Security Conference 2022

IEC 62443 CERTIFICATIONS

Jerome Hamel

Bureau Veritas

04/10/2022

IEC 62443 CERTIFICATIONS
TODAY'S SPEAKER

JEROME HAMEL

Head of Cybersecurity Technical Governance
Bureau Veritas Consumer Product Services

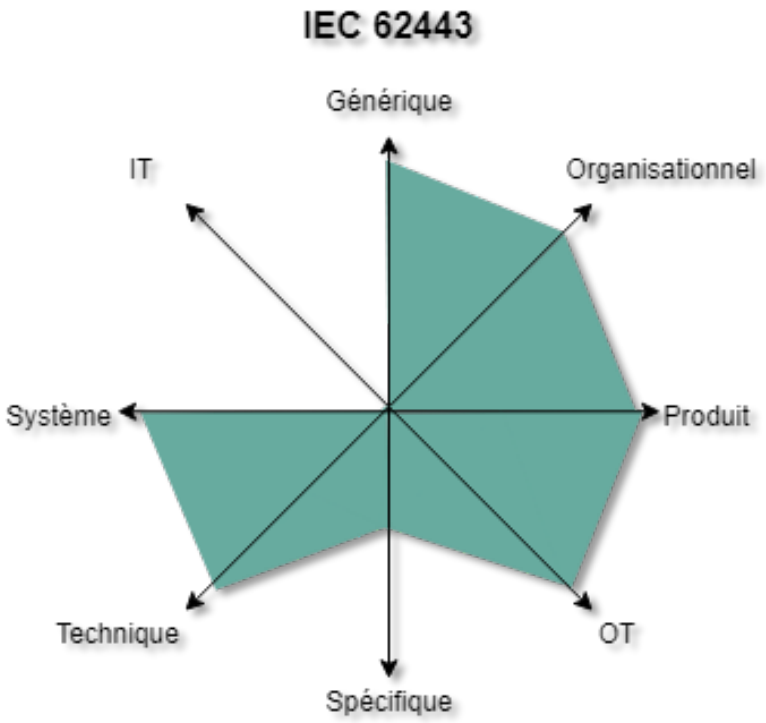
Contact: Jerome.Hamel.ext@bureauveritas.com

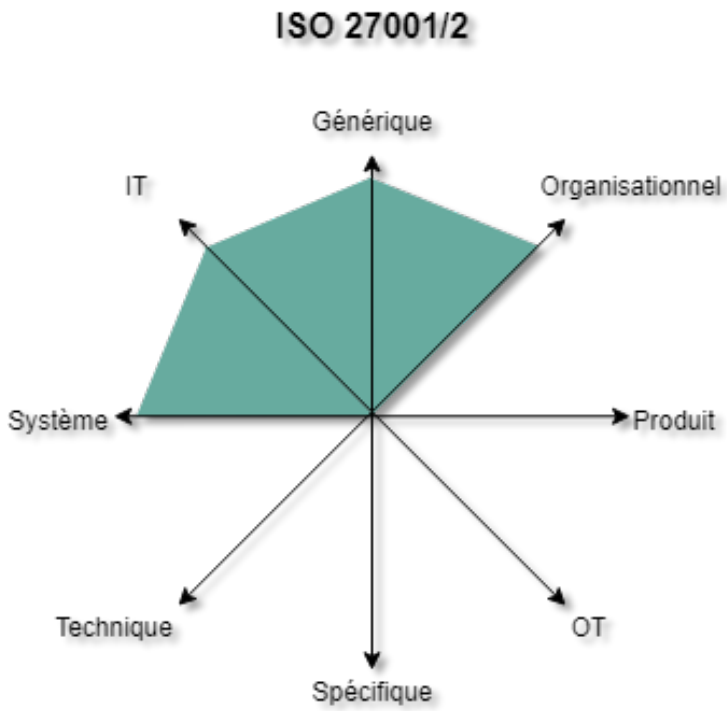
IECEE 62443 CERTIFICATIONS AGENDA

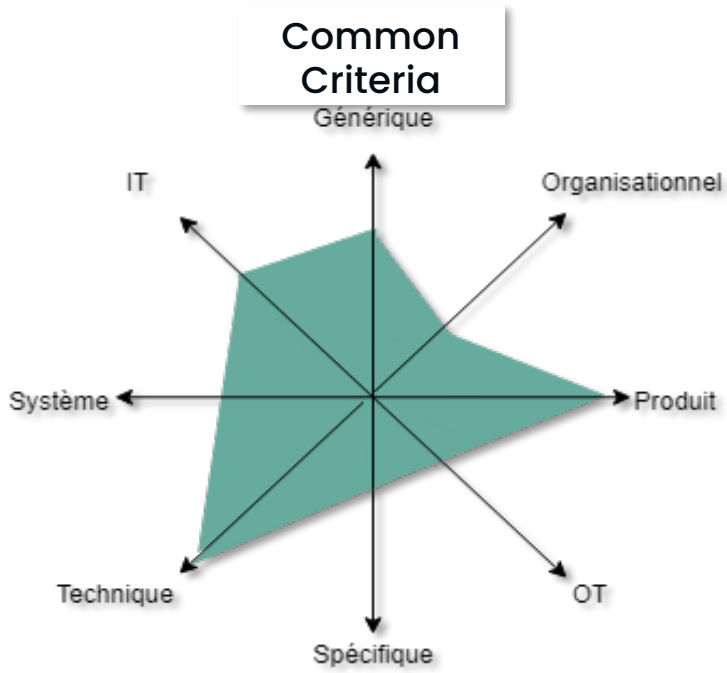
- Reminder of the approach and of the different IEC 62443 parts
- Overview of the IECEE IEC 62443 certification
- Findings after 3 years of projects execution with customers
- Adoption by more market sectors

CHALLENGES :
CYBERSECURITY DOES NOT ONLY INVOLVE THE PRODUCT

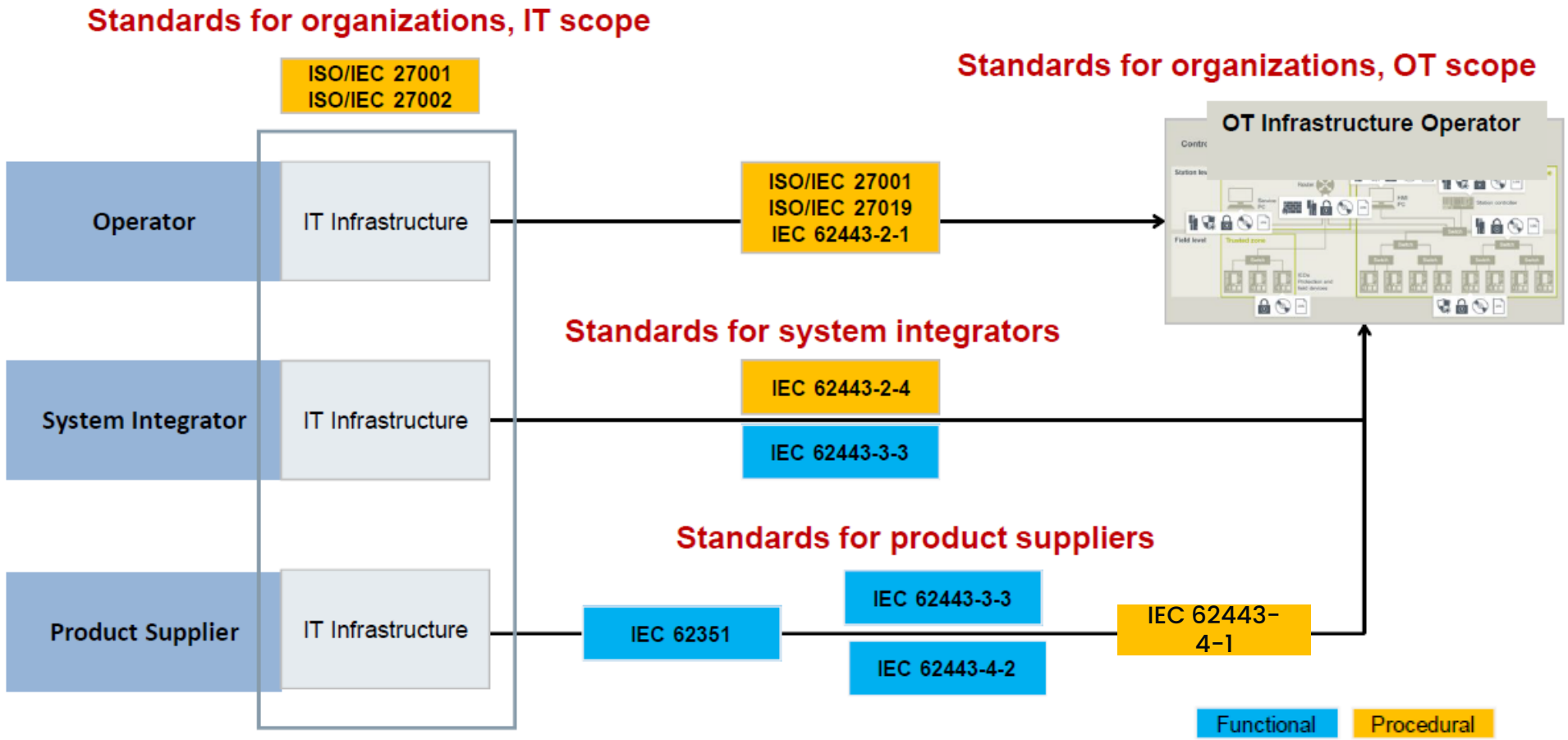
Approach | IEC 62443 vs other standards







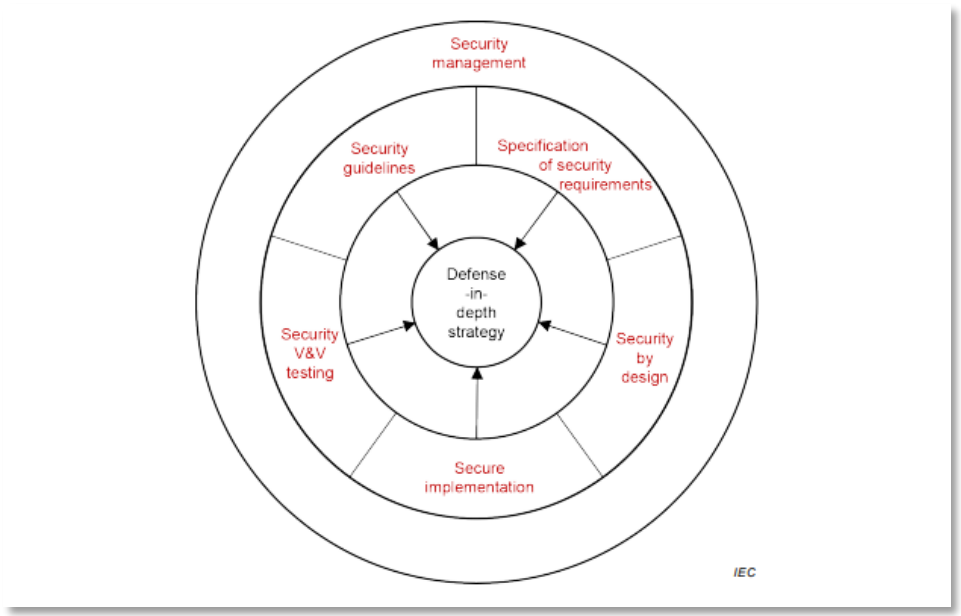
Approach | STANDARDs per roles

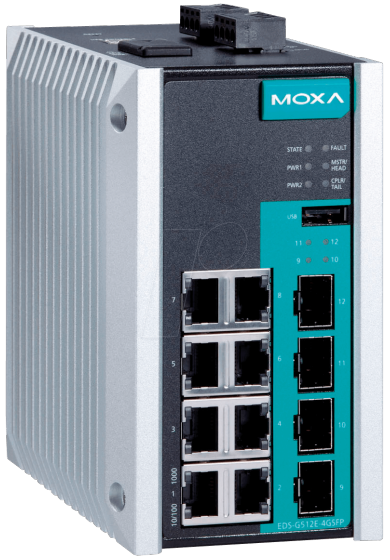


IEC 62443 Standard recognized the diversity of the roles involved in the cybersecurity & defined different requirements depending of each role.

You are a component supplier (HW/SW) :

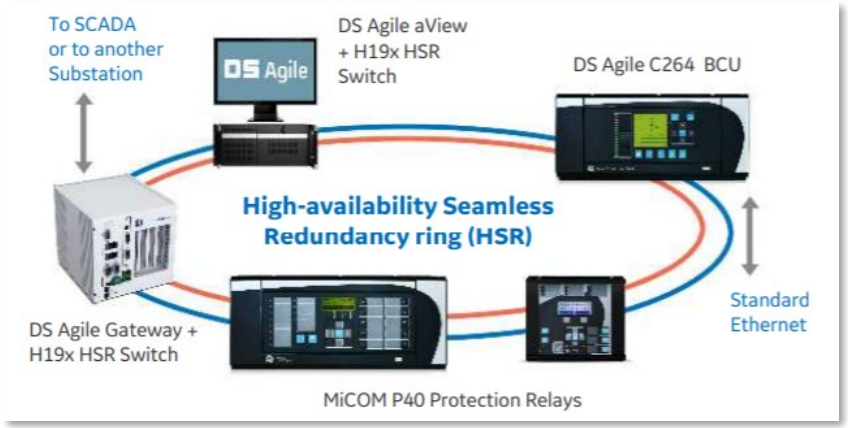
- Module 4-1 ensures and offers
  - “Secure by Design” components: cyber security is taken into account from the design phase
  - The assurance for you and your customers that all your products follow a secure life cycle
  - First step towards a 4-2 certification of your products

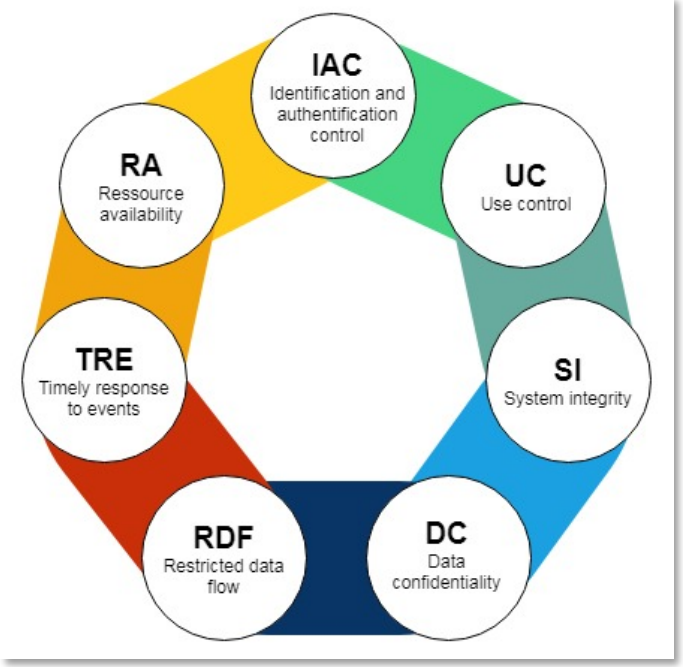


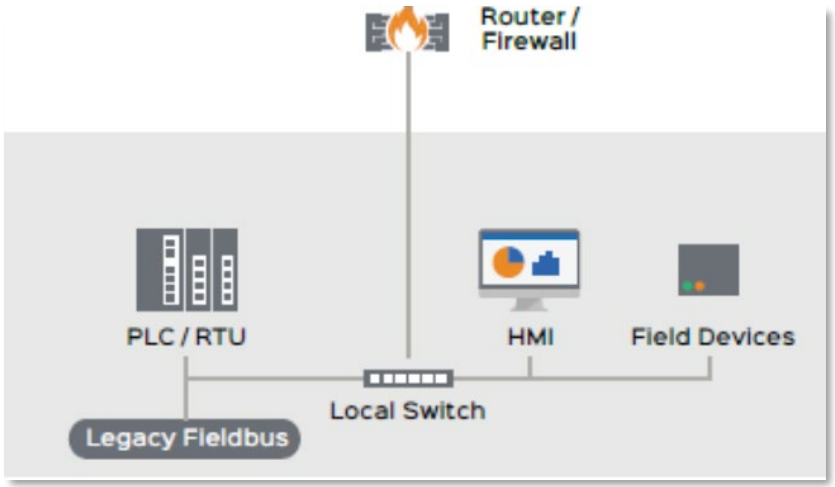


You supply or integrate a solution/system

- Module 3-3 allows you to certify your system for a required Security Level (SL)
  - System may be composed of your own components and/or other third party products
  - Content of 3-3 is similar to 4-2 (components)



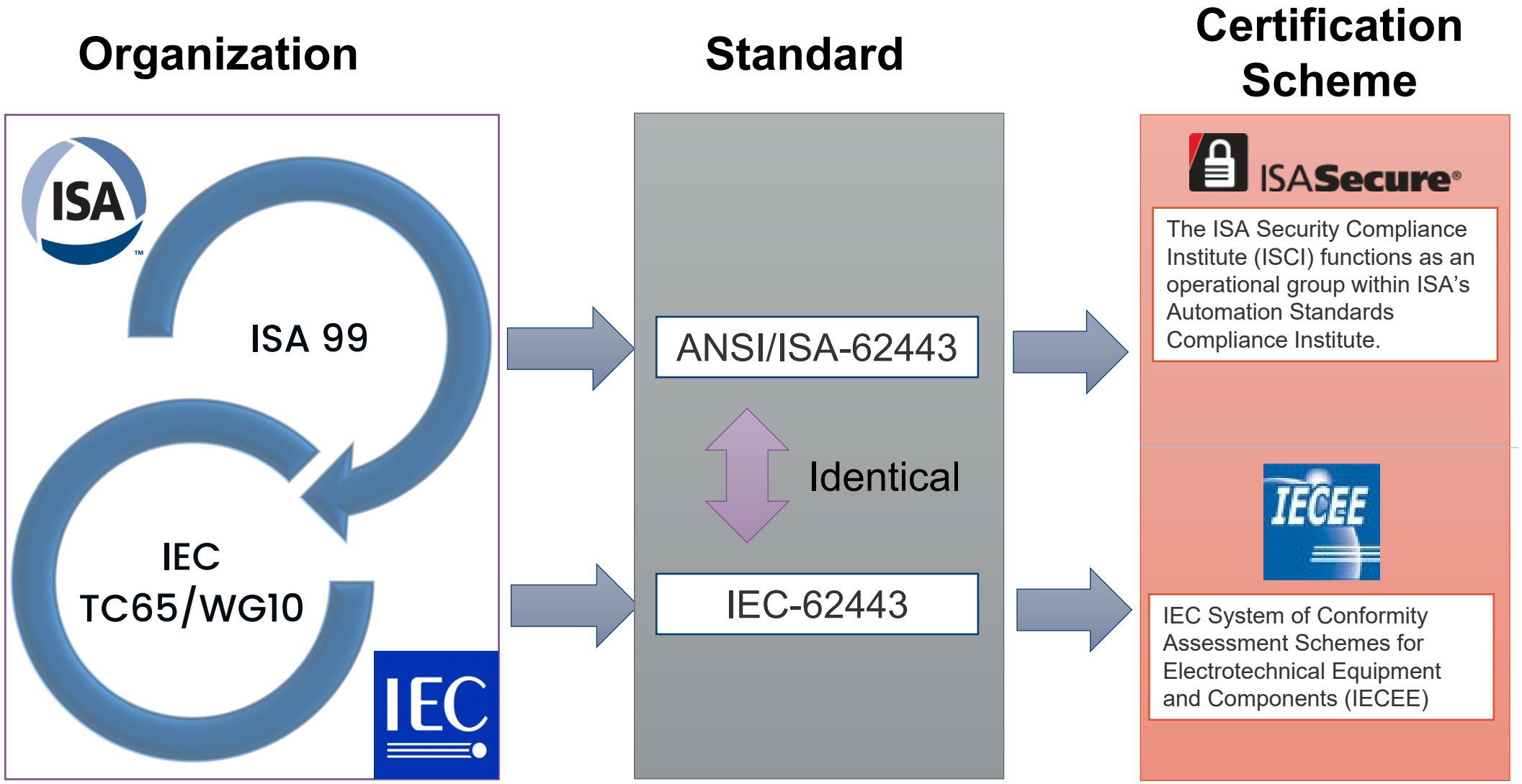




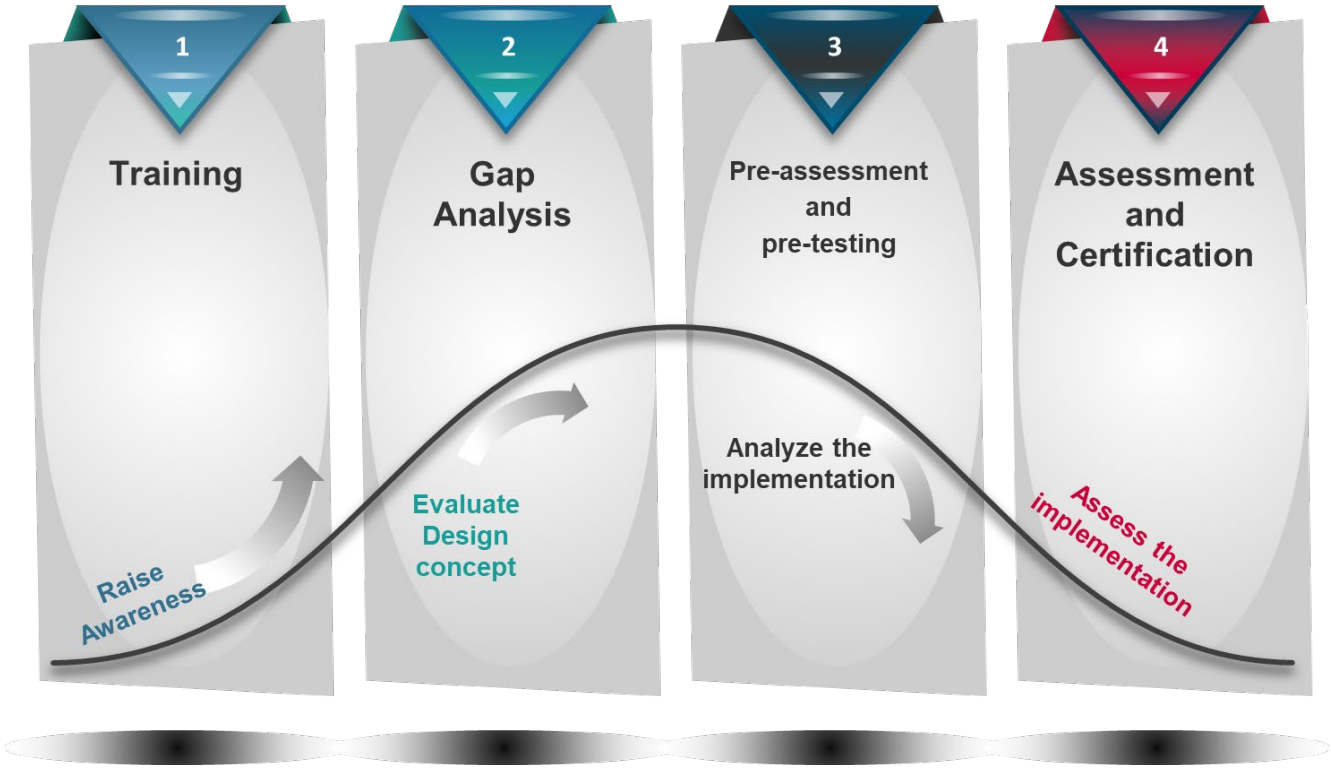
You are a service provider (internal or external) :

- Module 2-4 ensures
  - Integration & Maintenance teams have the required capabilities and follow cyber-secured processes
  - Reduction of risks of human error that could have an impact on the automation solution
  - Continuous improvement of the cyber security maturity level of your teams

Standards Development Organization Collaboration
ISA & IECEE Certifications

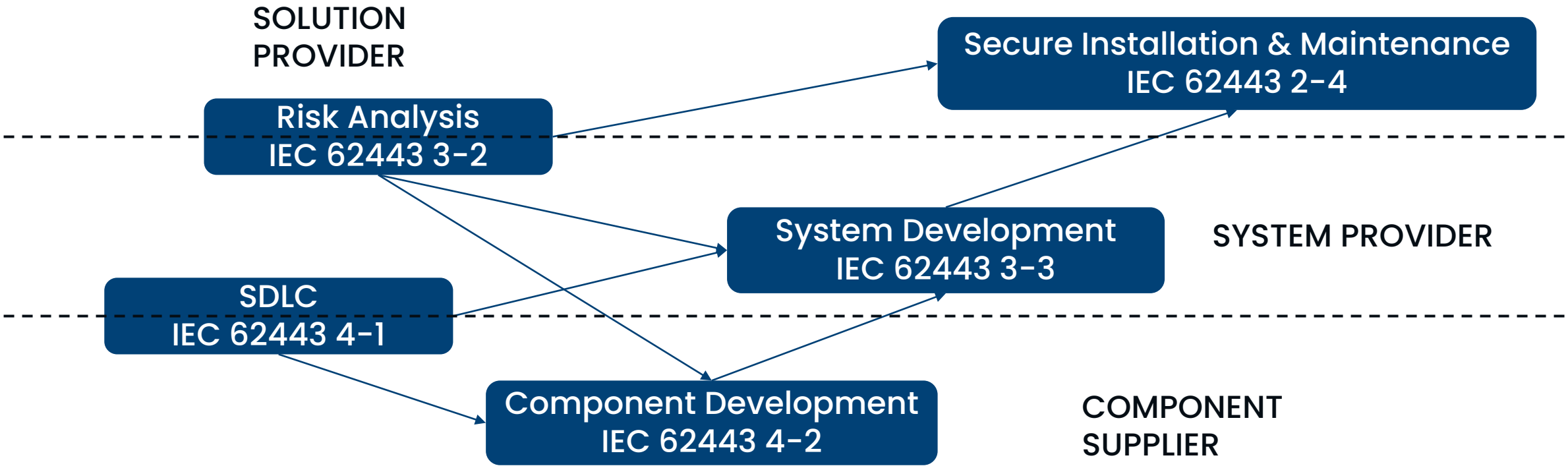


IEC 62443
CYBERSECURITY LEARNING PHASE



Between the initial “awareness” and the certification it can take up to 2 years

IEC 62443 Implementation Steps



- ❑ SDLC & Risk Analysis have to be in place for a “Secure by Design Product”
- ❑ This is requested prior to IEC 62443-4-2 certification

IECEE 62443 Evaluation & Certification Usual Project Steps

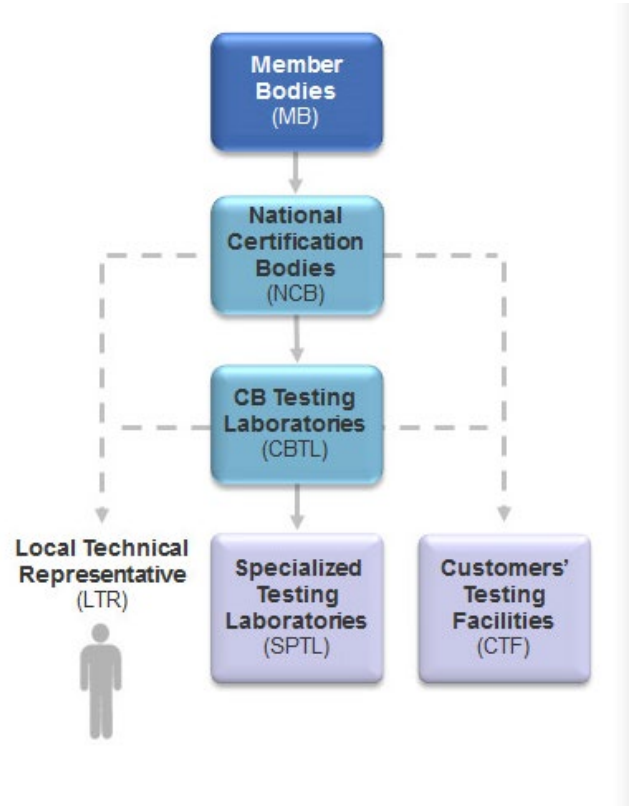
CBTL

- ❑Step 1 – Kick off Meeting: Initial meeting between the customer and the evaluators/certifiers.
- ❑Step 2 – Evidence analysis: Review by the evaluators of the provided set of documentation
- ❑Step 3 – Formal Audit Process or Product Test or Test Witnessing
- ❑Step 4 – Final Evaluation report

NCB

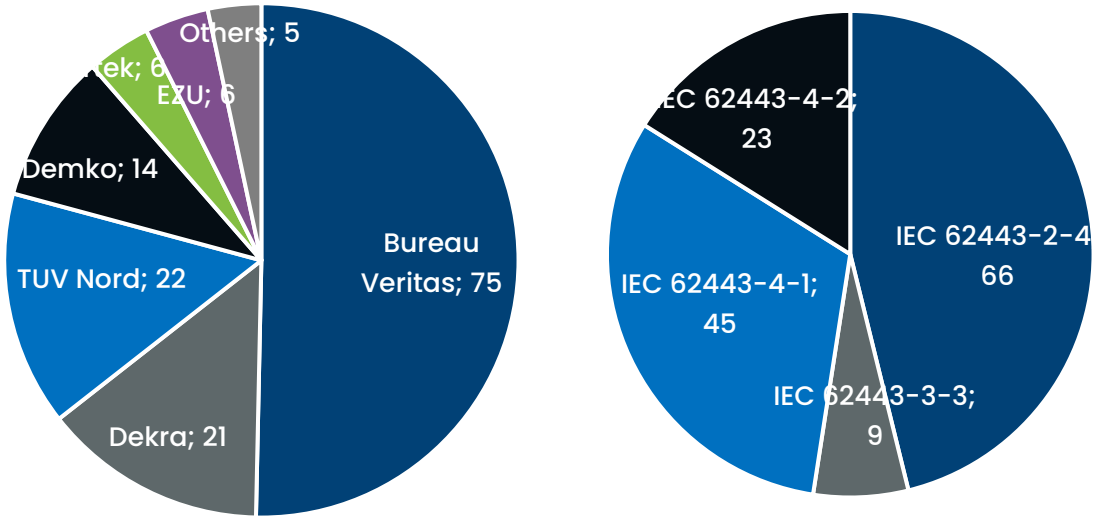
- ❑Step 5 – Certification review & Issue of certificate: Release of the IECEE certificate

CB Scheme



Trend in IECEE 62443 certification

Total number of IECEE 62443 issued certificates



Status as of September 26th 2022

Process before products

- **Companies started with process relative certification (2-4 & 4-1). From this year component certifications (4-2) are increasing**

Growing adoption

- **From 4 certificates end 2019 the numbers of certificates grown quickly from mid 2022 to achieve more than 150.**
- **Pushed by demands in RFQ the main represented sectors are**
  - ***Industry automation,***
  - ***Transportation (trains, subways, etc.)***
  - ***Grid (water, gas, electricity, pipelines…)***
- **The requirements being quite generic more sectors are adopting the IEC 62443:**
  - ***"security by design" as per requirements from the 4-1***
  - ***4-2 requirements for any component to be integrated in a larger system***
  - ***Some sectors are deriving or enriching the 62443 requirements to consider their specificities (see next slide)***

IEC 62443 in other verticals

IEC TR 60601-4-5

Edition 1.0 2021-01

TECHNICAL REPORT

IEC ISO IEC 81001-5-1

Edition 1.0 2021-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle

Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé – Partie 5-1: Sûreté – Activités du cycle de vie du produit

MEDICAL DEVICES

enisa European Rail ISAC

ZONING AND CONDUITS

Figure 1 Zoning and conduit methodology

Go

Alignment

Identify

S.R. CLC/TS 50701:2021

TECHNICAL SPECIFICATION CLC/TS 50701

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION July 2021

ICS 35.030; 45.020

English Version

Railway applications - Cybersecurity

Bahnanwendungen - IT-Sicherheit

This Technical Specification was approved by CENELEC on 2021-05-11.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

The overall process ste
CLC/TS50701:2021 ar
split for easier explana

RAILWAY SYSTEMS

E26

E26 (Apr 2022) Cyber resilience of ships

1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

E27

E27 (Apr 2022) Cyber resilience of on-board systems and equipment

1. General

1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

This document specifies unified requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

This UR does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, the following URs shall be applied:

- UR E10 for environmental performance for the system hardware
- UR E22 for safety of equipment for the functionality of the software

1.3 Scope

The requirements specified in this UR are applicable to computer based systems as defined in UR E26.

Navigation and radiocommunication systems may follow IEC 61162-460 instead of the requirements in this UR. See IACS UR E26 section 1.3

Note:

1. This Unified Requirement is to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024 and may be used for other ships as non-mandatory guidance. In order to allow sufficient time for non-mandatory pilot application of this UR, the application date of 1 January 2024 has been selected.
2. The "contracted for construction" date means the date on which the contract to build the vessel is signed between the prospective owner and the shipbuilder. For further details regarding the date of "contract for construction", refer to IACS Procedural Requirement (PR) No. 29.

SHIPS

SHIP COMPONENTS

News and Press Releases / ISASecure Announces ISA/IEC 62443 IIoT Component Security Assurance (ICSA) Certification Launch

ISASecure Announces ISA/IEC 62443 IIoT Component Security Assurance (ICSA) Certification Launch

September 01, 2022 | Durham, North Carolina

The ISASecure program is announcing the new ISASecure certification offering for industrial internet of things (IIoT) components based on the ISA/IEC 62443 series of standards.

INDUSTRIAL IOT DEVICES

Cybersecurity training