DS Elektrodag

-fremtidssikret elnet

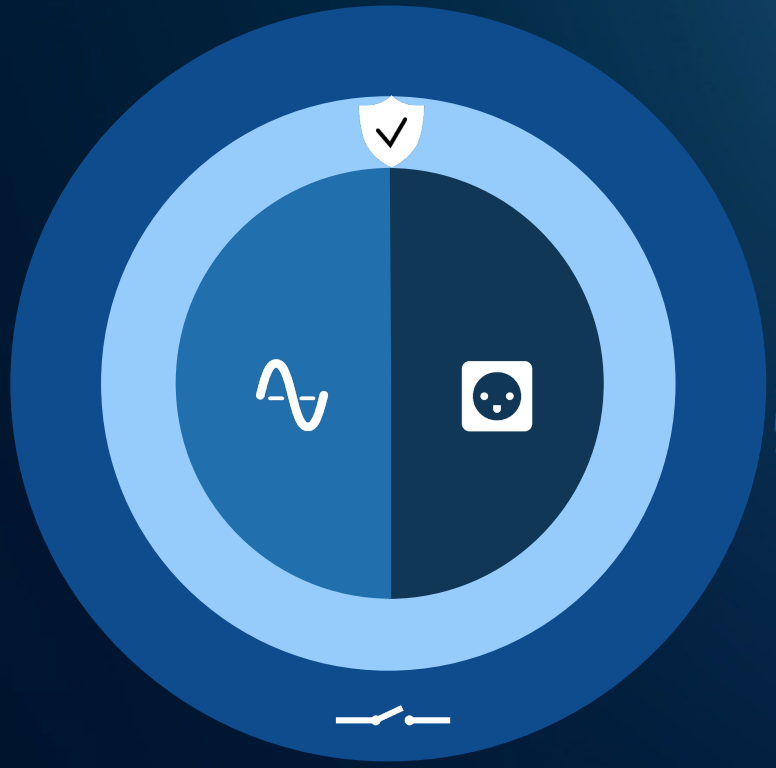
2. marts 2026

100 år

DANSK STANDARD

Fremtiden starter med standarder

DS Elektrodag
-fremtidssikret elnet



15.45 Beskyttelse af det fremtidssikrede elnet mod cyberangreb

v/ Jakob Kledal,

General Sales & Marketing Manager,
Hitachi Energy

DS
DANSK STANDARD

IEC 62443 - Industrial Control System Standards

Presented by Jakob Kledal Hub EU

H. Hadeli - Global Product Manager
Cybersecurity Solutions

Date
2026-02-26
Document ID: 8DAA008276 - Rev: A

Cybersecurity Risks in Critical Infrastructure

Why Control Systems Cybersecurity Matter?

Incidents remain high and disruptive.

More than one in five organizations (22%) reported a cybersecurity. Incident in the past year, with 40% causing operational disruption and nearly 20% taking over a month to remediate.

SANS State of ICS/OT Cybersecurity 2025

Digitalization, IT/OT Convergence

Off-the-shelf products

From proprietary to standardized protocols

Possible lateral access to OT systems via IT networks

Connectivity

Changing Threat Landscape

Hacktivists threat actors

AI-enabled attackers

Increased number of vulnerabilities

Geopolitical tensions drive sophisticated attacks

Regulation and Governance

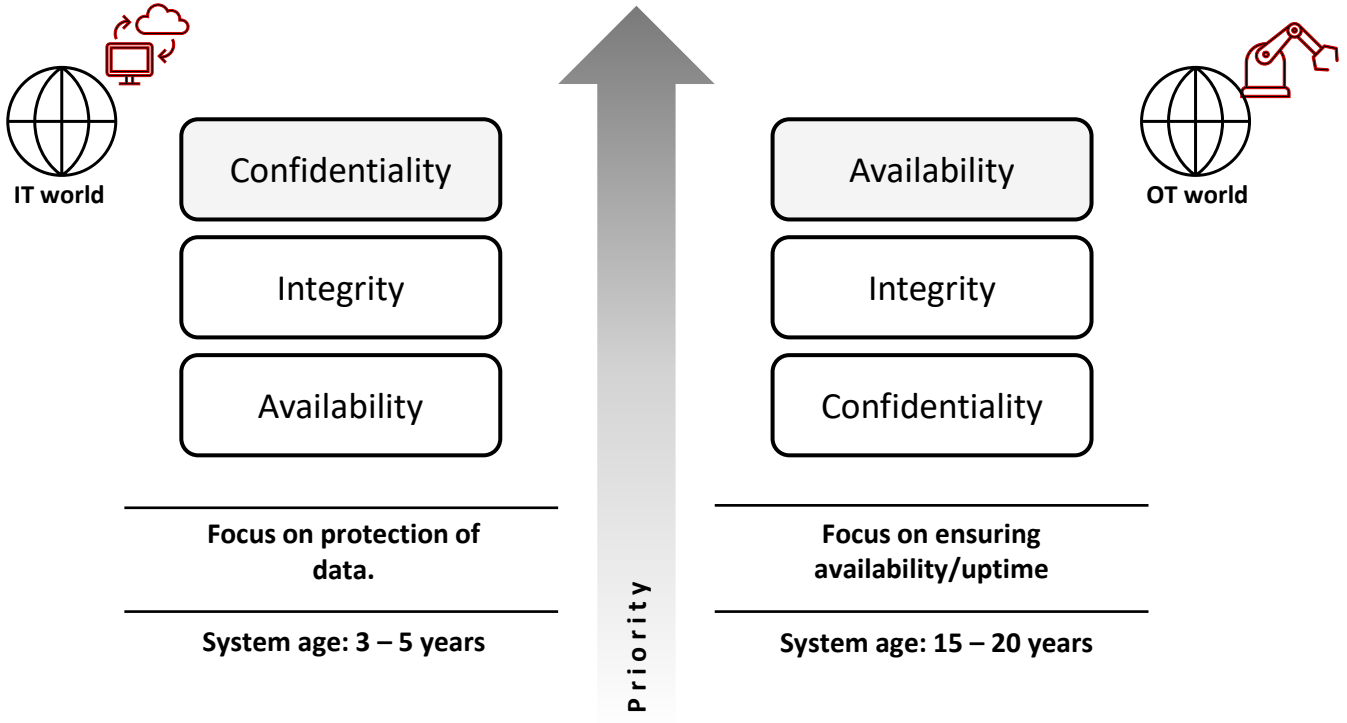
Regulatory bodies are raising the bar for critical system cybersecurity

Example, EU NIS2, EU CRA, US Cyber Incident Reporting for Critical Infrastructure Act, and many more across countries

Cybersecurity Objectives in IT vs. OT - Differences

Operational Technology (OT) environment or Industrial Control Systems (ICS) environment can affect the management of the cyber physical power system and can thus **affect safety and reliability**.

OT environment have different requirements and constraints when applying security measures to ensure that these **systems can continue to support the same power system safety and reliability levels.**



	Enterprise IT	Control Systems
Availability requirements	**95 – 99% (accept. downtime/year: 18.25 - 3.65 days)**	**99.9 – 99.999% (accept. downtime/year: 8.76 hrs – 5.25 minutes)**

OT system are built around a different set of challenges to ensure uninterrupted delivery of services

Vulnerability in Product with Digital Elements

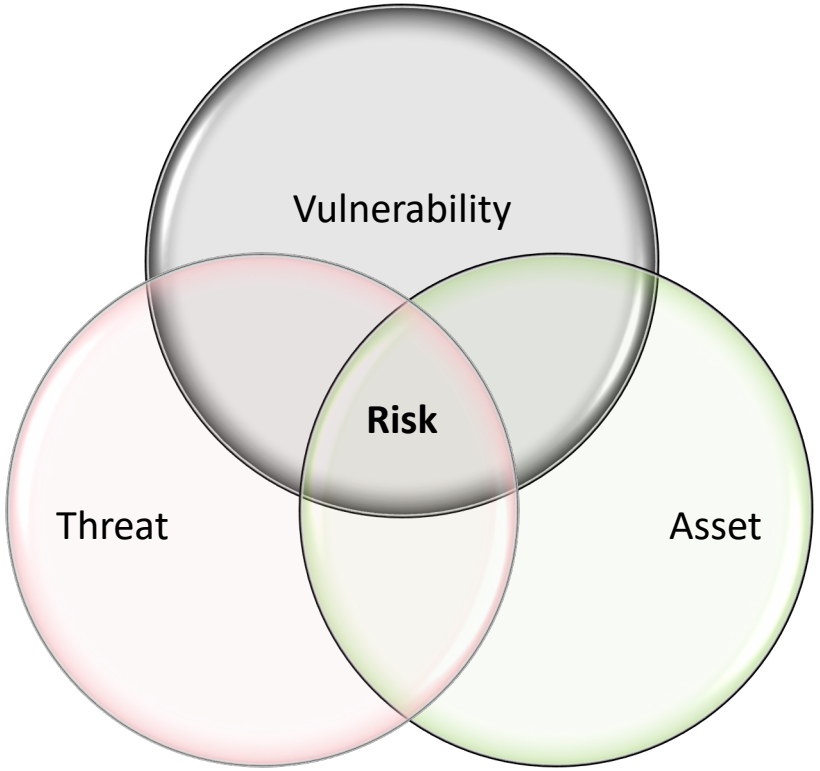
What is a Vulnerability?

It is a weakness, a behavior or set of conditions present in a system, product, component, or service that violates an implicit or explicit security policy such as confidentiality, integrity and availability.

The vulnerability is what an attacker uses to exploit the system and cause a cyber incident.

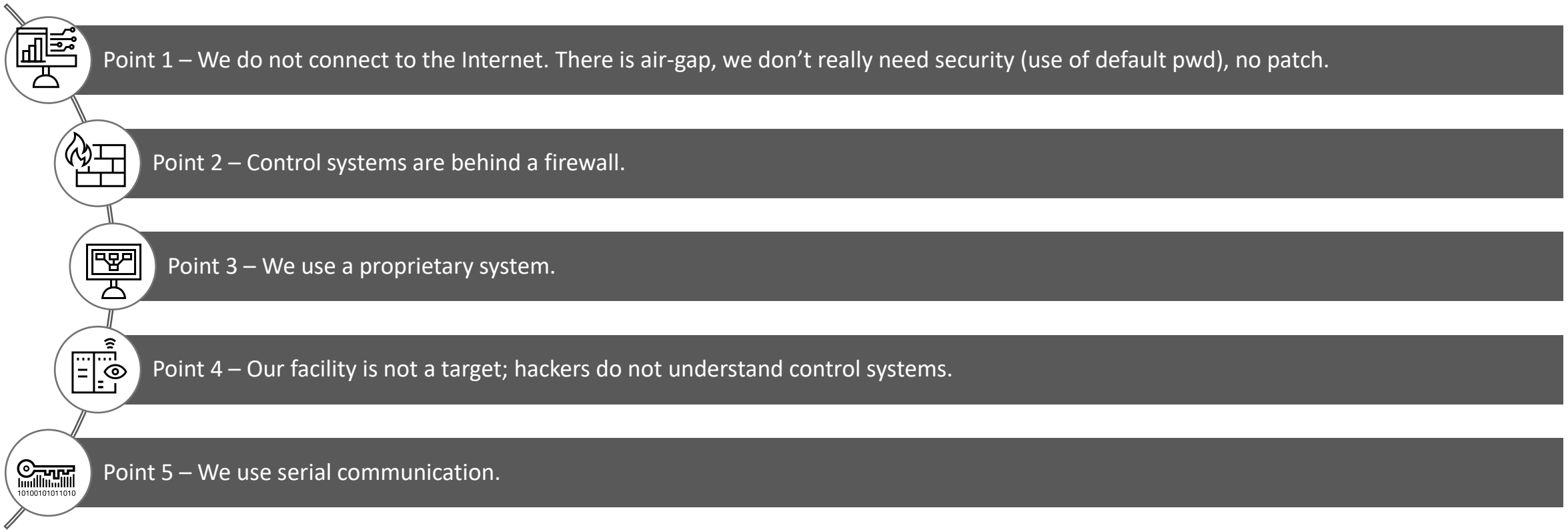
To address a vulnerability (reduce risk of cyber exploitation):

- Apply mitigation strategy
- Apply security update/remediation/patch (if available)



Vulnerability appears all the time. Every product with digital elements will eventually have one or many vulnerabilities along the time.

False Sense of Cybersecurity in Control System World

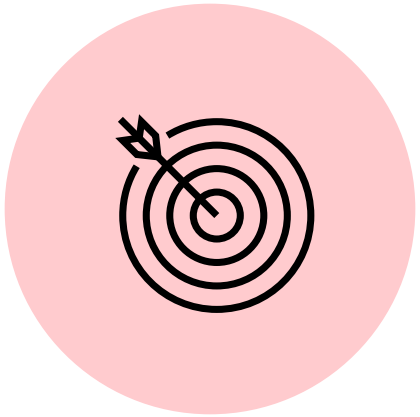


It is paramount to deploy the OT products, systems in a secure way, and cybersecurity has to be managed continously.

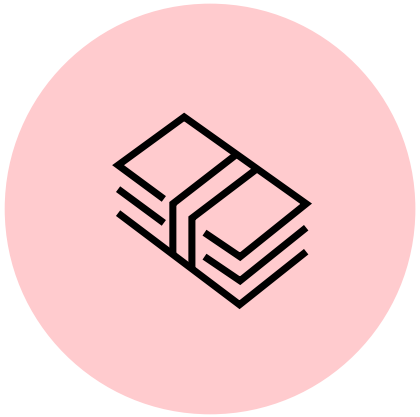
https://gca.isa.org/hs-search-results?term=myth&type=SITE_PAGE&type=BLOG_POST&type=LISTING_PAGE

Cybersecurity: It’s All About Risk Management

There is no such thing as 100% security.



Cybersecurity is not a destination but an evolving target.



Cybersecurity impacts usability and drives up costs.

Cybersecurity is a matter of shared responsibilities.

The Defense-In-Depth Principle in Solution Delivery

Protect

Zoning & Perimeter Protection

Malware Protection

Product and System Hardening

Secure Communication

- User account management
- https
- VPN
- Secure IEC 60870-5-104,
- Secure DNP 3.0 (IEC 62351)

Manage

Patch Management

Backup & Recovery

Account Management

- User account management
- Central account management
- Role-based access control
- Password complexity
- Two-factor authentication

Monitor

Security Logging & Monitoring

- Audit trails of all security relevant user activities
- Enables customers to monitor and respond to security events in real time

Cybersecurity is a Shared Responsibility

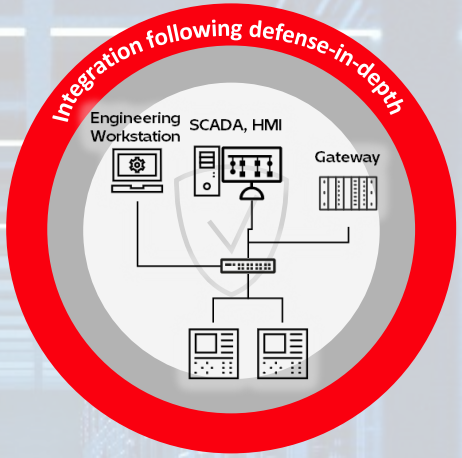
Cybersecurity is a Shared Responsibility

Suppliers

Deliver secure components & transparency

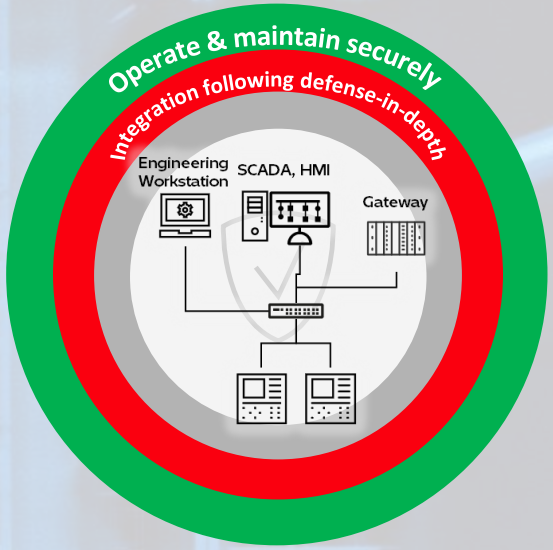
Hitachi Energy

Secure-by-design



Partner / System Integrator

Secure deployment

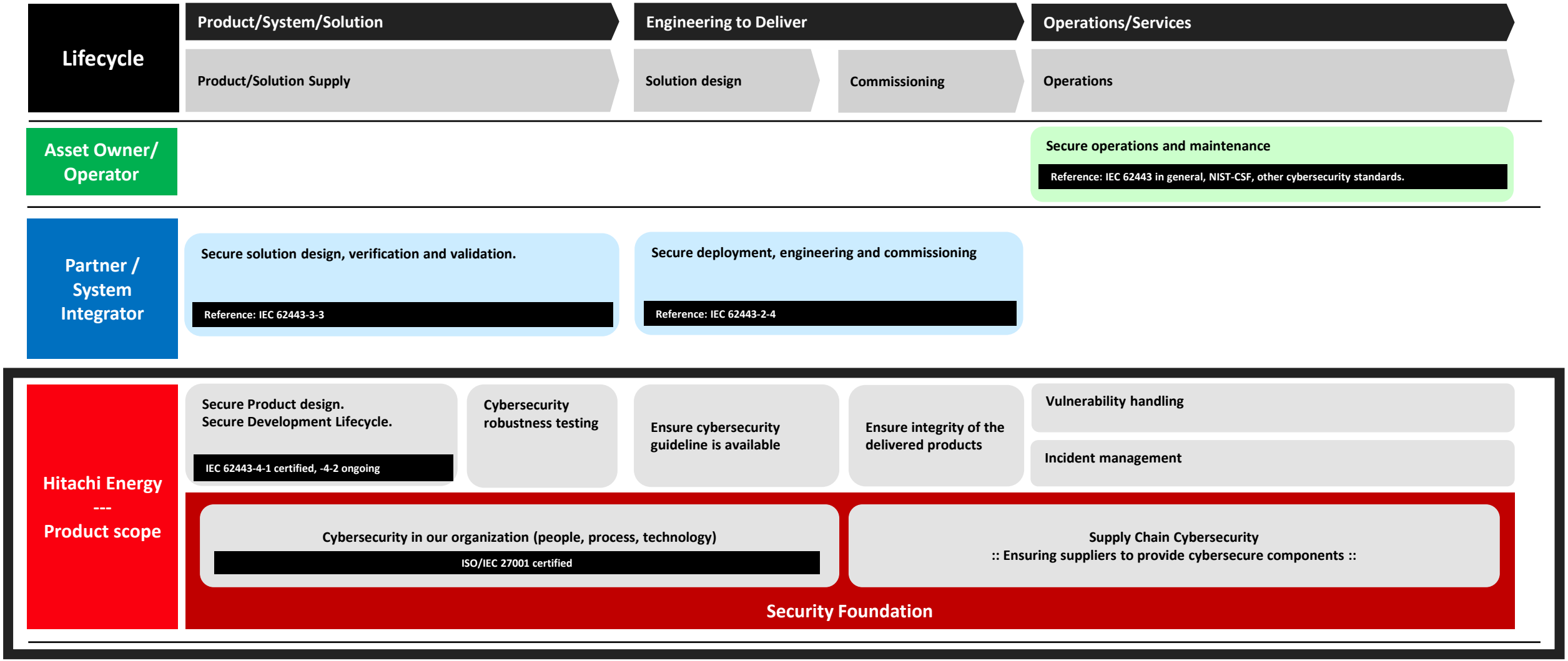


End Customer/Asset Owner

Secure operation & maintenance

Cybersecurity is a shared responsibility and must be built together across the entire supply chain. A weakness at one place puts everyone at risk.

Security Responsibility Across Supply Chain and Lifecycle View

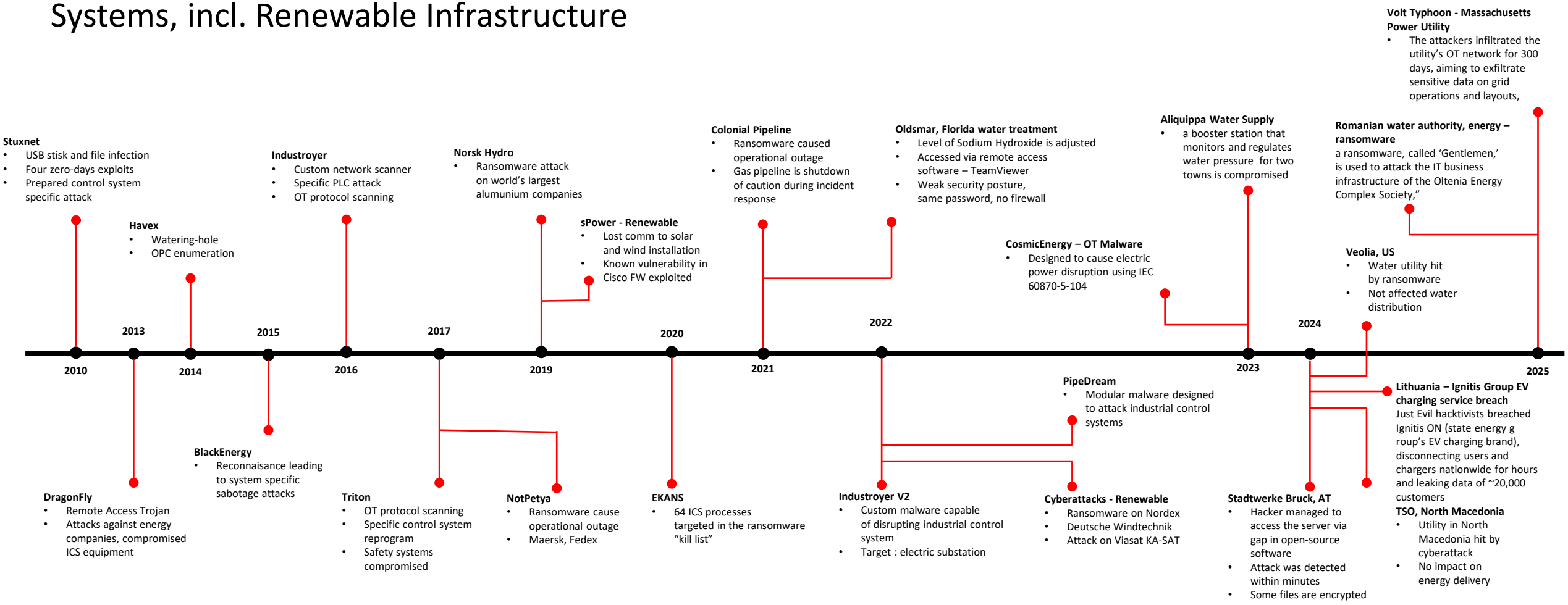


HITACHI

Outlook on Threats: What Is Happening Around the World?

HITACHI

Various Attacks Affecting Industrial Automation and Control Systems, incl. Renewable Infrastructure



Mission-critical, cybersecurity-standard-compliant redundant communications incl. wireless will be the key against cyber attacks.

Please find the references in the Notes.

© 2026 Hitachi Energy. All rights reserved.

HITACHI

Securing OT System by Adopting IEC 62443

What is ISA? And What is ISA/IEC 62443

ISA 99

Committee within the International Society of Automation (ISA) that produces the ISA/IEC 62443 standards.

Established in 2002 with over 500 members representing companies across various OT relevant sectors.

What is IEC 62443?

IEC 62443 is a consensus-based cybersecurity standard for automation and control system applications/operational technology found in industrial and critical infrastructure, including but not restricted to power utilities, water management systems, healthcare, and transport systems.

IEC 62443 are cybersecurity base standards, and technology independent.

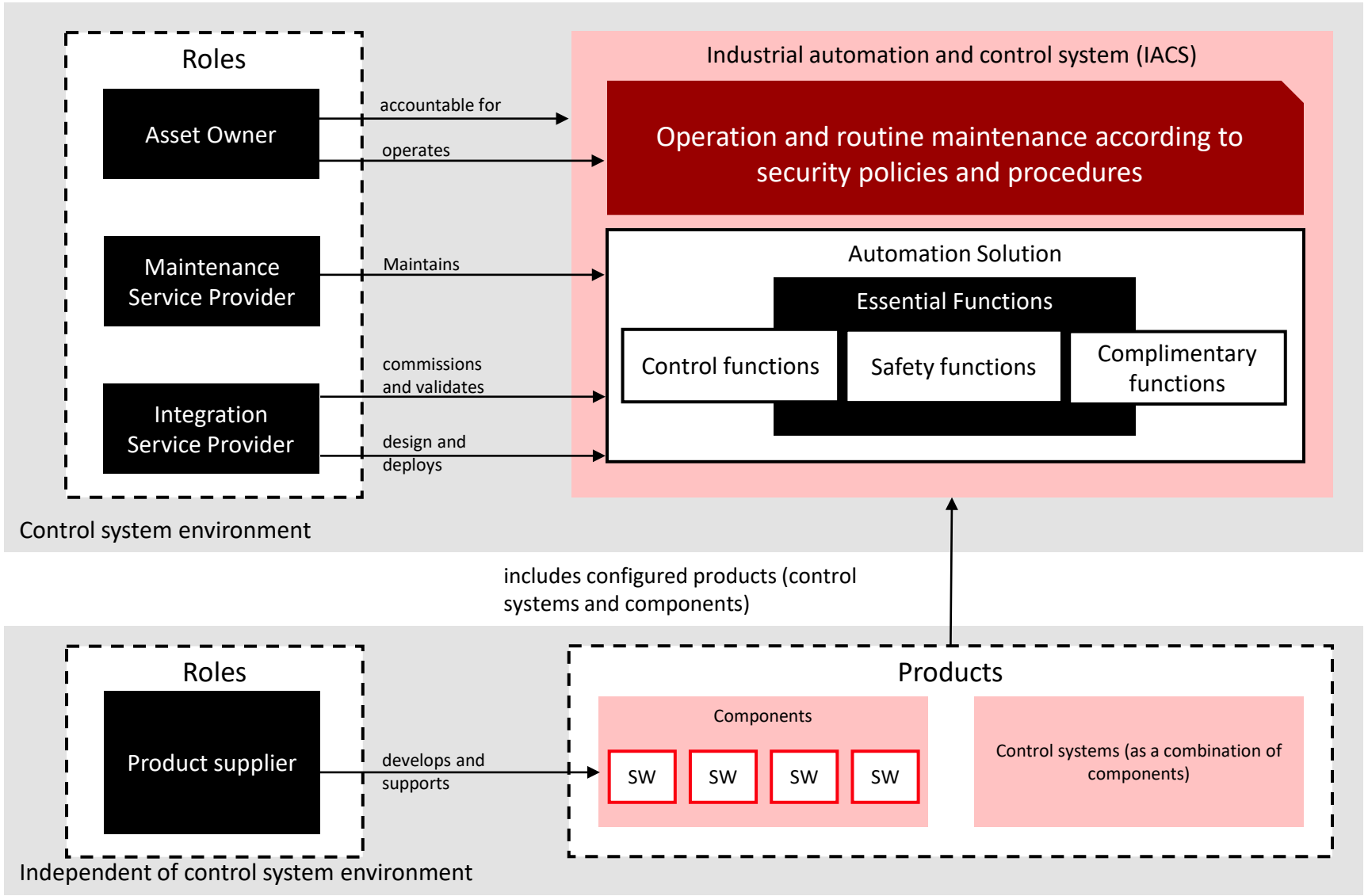
IEC 62443 can be applied across many technical areas.

Officially announced on November 17, 2021, by The International Society of Automation (ISA) and the ISA Global Cybersecurity Alliance (ISAGCA) that the International Electrotechnical Commission (IEC) has officially designated the IEC/ISA 62443 series of standards as “horizontal,” meaning that they are proven to be applicable to a wide range of different industries.

Principal Roles in Control System According to ISA/IEC 62443

Roles

- *Asset owner* – the organization that is accountable and responsible for the control system
- *Maintenance service provider* – the individual or organization that provides support activities for an Automation Solution
- *Integration service provider* – the organization that provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover to the Asset Owner
- *Product supplier* – the organization that manufactures and supports a hardware and/or software product.



IEC 62443 Publications

General

- Contains standards and reports that are general in nature.

TS 62443-1-1	62443-1-2	62443-1-3	62443-1-4	TS 62443-1-5	PAS 62443-1-6
Concepts and models	Master glossary of terms and abbreviations.	System security conformance metrics	IACS security lifecycle and use-cases	Scheme for IEC 62443 security profiles	Application of the 62443 series to the Industrial Internet of Things (IIoT)

Policies and Procedures

- Addresses the people and process aspects of an effective security program.

IEC 62443-2-1	PAS 62443-2-2	TR 62443-2-3	IEC 62443-2-4	TR 62443-2-5
Establishing an IACS security program	IACS security program ratings	Patch management in the IACS environment	Security program requirements for IACS service providrs	Implementation guidance for IACS asset owners

System

- Focuses on the technology related aspects of security.

TR 62443-3-1	IEC 62443-3-2	IEC 62443-3-3
Security technologies for IACS	Security risk assessment for system design	System security requirements and security level

Component

- Focuses on specific security related technical requirements of products and components.

IEC 62443-4-1	IEC 62443-4-2
Product security development lifecycle requirements	Technical security requirements for IACS components

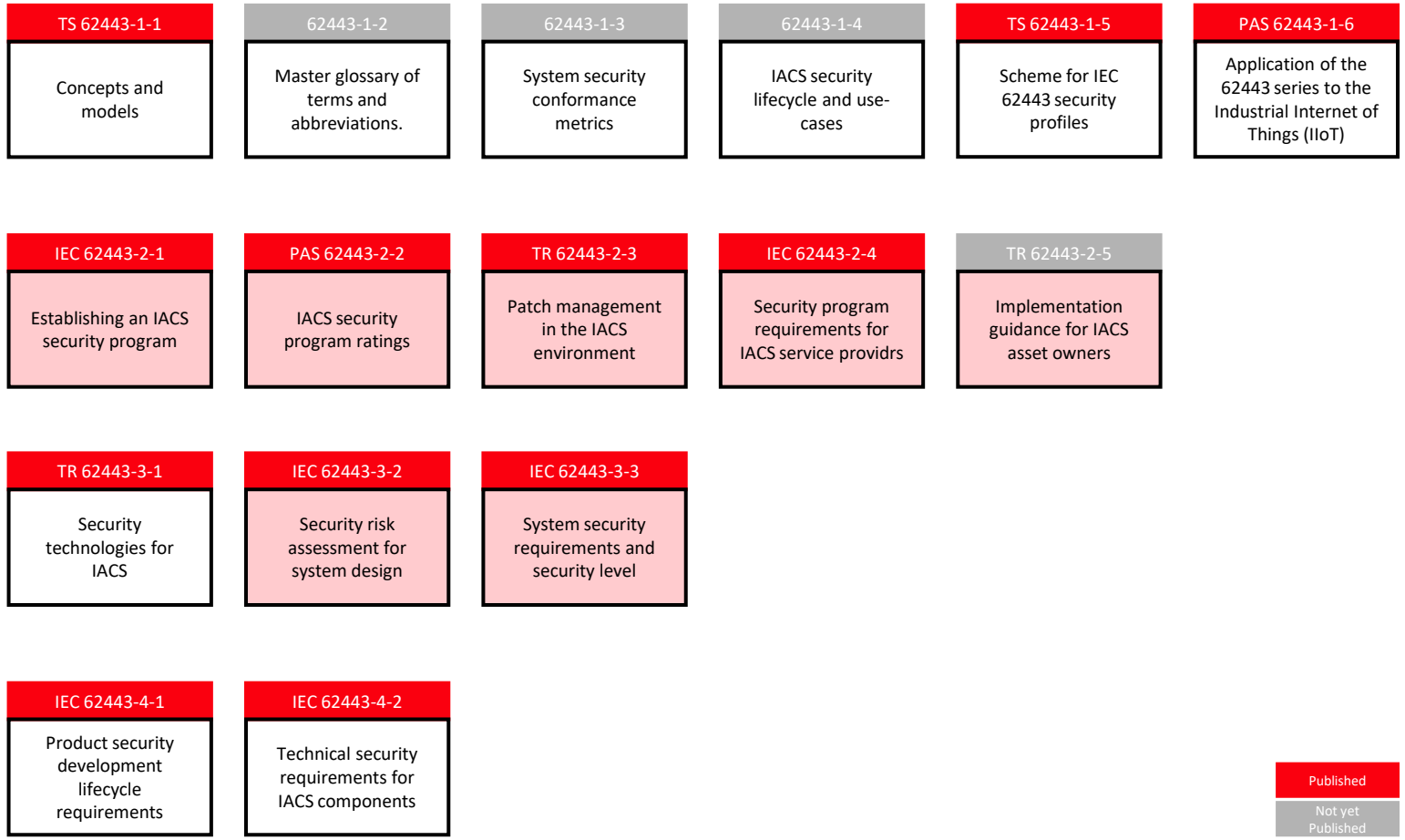
Source: Security of Industrial Automation and Control Systems - ISAGCA Quick Start Guide.pdf
Note that there are some other IEC 62443 publications on conformity assessment as well.

Published
Not yet Published

Standards Relevant to Asset Owner

Core activities of an asset owner

- Establish and sustain a Security Program that includes IACS-specific requirements
- Partition Zones and Conduits and perform associated Risk Assessments
- Document IACS requirements in the Cybersecurity Requirements Specification
- Procure products and services that meet IACS requirements
- Operate and maintain the IACS
- Assess the effectiveness of the IACS Security Program

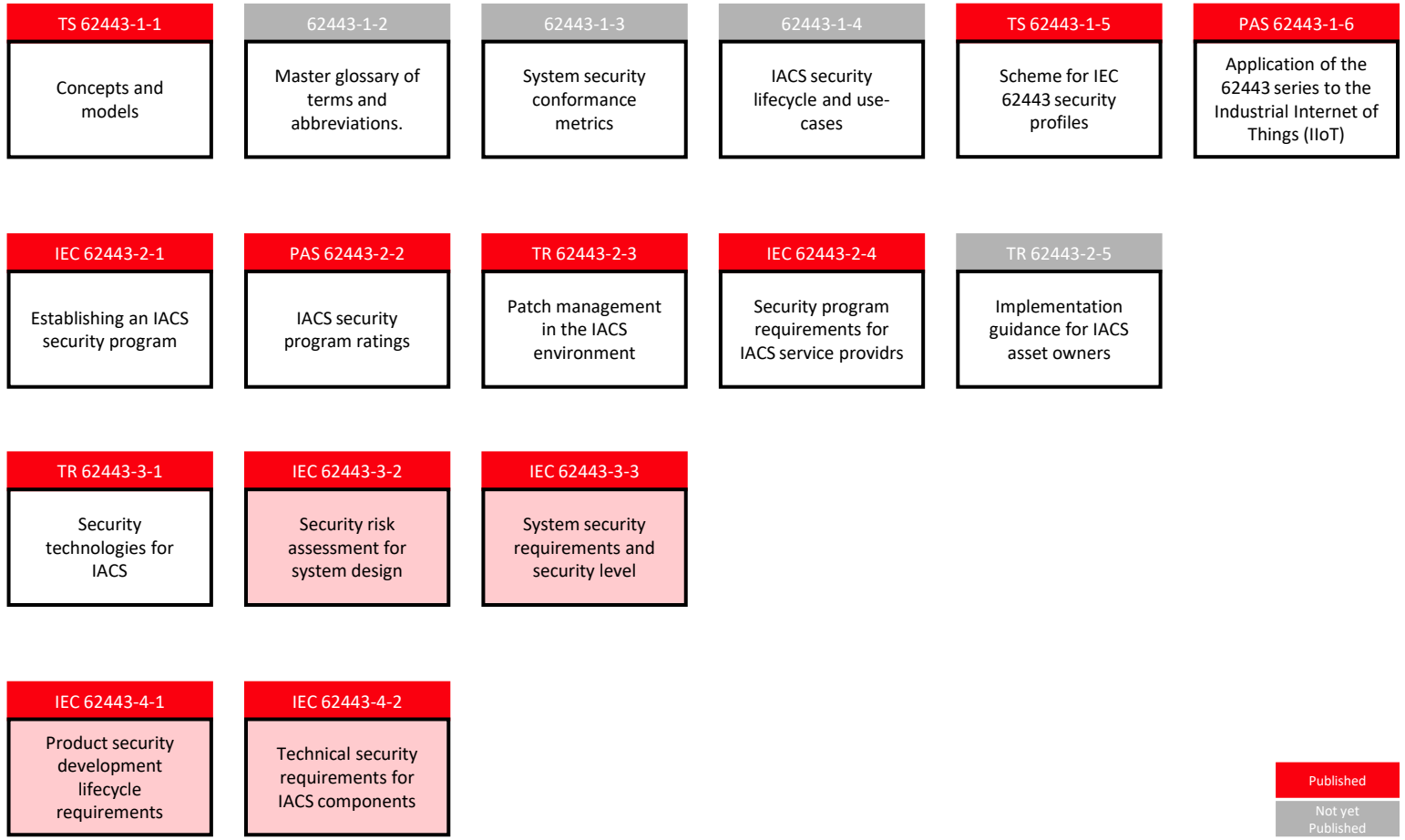


Public

Standards Relevant to Product Supplier

Core activities of a product supplier

- Establish and sustain a Security Development Lifecycle
- Provide Control System products that meet Security Level capabilities
- Provide Component products that meet Security Level capabilities
- Provide ongoing lifecycle support for their Control System and Component products

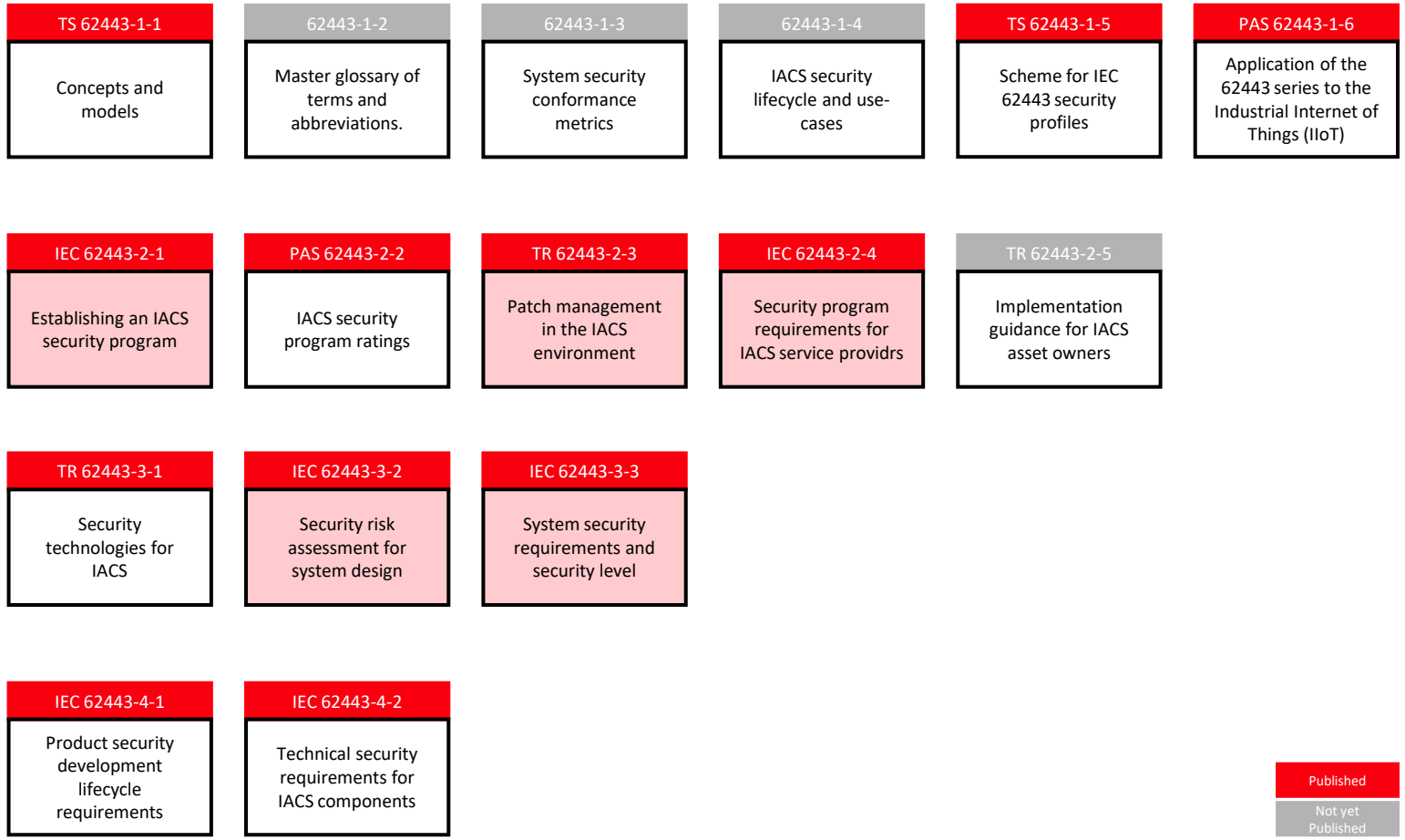


Public

Standards Relevant to Integration Service Provider

Core activities of a integration service provider

- Establish and sustain a Security Program for Automation Solution integration
- Design and implement Automation Solutions that meet the requirements in the Cybersecurity Requirements Specification
- Apply security patches during the Integration Phase of the Automation Solution lifecycle

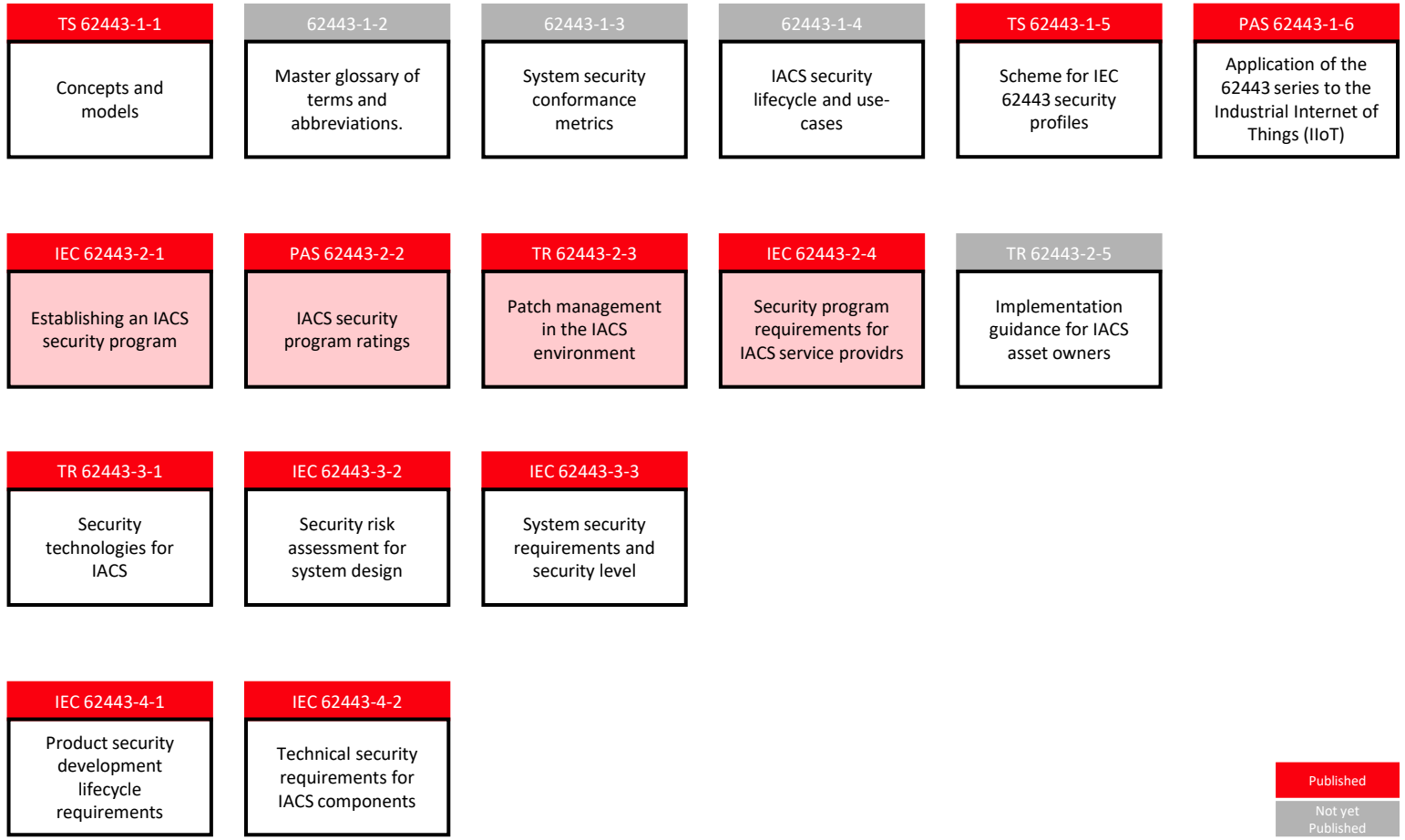


Public

Standards Relevant to Integration Service Provider

Core activities of a maintenance service provider

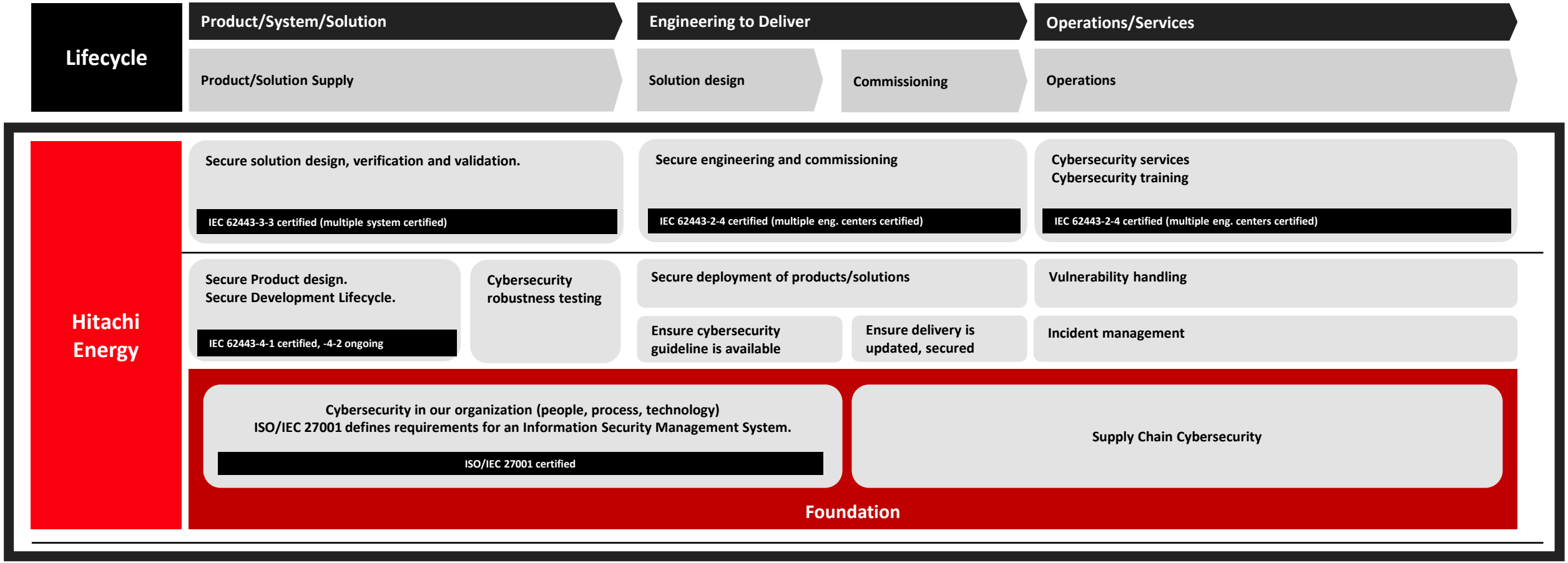
- Establish and sustain a Security Program for maintenance services
- Provide services and capabilities that meet the IACS security policies and procedures specified by the Asset Owner



Hitachi Energy’s Approach

HITACHI

Automation And Communication Cybersecurity Solutions End-to-End Across Lifecycle



We embed cybersecurity in our culture and embrace secure-by-design across products/systems/solutions lifecycle.

HITACHI

Cybersecurity Capabilities Overview on Products, System and Service Layers

IEC 62443-2-4 ML3

Engineering and Service teams

- Security assessment & monitoring
- Backup & recovery
- Security updates & hardening
- Malware protection
- Procedures & policies
- Perimeter protection

Hitachi Energy Automation and Communication Cybersecurity Services

IEC 62443-3-3 certified

SA system
Wired system
Windfarm system
Data center system

1. Centralized account management
2. Centralized activity logging
3. Asset management
4. Certificate creation and management
5. Quantum secured WAN
6. Anomaly detection technology
7. System backup and recovery
8. Patch management system
9. Endpoint security
10. Hardening and perimeter protection

Hitachi Energy Automation and Communication System Cybersecurity Capabilities

IEC 62443-4-1 ML3

IEC 62443-4-2
(RTU obtained, others ongoing)

- Hardened control system
- Product Backup & Recovery
- Product Security Event Logging
- Supervision and monitoring
- Secure Communication
- Ensure Products Integrity
- Account Management
- Role-Based Access Control

Hitachi Energy Automation and Communication Products Cybersecurity Capabilities

Public

IEC 62443 Certificates in Automation and Communication

IEC 62443-4-1

GA A&C

CsAC

IEC 62443-4-2

GA RTU530

GA RTU560

IEC 62443-3-3

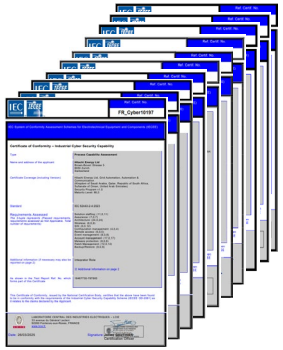
GA FOX615 Platform

GA SAS

GA XMC20 Platform

GA Windfarm Reference Arch.

IEC 62443-2-4



Certificates obtained in 39 countries across the world

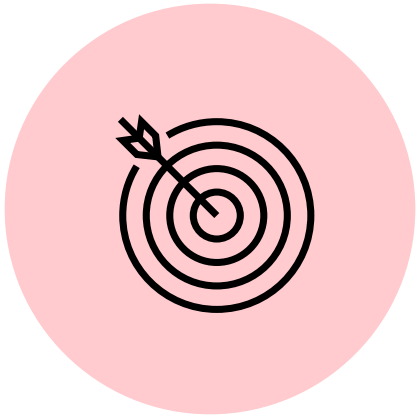
All Cyber- and Information Security certificates can be found here: link

HITACHI

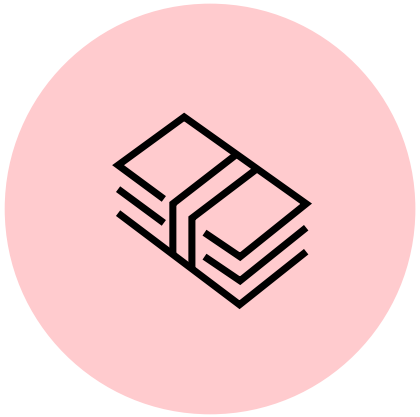
Closing Remark

Cybersecurity: It’s All About Risk Management

There is no such thing as 100% security.



Cybersecurity is not a destination but an evolving target.



Cybersecurity impacts usability and drives up costs.

Cybersecurity is a matter of shared responsibilities.

HITACHI


DS
DANSK STANDARD