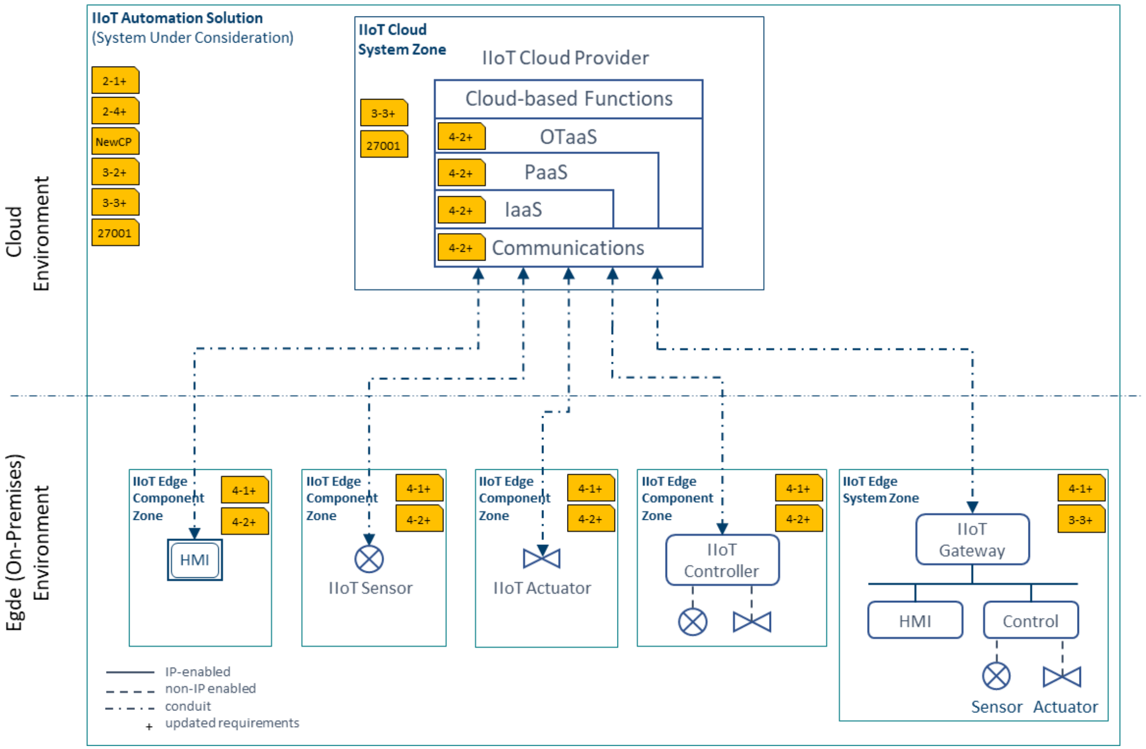

Asset Owner organization example
Asset Owner Role
Maintenance Service Provider Role
Product Supplier organization example
Product Supplier Role
Integration Service Provider Role
Maintenance Service Provider Role
Service Provider organization example
Integration Service Provider Role
Maintenance Service Provider Role
Cloud Provider organization example
Product Supplier role
Maintenance Service Provider role
Asset Owner (Operator) role

An organization that provides cloud-based functionality is a combination of the following ISA/IEC 62443 roles:

- Product Supplier – designs, develops and supports the cloud environment
- Maintenance Service Provider – implements updates/upgrades to the cloud environment
- Asset Owner – operates the cloud environment

Recommendation – ISA/IEC Standards Development Organization consider adding a Cloud Provider role to 62443 standards

Conformity assessment for IIoT Systems based on ISA/IEC 62443



Existing ISASecure certification programs

- Component Security Assurance (CSA)
- IIoT Component Security Assurance (ICSA)
- System Security Assurance (SSA)

Potential future ISASecure certification program developments

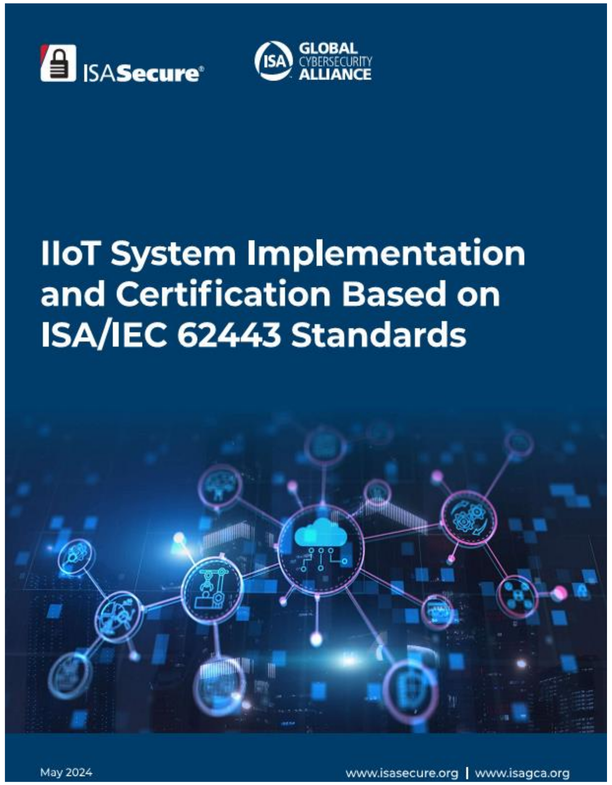
- IIoT Cloud Providers – Security program
- IIoT Edge Systems – Systems with Internet communication capabilities
- IIoT Cloud Components – IaaS, PaaS, SaaS
- IIoT Cloud Systems - OTaaS
- IIoT IACS – personnel, policy & process, technical

Assumes that 62443 standards have been updated to include IIoT specific requirements

Report Conclusions

- The concepts in ISA/IEC 62443 standards can be applied to IACS that use cloud-based functionality
- The scope of ISA/IEC 62443 should extend to the cloud environment when the cloud-based functionality has the capability to directly or indirectly change the physical state of the equipment under control
- Implementation of Essential Functions in the cloud does not meet ISA/IEC 62443 requirements
- This report proposes a new category of cloud service called operational technology as a service (OTaaS)
- The cloud provider is a new role not currently defined in the ISA/IEC 62443 series of standards
- There may be some requirements that should be added to ISA/IEC 62443 for the IIoT use case
- Conformity assessment schemes (e.g., certification) could be developed for IIoT systems, components and IACS

Report download



ISASecure®

ISA GLOBAL CYBERSECURITY ALLIANCE

IIoT System Implementation and Certification Based on ISA/IEC 62443 Standards

May 2024

www.isasecure.org | www.isagca.org

www.isasecure.org/iiot-paper