ISASecure®

Ensuring the security of automation that affects our everyday lives.

ISASecure Webinar Series

Eurotech Group Fast-Track to Cyber Resilience: ISASecure 62443-4-2 Certified Edge Solutions

Luca Varisco
Global CISO Eurotech Group

Massimiliano Latini
Cybersecurity Manager H-ON a TÜV Rheinland Company dba BYHON

About Authors

Luca Varisco CISO
Eurotech Group

in charge of the Security of the Company and overseeing the Eurotech products security. Experienced in all the challenges of both IT and OT worlds and regulations across the globe as CIO and CISO. Evangelist for ISASecure and 62443 framework as a key blueprint to integrate the IT/OT security.

🌐 **Eurotech.com**   in **Eurotech**

Massimiliano Latini Cyber Security Manager
H-ON a TÜV Rheinland Company dba BYHON

Also, Technical Director at H-ON - Mechanical Engineer with more than 20 years of experience in the safety and cybersecurity of industrial automation, ISA/IEC 62443 Cybersecurity Expert certified.

🌐 **byhon.it**   in **BYHON | Organization of H-ON a TÜV Rheinland Company**

eurotech
UNLEASHING THE POWER OF THE EDGE

we connect valuable assets
to the cloud & enable edge AI
in mission-critical applications

eurotech
UNLEASHING THE POWER OF THE EDGE
BYHON

30 + years of expertise

400 people

8 offices worldwide (IT, UK, US, JP, DE)

6 r&d hubs

45 + countries served

ISASecure®

eurotech
UNLEASHING THE POWER OF THE EDGE

SIMPLE
better time to market

SECURE
minimize risk

AGNOSTIC
open-source agnosticity
enabling AI at the edge

Co-founders of
Open-source IoT Working
Group Eclipse

IEC 62443

1992   **1999**   **2012**   **2021**   **2022**   **2023**   **2024**

HW
modules

HW subsystems

integrated HW
& SW

intelligent edge
devices

1st IoT Gateway
IEC 62443-4-2 SC-L2

1st EdgeAI
IEC 62443-4-2 SC-L2

Pioneers in OT cybersecurity: first programmable IoT gateway
and first Edge AI certified IEC 62443-4-2 SC-L2

ISASecure®

threat levels are on the rise

GLOBAL INCREASE IN CYBERATTACKS

- **3,205** compromises in 2023 (~9/day) with over 353 million victims.
- Average SME insurance claim of **$345K**
- A data breach costs **$4.88 million** on average
- **94% of organizations** have reported email security incidents.

(source - Forbes Cybersecurity Stats)

GEOPOLITICAL FACTORS

Cybersecurity is a **geopolitical instrument of power**: Example attacks include:[5] **Ukraine Powergrid** (2014-), **Iranian gas stations** (2023), Germany steel mills (2014), **Albania banks** (2023), **Danish Power** (2023), **Japanese Space Agency** (2024), **Dutch military** (2024), **Swedish government services** (2024)


MORE CONNECTED DEVICES LESS CONTROL

- Manufacturing organisations targeted through **social engineering**, **malicious data breaches** and **ransomware** attacks
- Increasing usage of smart sensors with high levels of exploitable vulnerabilities and low levels of security leading to **credential compromise**
- Meanwhile AI is enabling sophisticated **phishing**, **social engineering** and **disinformation** attacks to damage company reputations

global IoT cybersecurity regulations

cross-industry	US	EU	JP
	IoT Cybersecurity Improvement Act, 2020	Cyber Resilience Act (in draft, extension to NIS2)	IoT Security Safety Framework (IoT-SSF), 2024
	NISTIR 8259A, 2020	Radio Equipment Directive – RED, 2022	
	Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), 2022	NIS2, 2022	
	California Internet of Things (IoT) Security Law, 2020	PSTI (UK)	
	CRISP Act – State of New York, 2023		
	IEC 62443		
	Smart Buildings, NEC-70E, 2021 Pipeline Security Act, 2022 USA Water and Wastewater	Machinery Regulation (EU) 2023/1230	
		Shift2Rail	
	Maritime - IACS UR-E26, UR-E27		
	IEC 62351		
	IEC TR 60601-4-5 Medical Devices – MDISS, 2015		

EU mandates compliance to RED Article 3.3(d), (e) and (f) on cybersecurity commencing **Aug 1st 2025**

California Senate Bill 327, aka California Internet of Things (IoT) Security Law, in effect since **Jan 1st 2020**

- If you operate in any major economy or critical industry, cybersecurity is imposed by regulation
- Most of these regulations are heavily inspired by ISA/IEC 62443

ISASecure®

IEC 62443

ISASecure®

Why ISA/IEC 62443 for OT

A recap:

- Worldwide recognized standard for OT Security.

- Somehow referred by critical infrastructure regulations.

- A complete set covering all actors, governance, security and requirements for different device types.

ISA/IEC 62443 Series of Standards

General	62443-1-1 Terminology, concepts, and models	62443-1-2 Master glossary of terms and abbreviations	62443-1-3 System security conformance metrics	TR62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	62443-2-1 Establishing an IACS security program	62443-2-2 IACS security program ratings	TR62443-2-3 Patch management in the IACS environment	62443-2-4 Security program requirements for IACS service providers	TR62443-2-5 Implementation guidance for IACS asset owners
System	TR62443-3-1 Security technologies for IACS	62443-3-2 Security risk assessment for system design	62443-3-3 System security requirements and security levels		
Component	62443-4-1 Product security development lifecycle requirements	62443-4-2 Technical security requirements for IACS components			

References for Certification

The certification issued by an ISASecure® Accredited Certification Body is the highest global recognition for cyber security-related products and demonstrates that the applicable ISA/IEC 62443 requirements have been met throughout the whole lifecycle.
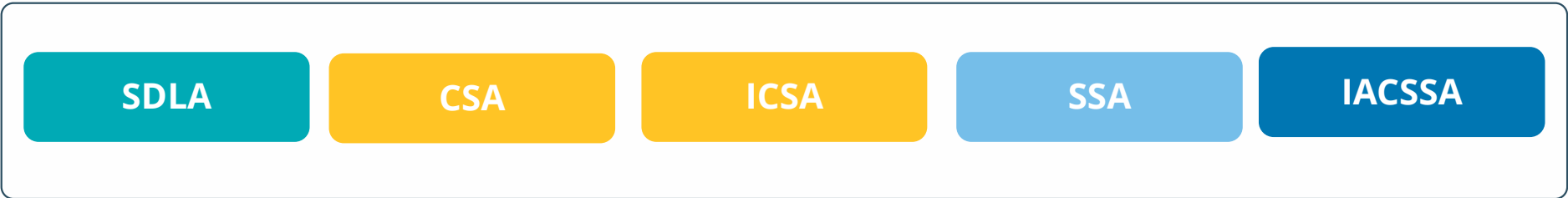
SDLA	CSA	ICSA	SSA	IACSSA

The goal of the ISA/IEC62443 Series is to improve Industrial Automation and Control System (IACS) using a risk-based, methodical, and complete process throughout the entire lifecycle, through the implementation of:
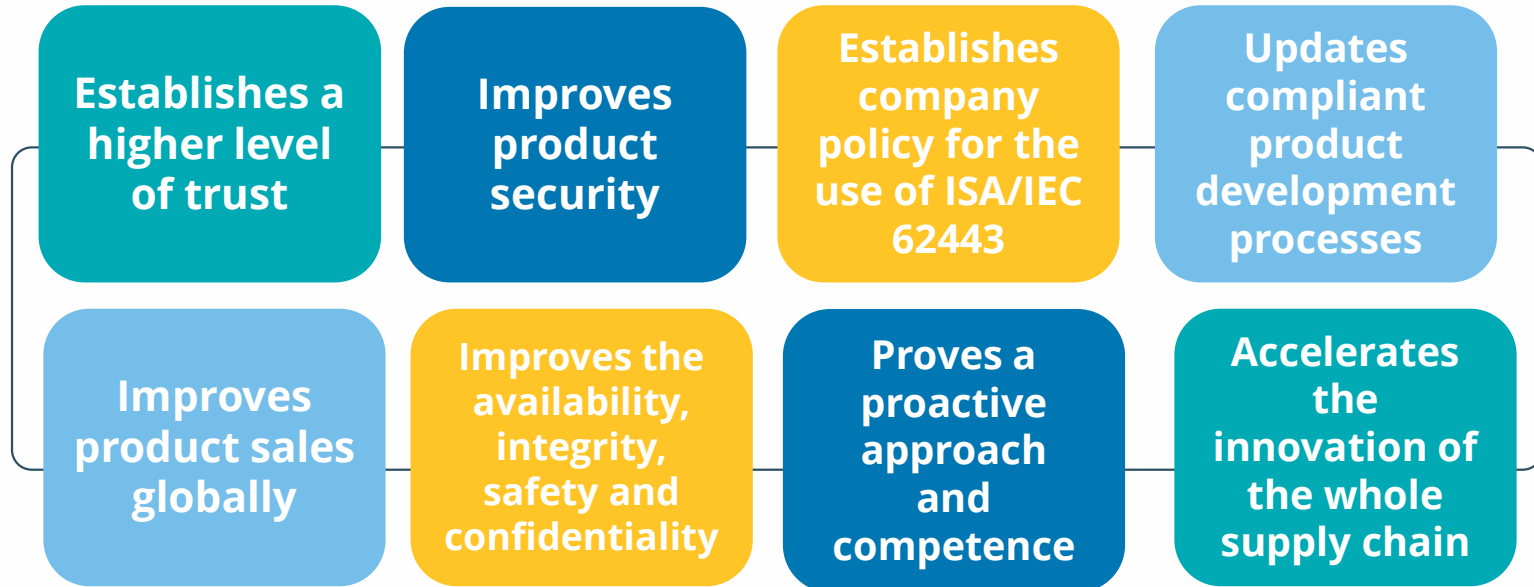- Safety
- Integrity
- Availability
- Confidentiality

Without people who are sufficiently trained, without risk-appropriate technologies and adequate security measures, an IACS exponentially increases its vulnerability to a cyber-attack.

How the ISASecure® scheme works

Security Development Lifecycle Assurance (SDLA)

Security Development Lifecycle Process Assessment (SDLPA)

System Security Assurance (SSA)

Security Development Lifecycle Process Assessment (SDLPA-S)

Security Development Artifacts for Systems (SDA-S)

Functional Security Assessment for Systems (FSA-S)

Vulnerability Identification Testing (VIT-S)

Component Security Assurance (CSA)

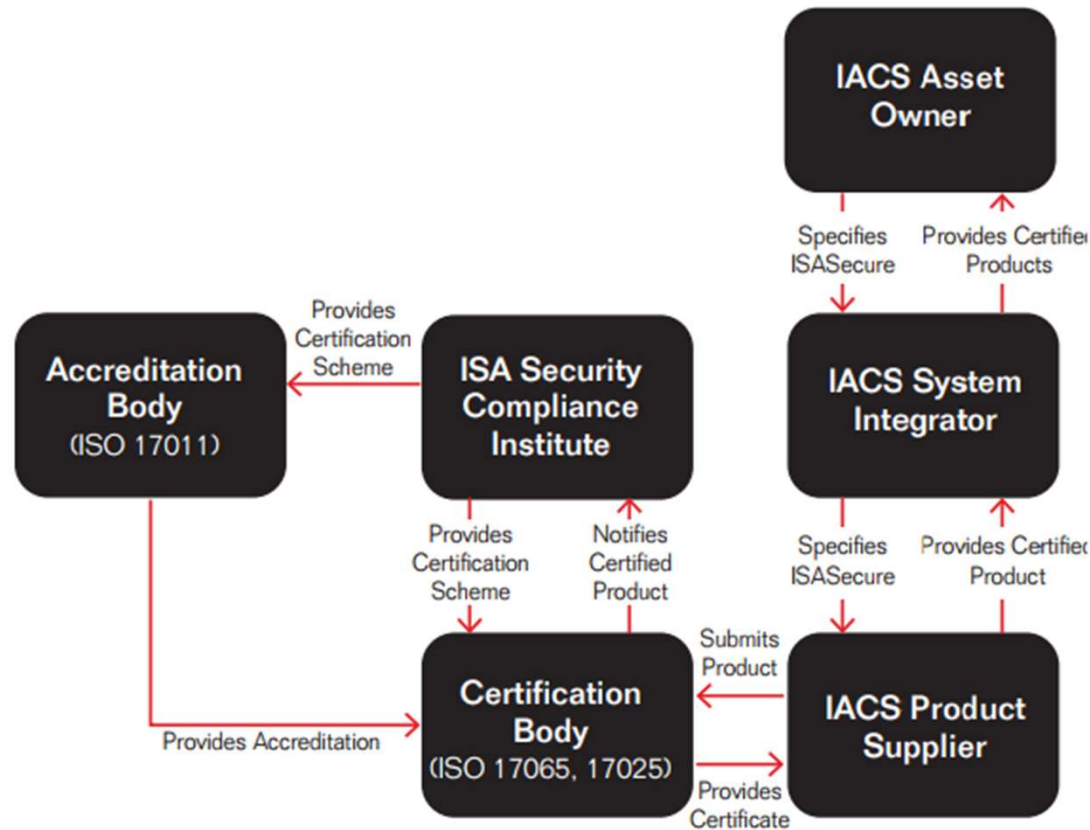Security Development Lifecycle Process Assessment (SDLPA-C)

Security Development Artifacts for Components (SDA-C)

Functional Security Assessment (FSA-C)
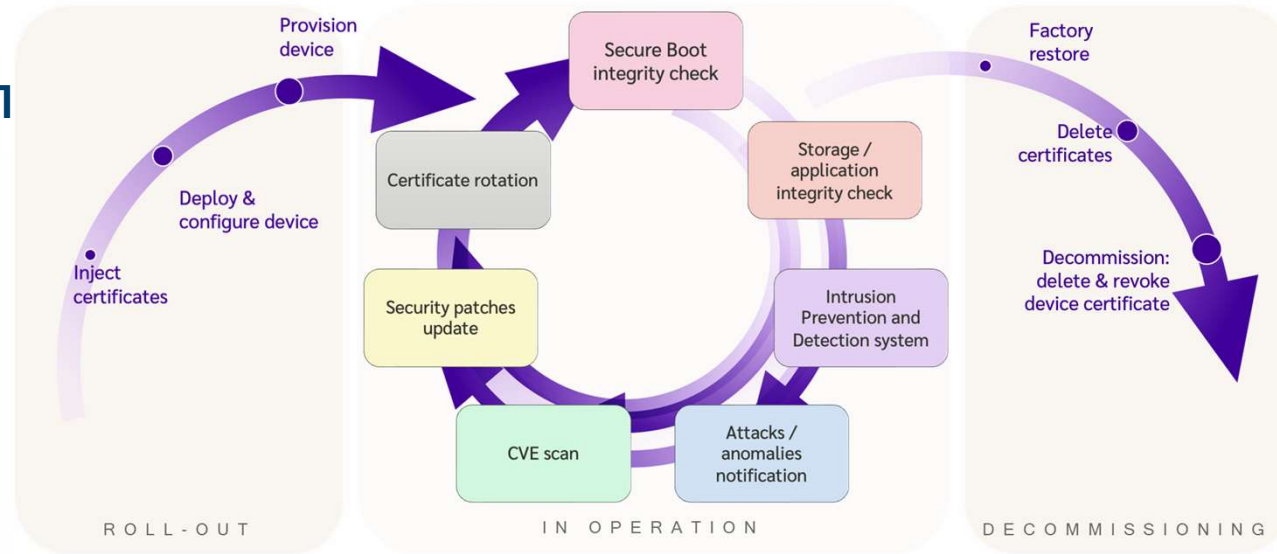
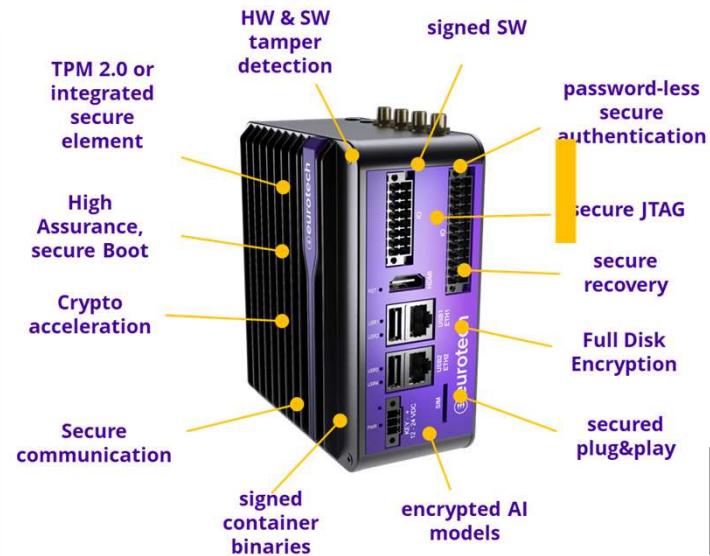Vulnerability Identification Testing (VIT-C)

How the ISASecure® scheme works

ISA/IEC 62443-4-1 ISASecure SDLA Secure Development Lifecycle

ISA/IEC 62443-4-2 ISASecure CSA Component Secure by Design

Regulation compliance fast track

eurotech

cybersecurity framework helps companies comply to Gov. requirements

support for monitoring and updates	support for purchasing compliance	encrypted communication and storage	data integrity, availability & optimized time to recovery	automated security reports	incident prevention, faster recovery, emergency remote procedures	identity theft prevention

remote management system, Intrusion Prevention/Detection, CVE scanning, threat model → *mitigated risks and lower efforts on monitoring and updates*

ISO27001 and 62443-4-1 certifications (i.e. technological *pedigree*) → *reduced risks and minimized efforts on purchasing compliance*

recovery plan, continuous backup, recovery partition, secure boot, anti-tampering → *data integrity, availability and optimized time to recovery*

simplified reporting system, CVE scans, threat/attack detection → *automated security report with full logs for forensic analysis*

Risk assessments and security policies, and their effectiveness

Supply chain: policies for procurement of systems and components

Technology: cryptography, encryption and multi-factor authentication

Business continuity: Managing business operations during security incidents and recovery

Incident response: a plan for handling security incidents

Reporting obligations: stringent times to communicate detailed info on incidents

People: Cybersecurity training and procedures for employees

state-of-the-art cryptography, trusted identity and trusted execution → *encrypted communication and storage*

incident response plan, failsafe recovery, audit log and remote access → *incident prevention, faster recovery, emergency remote procedures*

Zero Trust, automated processes and IEC62443-4-1 certification → *identity theft prevention, providing best practices out of the box*
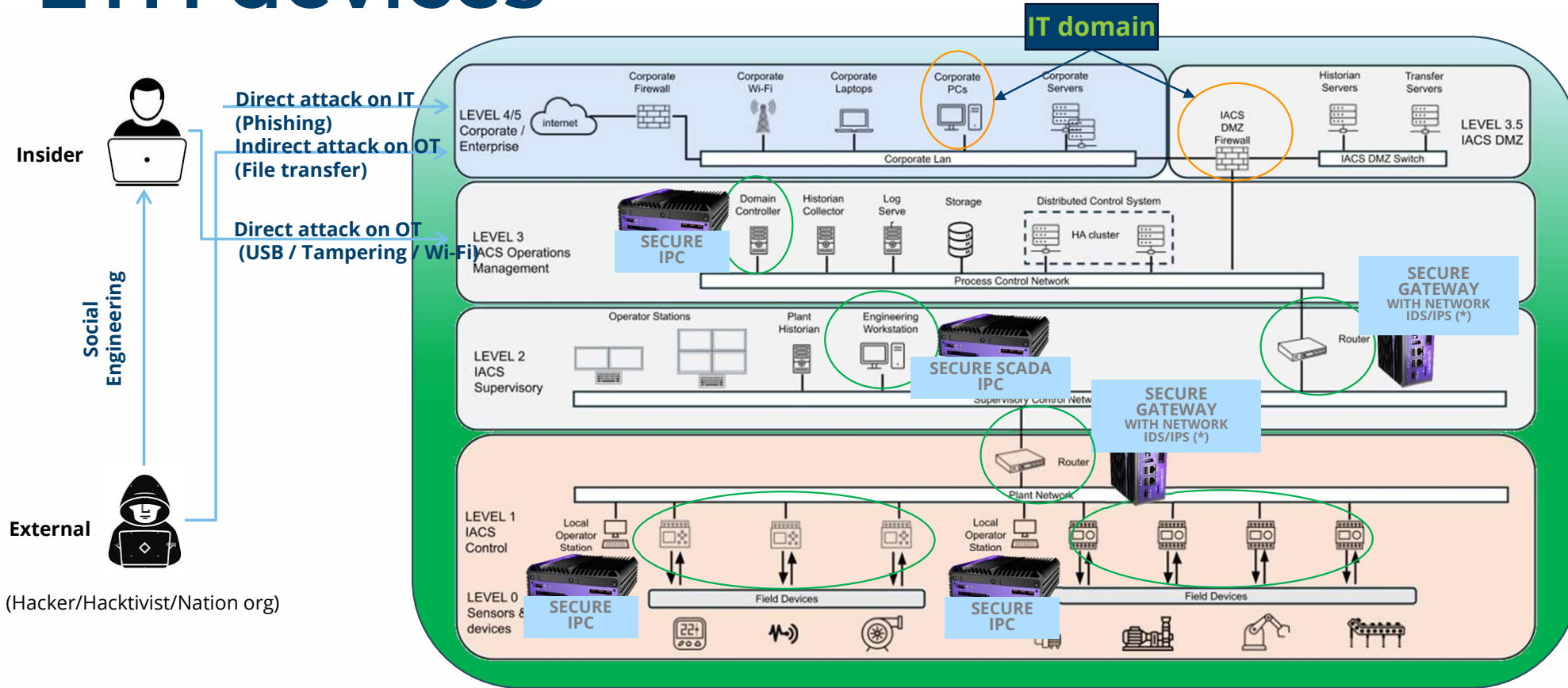
ISA**Secure**®

Most typical threat vectors
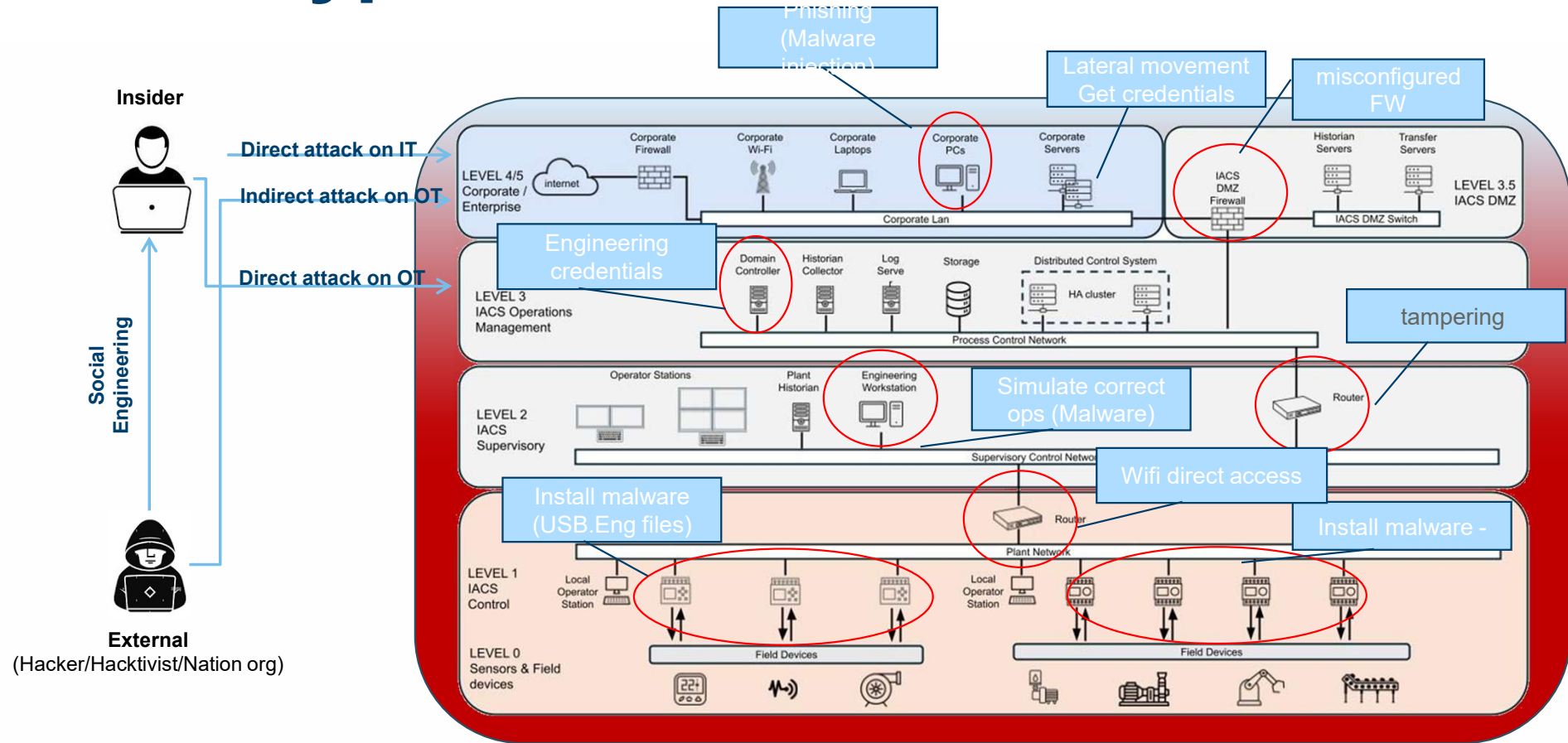
Protect with ISASecure 62443 ETH devices

(*) IDS = Intrusion Detection System
IPS = intrusion Prevention System

Conclusions

1. **In today's rapidly evolving cybersecurity landscape, organizations face increasing pressure to comply with regulations while maintaining operational efficiency.**

2. **Now you have a clear understanding of how to accelerate the cybersecurity compliance journey through the concrete experience of Eurotech and BYHON, utilizing advanced technologies and best practices to create a resilient, scalable, and compliant IIoT/OT infrastructure:**

- Eurotech enables customers to secure, orchestrate, deploy & maintain their Edge systems at scale. Eurotech provides a cybersecure certified edge hardware & software stack to accelerate time to market in critical applications, reduce risks and helps to solve the complexity of integration of the edge with any asset, any edge AIoT application.

- Eurotech is the company with the wide breath of host-network systems certified ISASecure with Security Level 2.

- BYHON, organization of H-ON a TÜV Rheinland Company, is an ANSI Accredited Product Certification Body in compliance with IEC 17065 and Chartered Lab for IEC 17025, that provides Functional Safety certification according to IEC 61508 and Cyber Security certification according to IEC 62443 standard and ISASecure® scheme.

ISASecure – IEC 62443 Conformance Certification

To recap all the ISASecure certification options:

• Component Security Assurance (CSA) - certification to ISA/IEC 62443-4-2

• IIoT Component Security Assurance (ICSA) - certification to ISA/IEC 62443-4-2

• System Security Assurance (SSA) - certification to ISA/IEC 62443-3-3

• Security Development Lifecycle Assurance (SDLA) - certification to ISA/IEC 62443-4-1

• ACS Security Assurance (ACSSA) - certification to ISA/IEC 62443-2-1, 2-4, 3-2 and 3-3

H-ON a TÜV Rheinland Company dba BYHON

Be Part of the Movement to
Prioritize OT Cybersecurity

Change the Culture

Recognize cybersecurity as a fundamental workplace tenet

alongside functionality, efficiency, and safety

Learn more | www.isagca.org

ISA Cybersecurity Resources

Free guidance, training, and more:

ISA Global Cybersecurity Alliance - www.isagca.org

A collaborative forum to advance OT cybersecurity and understanding of ISA/IEC 62443

ISASecure www.isasecure.org

The world's leading conformance certification program for ISA/IEC 62443

ICS4ICS www.ics4ics.org

Improve how cybersecurity incidents are managed with training, processes, and exercises

Get involved:

- ISA/IEC 62443 standards available from ISA (free access with ISA professional membership!)
- Cybersecurity training and certificate program
- Help develop the standard – open to all at no charge – www.isa.org/ISA99