ISASecure®

GLOBAL CYBERSECURITY ALLIANCE

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

May 2024

www.isasecure.org | www.isagca.org

Executive Summary

This report explores the use of the ISA/IEC 62443 series of standards for industrial automation and control systems (IACS) that include cloud-based functionality *(i.e.*, industrial internet of things (IIoT)). The scope of an "IIoT IACS" includes all the systems and components necessary for a complete IACS including sensors, actuators and controllers at the edge, services in the cloud and the communications between edge and cloud.

This report is a companion to the "IIoT Component Certification Based on the 62443 Standard" study, which explores the use of ISA/IEC 62443-4-2, "Technical security requirements for IACS components" for IIoT components.

Section 4 is intended for the asset owner and covers risk assessment, role mapping, system under consideration, zone and conduit partitioning and 62443 scope. To explore these concepts, Annex A includes example risk assessments for four IIoT use cases:

- Example use case 1 – cloud-based data analytics – non-operational
- Example use case 2 – cloud-based data analytics – operational
- Example use case 3 – cloud-based operator view and manipulation
- Example use case 4 – cloud-based non-essential control

Section 5 explores potential improvement opportunities to facilitate the use of ISA/IEC 62443 for IIoT IACS. These recommendations are offered for consideration by ISA/IEC 62443 standards development organizations in the next editions of ISA/IEC 62443 standards, profiles and technical reports.

Section 6 explores the structure and organization of conformity assessment schemes (*e.g.*, third-party certification) for IIoT systems and IACS. It is intended for organizations that are conformity assessment scheme owners such as the ISA Security Compliance Institute (ISASecure).

The main conclusions of this report include:

- The concepts in ISA/IEC 62443 standards can be applied to IACS that use cloud-based functionality. Concepts such as risk assessment, zone and conduit partitioning, and the system/component model can all be applied to an IIoT IACS.
- 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)* to provide transparency when cloud-based functionality has the capability to directly or indirectly change the physical state of the equipment under control.
- The cloud provider is a new role not currently defined in the ISA/IEC 62443 series. The cloud provider role includes aspects of product supplier, service provider and asset owner (operator) roles.

- A comparison between ISA/IEC 62443 standards and the Cloud Security Alliance Cloud Controls Matrix v4 indicates that there may be some requirements that should be added to the ISA/IEC 62443 standards for the IIoT use case.
- Conformity assessment schemes (*e.g.*, certification) could be developed for IIoT systems, components and IACS based on ISA/IEC 62443 standards, provided these standards are updated for the IIoT use case.

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.

Contents

Table of Tables

Table of Figures

Foreword

This report was developed as a joint project of the ISA Global Cybersecurity Alliance (ISAGCA) and the ISA Security Compliance Institute (ISCI). The project team included members that have experience in asset owner, service provider, product supplier, or cloud provider roles. Further information about these organizations can be found on their web sites, respectively isagca.org and isasecure.org.

The author gratefully acknowledges the participation of members of these organizations in this effort.

1 Introduction

This document reports the results of the second phase of a project to determine the applicability of the ISA/IEC 62443 standards and corresponding certifications to IIoT use cases. IIoT component devices such as IIoT gateways, controllers and sensors were covered in the first study in the series entitled "IIoT Component Certification based on the 62443 Standard." This report covers *IIoT systems*, including cloud-based functionality and edge/on-premises functionality integrated as a "system."

Project sponsors are the ISA Security Compliance Institute (ISCI), which develops ISASecure® certification programs based on ISA/IEC 62443, and the ISA Global Cybersecurity Alliance (ISAGCA), which champions the adoption of those standards. These results describe the application of ISA/IEC 62443 to *IIoT systems*, potential improvements to the existing standards and conformity/certification program approaches.

This document explores the following questions related to IIoT systems that incorporate cloud-based functionality:

- Can ISA/IEC 62443 standards be applied to IIoT systems?
- What enhancements are necessary to ISA/IEC 62443 standards when applied to IIoT systems?
- Can ISASecure certification schemes be used to certify IIoT systems?
- Which ISA/IEC 62443 role (or roles) are applicable to the IIoT cloud provider?

There are three main sections in this report that investigate different aspects of the applicability of ISA/IEC 62443 standards to IIoT:

- Section 4 – Applying ISA/IEC 62443 standards to IIoT systems, which investigates the use of ISA/IEC 62443 concepts such as roles, security lifecycles, risk assessment, zone and conduit partitioning, essential functions, and security level
- Section 5 – Enhancing ISA/IEC 62443 standards for IIoT systems, which investigates potential enhancements that would facilitate the use of ISA/IEC 62443 for IIoT systems
- Section 6 – Certifying IIoT systems using ISA/IEC 62443 standards, which investigates the structure and organization of conformity assessment schemes (*e.g.*, third-party certification) for IIoT systems.

There are many different IIoT system architectures currently available, and they continue to evolve. To investigate the applicability of ISA/IEC 62443 standards to IIoT systems, a subset of representative use cases was selected, specifically:

- Use case 1: cloud-based data analytics – non-operational
    - Non-essential data analytics functions, not used for operations, implemented in a public cloud using software as a service (SaaS)
    - All essential and non-essential control, view and manipulate functions implemented at the edge/on-premises

    - Example: predictive maintenance application in the cloud using artificial intelligence/machine learning communicating with sensors at the edge

- Use case 2: cloud-based data analytics – operational
    - Non-essential data analytics functions, used for operations, implemented in a public cloud using SaaS
    - Non-essential view functions implemented at the edge/on-premises using data from cloud-based data analytics
    - All essential control, view and manipulate functions implemented at the edge/on-premises
    - Example: condition monitoring in the cloud receiving data from sensors at the edge
- Use case 3: cloud-based operator view and manipulation
    - Non-essential view and manipulate functions implemented in a public cloud using SaaS
    - All essential control, view and manipulate functions implemented at the edge/on-premises
    - Example: supervisory control and data acquisition (SCADA) system in the cloud communicating with sensors and controllers at the edge
- Use case 4: cloud-based non-essential control
    - Non-essential control functions implemented in a public cloud using SaaS
    - All essential control view and manipulate functions implemented at the edge/on-premises
    - Example: advanced control functions (non-essential) performed in the cloud

NOTE: while this report explores the use of cloud-based operational view and control, it does not encourage or dissuade this approach. The intent of this report is to investigate the use of ISA/IEC 62443 standards for cloud-based IIoT IACS and recommend approaches for IIoT IACS assessments/certifications and enhancements to ISA/IEC 62443 standards to facilitate their use for IIoT.

NOTE: This report contains a risk assessment for several example use cases. The intent of this risk assessment is to explore ISA/IEC 62443 concepts such as system under consideration, partitioning into zones and conduits and applicability of ISA/IEC 62443 to the cloud environment. The results of the risk assessment in this report cannot be used for an actual IIoT IACS.

NOTE: The analysis in this report is based on ISA-62443-2-1-FDIS (draft), dated September 2023. The final published version may have changes that may impact this analysis.

NOTE: This document is an interpretation of ISA/IEC 62443 standards to facilitate understanding and application of the standard. It is not a product of the ISA99 committee that develops the ISA/IEC 62443 standards and, as such, may not represent the views of the committee.

The ISA99 and IEC TC65 WG10 standards development committees are investigating IIoT. This ISAGCA/ISCI effort has closely followed that work and will donate the results of the present effort to these standards development organizations. These results are also offered as input for developers of ISA/IEC 62443-based conformity assessment programs.

2 Scope

This report considers the use of ISA/IEC 62443 standards for IIoT components, IIoT systems, IIoT Automation Solutions and IIoT industrial automation and control systems (IACS) that use cloud-based technology and communicate using untrusted networks. The report extends the component, system, Automation Solution and IACS terminology used in ISA/IEC 62443 as follows:

- An *IIoT component* is a host component, network component, application component or embedded component that can communicate over an untrusted network and/or is hosted in the cloud. IIoT components can be physical or virtual and include, but are not limited to: sensors, actuators, controllers, networks, servers, applications and cloud service categories such as IaaS, PaaS, and SaaS.
- IIoT components are integrated into an *IIoT system*. The IIoT system is provided by a cloud provider and includes IIoT components implemented in the cloud and may also include IIoT components implemented at the edge/on-premises.
- An *IIoT Automation Solution* includes the set of IIoT components and systems implemented for a particular asset owner organization or facility. The IIoT Automation Solution can also include traditional IACS components and systems connected to an IIoT gateway.
- An IIoT IACS includes the IIoT Automation Solution, and the personnel, policies and processes required to design, implement, operate and maintain the IIoT IACS.

Whereas the industry definition for IIoT does not inherently imply a direct connection to an untrusted network (*e.g.*, the Internet), the IIoT systems for which assessment/certification is examined in this study, are assumed to have such a direct connection. While the expression “Internet connection” may be used for brevity – it is understood to also include the case of a direct connection to other networks judged to be untrusted.

In this report, the term “cloud” is defined as a “collection of networked remote servers” and the cloud deployment model can be either public, private or hybrid. Where additional specificity is needed, the terms “public cloud” or “private cloud” will be used, as defined in Annex C. A hybrid cloud can have the characteristics of a public cloud and the characteristics of a private cloud and is not considered in this report. The term “cloud” refers to a system architecture, not to the technology used to implement that architecture (*e.g.*, virtualization, containers, orchestration).

The report assesses the applicability of ISA/IEC 62443 standards to IIoT components, IIoT systems and IIoT IACS, and approaches to their certification based on the ISASecure certification program. It also addresses the use of ISA/IEC 62443 standards for cloud providers, specifically offering software as a service (SaaS) in a public cloud deployment model over an untrusted public network. Other solutions such as infrastructure as a service (IaaS), platform as a service (PaaS) and private/hybrid cloud environments are not fully considered in this report.

3 References

3.1 ISA/IEC 62443 Standards

For ease of reference in this report, we refer to the series of standards as "ISA/IEC 62443." Both the ISA and IEC versions of the ISA/IEC 62443 standards referenced in this report are listed. The normative content in the ISA and IEC versions of the document are the same.

ISA-62443-1-1-2007 Security for industrial automation and control systems, Part 1-1: Terminology, Concepts, and Models

IEC TS 62443-1-1:2009, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts, and models

IEC TS 62443-1-5:2023, Security for industrial automation and control systems – Part 1-5: Scheme for IEC 62443 security profiles

ISA-62443-2-1-FDIS (9/18/23), Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners

IEC 62443-2-4:2023, Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

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

IEC 62443-3-2:2020, Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

ANSI/ISA-62443-3-3-2013, Security for industrial automation and control systems, Part 3-3: System security requirements and security levels

IEC 62443-3-3:2013, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems, - Part 4-1: Secure product development lifecycle requirements

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

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

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

3.2 ISASecure Certification Specifications

SDLA-100 – ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme v2.1, as specified at www.isasecure.org

SDLA-300 – ISCI Security Development Lifecycle Assurance – Requirements for ISASecure Certification and Maintenance of Certification v1.9, as specified at www.isasecure.org

SDLA-312 – ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment v6.3, as specified at http://www.ISASecure.org

SSA-100 – ISCI System Security Assurance – ISASecure certification scheme v3.1, as specified at www.isasecure.org

SSA-300 – ISCI System Security Assurance – ISASecure SSA certification requirements v3.1, as specified at www.isasecure.org

4 Applying ISA/IEC 62443 Standards to IIoT Systems

This section investigates the application of ISA/IEC 62443 concepts such as risk assessment, essential functions, zone and conduit partitioning, security levels and role-based security requirements to several example IIoT use cases to determine if ISA/IEC 62443 standards can be used to enhance the security of IIoT systems. The primary audience for this section is asset owners who are planning to implement an IIoT-based IACS.

There are several questions that are addressed in this section of the report:

5.1 Can essential functions be implemented in the cloud portion of an IIoT IACS?

5.2 Can the security zone and conduit model be used for IIoT IACS?

5.3 When does the ISA/IEC 62443 series apply to the cloud portion of an IIoT IACS?

5.4 Are there any additional risk assessment considerations for IIoT IACS?

5.5 Can the roles of an IIoT IACS be mapped to ISA/IEC 62443 roles?

An ISA/IEC 62443 risk assessment was performed on several representative example use cases to determine the answers to these questions. The team performing the example risk assessment included members from asset owner, product supplier and service provider organizations.

Not all permutations of cloud-based computing were considered. The use cases selected were IIoT IACS where the cloud-based functionality uses software as a service (SaaS) on a public cloud with communications travelling over a public untrusted network (*e.g.*, Internet). The following use cases were considered:

- Example use case 1 – cloud-based data analytics – non-operational
- Example use case 2 – cloud-based data analytics – operational
- Example use case 3 – cloud-based operator view and manipulation
- Example use case 4 – cloud-based non-essential control

The details of the example use cases and the risk assessment can be found in Annex A.

4.1 Essential Functions

The definition of “cloud” is a “collection of remote networked servers,” which indicates that functions implemented in the cloud would be in a different security zone than the devices (*e.g.*, controllers, sensors and final elements) that interface with the physical domain. This section investigates if the implementation of essential functions in a cloud zone that communicates with an edge zone that interfaces to the physical domain would meet the requirements of ISA/IEC 62443.

The concept of an essential function is introduced in the ISA/IEC 62443 series of standards in “Part 3-3, System security requirements and security levels.” It is a very important concept to consider when designing the IIoT IACS.

Essential function

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

Note to entry: 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

The following requirements from ISA/IEC 62443-3-3, clause 5.2 take precedence over the individual system requirements (SRs) in the remainder of the document:

1. *Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment*
2. *Access controls shall not prevent the operation of essential functions, specifically:*
    a. *Accounts used for essential functions shall not be locked out, even temporarily*
    b. *Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time*
    c. *Identification and authentication shall not prevent initiation of the safety instrumented function (SIF). Similarly for authorization enforcement.*
    d. *Incorrectly timestamped audit records shall not adversely affect essential functions*
3. *Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode*
4. *A Denial of Service (DoS) event on the control system or safety instrumented system network shall not prevent the SIF from acting*

There are several implications for the designer of the IIoT IACS, regarding the implementation of essential functions (safety, essential control, essential view/manipulation) in a cloud zone:

- If the zone boundary goes into fail close or island mode, remote communications between the cloud zone and the edge zone would be interrupted which would result in the loss of essential functions (see requirement #3 above).
- A denial-of-service event on the network between cloud zone and edge zone would impact remote communications. If portions of the safety instrumented function are remote (*e.g.*, in the cloud), this would result in a loss of protection or spurious trip (see requirement #4 above).

Conclusion: the implementation of essential functions in the cloud environment of an IIoT IACS does not meet the requirements of ISA/IEC 62443 standards.

4.2 Security Zones and Conduits Partitioning

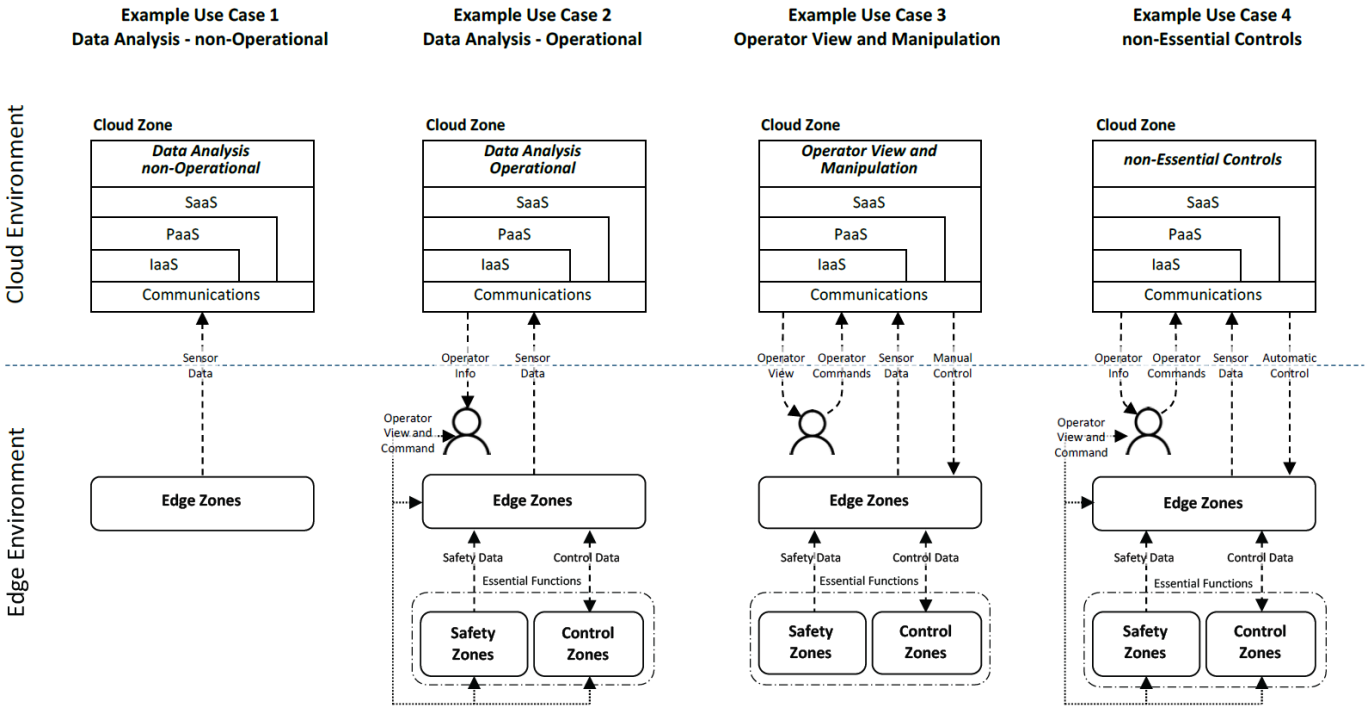


Figure 1 – Example Use Cases – Zone and Conduit Partitioning

Figure 1 (which is a duplicate of Annex A – Figure A.4) shows the partitioning of the IIoT system into security zones and conduits. The following assumptions were used to partition the IIoT systems in these example use cases:

- Safety functions are partitioned into one or more safety zones. All safety functions are considered to be essential functions. The safety zones are segregated from other zones using unidirectional secure conduits. Safety zones may not establish conduits directly with cloud zones.
- Essential control functions are partitioned into one or more control zones. Control zones are segmented from other zones using bidirectional secure conduits. Control zones may not establish conduits directly with cloud zones.
- Non-essential control functions may be partitioned into control zones, edge zones or cloud zones.
- Data acquisition functions may be partitioned into safety zones, control zones or edge zones.
- For example use cases 2 and 4, the operator can view operational data from a local interface in safety zones, control zones or edge zones.
- For example use cases 2, 3 and 4, the operator can view operational data from the cloud using a web-based interface.
- Cloud-based functionality such as data analytics, remote view and manipulation and non-essential controls are partitioned into cloud zones. In these example use cases, the cloud zone uses SaaS to host the cloud-based functionality in a public cloud.

4.3 ISA/IEC 62443 Scope

The ISA/IEC 62443 series of standards is defined as an IACS whose compromise can result in one or more of the following consequences [reference: ISA-62443-1-1:2007, clause 4.4]:

a) unauthorized access, theft or misuse of confidential information

b) publication of information to unauthorized destinations

c) loss of integrity or reliability of process data and production information

d) loss of system availability

e) process upsets leading to compromised process functionality, inferior product quality, lost production capacity, compromised process safety or environmental releases

f) equipment damage

g) personal injury

h) violation of legal and regulatory requirements

i) risk to public health and confidence

j) threat to a nation's security

While many of these consequences are possible for both IT and IACS systems, consequences e), f), g) and i) are typically specific to cyber-physical systems that can make changes in the physical domain. The risk assessment process in ISA/IEC 62443-3-2 is used as a method to determine whether ISA/IEC 62443 requirements are in scope for the IIoT cloud-based functionality.

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	Med-High	Medium	n/a	n/a	Med-High	Med-High	Med-High	n/a	Med-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	Med-High	Medium	Medium	Med-High	Med-High	Medium	Medium	Med-High	Med-High	Medium	Medium	Med-High	Med-High

Table 1 – Example Use Cases – Initial Risk

Table 1 (which is a duplicate of Annex A – Table A.8) shows the initial risk for each example use case. Based on the initial risk the rationale for determining the scope of ISA/IEC 62443 requirements for each example use case is as follows:

- Example use case 1 – cloud-based data analytics – non-operational
  In this case the cloud zone is not able to change the physical state of the equipment under control, so ISA/IEC 62443 does not apply to the cloud zone.

- Example use case 2 – cloud-based data analytics – operational
  In this case the cloud zone cannot directly change the state of the equipment under control, but data from the cloud zone could influence the operator to change the physical state (for example by spoofing the data). Whether ISA/IEC 62443 is in the scope of the cloud zone depends on the outcome of a risk analysis that includes operational technology (OT) considerations. For this example use case, the risk assessment indicated that the cloud zone only had risks associated with loss of confidential information, so it was decided that ISA/IEC 62443 does not apply to the cloud zone. Other similar use case risk assessments may conclude that the cloud environment is in the scope of ISA/IEC 62443.

- Example use case 3 – cloud-based operator view and manipulation
  In this case the operator can view and manually manipulate the physical state of the equipment under control from the cloud zone, so ISA/IEC 62443 is in the scope of the cloud zone.

- Example use case 4 – cloud-based non-essential control
  In this case an application in the cloud zone can automatically send a setpoint to a controller in the edge zone, which in turn can send a setpoint to a controller in the control zone, which can change the physical state of the equipment under control. Since the cloud zone can directly change the state of the equipment under control, ISA/IEC 62443 is in the scope of the cloud zone.

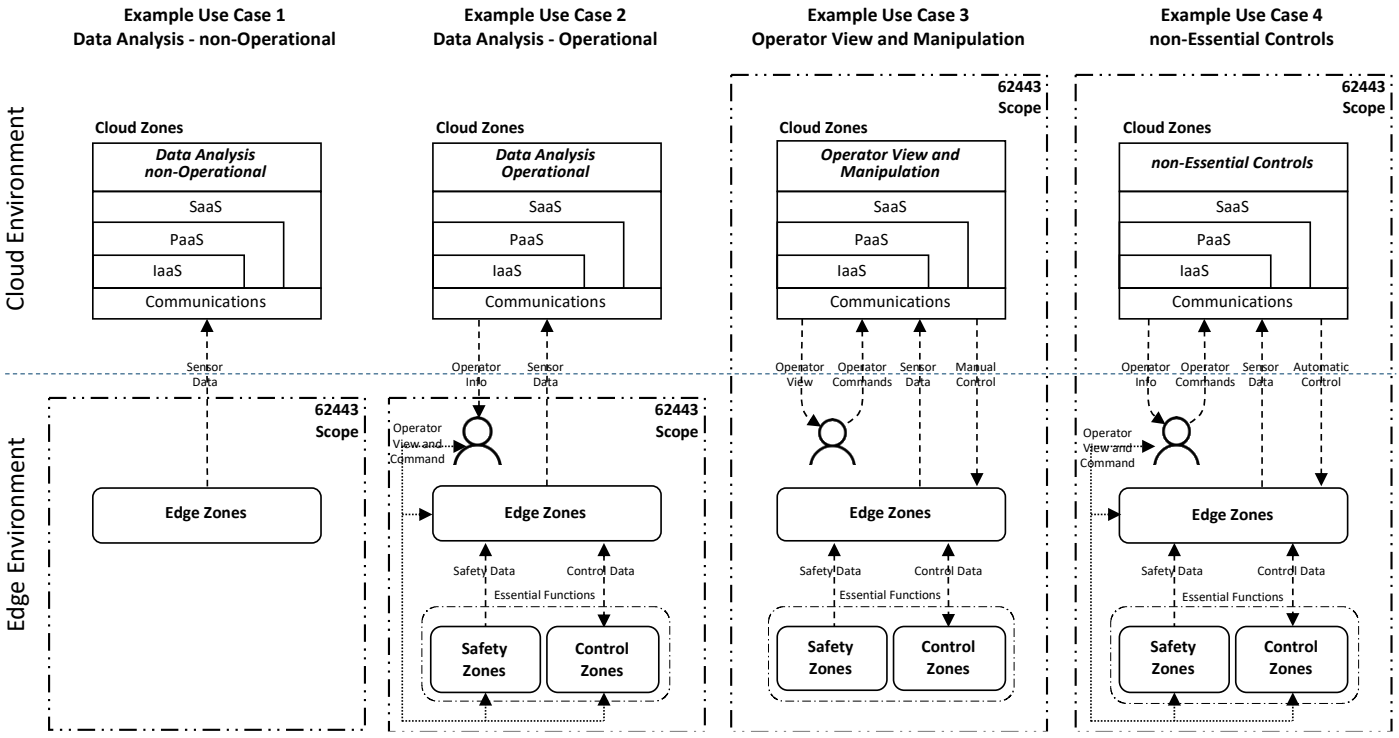


Figure 2 – Example Use Cases – ISA/IEC 62443 Scope

Figure 2 (which is a duplicate of Annex A – Figure A.6) shows the resulting scope of ISA/IEC 62443 requirements for each of the example use cases. For these example use cases, whether ISA/IEC 62443 is included in the scope of the cloud zone can be summarized as follows:

> *"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"*

4.4 Additional Risk Assessment Considerations

The intent of this section is to provide the asset owner with additional considerations to include as part of the risk assessment of an IIoT IACS.

- The asset owner may have limited knowledge of the threats and vulnerabilities in the cloud environment unless the cloud provider is included in the risk assessment process.
- The asset owner must typically accept the security measures implemented by the cloud provider unless otherwise contractually agreed.
- The asset owner may have limited ability to add compensating security measures in a shared public cloud environment.
- Management of change procedures may be difficult to implement between asset owner and cloud provider (*e.g.*, patch management) for changes in a public cloud environment.
- Business continuity and disaster recovery processes may be more difficult to implement when some responsibilities are delegated to a cloud provider.

- Incident detection, response and recovery procedures may be more difficult to implement when some responsibilities are delegated to a cloud provider.
- The asset owner may need to manage multiple cloud providers to implement an IIoT IACS.
- Extended supply chain (*e.g.*, SaaS, PaaS, IaaS from different cloud providers) may complicate change management and risk assessment for a public cloud environment.
- Essential functions should not be implemented in the cloud environment (see section 4.1).
- Essential functions zones should not be directly connected to a public, untrusted network (*e.g.*, Internet).
- Safety functions should be segregated from other functions in the edge environment (see ISA/IEC 62443-3-2, zone, conduit and risk assessment requirements **(**see ISA/IEC 62443-3-2, ZCR 3.3). Other essential functions should also be segregated from other functions in the edge environment.
- In the cloud environment, business functions (*e.g.*, email) should be segregated from IACS functions (see ISA/IEC 62443-3-2, ZCR 3.2).
- Implement secure conduits between cloud and edge zones based on the risk in each zone.
- Implement secure conduits between essential function and edge zones based on the risk in each zone
- Cloud-based authentication services (*e.g.*, federated identification and authentication) may introduce new vulnerabilities.
- The contractual agreement between asset owner and cloud provider that includes description of roles and responsibilities is a key risk mitigation.

4.5 Role-based Considerations

The ISA/IEC 62443 series of standards is organized according to security requirement type (process or technical) and role (asset owner, service provider, product supplier).

A key part of understanding how to apply the ISA/IEC 62443 series to IIoT systems is a mapping between the IIoT roles and ISA/IEC 62443 roles because this will determine which ISA/IEC 62443 standards are applicable for IIoT use cases.

The asset owner role is ultimately *accountable* for the security of the IACS and the associated equipment under control (EuC). But the *responsibility* for the security of the IACS is shared between asset owner, service provider and product supplier. This shared responsibility model becomes more complex when IACS functionality is being provided by a third-party cloud provider.

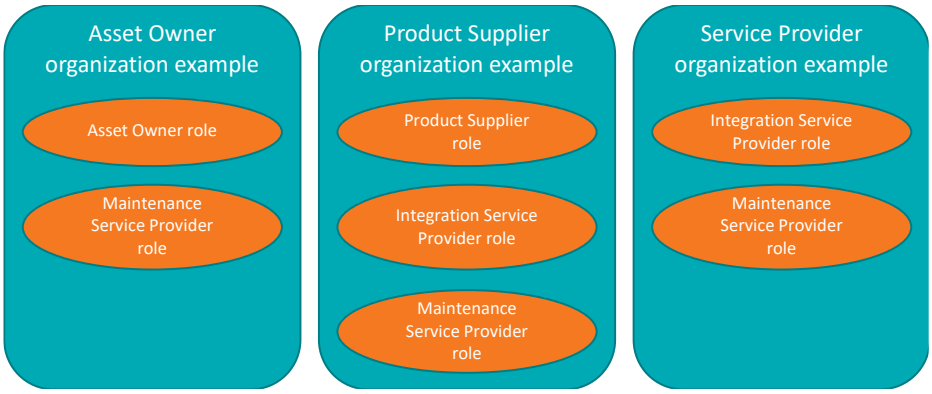


Figure 3 – Understanding Organization vs. Role

It is important to note that role and organization are different concepts. A role is a set of tasks and responsibilities that are assigned to and executed by a person or organization. An organization can have multiple roles; for example, a product supplier organization can provide both products and services. A role can also be split between people or organizations; for example, the maintenance service provider role is often split between an asset owner organization and a service provider organization. The ISA/IEC 62443 series defines roles but does not define the people or organizations that execute them. Figure 3 shows a few examples of the differences between organizations and the roles that they can assume.

4.5.1 Asset Owner

The process security requirements for the asset owner are described in ISA/IEC 62443-2-1, Security program requirements for asset owners. The asset owner is accountable and responsible for the security of the IACS and the associated equipment under control (EuC). The asset owner can delegate responsibilities to the service provider, including the responsibility to select product suppliers and technologies, based on the requirements documented in Part 2-4 of the series of standards.

The asset owner is also the operator of the IACS and the EuC. Although operations could also be delegated by the asset owner to a third party, this is not addressed by ISA/IEC 62443, since there is no role defined for operations service provider.

4.5.2 Service Provider

The process security requirements for the service provider are described in ISA/IEC 62443-2-4, *Security program requirements for service providers*. The service provider is accountable and responsible for the services it provides that have been delegated by the asset owner. The responsibilities defined in ISA/IEC 62443-2-4 are typically assigned to and executed by individuals in the service provider organization.

> *Service Provider*
>
> *individual or organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner [ISA/IEC 62443-2-4 Terms and definitions]*

This part of ISA/IEC 62443 specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution [ISA/IEC 62443-2-4 Scope]

There are two types of service provider roles currently defined in ISA/IEC 62443-2-4:

- Integration service provider, which is responsible for the design, implementation and testing of the Automation Solution (also known as the system integrator)
- Maintenance service provider, which is responsible for the maintenance and support of the Automation Solution during its operation and maintenance phases

4.5.3 Product Supplier

The process security requirements for the product supplier are described in ISA/IEC 62443-4-1, Secure product development lifecycle requirements. The technical security requirements for the products created by the product supplier are described in ISA/IEC 62443-3-3, System security requirements and security levels, and ISA/IEC 62443-4-2, Technical security requirements for IACS components. The product supplier is accountable and responsible for the security of the products they supply along with the support required to maintain the product's security.

Product Supplier

manufacturer of hardware and/or software product [ISA/IEC 62443-3-3 Terms and definitions]

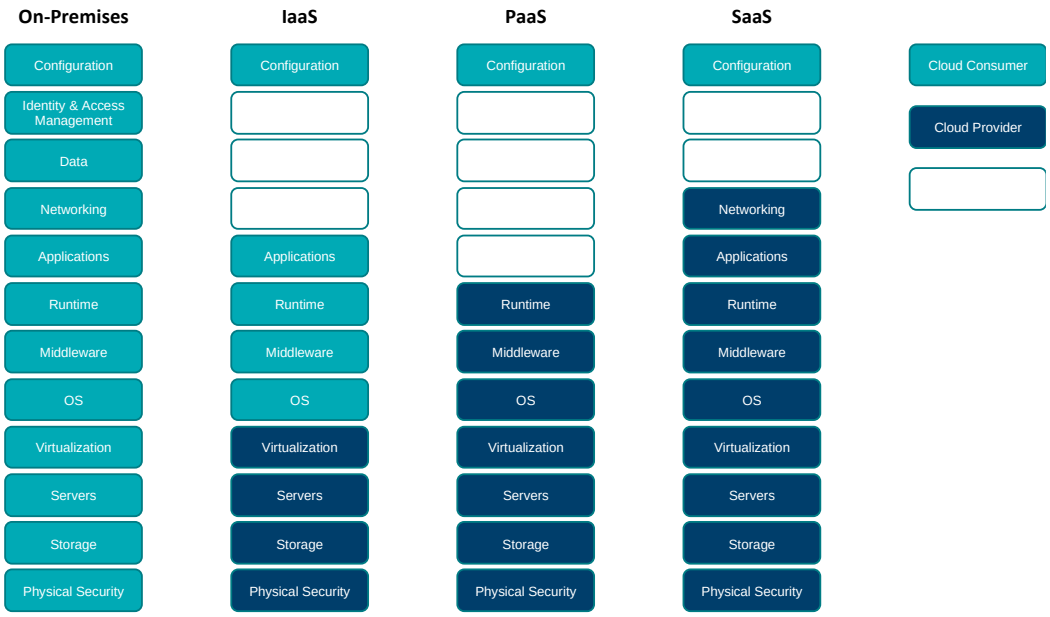
This part of ISA/IEC 62443 specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development lifecycle (SDL) for the purpose of developing and maintaining secure products. … These requirements apply to the developer and maintainer of the product, but not to the integrator or user of the product. [ISA/IEC 62443-4-1 Scope]

The product supplier primarily supplies technology and information, as defined in ISA/IEC 62443-4-1, ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2.

4.5.4 Cloud Provider

The cloud provider role is not currently defined in the ISA/IEC 62443 series. When the asset owner contractually delegates certain responsibilities to a cloud provider, key questions that influence the selection of ISA/IEC 62443 requirements are:

- *How are responsibilities between the organization with the asset owner role and the organization with the cloud provider role shared?*
- *Can the cloud provider role be mapped to one or more ISA/IEC 62443 organizational roles?*



Source: CISA Cloud Security Technical Reference Architecture, Version 1.0, August 2021

Figure 4 – Shared Cloud Security Responsibilities Model

Figure 4 shows an example of the shared cloud security responsibilities between cloud consumer (asset owner) and cloud provider. The source of this shared responsibilities model is a the CISA Cloud Security Technical Reference Architecture [13] where the cloud consumer is a government agency, but the concept is similar for any asset owner/cloud provider relationship.

The figure shows that as the level of cloud functionality increases (IaaS, PaaS, SaaS) the responsibilities that are delegated from the asset owner to the cloud provider significantly increases. This requires an increased level of trust between asset owner and cloud provider and may have a significant impact on overall risk (see Annex A). One method to mitigate this risk is to establish more detailed and comprehensive contractual service agreements between asset owner and cloud provider.

Is the Cloud Provider a Service Provider or Product Supplier?

This report attempts to address the key question of whether the cloud provider maps to the ISA/IEC 62443 service provider role, the product supplier role, both roles or an entirely different role. The answer to this question is important to select the standards that would form the basis for a certification scheme, and to provide guidance on how to enhance the ISA/IEC 62443 series for IIoT systems.

In the traditional IACS, the product supplier is responsible for developing and maintaining system and component products, the integration service provider is responsible for integrating these products into an IACS, the maintenance service provider is responsible for maintaining and updating the IACS, and the asset owner is responsible for operating the IACS.

For the cloud environment, the cloud provider is responsible for developing, integrating, maintaining and operating the cloud-based functionality of an IIoT IACS. So, the cloud provider role includes requirements from the product supplier, service provider and asset owner (operator) roles for the cloud environment. But not all the

requirements from these roles apply to the cloud provider. For example, section 4.1 of this report concludes that essential functions implemented in the cloud environment would not meet ISA/IEC 62443 requirements, so requirements associated with essential functions would not apply to the cloud provider.

Another key consideration is the risk assessment process that is used to assess the security of an IIoT IACS. In the ISA/IEC 62443 series, the asset owner and integration service provider use the methodology described in ISA/IEC 62443-3-2, Security risk assessment for system design, to assess and mitigate the cybersecurity risk of the IIoT system. The product supplier uses threat modeling and security context as the security assessment methodology for product development, as described in ISA/IEC 62443-4-1, Secure product development lifecycle requirements.

Cloud providers that use a development, security and operations (DevSecOps) approach use threat modeling during the development of their cloud-based functions, and risk assessment for the security assessment and operation of their cloud-based functions. A cloud provider using a DevSecOps approach acts as product supplier, service provider and asset owner (operator) ISA/IEC 62443 organizational roles.

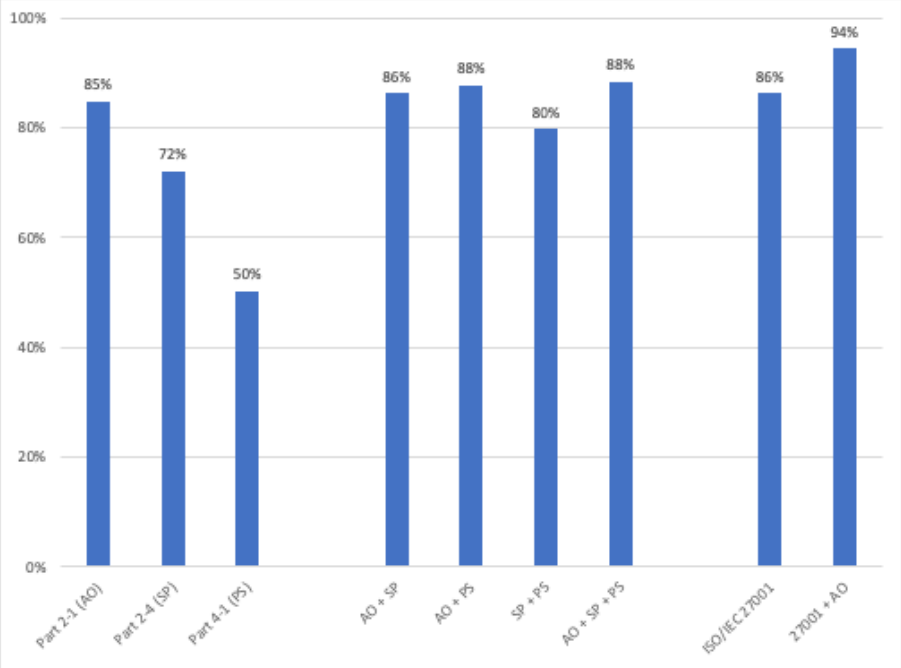


Figure 5 – ISA/IEC 62443 Cross Reference to CSA CCM v4

Figure 5 takes another approach to answering the question of which ISA/IEC 62443 roles a cloud provider organization has by comparing several ISA/IEC 62443 standards against the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) [12]. Although the CSA CCM does not include requirements specific to IACS, it is useful when used as a benchmark for the cloud provider role. This cross reference shows that:

- Part 2-1 (asset owner) covers 85% of CSA CCM requirements
- Part 2-4 (service provider) covers 72% of CSA CCM requirements
- Part 4-1 (product supplier) covers 50% of CSA CCM requirements

Combining several ISA/IEC standards together shows that:

- Part 2-1 (asset owner) and Part 2-4 (service provider) covers 86% of CSA CCM requirements
- Part 2-1 (asset owner) and Part 4-1 (product supplier) covers 88% of CSA CCM requirements
- Part 2-4 (service provider) and Part 4-1 (product supplier) covers 80% of CSA CCM requirements
- Part 2-1 (asset owner), Part 2-4 (service provider) and Part 4-1 (product supplier) covers 88% of CSA CCM requirements

When developing a cross reference between standards, it is often difficult to find an exact match between requirements, so coverage in this analysis is defined as full or partial coverage of requirements.

Finally, the cross-reference provided with the CSA CCM requirements shows that the ISO/IEC 27001 standard covers 86% of requirements, although many of the CSA CCM requirements are only partially covered. However, neither CSA CCM nor ISO/IEC 27001 cover the unique requirements for cyber-physical systems that are covered by ISA/IEC 62443. Examples of these unique requirements are the systematic inclusion of health/safety/environment consequences in the risk assessment process, partitioning of the system into zones and conduits and the requirements associated with essential functions. Combining ISO/IEC 27001 requirements and ISA/IEC 62443-2-1 requirements covers 94% of the CSA CCM requirements.

Annex B includes a listing of the cross references between CSA CCM v4 and the key standards in the ISA/IEC 62443 Series.

The cross-reference analysis above leads to the following conclusions:

- ISA/IEC 62443-4-1 (product supplier) alone may not sufficiently cover the requirements for a cloud provider (50% of CSA CCM requirements)
- ISA/IEC 62443-2-4 (service provider) alone may not sufficiently cover the requirements for a cloud provider (72% of CSA CCM requirements).

Therefore, the cloud provider role may not map directly to either the service provider role (part 2-4) or the product supplier role (Part 4-1) as currently described in the ISA/IEC 62443 series.

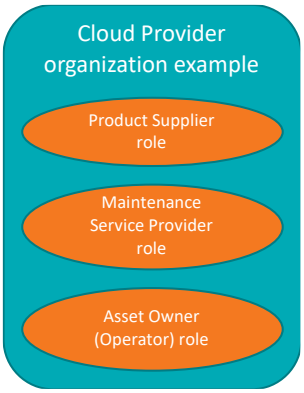


Figure 6 – Cloud Provider Role Mapping

Figure 6 shows the ISA/IEC 62443 roles that a cloud provider organization has for the cloud portion of an IIoT IACS, based on the existing ISA/IEC 62443 role model:

- The cloud provider organization has the product supplier role because they design and develop products that are offered as services (IaaS, PaaS, SaaS)
- The cloud provider organization has the maintenance service provider role because they update and maintain the products that they have developed, for example by using a process such as continuous integration/continuous deployment (CI/CD)
- The cloud provider organization has the asset owner role because they operate the cloud portion of the IIoT IACS. In ISA/IEC 62443, the asset operator role is part of the asset owner role.

5 Enhancing ISA/IEC 62443 Standards for IIoT Systems

This section investigates potential improvements to the ISA/IEC 62443 series of standards to better address the risks and requirements for IACS that include cloud-based functionality (called IIoT IACS in this report).

Since the security requirements in the ISA/IEC 62443 series of standards are performance based, they apply to all technologies that are used for IACS. However, when new technologies come along, the security requirements may need to be updated to ensure that potential new vulnerabilities are addressed. The recommendations in this section are intended for consideration by standards development organizations to improve the use of ISA/IEC 62443 standards for IIoT use cases.

5.1 Cloud Provider Role

As discussed in section 4.5.4 of this report, the cloud provider role does not map directly to either the service provider role (Part 2-4) or the product supplier role (Part 4-1) as currently described in the ISA/IEC 62443 series. The cloud provider role also includes elements of the asset owner role because the cloud provider operates the cloud portion of the IIoT IACS. There are two alternatives for ISA/IEC 62443 standards development organizations to consider:

1. Create a new ISA/IEC 62443 standard that includes the policy and process requirements for the cloud provider role.
2. Update ISA/IEC 62443 Parts 2-1, 2-4 and 4-1 to include additional requirements for the IIoT use case, and create a profile using ISA/IEC 62443-1-5 for the cloud provider role

Note that the majority of the study team favored alternative number two, while some favored alternative number one.

> *Recommendation: Define the requirements for the cloud provider role by creating a new ISA/IEC 62443 standard or updating Parts 2-1, 2-4 and 4-1 and creating a new profile using Part 1-5.*

In the remainder of the report this new standard or profile is designated as “NewCP.”

5.2 Operational Technology as a Service (OTaaS)

As discussed in section 4.3 of this report, the scope of the ISA/IEC 62443 series extends into the cloud when cloud-based functionality can directly or indirectly control or manipulate systems or components that have the capability to change the physical state of equipment under control. Having a commonly used term to describe this as a category of cloud service would make it transparent when a cloud-based service has the capability to directly or indirectly modify physical entities or environments. This transparency is very important when designing and assessing the risk of a cloud-based solution with this capability. For this reason, it is recommended that a new category of cloud service is defined called “operational technology as a service (OTaaS)”

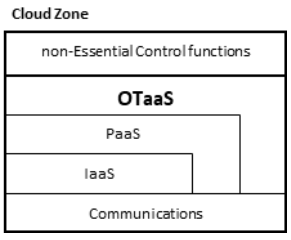


Figure 7 - Operational Technology as a Service (OTaaS)

> *Recommendation: Define a new category of cloud service called operational technology as a service (OTaaS) that includes functionality that provides the capability to control or manipulate*

systems or components that can directly or indirectly change the physical state of the equipment under control from the cloud environment.

5.3 Management of Change

Change management processes for the traditional IACS are typically more rigorous than IT systems because the consequences of a system or component failure may have significant health, safety or environmental impact. ISA/IEC 62443-2-1 (FDIS), CM 1.4 requires that "the asset owner shall have policies and procedures to authorize, validate and approve changes to the current configuration baseline and infrastructure drawings/documentation, including revision and patch levels."

Key aspects of the typical management of change (MoC) process for an asset owner include:

- Assessing the risks of the change
- Mitigating the risks of the change (*e.g.*, verification, validation, testing)
- Planning and scheduling the implementation of the change (especially with operations)
- Approving the implementation of the change

It may be challenging to meet these requirements when change management is delegated to a cloud provider that is using CI/CD processes to update cloud-based OTaaS functionality. Even more challenging is the management of a change that is made somewhere in the supply chain of the main cloud provider. For example, a change made by the IaaS cloud provider in the following supply chain: IaaS → PaaS → OTaaS → asset owner.

Recommendation: Update the relevant parts of ISA/IEC 62443 to include any new or changed requirements for cloud providers management of change processes used for OTaaS functionality (e.g., CI/CD).

5.4 Risk Assessment and Zone and Conduit Partitioning

Section 4 of this report shows that the risk assessment and zone/conduit partitioning concepts that are described in ISA/IEC 62443-3-2 can be applied to an IACS that includes cloud-based functionality. However, the following are some potential changes that should be considered to improve ISA/IEC 62443-3-2 for use with cloud-based IACS:

- Clarify when the system under consideration (the scope of the IACS risk assessment) includes the cloud-based functionality, and when it does not.
- Clarify that the partitioning requirement ZCR 3.2, Separate business and IACS assets, also applies to cloud-based IACS functionality.
- Clarify that the partitioning recommendation ZCR 3.6, Separate devices connected via external networks, applies to cloud-based IACS functionality.
- Add requirements to partition multiple tenants that are using the same cloud-based resources.
- Add requirements to partition independent cloud-based IACS for the same tenant.

- Add requirements to consider the geographic location of cloud-based resources used for IACS where needed.

  Recommendation: Update the risk assessment and zone/conduit partitioning requirements in Part 3-2 to address the risks associated with the use of cloud-based functionality for IACS.

5.5 System/Component Modeling

An IACS that uses cloud-based functionality for part of its Automation Solution can use one or more of the following categories of cloud services: IaaS, PaaS and SaaS. This paper also introduces the concept of OTaaS. The implementation of the cloud-based functionality can also use public cloud, private cloud, or a hybrid cloud. All of these permutations should be incorporated into the ISA/IEC 62443 system/component model that is used in ISA/IEC 62443-3-3 (for systems) and ISA/IEC 62443-4-2 (for components).

Using the current system/component model a potential mapping could be: (Note: this mapping is used as the basis for the certification discussion in section 6)

- IaaS (processing and storage) – host component (ISA/IEC 62443-4-2)
- IaaS (networking) – network component (ISA/IEC 62443-4-2)
- PaaS (processing, storage, network, OS, database) – host component (ISA/IEC 62443-4-2)
- SaaS – application component (ISA/IEC 62443-4-2)
- OTaaS – application component with control, and/or view/manipulate functions (ISA/IEC 62443-4-2)
- IIoT system – system (ISA/IEC 62443-3-3)

  Recommendation: Include a way to model SaaS, PaaS, IaaS, OTaaS and an IIoT system in the ISA/IEC 62443 system/component model.

5.6 IIoT-related Technologies

Virtualization

The National Institute of Standards and Technology (NIST) defines virtualization as “the simulation of the software and/or hardware upon which other software runs.” There are several types of virtualization that are defined by NIST:

- *Hardware virtualization* is used to run many instances of operating systems (OS) on a single physical server. Multiple applications may run in each virtualized OS.
- *Operating system virtualization* is used to run many instances of virtualized OS on a single actual OS kernel (OS container). Multiple applications may run in each virtualized OS.
- *Application virtualization* is used to run many instances of applications on a shared OS kernel. The applications are isolated from one another in *containers* and may be managed by an *orchestrator*.

- *Network virtualization* is used to run many instances of networks on a single physical network. Virtual local area networks (VLANs) and software defined networks (SDN) are two types of network virtualization.

Most requirements in ISA/IEC 62443 are written as performance (outcome-based) requirements and would apply to both physical and virtual implementations of an IACS or its systems and components. However, some requirements use language such as "network" or "device," which may imply a physical implementation.

> *Recommendation: Update ISA/IEC 62443 definitions and requirements in such a way that they can be implemented either physically or virtually unless specifically required to be physical.*

Virtualization technologies use physical or virtual resources that are shared by several instances. There is typically a layer that manages the allocation of resources such as a hypervisor that manages OS instances, a controller that manages the control plane of SDN, or an orchestrator that manages application containers. These shared resource management layers are susceptible to exploitable vulnerabilities and human error.

Virtualization technology can pose a challenge when designing the zone and conduit model. While each virtual instance (*e.g.*, virtual machine, container) can be partitioned into a separate zone, the shared resource management layer is a potential common cause failure point for all virtual instances. Similarly, each SDN can be partitioned into a separate conduit, but the SDN controller is a potential common cause failure point. Thus, the expected security benefit by partitioning virtual instances into separate zones may not be achieved due to the common cause failure point of the shared resource management layer.

> *Recommendation: Update the risk assessment and zone/conduit partitioning requirements in ISA/IEC 62443 Part 3-2, and the technical requirements in Parts 3-3 and 4-2 to address the use of virtualization technologies and shared resource management layers.*

Federated Identities

In the traditional IACS, many asset owners have discovered that the separation of IT and IACS authentication domains (*e.g.*, Windows Active Directory) provides significant risk reduction. This separation makes it more difficult for an attacker to pivot from the IT environment to the IACS environment. It also allows the IACS environment to be isolated from the IT environment in the event of an attack.

ISA/IEC 62443 requirements that support the separation of IT and IACS authentication domains are:

- ISA/IEC 62443-2-1-FDIS NET 1.1 requires that "the asset owner shall have policies and procedures segmenting IACS from non-IACS zones and limiting any interconnections to the minimum necessary for IACS operations and within tolerable risk."
- ISA/IEC 62443-3-2 ZCR 3.2 requires that "IACS assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets" which would also include authentication domains.

In IIoT Systems, it is possible to use federated identity technologies to enable single sign-on capabilities between cloud and edge systems. These technologies establish trust relationships between zones to allow the exchange of identity and authentication information. The above requirements would *not* preclude the use of federated identity

technology for IACS with cloud-based functionality because the cloud and edges zones (as shown in the example use cases) are all within the same IACS environment.

> *Recommendation: Develop ISA/IEC 62443 requirements for the usage (or restriction) of federated identity management across zone boundaries (e.g., cloud zone, edge zones).*

6 Conformity Assessment of IIoT Systems Using ISA/IEC 62443 Standards

6.1 Introduction

This section describes a model for the development of a conformity assessment scheme for IIoT IACS. A conformity assessment that is performed by a third party that is accredited based on the ISO/IEC 17000 series of standards is called a certification. This section uses the ISASecure certification model, where multiple standards can be referenced in a single certification scheme.

The primary audience for this section is organizations that are conformity assessment scheme owners. This model assumes that the enhancements identified in section 5 of this report to facilitate the application of ISA/IEC 62443 standards to IIoT systems have been made in the standards or otherwise addressed (identified with a + in this report). This document recommends that a new cloud provider role is established in the ISA/IEC 62443 series with either a new standard or profile (designated "NewCP" in this report).

The ISAGCA report *Applying ISO/IEC 27001/2 and ISA/IEC 62443 Series for Operational Technology Environments* concludes that "ISA/IEC 62443 does not include all elements needed to secure OT. ISO/IEC 27001/2 provides ISMS requirements and control/guidance that are fully common to IT and OT and are not found in ISA/IEC 62443. Therefore, a method for applying both standards to OT infrastructure is recommended…"

6.2 Conformity Assessment Reference Model

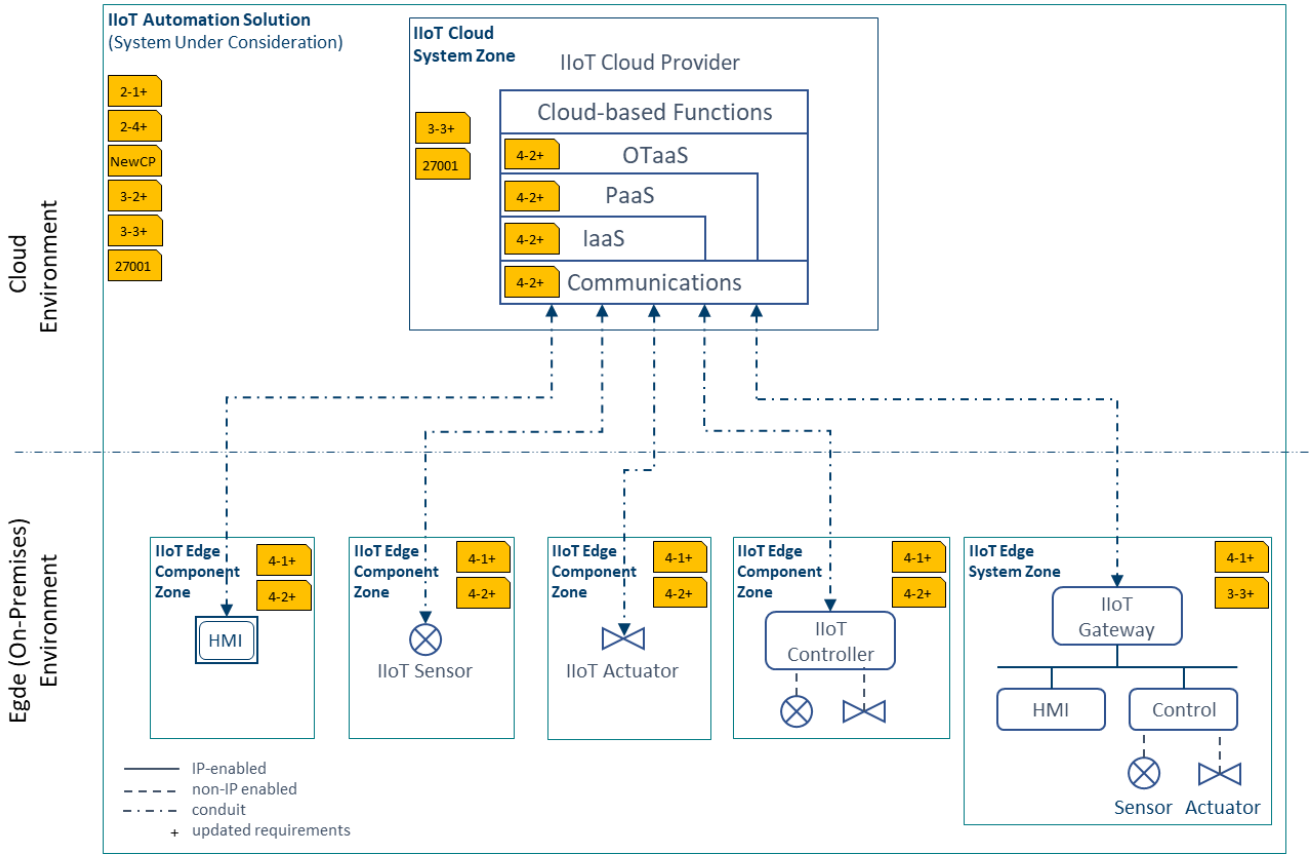


Figure 8 – IIoT Conformity Assessment Reference Model

Figure 8 shows a reference model, based on ISA/IEC 62443 concepts, for an IACS Automation Solution with IIoT cloud-based functionality.

The following terms are used in this IIoT conformity assessment reference model:

- IIoT edge components – components such as sensors, actuators, controllers, gateways, or human-machine interfaces (HMIs) that directly connect to cloud services
- IIoT edge systems – systems such as distributed control systems that connect to cloud services via an IIoT gateway
- IIoT cloud components – cloud services such as IaaS, PaaS, SaaS or OTaaS
- IIoT cloud systems – the set of IIoT cloud components that together provide IIoT cloud-based functionality
- IIoT Automation Solution – the set of IIoT cloud systems, IIoT edge components and IIoT edge systems that provide a complete solution for a particular facility. For risk assessment purposes, the IIoT Automation Solution is also the system under consideration.
- IIoT IACS – the combination of an IIoT Automation Solution and an associated security program that provides the security policies, processes and procedures to support it.

6.3 IIoT Cloud Providers

A conformity assessment scheme of the security program (processes, policies and procedures) that the cloud provider uses to deliver OTaaS, SaaS, PaaS and/or IaaS could be developed in a manner like the ISASecure Security Development Lifecycle Assessment (SDLA) for IACS product suppliers. However, while SDLA is based on ISA/IEC 62443-4-1, a certification scheme for cloud providers would have to be based on a new ISA/IEC 62443 standard or profile (called Part NewCP in this document):

- ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*
- ISA/IEC 62443-NewCP, *Security for industrial automation and control systems – Part NewCP: Security program requirements for IACS cloud providers*

6.4 IIoT Edge Components

The ISAGCA report *IIoT Component Certification Based on the 62443 Standard* [10] studied the applicability of ISA/IEC 62443 standards and certifications to IIoT components. This study concluded that "a certification that addresses such IIoT devices and gateways could be constructed based upon existing ISA/IEC 62443-4-2 certification programs by incorporating a manageable number of program enhancements." These enhancements are documented in the report.

The report's recommendations are based upon the following ISA/IEC 62443 standards:

- ISA/IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements* (updated to include IIoT security requirements)

- ISA/IEC 62443-4-2, *Security for industrial automation and control systems – Part 4-2: Technical requirements for IACS components* (updated to include IIoT security requirements)

Conformity assessment of an overall IIoT system would require that the IIoT components at the edge that communicate with the cloud conform and/or are certified to meet the recommendations documented in this ISAGCA report or future enhanced ISA/IEC 62443 standards.

A conformity assessment scheme based on this report has been recently introduced by the ISA Security Compliance Institute and is called "ISASecure IIoT Component Security Assurance" (ICSA).

6.5 IIoT Edge Systems

A conformity assessment scheme for control systems that are in edge zones could be modeled after the existing ISASecure System Security Assurance scheme with updated requirements for the IIoT use case.

The standards that could form the basis for this conformity assessment scheme are:

- ISA/IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements* (updated to include IIoT security requirements)
- ISA/IEC 62443-3-3, *Security for industrial automation and control systems – Part 3-3: System security requirements and security levels* (updated to include IIoT security requirements)

6.6 IIoT Cloud Components

The individual cloud service supplied by a cloud provider could be modeled as "components" of an IIoT cloud system. The conformity assessment of an IIoT cloud system would require that the cloud provider's processes, policies and procedures employed to provide this IIoT system have been certified according to section 6.3.

The following standards could form the basis for the IIoT cloud component conformity assessment scheme:

- ISA/IEC 62443-NewCP, *Security for industrial automation and control systems – Part NewCP: Security program requirements for IACS cloud providers*
- ISA/IEC 62443-4-2, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components* (updated to include IIoT security requirements)

Cloud-based components could be modelled as follows (see section 5.5):

- IaaS (processing and storage) – host component (ISA/IEC 62443-4-2+)
- IaaS (networking) – network component (ISA/IEC 62443-4-2+)
- PaaS (processing, storage, network, OS, database) – host component (ISA/IEC 62443-4-2+)
- SaaS – application component (ISA/IEC 62443-4-2+)
- OTaaS – application component with control, view and/or manipulate functionality (ISA/IEC 62443-4-2+)

6.7 IIoT Cloud Systems

A conformity assessment scheme for the IIoT cloud system could be developed in a manner like the ISASecure System Security Assessment (SSA). The conformity assessment of an IIoT cloud system would require that the cloud provider's processes policies, and procedures employed to provide this IIoT system have been certified according to section 6.3.

The following standards could from the basis for the IIoT cloud system conformity assessment scheme:

- ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*
- ISA/IEC 62443-NewCP, *Security for industrial automation and control systems – Part NewCP: Security program requirements for IACS cloud providers*
- ISA/IEC 62443-3-3, *Security for industrial automation and control systems – Part 3-3: System security requirements and security levels* (updated to include IIoT security requirements)

6.8 IIoT IACS

A conformity assessment scheme could be developed for a cloud-based IACS, which is the IIoT Automation Solution plus the polices, processes and procedures to manage it. This would be an assessment based on the ISA/IEC 62443 standards required for the asset owner role and could include the following standards:

- ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*
- ISA/IEC 62443-2-1, *Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners* (updated to include IIoT security requirements)
- ISA/IEC 62443-2-4, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers* (updated to include IIoT security requirements)
- ISA/IEC 62443-NewCP, *Security for industrial automation and control systems – Part NewCP: Security program requirements for IACS cloud providers*
- ISA/IEC 62443-3-2, *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design* (updated to include IIoT security requirements)
- ISA/IEC 62443-3-3, *Security for industrial automation and control systems – Part 3-3: System security requirements and security levels* (updated to include IIoT security requirements)

6.9 Conformity Assessment Example

An asset owner organization has a contract with an IIoT cloud provider organization to provide an IIoT SCADA system that is implemented using OTaaS. The IIoT cloud provider is responsible for the development, support and operation of the cloud portion of the IIoT SCADA system. The asset owner is accountable for the security of the IIoT IACS, and for the operation of the IIoT IACS and the equipment under control.

The asset owner has a contract with an integration service provider organization to install the IIoT edge devices and configure the IIoT SCADA system.

The asset owner also has a contract with a maintenance service provider to maintain and support the edge devices. The maintenance and support of the IIoT SCADA system is provided by the cloud provider.

For this example, the following conformity assessments would apply:

- The cloud provider would have their policies, processes and procedures assessed using the conformity assessment scheme described in section 6.3.
- The IIoT edge components would be assessed using the ICSA conformity assessment scheme described in section 6.4.
- The IIoT edge systems would be assessed using the conformity assessment scheme described in section 6.5.
- IIoT cloud components that are used to build the IIoT SCADA system (*e.g.*, PaaS, SaaS) would be assessed using the conformity assessment scheme described in section 6.6.
- The IIoT SCADA system would be assessed using the conformity assessment scheme described in section 6.7.
- The IIoT IACS would be assessed using the conformity scheme described in section 6.8.
- The integration service provider and maintenance service provider would be assessed using existing conformity assessment schemes based on ISA/IEC 62443-2-4 (updated to include IIoT security requirements)

7 Conclusions

The main conclusions of this report are:

- The concepts in ISA/IEC 62443 standards can be applied to IACS that use cloud-based functionality. Concepts such as risk assessment, zone and conduit partitioning and the system/component model can all be applied to an IIoT IACS.
- 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)* to provide transparency when cloud-based functionality has the capability to directly or indirectly change the physical state of the equipment under control.
- The cloud provider is a new role not currently defined in the ISA/IEC 62443 series of standards. The cloud provider role includes aspects of the product supplier, service provider and asset owner (operator) roles.
- A comparison between ISA/IEC 62443 standards and the Cloud Security Alliance Cloud Controls Matrix v4 indicates that 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, based on ISA/IEC 62443 standards, provided these standards are updated for the IIoT use case.

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.

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

Annex A – Example IIoT System Risk Assessment

A.1 Example Use Cases

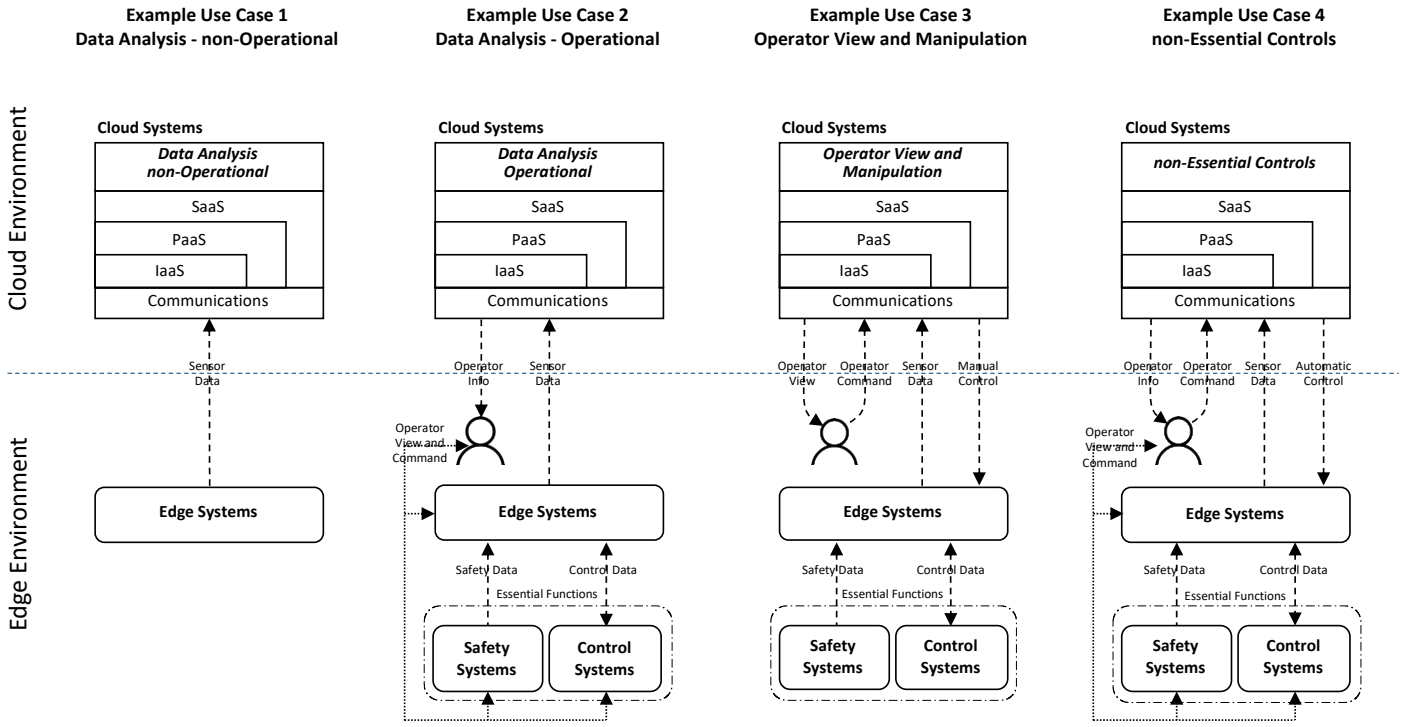


Figure A.1 – Example Use Cases – Functional View

There are four use cases considered in this report, which are shown in Figure A.1 and summarized in Table A.1. These use cases are based on the implementation of cloud-based functionality in a public cloud, using a SaaS cloud service category, with communications between cloud and edge over an untrusted publicly accessible network. PaaS and IaaS may be used to support the SaaS cloud service. Other deployment models such as private cloud, hybrid cloud, private networks between edge and cloud and edge computing are not considered in this example risk assessment.

A.1.1 Use Case 1: Cloud-based Data Analytics – non-Operational

The first use case explores the use of cloud-based data analytics and view of the data analytics results from the cloud by non-operations personnel. An example would be an artificial intelligence/machine learning application that is used for predictive maintenance.

The cloud-based functionality would be offered by a cloud provider in a public cloud using SaaS. The SaaS application could be hosted by other PaaS/IaaS cloud providers. The asset owner is accountable for the overall IIoT IACS but may delegate certain responsibilities to the SaaS cloud provider (see Figure 4 – Shared Cloud Security Responsibilities Model).

The edge/on-premises functionality for this use case is data acquisition from IIoT sensors. An IIoT gateway consolidates the acquired data and forwards it to the SaaS cloud-based application. The asset owner is accountable for the overall IIoT IACS but may delegate certain responsibilities to an integration service provider or maintenance service provider.

Communications between the SaaS cloud application and the edge/on-premises devices is via a public (untrusted) network such as the Internet.

A.1.2 Use Case 2: Cloud-based Data Analytics – Operational

The second use case explores the use of cloud-based data analytics and view of the data analytics results by operations personnel. This use case is like use case 1 except that the results of the data analytics are used by operations personnel *to make operational decisions and locally manipulate the equipment under control*. Compromise of the data received by operations personnel may *indirectly* impact the equipment under control which may result in physical consequences. An example would be a condition monitoring system that advises the operator to make operational changes to the equipment under control.

The cloud-based functionality would be offered by a cloud provider in a public cloud using SaaS. The SaaS application could be hosted by other PaaS/IaaS cloud providers. The asset owner is accountable for the overall IIoT IACS but may delegate certain responsibilities to the SaaS cloud provider (see Figure 4 – Shared Cloud Security Responsibilities Model).

The edge/on-premises functionality for this use case is data acquisition from IIoT devices such as sensors, actuators and controllers. An IIoT gateway consolidates the acquired data and forwards it to the SaaS cloud-based application. The edge devices would allow *local manipulation* of the equipment under control. The asset owner is accountable for the overall IIoT system but may delegate certain responsibilities to an integration service provider or maintenance service provider.

Communications between the SaaS cloud application and the edge/on-premises devices is via a public (untrusted) network such as the internet.

In this example, essential functions are partitioned into safety zones and control zones that are implemented on network segments that are not directly connected to a public (untrusted) network.

A.1.3 Use Case 3: Cloud-based Operator View and Manipulation

The third use case explores the use of cloud-based view and manipulation of the equipment under control from the cloud by operations personnel. An example would be a cloud-based SCADA system that provides view and manipulation for geographically distributed edge devices.

The cloud-based functionality would be offered by a cloud provider in a public cloud using SaaS. The SaaS application could be hosted by other PaaS/IaaS cloud providers. The asset owner is accountable for the overall IIoT IACS but may delegate certain responsibilities to the SaaS cloud provider (see Figure 4 – Shared Cloud Security Responsibilities Model).

The edge/on-premises functionality for this use case is data acquisition and manipulation to/from IIoT devices such as sensors, actuators and controllers. An IIoT gateway consolidates the acquired data and forwards it to the SaaS cloud-based application. The edge devices would allow *manual manipulation* from the cloud-based application. The asset owner is accountable for the overall IIoT IACS but may delegate certain responsibilities to an integration service provider or maintenance service provider.

Communications between the SaaS cloud application and the edge/on-premises devices is via a public (untrusted) network such as the internet.

In this example, essential functions are partitioned into safety zones and control zones which are implemented on network segments that are not directly connected to a public (untrusted) network.

A.1.4 Use Case 4: Cloud-based non-Essential Control

The fourth use case explores the use of cloud-based non-essential control, view of the non-essential control results by operations personnel and automatic manipulation of the equipment under control from the cloud. This use case is like use case 3 except that the cloud-based application implements *closed loop automatic control* and sends outputs to the setpoints of edge controllers without human intervention. The controls implemented in the cloud are non-essential, that is, the equipment under control continues to operate satisfactorily (but perhaps not optimally) if the cloud-based control functions are not available. An example would be a cloud-based advanced control application that provides non-essential control/view functions.

The cloud-based functionality would be offered by a cloud provider in a public cloud using SaaS. The SaaS application could be hosted by other PaaS/IaaS cloud providers. The asset owner is accountable for the overall IIoT IACS but may delegate certain responsibilities to the SaaS cloud provider (see Figure 4 – Shared Cloud Security Responsibilities Model).

The edge/on-premises functionality for this use case is data acquisition and manipulation to/from IIoT devices such as sensors, actuators and controllers. An IIoT gateway consolidates the acquired data and forwards it to the SaaS cloud-based application. The edge devices would allow *automatic control* from the cloud-based application. The asset owner is accountable for the overall IIoT IACS but may delegate certain responsibilities to an integration service provider or maintenance service provider.

Communications between the SaaS cloud application and the edge/on-premises devices is via a public (untrusted) network such as the Internet.

In this example, essential functions are partitioned into safety zones and control zones which are implemented on network segments that are not directly connected to a public (untrusted) network.

	Use Case 1	Use Case 2	Use Case 3	Use Case 4
Title	**Cloud-based Data Analytics non-Operational**	**Cloud-based Data Analytics Operational**	**Cloud-based Operator View and Manipulation**	**Cloud-based non-Essential Control**
Cloud functions zones	• data analytics used for non-operational purpose • non-essential view of data analytics results by non-operations personnel (*e.g.*, maintenance)	• data analytics used for operational purpose • non-essential view of data analytics results by operations personnel	• non-essential manual manipulation of Equipment Under Control • non-essential view of Equipment Under Control by operations personnel	• non-essential automatic control of Equipment Under Control • non-essential view of Equipment Under Control by operations personnel
Edge functions zones	• data acquisition	• data acquisition • non-essential controls • non-essential view and manipulation	• data acquisition • non-essential controls • non-essential view and manipulation	• data acquisition • non-essential controls • non-essential view and manipulation
Essential functions zones	• none	• safety • essential controls • essential view and manipulation	• safety • essential controls • essential view and manipulation	• safety • essential controls • essential view and manipulation
Communication functions	• edge to cloud	• edge to/from cloud • control to/from edge • safety to edge	• edge to/from cloud • control to/from edge • safety to edge	• edge to/from cloud • control to/from edge • safety to edge
Example	• preventive maintenance in the cloud	• condition monitoring in the cloud	• SCADA in the cloud	• advanced control in the cloud

Table A.1 – Example Use Cases – Summary of Functions

A.2 Risk Assessment

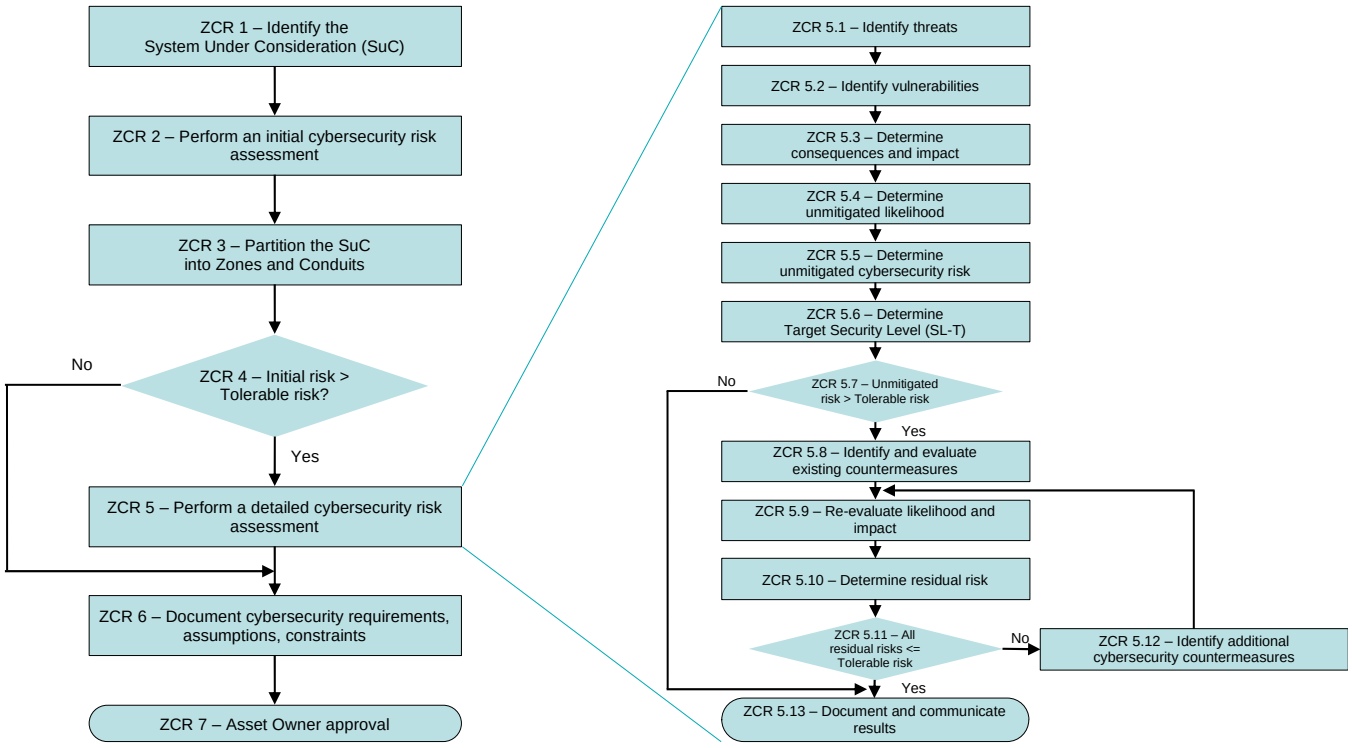


Figure A.2 – ISA/IEC 62443-3-2 Risk Assessment Process

This annex applies the risk assessment process found in ISA/IEC-62443-3-2:2020 to the use cases described above to determine a target security level for each zone. This annex follows the risk assessment process up to an including ZCR 5.6, determine target security level. It does not include the detailed risk assessment steps in ZCR 5.7 through ZCR 5.12, or the final documentation and approval in ZCR 6 and ZCR 7.

The following steps of the risk assessment are described in following subsections:

- A.2.1 Identify the system under consideration (SuC) (ZCR 1)
- A.2.2 Perform an initial cybersecurity risk assessment (ZCR 2)
- A.2.3 Identify essential functions
- A.2.4 Partition the SuC into zones and conduits (ZCR 3)
- A.2.5 Perform a detailed cybersecurity risk assessment for each zone and conduit (ZCR 5.1 through 5.6)

Important 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 team with experience in the asset owner, service provider, product supplier, and cloud provider roles, and cybersecurity consultants familiar with ISA/IEC 62443.

A.2.1 Identify the System Under Consideration (ZCR 1)

The first step in the risk assessment process described in ISA/IEC 62443-3-2 ZCR 1 is to determine the scope of the risk assessment. The scope is determined by selecting the *system under consideration*, which is a collection of one or more IACS system or component assets.

For this example risk assessment, the system under consideration (scope) has been set to include the cloud systems, even though example use case 1 and 2 cannot directly impact the physical domain. This has been done so that the analysis can consider the risk consistently between the example use cases. In an actual ISA/IEC 62443 risk assessment, the system under consideration (scope) would only include those systems where there is a potential for impact to the physical domain.

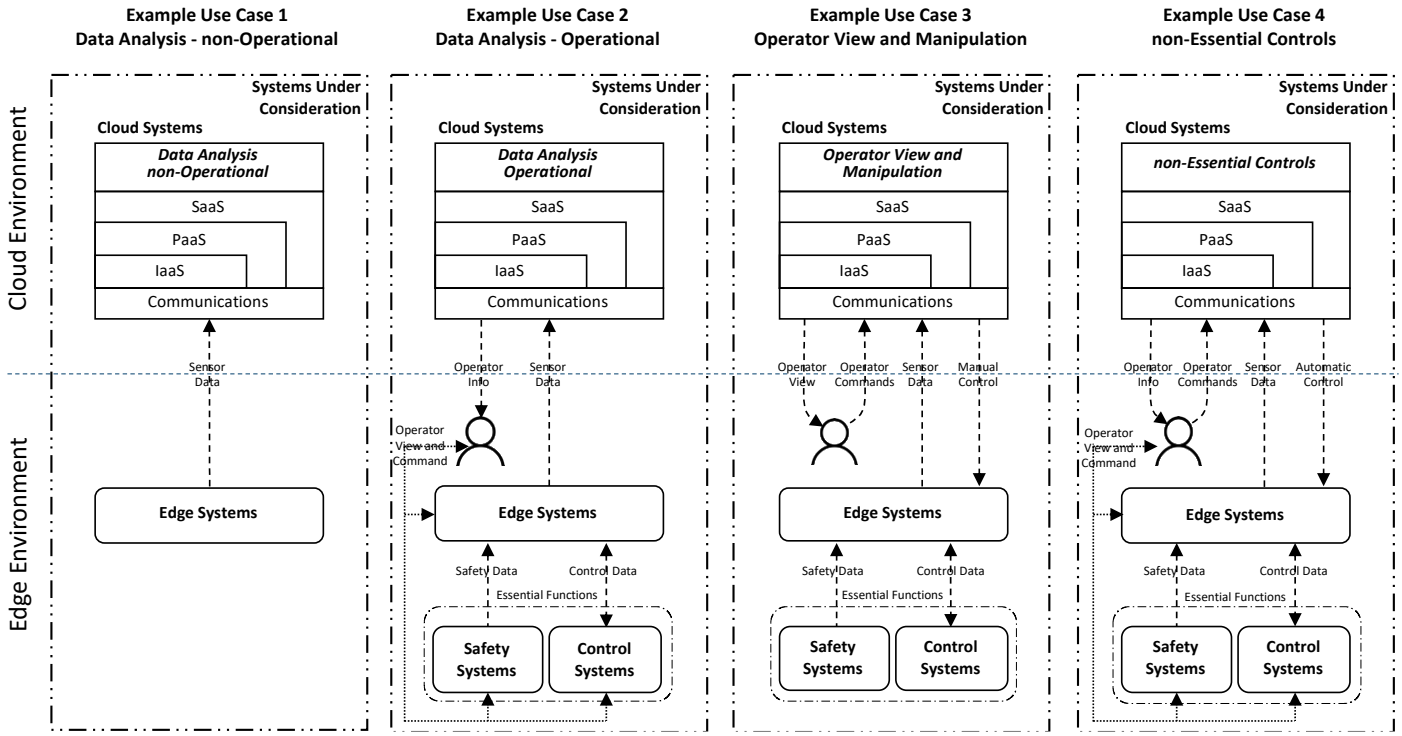


Figure A.3 – Example Use Cases – Systems Under Consideration

A.2.2 Perform an Initial Cybersecurity Risk Assessment (ZCR 2)

The purpose of the initial cybersecurity risk assessment is to gain a high-level understanding of the worst-case risk the system under consideration presents to the organization should it be compromised. In our use case examples, we have not identified the specific equipment under control to which the use cases apply, so we must make assumptions about the worst-case risk for use in the remainder of the risk assessment. Table A.2 shows the worst-case consequence impact assumptions used in the analysis, based on Table A.3 ISA/IEC 62443-3-2:2020, Annex B Figure B.3 (see A.2.5.2), and the descriptions of the use cases in section A.1.

	Use Case 1 **Cloud-based Data Analytics non-Operational**	**Use Case 2** **Cloud-based Data Analytics Operational**	**Use Case 3** **Cloud-based Operator View and Manipulation**	**Use Case 4** **Cloud-based Non-Essential Control**
Health, Safety, Environmental	Low	High	High	High
Operational	Low	High	High	High
Financial	Medium	High	High	High

Table A.2 – Worst-case Impact Assumptions for Example Use Cases

A.2.3 Identify Essential Functions and Partition into Zones and Conduits (ZCR 3)

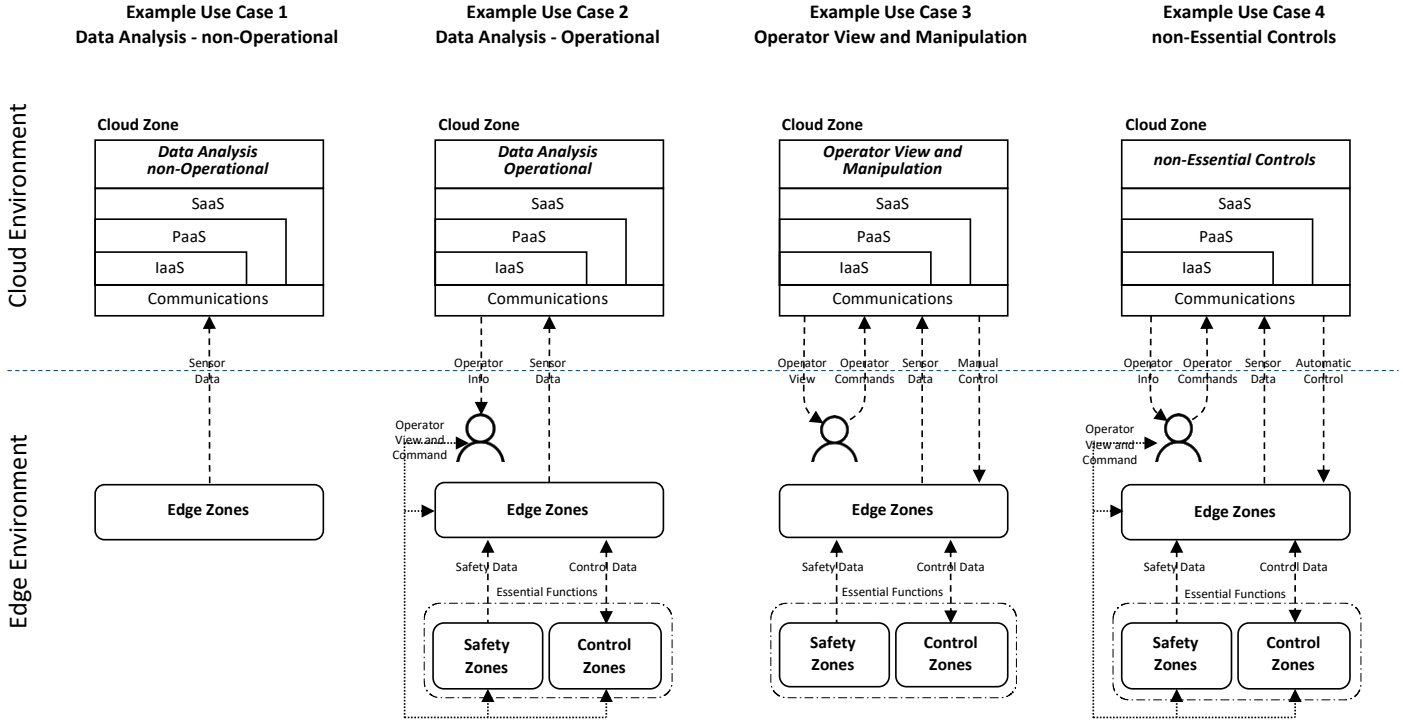


Figure A.4 – Example Use Cases – Zone and Conduit Partitioning

The partitioning of the IIoT systems into zones and conduits is an important step in applying the ISA/IEC 62443 series of standards. The requirements and recommendations for partitioning into zones and conduits are described in ISA/IEC 62443-3-2:2020 clause 5.4.3 and identified as ZCR 3:

- Establish zones and conduits (ZCR 3.1) – group IACS assets into zones based on risk and identify the conduits that interconnect these zones
- Separate business and control system assets (ZCR 3.2) – separate business functions (IT) and control functions (IACS) into separate zones

- Separate safety instrumented system assets (ZCR 3.3) – separate safety functions into zones that are separate from all other zones. Safety functions are one type of essential functions
- Separate essential control system assets (ZCR 3.3) – separate control systems that have essential functions into separate zones
- Consider temporarily connected devices (ZCR 3.4) – consider the additional risk that temporary devices (*e.g.*, laptops, smartphones, USB drives) may pose to the zone that they connect to
- Separate wireless devices (ZCR 3.5) – wireless devices should be grouped into zones that are separated from wired devices
- Separate devices connected via external networks (ZCR 3.6) – devices that are permitted to make connections to the system under consideration via external networks should be grouped in a separate zone or zones. This requires that cloud-based functionality must be separated into separate zones.

Based on these requirements and recommendations, the functionality in each use case has been partitioned into safety zones (essential), control zones (essential), edge zones and cloud zones. It is important to note that the security zone model for an actual IIoT system may have a further subdivision of zones, such as separate cloud zones for IACS functions and IT functions.

Safety Zones (essential)

Assets that execute safety functions (health, safety, environment) are partitioned into safety zones in the IIoT system. All safety zones are essential function zones, as defined in section 4.2. In these examples, safety zones can only communicate with edge zones in one direction (from safety zone to edge zone). This significantly reduces the attack surface to which the safety zone is exposed.

Control Zones (essential)

Assets that execute *essential* control functions (*e.g.*, high availability is required) are partitioned into control zones in the IIoT system. Control zones can communicate with edge zones in both directions (control zone to/from edge zone). This reduces the attack surface to which the control zone is exposed because it is not directly connected to an untrusted network.

Edge Zones

Assets that execute non-essential functions at the edge are grouped into edge zones. Edge zones can include data acquisition functions, non-essential control functions, edge computing functions and one or more IIoT gateway functions that communicate with the cloud zone. Edge zones can communicate with safety zones, control zones and cloud zones. Data communications between edge and cloud zones is one-directional for use cases 1 and 2, and bi-directional for use cases 3 and 4.

Cloud Zones

Assets that execute data analytics for non-operational functions, data analytics for operational functions, non-essential view and manipulation functions or non-essential control functions are grouped into cloud zones depending on use case. In all cases, it is assumed that these functions are provided by a SaaS cloud provider. The SaaS cloud provider can in turn use PaaS and/or IaaS services from another cloud provider. The cloud zone communicates with the edge zone.

Conduits

There are three conduits identified in the example: cloud zone – edge zone conduit, edge zone – safety zone conduit, and edge zone – control zone conduit. Additional conduits may be present if these zones are further subdivided, but this was not considered in this risk assessment.

The cloud zone – edge zone conduit uses a public, untrusted network (*e.g.*, the Internet).

The edge zone – safety zone conduit uses a private, trusted network that is one-directional and under the administration of the asset owner (data flow from safety zone to edge zone).

The edge zone – control zone conduits use a private, trusted network that is bi-directional and under the administration of the asset owner (data flow control zone to/from edge zone).

A.2.4 Compare High-Level Risk to Tolerable Risk (ZCR 4)

This step in the risk assessment process determines if a detailed risk assessment according to ZCR 5 is necessary. If the initial risk determined in ZCR 2 is greater than the risk that the organization can tolerate, a detailed risk assessment is necessary. Since the worst-case risk for use cases 2, 3 and 4 are High, it calls for a more detailed risk assessment. For use case 1, the worst-case risk is medium, so a detailed risk assessment may or may not be required based on the organization's tolerance for risk. For this example, the risk assessment team decided to complete a detailed risk assessment for use case 1.

A.2.5 Perform a Detailed Cybersecurity Risk Assessment for Each Zone and Conduit (ZCR 5)

When the initial risk is greater than the tolerable risk, the risk assessment process calls for a detailed risk assessment as described in ISA/IEC 62443-3-2:2020 ZCR 5. In this example, the process steps in the sections listed below are followed until ZCR 5.6, the detailed design of security measures (ZCR 5.7 through 5.12) is left to the reader.

A.2.5.1 Identify threats and vulnerabilities (ZCR 5.1, 5.2)

A.2.5.2 Determine consequences and impact (ZCR 5.3)

A.2.5.3 Determine unmitigated likelihood (ZCR 5.4)

A.2.5.4 Determine unmitigated cybersecurity risk (ZCR 5.5)

A.2.5.5 Determine target security level (ZCR 5.6)

A.2.5.1 Identify Threats and Vulnerabilities (ZCR 5.1, 5.2)

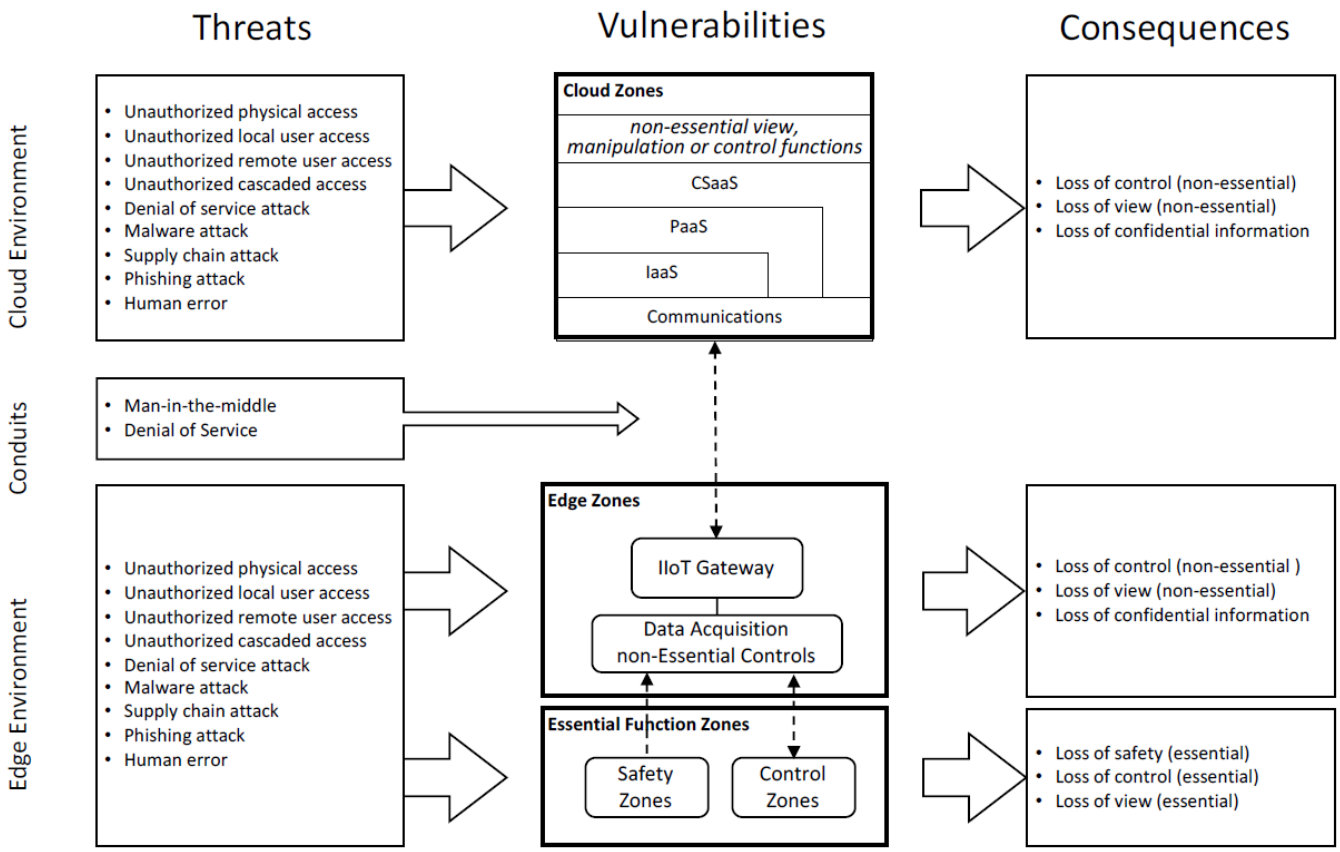


Figure A.5 – Example Risk Assessment Model

Figure A.5 shows the general risk assessment model used for the example use cases. This model incorporates the list of threats for each environment, vulnerabilities that the threats can exploit and the consequences of a successful compromise.

Threat Types

- Unauthorized physical access – human user physical access to the IIoT IACS
- Unauthorized local user access – local human user access to the IIoT IACS (*e.g.*, workstation login)
- Unauthorized remote user access – remote human user access to the IIoT IACS
- Unauthorized cascaded access (pivot) – user access to a zone through another zone
- Denial of service attack – loss of function through loss of availability
- Malware attack – malicious software such as virus or ransomware
- Supply chain attack – attack through the supply chain such as product supplier, PaaS supplier or IaaS supplier (*e.g.*, malicious firmware)
- Phishing attack – use of deception to manipulate humans into divulging confidential information

- Human error – accidental human error (design, integration, operation or maintenance)
- Man in the middle attack – attack on the conduits between zones

Vulnerabilities

- In the analysis of unmitigated risk, it is assumed that vulnerabilities exist in the IIoT IACS which can be exploited by an attacker. The vulnerabilities can be either known (*e.g.*, unpatched) or zero day.
- Each zone exposes an attack surface to the threats described above. The attack surface is a set of attack vectors that provide a path or means for an attacker to exploit a zone.

Consequences

For the typical risk assessment, the consequences of failure of the equipment under control are used to assess risk. In this risk assessment model, the consequences of failure of the IIoT IACS are used to assess risk. The consequences of IIoT system failure are described below:

- Loss of safety (essential) – loss of safety functions (health, safety, environment)
- Loss of control (essential) – loss of essential control functions (*e.g.*, high availability control required)
- Loss of view (essential) – loss of essential view or manipulation functions
- Loss of control (non-essential) – loss of non-essential control functions
- Loss of view (non-essential) – loss of non-essential view or manipulation functions
- Loss of confidential information – loss of confidential, sensitive, or proprietary information

A.2.5.2 Determine Consequences and Impact (ZCR 5.3)

The next step in the detailed risk assessment process described in ISA/IEC 62443-3-2 is to determine the consequences and impact of a compromise for each security zone. Table A.3 shows a consequence or impact severity table from ISA/IEC 62443-3-2:2020 Annex B Table B.3, which will be used for this example risk assessment.

	Operational			Financial			HSE		
Category	**Outage at one site**	**Outage at multiple sites**	**National infrastructure and services**	**Cost (Million USD)**	**Legal**	**Public confidence**	**People onsite**	**People offsite**	**Environment**
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanor criminal offense	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on community.	<5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits

Table A.3 – ISA/IEC 62443-3-2:2020 Annex B Table B.3 (informative)

Table A.4 shows an example assessment of the unmitigated impact severity for each consequence type, use case and zone using the example impact scale from Table A.3.

The acronym "n/a" means "not applicable" and indicates that the functionality associated with the consequence type has not been selected for that zone. For example, essential functions have not been selected for implementation in the cloud environment (see section 4.2).

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 and Manipulation				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	Medium	Low	n/a	n/a	Medium	Medium	Medium	n/a	Medium	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	Medium	Low	Low	Medium	Medium	Low	Low	Medium	Medium	Low	Low	Medium	Medium

Table A.4 – Example Use Cases – Impact Severity

Impact severity assumptions:

- Impact severity is unmitigated before security measures have been implemented.
- Impact severity is based on the functions implemented in that security zone. Cascaded access (pivoting) is considered in the likelihood assessment.
- Essential functions are only implemented in safety zones or control zones.
- There is a policy that essential functions are not implemented in edge zones or cloud zones.
- The loss or compromise of an essential function could have high impact severity.
- The loss or compromise of a non-essential function could have low or medium impact severity.
- The loss or compromise of a non-essential function in the control zone could have medium impact severity.
- The loss of confidential information in the edge or cloud zone could have medium impact severity.
- Authentication domains for cloud zones, edge zones, control zones and safety zones are segregated.
- Initial security measures in place: cloud zone – edge zone conduit is encrypted over an untrusted public network, safety zone – edge zone conduit is unidirectional over a private network, control zone – edge zone conduit is bidirectional over a private network

A.2.5.3 Determine Unmitigated Likelihood (ZCR 5.4)

The next step in the detailed risk assessment process described in ISA/IEC 62443-3-2 is to determine the likelihood of a compromise for each security zone. Table A.5 shows a likelihood table from ISA/IEC 62443-3-2:2020 Annex B Table B.2, which will be used for this example risk assessment. The likelihood scale has been modified by inverting the likelihood scale from Part 3-2 Table B.2.

Likelihood scale	Guideword	Likelihood description	Frequency-based guidance
5	Certain	Almost certain	>10^{-1} per year (High demand)
4	Likely	Likely to occur	10^{-1} to 10^{-3} per year (Low demand)
3	Possible	Quite possible or not unusual to occur	10^{-3} to 10^{-4} per year
2	Unlikely	Conceivably possible, but very unlikely to occur	10^{-4} to 10^{-5} per year
1	Remote	So unlikely that it can be assumed it will not occur	<10^{-5} per year

Table A.5 – ISA/IEC 62443-3-2:2020 Annex B Table B.2 (modified) (informative)

Table A.6 shows an example assessment of the unmitigated likelihood for each threat type, use case and zone using the example likelihood scale from Table A.5.

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				Operator View and 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
Unauthorized cascaded access (pivot)	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely	Likely
Denial of Service attack	Possible	Likely	Possible	Possible	Possible	Likely	Possible	Possible	Possible	Likely	Possible	Possible	Possible	Likely
Man-in-the-Middle attack	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely
Malware attack	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely
Supply chain attack	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, integration, operation, maintenance)	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely	Possible	Possible	Likely	Likely

Table A.6 – Example Use Cases – Threat/Vulnerability Likelihood

Likelihood assessment assumptions:

- Basic security measures are in place, such as physical access control, user access control, data flow control and patch management.
- Unpatched system or component likelihood includes untimely patch installation and zero-day vulnerability.
- Unauthorized local user access includes insider access.
- Unauthorized remote user access assumes access to the zone is available.
- Phishing attack assumes the entry point is outside safety zones and control zones.
- IIoT system is assumed to have vulnerabilities that can be exploited.

A.2.5.4 Determine Unmitigated Cybersecurity Risk (ZCR 5.5)

The next step in the detailed risk assessment is to assess the unmitigated risk, based on the impact severity (determined in section A.2.5.2) and the unmitigated likelihood (determined in section A.2.5.3). Table A.7 shows the risk matrix from ISA/IEC 62443-3-2:2020 Annex B, Figure B.1, which is used for this example risk assessment.

Likelihood	Impact Severity: Low	Impact Severity: Medium	Impact Severity: High
Remote	Low	Low	Med-Low
Unlikely	Low	Med-Low	Medium
Possible	Med-Low	Medium	Med-High
Likely	Medium	Med-High	High
Certain	Med-High	High	High

Table A.7 – ISA/IEC 62443-3-2:2020 Annex B Figure B.1 Risk Matrix (modified) (informative)

Table A.8 shows an example assessment of the unmitigated cybersecurity risk for each consequence type, use case and zone. The table uses the impact severity from Table A.4, the highest likelihood from Table A.6, and the risk matrix from Table A.7 to determine the initial risk for each type of consequence.

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	Med-High	Medium	n/a	n/a	Med-High	Med-High	Med-High	n/a	Med-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	Med-High	Medium	Medium	Med-High	Med-High	Medium	Medium	Med-High	Med-High	Medium	Medium	Med-High	Med-High

Table A.8 – Example Use Cases – Initial Risk

The results of the example assessment of unmitigated cybersecurity risk indicate the following conclusions:

- The unmitigated risks for use case 3 and use case 4 are the same because in both cases the cloud zone can make changes to the edge zone, which in turn could affect the physical domain.
- The unmitigated risks for safety zones and control zones are high because there is the possibility of loss or compromise of essential functions.
- For edge zones, the unmitigated risk is medium-high because the functionality is limited to non-essential functions, but the likelihood is likely because the attack surface is large.
- For cloud zones, the unmitigated risk is medium-high because of the potential loss of confidential information and the potential to indirectly affect the physical domain, and likelihood is likely because the attack surface is large.

The risk for conduits is inherited from the maximum risk of the zones that they interconnect:

- Safety zone – edge zone conduit is high.
- Control zone – edge zone conduit is high.
- Edge – cloud conduit is medium-high.

A.2.5.5 Determine Security Level Target (ZCR 5.6)

There is no prescribed method for establishing the target security level (SL-T) in ISA/IEC 62443-3-2. Some organizations choose to establish SL-T based on a mapping of unmitigated risk level to target security level in order to reduce risk to a tolerable level. Other organizations use a bottom-up approach by selecting a capability security level based on the security requirements in ISA/IEC 62443-3-3. Both methods will be discussed in this section.

For the first method, Table A.9 shows an example of a mapping between the unmitigated risk level (from Table A.7) and the target security level needed to reduce the risk to a tolerable level (low in this example).

Unmitigated Risk Level (Table A.7)

Likelihood \ Impact Severity	Low	Medium	High
Remote	Low	Low	Med-Low
Unlikely	Low	Med-Low	Medium
Possible	Med-Low	Medium	Med-High
Likely	Medium	Med-High	High
Certain	Med-High	High	High

Target Security Level

Likelihood \ Impact Severity	Low	Medium	High
Remote	SL 1	SL 1	SL 2
Unlikely	SL 1	SL 2	SL 3
Possible	SL 2	SL 3	SL 4
Likely	SL 3	SL 4	SL 4
Certain	SL 4	SL 4	SL 4

Table A.9 – Example Asset Owner Risk Matrix – Target Security Level Mapping (informative)

Table A.10 shows the resulting target security level for each example use case, zone type and consequence type using the mapping in Table A.9. The results show that in all example use cases, a target security level of SL-T 4 is needed to mitigate the security risks identified in the risk assessment.

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

Table A.10 – Example Use Cases – Target Security Level Using Part 3-2

Table A.11 shows an alternative approach to determining the security level based on a review of the individual base requirements and requirement enhancements in ISA/IEC 62443-3-3 and considering the risks and attack surface presented by each Zone. Table A.11 shows an example assessment of the capability security level for each example use case, zone type and foundational requirement. The SL-C was determined by selecting the highest SL-C for each foundational requirement.

Security Level - Capability	Use Case 1 Zones		Use Case 2 Zones				Use Case 3 Zones				Use Case 4 Zones			
Foundational Requirement	**Edge**	**Cloud**	**Safety**	**Control**	**Edge**	**Cloud**	**Safety**	**Control**	**Edge**	**Cloud**	**Safety**	**Control**	**Edge**	**Cloud**
FR 1- Identification and Authenication Control	SL 3	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
FR 2 - Use Control	SL 3	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
FR 3 - System Integrity	SL 4	n/a	SL 2	SL 3	SL 4	n/a	SL 2	SL 3	SL 4	SL 4	SL 2	SL 3	SL 4	SL 4
FR 4 - Data Confidentiality	SL 4	n/a	SL 2	SL 2	SL 4	n/a	SL 2	SL 2	SL 4	SL 4	SL 2	SL 2	SL 4	SL 4
FR 5 - Restricted Data Flow	SL 3	n/a	SL 4	SL 4	SL 3	n/a	SL 4	SL 4	SL 3	SL 3	SL 4	SL 4	SL 3	SL 3
FR 6 - Timely Respose to Events	SL 3	n/a	SL 3	SL 3	SL 3	n/a	SL 3	SL 3	SL 3	SL 3	SL 3	SL 3	SL 3	SL 3
FR 7 - Resource Availability	SL 3	n/a	SL 3	SL 3	SL 3	n/a	SL 3	SL 3	SL 3	SL 3	SL 3	SL 3	SL 3	SL 3
SL-C (Maximum)	SL 4	n/a	SL 4	SL 4	SL 4	n/a	SL 4	SL 4	SL 4	SL 4	SL 4	SL 4	SL 4	SL 4

Table A.11 – Example Use Cases – Capability Security Level Using Part 3-3

A.3 Determine the Scope of ISA/IEC 62443

Based on the results of the risk assessment of the various use cases, the scope of ISA/IEC 62443 requirements can be determined. Table A.8 shows that the risk profile of use cases 3 and 4 are identical, and that they have risks associated with cyber-physical systems (*e.g.*, loss of control, loss of view/manipulation). For these reasons, ISA/IEC 62443 requirements should apply to the safety, control, edge *and cloud zones* for use cases 3 and 4.

Use cases 1 and 2 have different risk profiles but in both cases the cloud zone only has risk associated with loss of confidential information. Since the cloud zone does not have risks associated with cyber-physical systems, the requirements of ISA/IEC 62443 should not be applied to the cloud zone for use cases 1 and 2.

Figure A.6 shows the resulting scope of ISA/IEC 62443 requirements for each use case based on the example risk assessment. For these use cases, the scope of ISA/IEC 62443 can be summarized as:

> *"If the cloud zone outputs control signals to the edge zone, which in turn can directly or indirectly change the physical state of the equipment under control, then the scope of ISA/IEC 62443 requirements should apply to the cloud zone."*

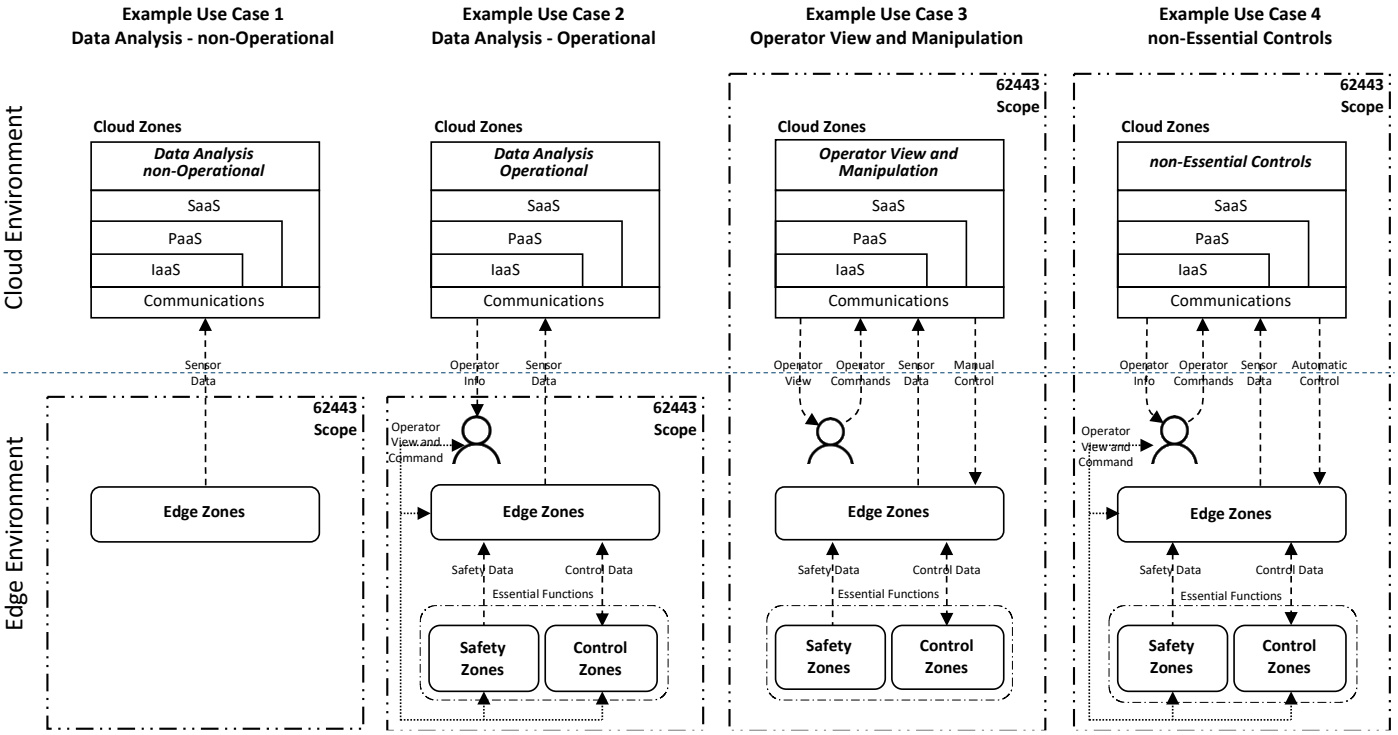


Figure A.6 – Example Use Cases – ISA/IEC 62443 Scope

Figure A.6 shows the application of this definition of scope to the four use cases that are being examined:

- Use case 1 – In this use case, the cloud-based functionality is not able to impact the cyber-physical domain, so ISA/IEC 62443 standards would not apply to the cloud environment. This is similar to the traditional IACS, where IT systems are not in the scope of ISA/IEC 62443 standards.
- Use case 2 – In this use case, the cloud-based functionality cannot impact the physical domain directly, because there is a person in the middle who is able to filter the information provided by the cloud-based functions. However, if the cloud environment is compromised, then the information provided could be spoofed and result in the person taking incorrect actions in the cyber-physical domain. Based on the results of the risk assessment in this annex, it was decided for this example that ISA/IEC 62443 standards do not apply to the cloud environment. However, in other use cases where the risk of spoofing information provided to the operator is higher, the decision could be made to include ISA/IEC 62443 in the scope of the cloud environment.
- Use case 3 – In this use case, the cloud-based functionality can directly or indirectly impact the cyber-physical domain because the equipment under control can be directly viewed and/or manipulated from the cloud environment so ISA/IEC 62443 should be in the scope of the cloud environment.
- Use case 4 – In this use case, the cloud-based functionality can directly impact the cyber-physical domain without human intervention, so the ISA/IEC 62443 should be in the scope of the cloud environment.

Annex B – CSA Cloud Controls Matrix v4 Cross Reference

The following table provides a cross reference between the Cloud Security Alliance (CSA) Cloud Controls Matrix version 4, and the core ISA/IEC 62443 standards. A √ indicates that the ISA/IEC 62443 standard provides partial or full coverage for the associated CSA CCM requirement. The difference level shows an estimate of the degree of coverage where 0 indicates the CSA requirement is not met by ISA/IEC 62443, and 4 indicates that the CSA requirement is fully met. Portions of this annex are © Copyright 2021-2022 Cloud Security Alliance and are used with permission.

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
A&A-01	Audit & Assurance	Audit and Assurance Policy and Procedures	3	√	√			√	
A&A-02	Audit & Assurance	Independent Assessments	2	√	√			√	
A&A-03	Audit & Assurance	Risk Based Planning Assessment	4	√	√	√		√	
A&A-04	Audit & Assurance	Requirements Compliance	3	√	√	√		√	
A&A-05	Audit & Assurance	Audit Management Process	3	√	√	√		√	
A&A-06	Audit & Assurance	Remediation	3	√	√	√		√	
AIS-01	Application & Interface Security	Application and Interface Security Policy and Procedures	3	√	√		√	√	√
AIS-02	Application & Interface Security	Application Security Baseline Requirements	4	√	√		√	√	√
AIS-03	Application & Interface Security	Application Security Metrics	1						
AIS-04	Application & Interface Security	Secure Application Design and Development	4				√	√	√
AIS-05	Application & Interface Security	Automated Application Security Testing	3		√		√	√	√
AIS-06	Application & Interface Security	Automated Secure Application Deployment	2	√	√			√	
AIS-07	Application & Interface Security	Application Vulnerability Remediation	4	√	√			√	
BCR-01	Business Continuity Management and Operational Resilience	Business Continuity Management Policy and Procedures	4	√	√		√		√
BCR-02	Business Continuity Management and Operational Resilience	Risk Assessment and Impact Analysis	3	√	√	√		√	
BCR-03	Business Continuity Management and Operational Resilience	Business Continuity Strategy	4	√	√	√			
BCR-04	Business Continuity Management and Operational Resilience	Business Continuity Planning	3	√	√		√		√

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
BCR-05	Business Continuity Management and Operational Resilience	Documentation	3	√	√		√		√
BCR-06	Business Continuity Management and Operational Resilience	Business Continuity Exercises	3	√	√		√		√
BCR-07	Business Continuity Management and Operational Resilience	Communication	2	√	√				
BCR-08	Business Continuity Management and Operational Resilience	Backup	4	√	√		√		√
BCR-09	Business Continuity Management and Operational Resilience	Disaster Response Plan	3	√	√				
BCR-10	Business Continuity Management and Operational Resilience	Response Plan Exercise	3	√	√				
BCR-11	Business Continuity Management and Operational Resilience	Equipment Redundancy	2	√					
CCC-01	Change Control and Configuration Management	Change Management Policy and Procedures	3	√	√		√	√	√
CCC-02	Change Control and Configuration Management	Quality Testing	4	√	√		√	√	√
CCC-03	Change Control and Configuration Management	Change Management Technology	3	√	√		√	√	√
CCC-04	Change Control and Configuration Management	Unauthorized Change Protection	4	√	√		√	√	√
CCC-05	Change Control and Configuration Management	Change Agreements	3	√	√		√	√	√
CCC-06	Change Control and Configuration Management	Change Management Baseline	2	√	√			√	
CCC-07	Change Control and Configuration Management	Detection of Baseline Deviation	4	√	√		√	√	√

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	**Control Domain**	**Control Title**		**Part 2-1**	**Part 2-4**	**Part 3-2**	**Part 3-3**	**Part 4-1**	**Part 4-2**
CCC-08	Change Control and Configuration Management	Exception Management	3	√	√			√	
CCC-09	Change Control and Configuration Management	Change Restoration	4	√	√		√		√
CEK-01	Cryptography, Encryption & Key Management	Encryption and Key Management Policy and Procedures	4	√	√		√	√	√
CEK-02	Cryptography, Encryption & Key Management	CEK Roles and Responsibilities	4	√	√		√	√	√
CEK-03	Cryptography, Encryption & Key Management	Data Encryption	4	√	√		√	√	√
CEK-04	Cryptography, Encryption & Key Management	Encryption Algorithm	4	√	√		√	√	√
CEK-05	Cryptography, Encryption & Key Management	Encryption Change Management	4	√	√		√		√
CEK-06	Cryptography, Encryption & Key Management	Encryption Change Cost Benefit Analysis	0						
CEK-07	Cryptography, Encryption & Key Management	Encryption Risk Management	2	√	√	√			
CEK-08	Cryptography, Encryption & Key Management	CSC Key Management Capability	0						
CEK-09	Cryptography, Encryption & Key Management	Encryption and Key Management Audit	2	√				√	
CEK-10	Cryptography, Encryption & Key Management	Key Generation	4	√	√		√	√	√
CEK-11	Cryptography, Encryption & Key Management	Key Purpose	4	√	√		√	√	√
CEK-12	Cryptography, Encryption & Key Management	Key Rotation	3	√	√		√	√	√
CEK-13	Cryptography, Encryption & Key Management	Key Revocation	3	√	√		√	√	√
CEK-14	Cryptography, Encryption & Key Management	Key Destruction	4	√	√		√	√	√
CEK-15	Cryptography, Encryption & Key Management	Key Activation	4	√	√		√	√	√
CEK-16	Cryptography, Encryption & Key Management	Key Suspension	4	√	√		√	√	√
CEK-17	Cryptography, Encryption & Key Management	Key Deactivation	4	√	√		√	√	√
CEK-18	Cryptography, Encryption & Key Management	Key Archival	4	√	√		√	√	√
CEK-19	Cryptography, Encryption & Key Management	Key Compromise	4	√	√		√	√	√
CEK-20	Cryptography, Encryption & Key Management	Key Recovery	4	√	√		√	√	√
CEK-21	Cryptography, Encryption & Key Management	Key Inventory Management	4	√	√		√	√	√
DCS-01	Datacenter Security	Off-Site Equipment Disposal Policy and Procedures	4	√	√		√	√	√

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	**Control Domain**	**Control Title**		**Part 2-1**	**Part 2-4**	**Part 3-2**	**Part 3-3**	**Part 4-1**	**Part 4-2**
DCS-02	Datacenter Security	Off-Site Transfer Authorization Policy and Procedures	2	√	√				
DCS-03	Datacenter Security	Secure Area Policy and Procedures	2	√				√	
DCS-04	Datacenter Security	Secure Media Transportation Policy and Procedures	2	√	√				
DCS-05	Datacenter Security	Assets Classification	4	√	√		√		√
DCS-06	Datacenter Security	Assets Cataloguing and Tracking	4	√	√		√		√
DCS-07	Datacenter Security	Controlled Access Points	1	√					√
DCS-08	Datacenter Security	Equipment Identification	4	√	√		√	√	√
DCS-09	Datacenter Security	Secure Area Authorization	2	√					
DCS-10	Datacenter Security	Surveillance System	2	√					
DCS-11	Datacenter Security	Unauthorized Access Response Training	1					√	
DCS-12	Datacenter Security	Cabling Security	3	√	√		√		√
DCS-13	Datacenter Security	Environmental Systems	2	√		√	√		√
DCS-14	Datacenter Security	Secure Utilities	2	√		√	√		√
DCS-15	Datacenter Security	Equipment Location	0						
DSP-01	Data Security and Privacy Lifecycle Management	Security and Privacy Policy and Procedures	3	√	√		√		√
DSP-02	Data Security and Privacy Lifecycle Management	Secure Disposal	4	√	√		√	√	√
DSP-03	Data Security and Privacy Lifecycle Management	Data Inventory	2	√					
DSP-04	Data Security and Privacy Lifecycle Management	Data Classification	2	√					
DSP-05	Data Security and Privacy Lifecycle Management	Data Flow Documentation	4	√	√	√	√	√	√
DSP-06	Data Security and Privacy Lifecycle Management	Data Ownership and Stewardship	3	√	√	√			

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
DSP-07	Data Security and Privacy Lifecycle Management	Data Protection by Design and Default	4					√	
DSP-08	Data Security and Privacy Lifecycle Management	Data Privacy by Design and Default	0						
DSP-09	Data Security and Privacy Lifecycle Management	Data Protection Impact Assessment	3	√	√			√	
DSP-10	Data Security and Privacy Lifecycle Management	Sensitive Data Transfer	2	√	√	√	√	√	√
DSP-11	Data Security and Privacy Lifecycle Management	Personal Data Access, Reversal, Rectification and Deletion	0						
DSP-12	Data Security and Privacy Lifecycle Management	Limitation of Purpose in Personal Data Processing	0						
DSP-13	Data Security and Privacy Lifecycle Management	Personal Data Sub-processing	0						
DSP-14	Data Security and Privacy Lifecycle Management	Disclosure of Data Sub-processors	0						
DSP-15	Data Security and Privacy Lifecycle Management	Limitation of Production Data Use	2	√	√		√	√	√
DSP-16	Data Security and Privacy Lifecycle Management	Data Retention and Deletion	4	√	√	√	√	√	√
DSP-17	Data Security and Privacy Lifecycle Management	Sensitive Data Protection	4	√	√		√	√	√
DSP-18	Data Security and Privacy Lifecycle Management	Disclosure Notification	0						
DSP-19	Data Security and Privacy Lifecycle Management	Data Location	1			√		√	
GRC-01	Governance, Risk and Compliance	Governance Program Policy and Procedures	2	√				√	
GRC-02	Governance, Risk and Compliance	Risk Management Program	3	√	√	√			
GRC-03	Governance, Risk and Compliance	Organizational Policy Reviews	4	√					

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
GRC-04	Governance, Risk and Compliance	Policy Exception Process	2	√				√	
GRC-05	Governance, Risk and Compliance	Information Security Program	2	√				√	
GRC-06	Governance, Risk and Compliance	Governance Responsibility Model	4	√	√				
GRC-07	Governance, Risk and Compliance	Information System Regulatory Mapping	3	√	√	√		√	
GRC-08	Governance, Risk and Compliance	Special Interest Groups	0						
HRS-01	Human Resources	Background Screening Policy and Procedures	3	√	√				
HRS-02	Human Resources	Acceptable Use of Technology Policy and Procedures	0						
HRS-03	Human Resources	Clean Desk Policy and Procedures	2	√	√	√	√	√	√
HRS-04	Human Resources	Remote and Home Working Policy and Procedures	2	√	√		√		√
HRS-05	Human Resources	Asset returns	0						
HRS-06	Human Resources	Employment Termination	0						
HRS-07	Human Resources	Employment Agreement Process	1	√	√				
HRS-08	Human Resources	Employment Agreement Content	2	√	√				
HRS-09	Human Resources	Personnel Roles and Responsibilities	3	√	√			√	
HRS-10	Human Resources	Non-Disclosure Agreements	2	√	√			√	
HRS-11	Human Resources	Security Awareness Training	4	√	√			√	
HRS-12	Human Resources	Personal and Sensitive Data Awareness and Training	3	√	√			√	
HRS-13	Human Resources	Compliance User Responsibility	3	√	√			√	
IAM-01	Identity & Access Management	Identity and Access Management Policy and Procedures	4	√	√		√	√	√
IAM-02	Identity & Access Management	Strong Password Policy and Procedures	4	√	√		√	√	√
IAM-03	Identity & Access Management	Identity Inventory	4	√	√		√		√
IAM-04	Identity & Access Management	Separation of Duties	4	√	√		√	√	√
IAM-05	Identity & Access Management	Least Privilege	4	√	√		√	√	√
IAM-06	Identity & Access Management	User Access Provisioning	4	√	√		√		√
IAM-07	Identity & Access Management	User Access Changes and Revocation	4	√	√		√		√

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
IAM-08	Identity & Access Management	User Access Review	4	√	√		√		√
IAM-09	Identity & Access Management	Segregation of Privileged Access Roles	2	√			√	√	√
IAM-10	Identity & Access Management	Management of Privileged Access Roles	2	√	√		√	√	√
IAM-11	Identity & Access Management	CSCs Approval for Agreed Privileged Access Roles	0						
IAM-12	Identity & Access Management	Safeguard Logs Integrity	4	√	√		√	√	√
IAM-13	Identity & Access Management	Uniquely Identifiable Users	4	√	√		√		√
IAM-14	Identity & Access Management	Strong Authentication	4	√	√		√	√	√
IAM-15	Identity & Access Management	Passwords Management	4	√	√		√	√	√
IAM-16	Identity & Access Management	Authorization Mechanisms	3	√	√		√	√	√
IPY-01	Interoperability & Portability	Interoperability and Portability Policy and Procedures	1	√			√		
IPY-02	Interoperability & Portability	Application Interface Availability	0						
IPY-03	Interoperability & Portability	Secure Interoperability and Portability Management	4	√	√		√	√	√
IPY-04	Interoperability & Portability	Data Portability Contractual Obligations	0					√	
IVS-01	Infrastructure & Virtualization Security	Infrastructure and Virtualization Security Policy and Procedures	2	√				√	
IVS-02	Infrastructure & Virtualization Security	Capacity and Resource Planning	3	√			√		√
IVS-03	Infrastructure & Virtualization Security	Network Security	4	√	√		√		√
IVS-04	Infrastructure & Virtualization Security	OS Hardening and Base Controls	3	√	√		√	√	√
IVS-05	Infrastructure & Virtualization Security	Production and Non-Production Environments	0						
IVS-06	Infrastructure & Virtualization Security	Segmentation and Segregation	0						
IVS-07	Infrastructure & Virtualization Security	Migration to Cloud Environments	4	√	√				
IVS-08	Infrastructure & Virtualization Security	Network Architecture Documentation	4	√	√	√	√	√	√
IVS-09	Infrastructure & Virtualization Security	Network Defense	4	√	√		√		√
LOG-01	Logging and Monitoring	Logging and Monitoring Policy and Procedures	4	√	√				
LOG-02	Logging and Monitoring	Audit Logs Protection	4	√	√		√		√
LOG-03	Logging and Monitoring	Security Monitoring and Alerting	4	√	√		√		√

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
LOG-04	Logging and Monitoring	Audit Logs Access and Accountability	4	√	√		√		√
LOG-05	Logging and Monitoring	Audit Logs Monitoring and Response	4	√	√		√		√
LOG-06	Logging and Monitoring	Clock Synchronization	4	√	√		√		√
LOG-07	Logging and Monitoring	Logging Scope	4	√	√		√		√
LOG-08	Logging and Monitoring	Log Records	4	√	√		√		√
LOG-09	Logging and Monitoring	Log Protection	4	√	√		√	√	√
LOG-10	Logging and Monitoring	Encryption Monitoring and Reporting	4	√	√		√	√	√
LOG-11	Logging and Monitoring	Transaction/Activity Logging	4	√	√		√	√	√
LOG-12	Logging and Monitoring	Access Control Logs	2	√					
LOG-13	Logging and Monitoring	Failures and Anomalies Reporting	3	√	√		√		
SEF-01	Security Incident Management, E-Discovery, & Cloud Forensics	Security Incident Management Policy and Procedures	3	√	√		√	√	√
SEF-02	Security Incident Management, E-Discovery, & Cloud Forensics	Service Management Policy and Procedures	4	√	√		√	√	√
SEF-03	Security Incident Management, E-Discovery, & Cloud Forensics	Incident Response Plans	3	√	√		√	√	√
SEF-04	Security Incident Management, E-Discovery, & Cloud Forensics	Incident Response Testing	0						
SEF-05	Security Incident Management, E-Discovery, & Cloud Forensics	Incident Response Metrics	0						
SEF-06	Security Incident Management, E-Discovery, & Cloud Forensics	Event Triage Processes	3	√	√		√	√	√
SEF-07	Security Incident Management, E-Discovery, & Cloud Forensics	Security Breach Notification	3	√	√				
SEF-08	Security Incident Management, E-Discovery, & Cloud Forensics	Points of Contact Maintenance	2	√	√				
STA-01	Supply Chain Management, Transparency, and Accountability	SSRM Policy and Procedures	3	√	√				

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
STA-02	Supply Chain Management, Transparency, and Accountability	SSRM Supply Chain	3	√	√				
STA-03	Supply Chain Management, Transparency, and Accountability	SSRM Guidance	2	√	√				
STA-04	Supply Chain Management, Transparency, and Accountability	SSRM Control Ownership	2	√	√				
STA-05	Supply Chain Management, Transparency, and Accountability	SSRM Documentation Review	3	√	√				
STA-06	Supply Chain Management, Transparency, and Accountability	SSRM Control Implementation	3	√	√				
STA-07	Supply Chain Management, Transparency, and Accountability	Supply Chain Inventory	1	√					
STA-08	Supply Chain Management, Transparency, and Accountability	Supply Chain Risk Management	1	√				√	
STA-09	Supply Chain Management, Transparency, and Accountability	Primary Service and Contractual Agreement	1	√					
STA-10	Supply Chain Management, Transparency, and Accountability	Supply Chain Agreement Review	1	√					
STA-11	Supply Chain Management, Transparency, and Accountability	Internal Compliance Testing	1	√					
STA-12	Supply Chain Management, Transparency, and Accountability	Supply Chain Service Agreement Compliance	2	√	√			√	
STA-13	Supply Chain Management, Transparency, and Accountability	Supply Chain Governance Review	1	√				√	
STA-14	Supply Chain Management, Transparency, and Accountability	Supply Chain Data Security Assessment	1	√					
TVM-01	Threat & Vulnerability Management	Threat and Vulnerability Management Policy and Procedures	4	√	√			√	
TVM-02	Threat & Vulnerability Management	Malware Protection Policy and Procedures	4	√	√		√	√	√

Cloud Security Alliance – Cloud Control Matrix v4.03			Difference Level	ISA/IEC 62443					
Control ID	Control Domain	Control Title		Part 2-1	Part 2-4	Part 3-2	Part 3-3	Part 4-1	Part 4-2
TVM-03	Threat & Vulnerability Management	Vulnerability Remediation Schedule	4	√	√			√	
TVM-04	Threat & Vulnerability Management	Detection Updates	4	√	√		√		√
TVM-05	Threat & Vulnerability Management	External Library Vulnerabilities	2	√				√	
TVM-06	Threat & Vulnerability Management	Penetration Testing	2					√	
TVM-07	Threat & Vulnerability Management	Vulnerability Identification	3	√	√			√	
TVM-08	Threat & Vulnerability Management	Vulnerability Prioritization	3	√	√			√	√
TVM-09	Threat & Vulnerability Management	Vulnerability Management Reporting	3	√	√			√	
TVM-10	Threat & Vulnerability Management	Vulnerability Management Metrics	1						
UEM-01	Universal Endpoint Management	Endpoint Devices Policy and Procedures	3	√	√		√		√
UEM-02	Universal Endpoint Management	Application and Service Approval	3	√	√		√	√	√
UEM-03	Universal Endpoint Management	Compatibility	3	√	√		√	√	√
UEM-04	Universal Endpoint Management	Endpoint Inventory	4	√	√				
UEM-05	Universal Endpoint Management	Endpoint Management	3	√	√		√	√	√
UEM-06	Universal Endpoint Management	Automatic Lock Screen	4	√	√		√		√
UEM-07	Universal Endpoint Management	Operating Systems	4	√	√			√	
UEM-08	Universal Endpoint Management	Storage Encryption	4	√	√		√		√
UEM-09	Universal Endpoint Management	Anti-Malware Detection and Prevention	4	√	√		√		√
UEM-10	Universal Endpoint Management	Software Firewall	2	√	√		√	√	√
UEM-11	Universal Endpoint Management	Data Loss Prevention	2		√				
UEM-12	Universal Endpoint Management	Remote Locate	0						
UEM-13	Universal Endpoint Management	Remote Wipe	3	√	√		√	√	√
UEM-14	Universal Endpoint Management	Third-Party Endpoint Security Posture	4	√	√		√		√

Annex C – Terms, Definitions and Abbreviations

C.1 Terms and Definitions

C.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 ISA/IEC 62443-1-1]

C.1.2
Automation Solution
control system and any complementary hardware and software components that have been installed and configured to operate in an IACS

Note 1 to entry: Automation Solution is used as a proper noun in this part of ISA/IEC 62443-2-1

Note 2 to entry: the difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (for example, a specific number of workstations, controllers and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: the Automation Solution may be comprised of components from multiple suppliers, including the product supplier of the control system.

[SOURCE: ISA/IEC 62443-2-1]

C.1.3
capability security level
security level that a component or system can provide when properly configured and integrated

Note 1 to entry: 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 ISA/IEC 62443-3-3 A.2.2]

C.1.4
certification scheme
certification system related to specified products, to which the same specified requirements, specific rules and procedures apply

Note 1 to entry: 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 to entry: the rules, procedures and management for implementing product, process and service certification are stipulated by the certification scheme.

[SOURCE ISO/IEC 17065, notes adapted]

C.1.5
certification scheme owner
person or organization responsible for developing and maintaining a specific certification scheme

[SOURCE ISO/IEC 17065]

C.1.6
cloud
collection of networked remote servers

Note 1 to entry: the use of the term “cloud” in this report includes public or private deployment models.

[SOURCE IEC 20294:2018, 3.5.8]

C.1.7
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand

Note 1 to entry: examples of resources include servers, operating systems, networks, software, applications and storage equipment.

Note 2 to entry: self-service provisioning refers to the provisioning of resources provided to cloud services (3.1.2) performed by cloud service customers (3.3.2)

[SOURCE: ISO/IEC 17788:2014, 3.2.5 cloud computing with notes added from ISO/IEC 22123:2023(en)]

C.1.8
cloud service
one or more capabilities offered via cloud computing invoked using a defined interface

Note 1 to entry: capabilities of computing can include infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) for cloud-based infrastructure, application, security and storage services

[SOURCE: ISO/IEC 17788:2014, 3.2.8 cloud service with Note 1 added from 3.2.15]

C.1.9
cloud service customer
party which is in a business relationship for the purpose of using cloud services

[SOURCE: ISO/IEC 17788:2014]

C.1.10
cloud service provider
party that makes cloud-based services available

[SOURCE: ISO/IEC 17788:2014, 3.2.15]

Note 1 to entry: the term “cloud provider” is used in this report instead of cloud service provider to distinguish between the cloud provider role and the service provider role defined in ISA/IEC 62443-2-4.

C.1.11
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 ISA/IEC 62443-4-2]

C.1.12

control system

hardware and software components of an IACS

Note 1 to entry: control systems include systems that perform monitoring functions.

[SOURCE ISA/IEC 62443-4-2, with note from [SSA-100]

C.1.13

edge

the part of an IIoT system that is close to the data sources and not in the cloud (on premises)

Note 1 to entry: “the edge” includes IIoT components such as gateways, sensors, controllers, actuators and edge computing such as distributed computing and data storage. Edge devices are geographically and logically located on-premises and near the data sources (*e.g.*, sensors, controllers, actuators)

C.1.14

edge computing

distributed computing paradigm that brings computation and data storage closer to the sources of data

C.1.15

embedded device

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

Note 1 to entry: 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 (*e.g.*, PLC, field sensor devices, SIS controller, DCS controller).

[SOURCE ISA/IEC 62443-4-2]

C.1.16

equipment under control

equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical or other activities

[SOURCE ISA/IEC 62443-1-1]

C.1.17

essential function

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

Note 1 to entry: 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 ISA/IEC 62443-4-2]

C.1.18

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 1 to entry: typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (*e.g.*, keyboard, mouse, etc.).

[SOURCE ISA/IEC 62443-4-2]

C.1.19

industrial internet of things (IIoT)

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

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

C.1.20

IIoT Automation Solution

an Automation Solution that uses cloud-based functionality

C.1.21

IIoT component

component with the capability to communicate with cloud-based services over an untrusted network

C.1.22

IIoT device

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

Note 1 to entry: an IIoT device can be a sensor or an actuator, or may communicate with sensors or actuators.

Note 2 to entry: 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 to entry: 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 to entry: 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."

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

C.1.23

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 to entry: from Industrial Internet Consortium IIoT volume G1 reference architecture: The proximity network connects the sensors, actuators, devices, control systems and assets, collectively called edge nodes.

Note 2 to entry: the access network may be the Internet or other network judged insecure. Functions hosted on an IIoT gateway may also include data translation, processing, and control.

Note 3 to entry: an IIoT gateway device is a type of network device (see 3.1.30).

Note 4 to entry: 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.

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

C.1.24
IIoT IACS
industrial automation and control system that uses cloud-based functionality

C.1.25
IIoT system
system providing functionalities of industrial internet of things

Note 1 to entry: IIoT system is inclusive of IIoT devices, IIoT gateways, sensors, actuators and cloud-based IIoT functionality.

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

C.1.26
industrial automation and control system (IACS)
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 ISA/IEC 62443-4-2]

C.1.27
infrastructure as a service (IaaS)
cloud services category in which the cloud service customer can provision and use processing, storage or networking resources

[SOURCE: adapted from ISO/IEC 22428-1:2020]

C.1.28
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 1 to entry: typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

[SOURCE ISA/IEC 62443-4-2]

C.1.29
non-essential function
a function that is not an essential function

C.1.30

operational technology as a service (OTaaS)

cloud service category in which the cloud service customer can directly or indirectly change the physical state of the equipment under control.

C.1.31

platform as a service (PaaS)

cloud service category in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud provider

[SOURCE: adapted from ISO/IEC 22428-1:2020]

C.1.32

private cloud

cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer

[SOURCE: ISO/IEC 22428-1:2020]

C.1.33

product supplier

manufacturer of hardware or software product used in an IACS

[SOURCE 62443-2-1]

C.1.34

public cloud

cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud provider

[SOURCE: ISO/IEC 22428-1:2020]

C.1.35

security level

measure of confidence that the system under consideration, security zone or conduit is free from vulnerabilities and functions in the intended manner

Note 1 to entry: there are three types of security levels: capability security level (SL-C), target security level (SL-T) and achieved security level (SL-A).

[SOURCE ISA/IEC 62443-3-2 Annex A]

C.1.36

security zone

grouping of logical or physical assets that share common security requirements

Note 1 to entry: 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 ISA/IEC 62443-3-3]

C.1.37

sensor and actuator

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

[SOURCE ISA/IEC 62443-1-1 modified]

C.1.38

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 to entry: software applications typically execute on host devices or embedded devices.

Note 2 to entry: 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.

C.1.39

software as a service (SaaS)

cloud service category in which the cloud service customer can use the cloud provider's applications

[SOURCE: adapted from ISO/IEC 22428-1:2020]

C.1.40

system under consideration (SuC)

defined collection of IACS assets that are needed to provide a complete automation solution including any relevant network infrastructure assets

Note 1 to entry: a SuC consists of one or more zones and related conduits. All assets within an SuC belong to either a zone or conduit.

[SOURCE: ISA/IEC 62443-3-2]

C.1.41

target security level

desired security level for a particular IACS, zone or conduit

[SOURCE ISA/IEC 62443-3-2 Annex A]

C.1.42

update

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

[SOURCE ISA/IEC 62443-4-2]

C.1.43

upgrade

incremental hardware or software change in order to add new features

[SOURCE ISA/IEC 62443-4-2]

C.1.44

zone

see security zone

C.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
AO	asset owner
CSA	ISASecure Component Security Assurance
CSA	Cloud Security Alliance
CI/CD	continuous integration/continuous delivery
EuC	equipment under control (from ISA/IEC 62443-1-1)
HMI	human machine interface
IaaS	infrastructure as a service
IACS	industrial automation and control system(s)
ICSA	IIoT Component Security Assurance (from ISASecure)
IEC	International Electrotechnical Commission
IoT	internet of things
IIoT	industrial internet of things
ISA	International Society of Automation
ISAGCA	ISA Global Cybersecurity Alliance
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
MoC	management of change
NA or N/A	not applicable
NIST	National Institute of Standards and Technology
OS	operating system
OTaaS	operational technology as a service
PaaS	platform as a service
PLC	programmable logic controller
PS	product supplier
SaaS	software as a service
SCADA	supervisory control and data acquisition
SDLA	Security Development Lifecycle Assurance (from ISASecure)
SDN	software defined network
SL-C	capability security level
SL-T	target security level
SP	security program, service provider, special publication
SR	system requirement (from ISA/IEC 62443-3-3)
SR	specification of security requirements (from ISA/IEC 62443-4-1)
SSA	System Security Assurance (from ISASecure)
SUC	system under consideration (from ISA/IEC 62443-3-2)
ZCR	zone and conduit requirement (from ISA/IEC 62443-3-2)

Annex D – Bibliography

1. ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements
2. ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls
3. ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
4. ISO/IEC 27018:2019, Information technology – Security techniques – Code of practice for protection of personally identifiable information :2013(PII) in public clouds acting as PII processors
5. ISO/IEC 27036-1:2021, Cybersecurity – Supplier relationships – Part 1: Overview and concepts
6. ISO/IEC 27036-2:2022, Cybersecurity – Supplier relationships – Part 2: Requirements
7. ISO/IEC 27036-3:2023, Cybersecurity – Supplier relationships – Part 3: Guidelines for hardware, software, and services supply chain security
8. ISO/IEC 27036-4:2016, Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services
9. Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments, July 2021. ISA Global Cybersecurity Alliance
10. IIoT Component Certification Based on the 62443 Standard, October, 2021. ISA Global Cybersecurity Alliance
11. LOGIIC Project 12 Safety Instrumentation, April, 2021. Linking Oil and Gas Industry to Improve Cybersecurity
12. Cloud Security Alliance Cloud Controls Matrix, Version 4.0.3. Cloud Security Alliance
13. CISA Cloud Security Technical Reference Architecture, Version 1.0, August, 2021. US Cybersecurity & Infrastructure Security Agency
14. The Industrial Internet of Things, Volume G1: Reference Architecture, Version 1.9, June, 2019. Industrial Internet Consortium
15. The Industrial Internet of Things, Volume G4: Security Framework, September, 2016. Industrial Internet Consortium
16. The Industrial Internet of Things, Volume G8: Vocabulary, Version 3.0, March, 2022. Industrial Internet Consortium
17. Key Safety Challenges for the IIoT, Version 1.0, December, 2017. Industrial Internet Consortium.
18. Industrial IoT Architecture Patterns. AWS, December 17, 2021
19. Microsoft Azure IoT Reference Architecture. Version 2.1, September, 2018

20. IoT Security Standards Gap Analysis. Enisa, Version 1, January, 2019

21. Design Patterns for the Industrial Internet of Things. Gedare Bloom, Bassma Alsulami, Ebelechukwu Nwafor, Ivan Cibrario Bertolotti. IEEE 2018

Founded by the International Society of Automation (ISA), the **ISASecure** certification program certifies conformance to the ISA/IEC 62443 series of internationally adopted industrial security standards.

ISASecure assesses automation and control products and systems to ensure they are robust against network attacks, free from known vulnerabilities and meet the security capabilities defined in the ISA/IEC 62443 standards.

All ISASecure certifications are conducted by globally recognized ISO/IEC 17065 accredited certification bodies.

The **ISA Global Cybersecurity Alliance** (ISAGCA) is a collaborative forum to advance OT cybersecurity awareness, education, readiness, standardization, and knowledge sharing.

ISAGCA is made up of 50+ member companies and industry groups, representing more than $1.5 trillion in aggregate revenue across more than 2,400 combined worldwide locations.

Automation and cybersecurity provider members serve 31 different industries, underscoring the broad applicability of the ISA/IEC 62443 series of standards.

ISASecure®

ISA GLOBAL CYBERSECURITY ALLIANCE

International Society of Automation
3252 S. Miami Blvd., #102
Durham, NC 27703

www.isasecure.org
www.isagca.org

06-0524