The webinar will start at 11am (Eastern Time)

Simplify Procurement and Increase Automation and Control Security with IEC 62443 Certifications

An ISASecure End User Perspective

Kenny Mesker

Board Chair, ISASecure

ISASecure®

About Me

- Board Chair, ISASecure
- Chevron Enterprise OT Cybersecurity Architect and Distinguished Engineer, PCN/SCADA
- Member (former Chair) AFPM Cybersecurity Sub-committee
- ISA99 WG4 TG3
- Texas A&M Electrical Engineering

Overview

The quest of using certification to make the process of realizing efficient risk management by leveraging certification to enhance procurement and supply chain management (SCM) processes is based on three foundations:

- Established legitimacy of certification
  - Who publishes it?
  - Who conducts it?
  - Who awards it?
  - Do I trust them?
- Aligned internal goals of asset owning organization with certification
  - Are the goals of the certification the same as the goals of my organization?
- Encouraging certification as means of procurement value differentiation
  - Does the certification make the procurement or SCM process more efficient?
  - Create more value?
  - Increase cybersecurity assurance?
  - Provide automation opportunities?

ISASecure®

ISA99 Global Standards Committee

- The ISA99 committee was **formed in 2002** to define what is required to secure automation and control systems. For several years the committee has been working closely with technical committee 65 of the International Electrotechnical Commission (IEC) to develop and deliver the ISA/IEC 62443 series of standards that provide requirements and guidance in this area.

- The majority of standards in this series are now available, representing **over 500 normative requirements** and associated rationale that address all phases of the system life cycle, from development and delivery to operation and support.

- The **committee has over 1000 members,** representing a wide range of industry sectors and constituency groups from all areas of the world. Collectively this represents one of the largest and most diverse bodies of expertise in the subject of operations cybersecurity.

- While the committee's primary purpose is the development and enhancement of the ISA/IEC 62443 standards, it also includes work groups devoted to promoting increased awareness, promotion and adoption of proven and effective practices. This is further extended in the form of several **formal and informal liaison relationships with** other standards development organizations, consortia and interest groups such as ISASecure and ISAGCA.

- The ISA99 committee is **willing to engage with sector, industry, government and company programs** in their efforts to address automation systems cybersecurity. Those interested in pursuing such engagements are encouraged to contact the committee leadership at ISA99chair@gmail.com.

ISA/IEC 62443 Standards

General

ISA-62443-1-1	ISA-TR62443-1-2	ISA-62443-1-3	ISA-TR62443-1-4
Concepts and models	Master glossary of terms and abbreviations	System security conformance metrics	IACS security lifecycle and use-cases

Policies & Procedures

ISA-62443-2-1	ISA-62443-2-2	ISA-TR62443-2-3	ISA-62443-2-4	ISA-TR62443-2-5
Security program requirements for IACS asset owners	IACS protection levels	Patch management in the IACS environment	Requirements for IACS service providers	Implementation guidance for IACS asset owners

System

ISA-TR62443-3-1	ISA-62443-3-2	ISA-62443-3-3
Security technologies for IACS	Security risk assessment and system design	System security requirements and security levels

Component

ISA-62443-4-1	ISA-62443-4-2
Secure product development lifecycle requirements	Technical security requirements for IACS components

Status Key

- 💡 Development Planned
- ✏️ In Development
- 🔍 Out for Comment or Vote
- ☑ C Approved with comments
- ☑ Approved
- 📄 Published
- ➡️ Adopted
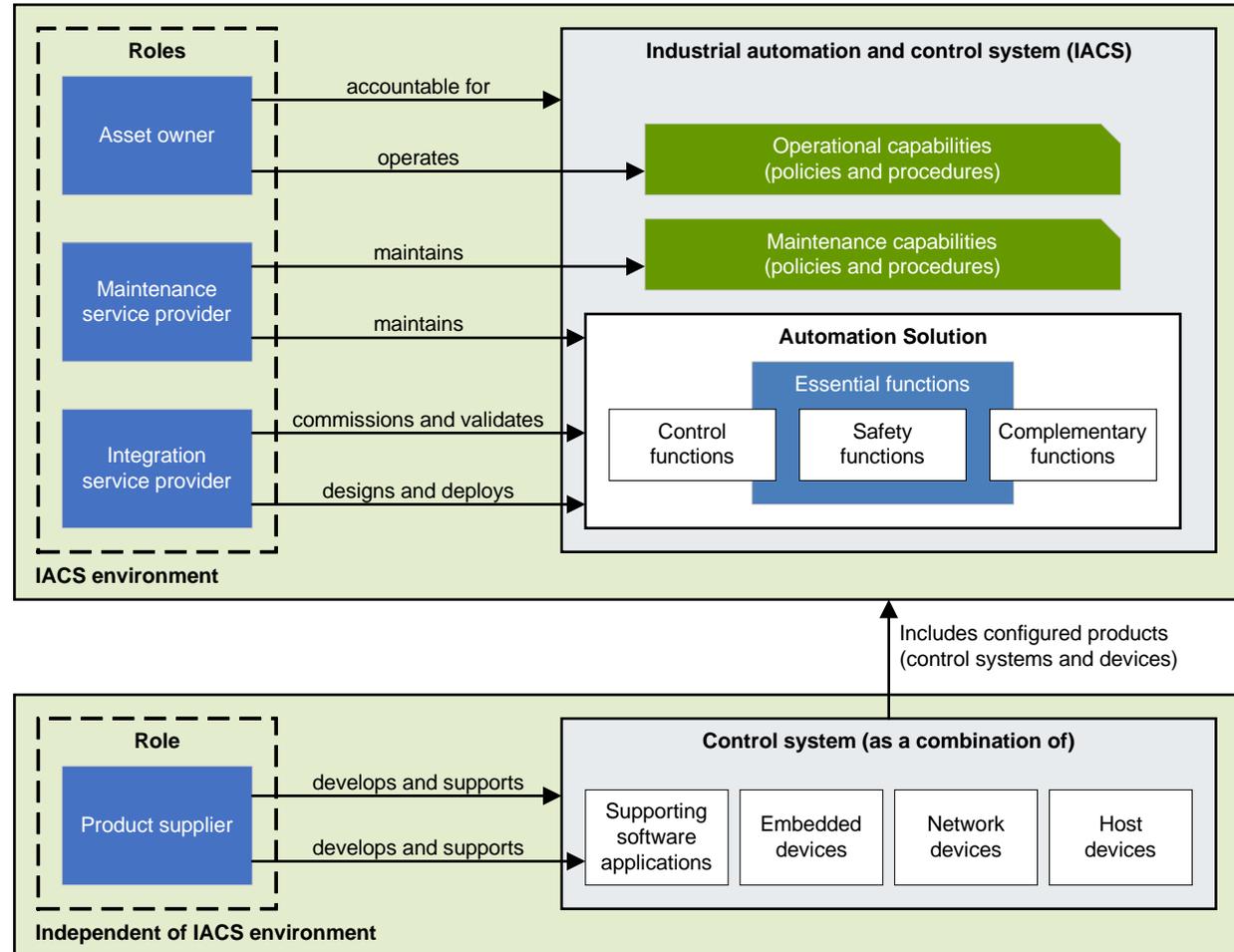- 🔍 Published (under revision)

ISA

ISA/IEC 62443 Automation Security Lifecycle
Usually in terms of developing, integrating, and operating...we're about to change that
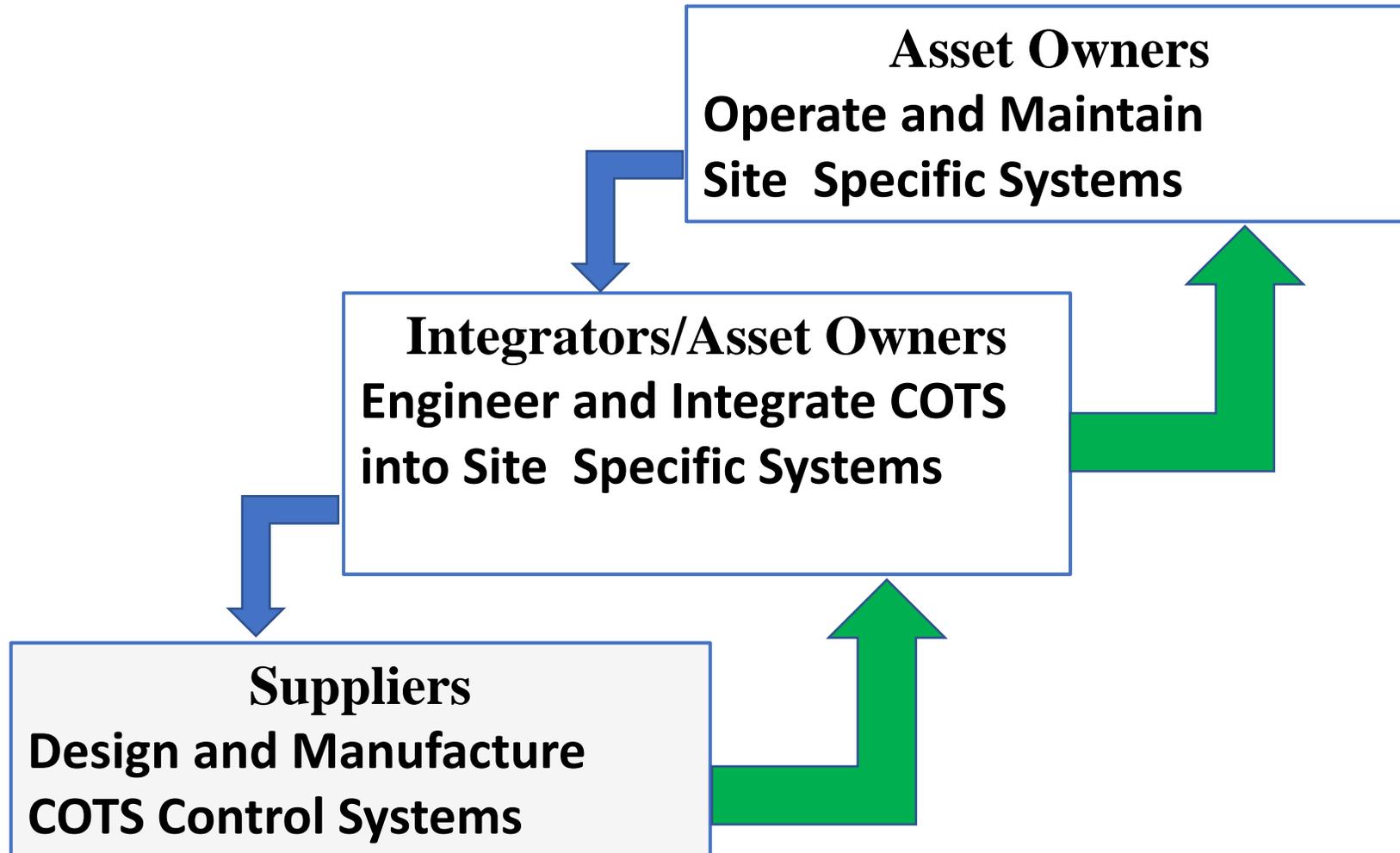
Stakeholder Roles, Responsibilities and relevant 62443 standards

- **Asset Owner**
  - Part 1-1 – Concepts and models
  - Part 2-1 – Security program requirements
  - Part 2-2 – Security protection rating
  - Part 2-3 – Patch management
  - Part 3-2 – Risk assessment and system design

- **Maintenance Service Provider**
  - Part 1-1 – Concepts and models
  - Part 2-4 – Service providers

- **Integration Service Provider**
  - Part 1-1 – Concepts and models
  - Part 2-4 – Service providers
  - Part 3-2 – Risk assessment and system design
  - Part 3-3 – System requirements and security levels

- **Product Supplier**
  - Part 1-1 – Concepts and models
  - Part 3-3 – System requirements and security levels
  - Part 4-1 – Security development lifecycle
  - Part 4-2 – Component requirements

ISASecure

Globally recognized ISA/IEC 62443 certification brand

- Started in 2007, first certification in 2011
- Certifies systems, components, development organizations
- Eight certification bodies around the globe
- Promotes adoption of ISA/IEC 62443 standards in collaboration with ISAGCA and ISA99 standards committee.
- OPAF agreement to use ISASecure scheme for assessing prototype components
- Can certify IOT components/devices today
- New certifications in development 1) IIOT system certification 2) facility certification for building management systems (BMS).

ISASecure supporters past and present

I'm sure you trust *someone* on this list

ISASecure Certification Bodies Internationally Accredited to ISO/IEC 17065 & ISO/IEC 17025

Supporting Accreditation Bodies

1. Singapore Accreditation Council - Singapore
2. ANSI/ANAB-North America
3. Japan Accreditation Board-Japan
4. DAkkS-Germany
5. RvA Dutch Accreditation Council - Netherlands

Certification Bodies

1. *CSSC - Japan*
2. *Exida – USA/Global*
3. *TUV Rheinland – Germany/Global*
4. *DNV GL – Singapore (in progress)*
5. *TUV SUD – Singapore (in progress)*
6. *Applied Risk – Netherlands/EU*
7. *Trusted Labs – Netherlands/EU*
8. *CSA Group – Canada/Global*

100% Aligned to ISA/IEC 62443 Standards

Process Certifications - Security Development Lifecycle Assurance **(SDLA)**
- Shows that a company has a documented process that complies ISA/IEC 62443-4-1 (Product Development Lifecycle Requirements)
- Shows that this process is being followed by that company for a sampling of products

Product (Component) Certifications – Component Security Assurance **(CSA)**
- Shows that a particular product is compliant with the requirements of ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 (Technical Security Requirements for IACS Components)
- ISASecure certifies 4 component categories described in the ISA/IEC 62443-4-2 standard including network devices, applications, embedded devices and host devices
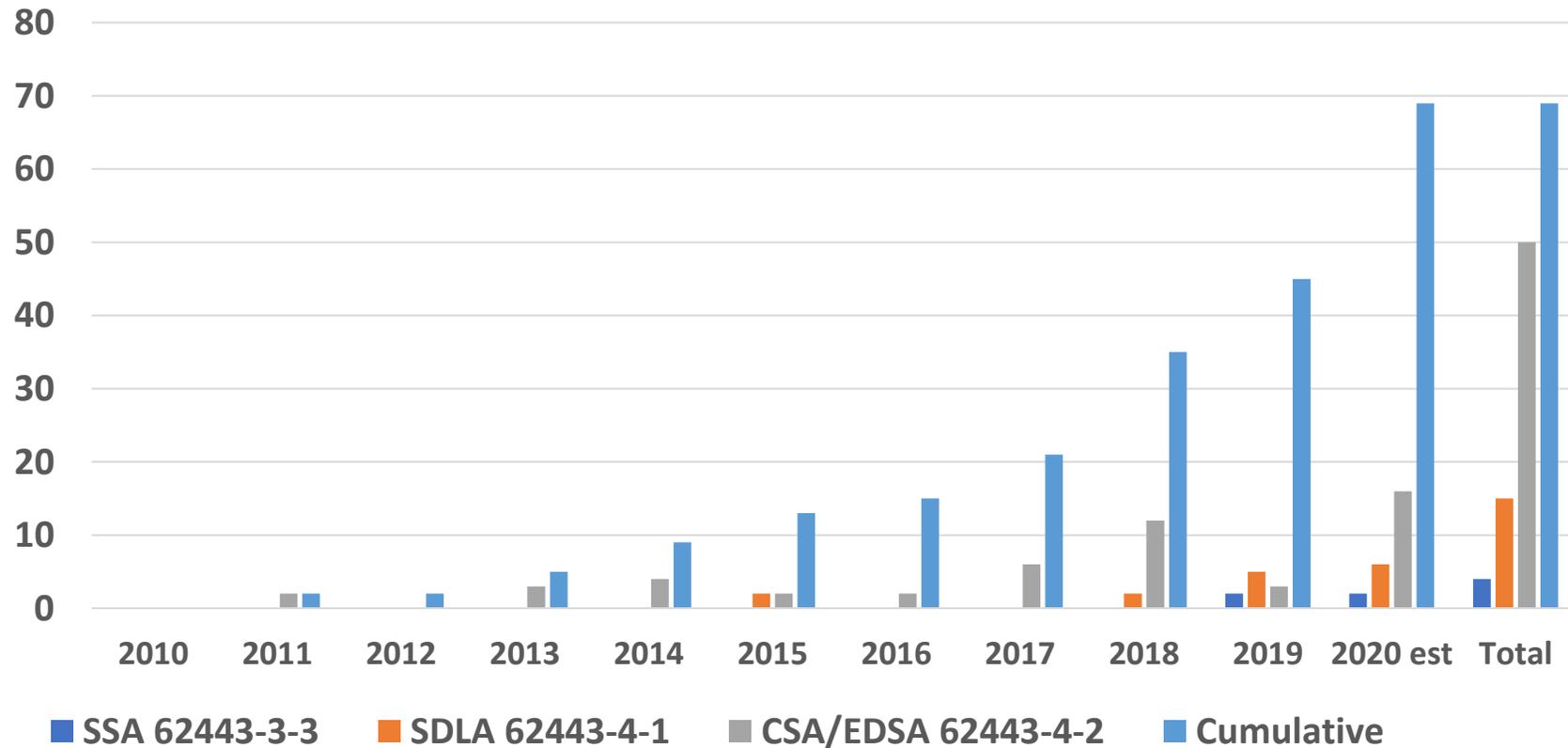
System Certifications - System Security Assurance **(SSA)**
- Shows that a system (collection of components) is compliant with the requirements ISA/IEC62443-4-1 and ISA/IEC 62443-3-3 (System Security Requirements and Security Levels)

ISASecure®

ISASecure Certification Growth

ISASecure Certifications by Year

Where Procurement Is Today

OT asset owner procurement organizations currently experience:

- Long cycle times
  - Between 30 and 300 days to complete risk analysis, alternatives analysis, and cybersecurity assurance
- Reliance on IT-oriented cybersecurity assurance requirements
- Increased cost due to laborious processes
  - Supplier burden to meet assurance requirements
  - Asset owner assessor burden to verify responses
- Low level of assurance due to lack of validation
- Very little automation – most of this is manual work

Let's look at each of these to see how certification adoption can improve the process.

ISASecure®

Long Cycle Times

Most organizations in the OT critical infrastructure verticals experience huge cycle times between RFI/RFP and purchase.

Problem:

- Suppliers generally are held responsible for completing lengthy and complex cybersecurity questionnaires.
- Internal assessments create churn as timing is based on availability of qualified assessors and recycle times to fill information gaps during assessment.

Solution:

- Replace cybersecurity questionnaires with recognition of certifications – such as ISASecure certification to IEC 62443.
- Internal assessment becomes the act of simply verifying certification is valid and maintained.
- Create supplier agility by reducing work burden associated with assurance.

ISASecure®

IT-oriented Cybersecurity Assurance Requirements

Most organizations have ubiquitous cybersecurity policy – even in OT environments – that is primarily aligned with IT requirements. **This will not change anytime soon.** However, it is still possible to realize the benefits of OT cybersecurity assurance in procurement processes.

Problem:
- IT standards and control sets are large and difficult to interpret in terms of OT requirements.
- Results in a very large set of requirements for suppliers to attest to, regardless of control set (NIST 800, ISO 2700x, etc).

Solution:
- Map internal IT cybersecurity assurance requirements to IEC 62443.
- Adopt IEC 62443 certification recognition as supplier attestation.
- Also allows reduction of relevant questions, even if supplier/system/components aren't certified, *so it's just a good idea in general*.

ISASecure®

Increased Cost Due to Laborious Processes

Cybersecurity assurance during procurement processes incurs cost – both obvious and hidden.

Problem:

- Internal assessments take time and resources. This is an obvious cost to the organization.
- Supplier responses take time and resources. This cost is likely to be reflected in product price. This is a hidden cost.

Solution:

- Adopt IEC 62443 certification recognition as supplier attestation so that suppliers can focus their spend on value: the certification.
- Internal assessments become, as previously noted, merely an exercise in certification validation.

ISASecure®

Low Level of Assurance Due to Lack of Validation

This is the most significant cost of antiquated procurement: the lack of true insight into whether risk has been reduced. How do you *know* that suppliers are applying the cybersecurity measures they attested to? FAT testing? SAT testing? Isn't that too late?

Problem:

- It is extremely difficult to validate that supplier responses are accurate. Or that the supplier interpreted the control language in the questionnaire the same way you did.
- How do you know your internal assessors interpreted the response correctly?

Solution:

- Certification levels the playing field and endorses a common set of expectations. Everyone is using the same rules.
- Adopting certification as an assurance mechanism transfers no risk to the supplier and reduces risk to the asset owner.

ISA**Secure**®

Very little automation – most of this is manual work

Is your organization undergoing a digital transformation? Even if you don't think it is, it likely is at least at some level. How do you think questionnaires and manual assessment processes look to the board?

Problem:
- Put simply, most procurement processes engage a low level of technology to make the process efficient.
- Multiple engagements with suppliers typically still require similarly lengthy processes, even if there is a prior relationship.
- One size fits none. Or at least so few as to essentially be none.

Solution:
- Certification recognition allows the creation of vendor and supplier approval lists that can form the foundation of automated vendor management systems (VMS). It becomes an exercise in maintaining the VMS rather than going back through "box checking" exercises.
- If integrated with risk management systems, the entire process of automating risk reduction during procurement can be automated.

ISASecure®

Where To Get More Information

- The ISASecure website:
    https://www.isasecure.org

- Procurement language:
    https://www.isasecure.org/en-US/Documents/ISCI-Certification-Addendum_Procurement-Language.docx

ISA Security Compliance Institute (ISCI) Certification Addendum

In accordance with IEC 62443, this addendum serves as the minimal requirements for any supplier providing network-connectable products and systems, as part of a contractual bid to COMPANY NAME, referred to as "The Procuring Organization" henceforth.

Background

The ISA Security Compliance Institute (ISCI), a not-for-profit automation controls industry consortium, manages the ISASecure conformance certification program. ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities.

The ISASecure designation is earned by industrial control suppliers for products that demonstrate adherence to industry consensus cyber security specifications for security characteristics and supplier development practices.

Certification Overview

ISCI offers three certifications with four security assurance levels (SAL) in alignment with ISA/IEC 62443. There is an expectation that any product and/or system meet the appropriate certification criteria summarized below. For more details and how to apply for certification, visit isasecure.org/en-US.

1. **ISASecure Component Security Assurance (CSA) Certification**

Component Security Assurance (CSA) focuses on the security of individual device characteristics and supplier development practices for those devices. The CSA certification is designed to certify to international standard IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development requirements and to the international standard IEC 62443-4-2 Security for industrial automation and control systems Part

ISASecure®

Please join us in securing automation that affects our every day lives.

Kenny Mesker

Board Chair, ISASecure

ISASecure®