# TeleTrusT-EBCA "PKI-Workshop" 2022

**Berlin, 29.09.2022**

# IoT Firmware Cybersecurity according to IEC 62443

**Hamza Ben Ammar, Teligencia**

TeleTrusT

*Pioneers in IT security.*

Bundesverband IT-Sicherheit e.V.

Teligencia

# IoT Security according to IEC 62443

**Dipl.Ing Hamza Ben Ammar**

# PKI & STANDARDS

# PKI & IoT Devices

Legislative and industry bodies have addressed the unique nature of data security within different IoT verticals.

**Data security requirements (examples):**

- HIPAA
- PCI
- FERPA
- CALEA

are evaluated to ensure the standards are sufficient to secure IoT devices and make sure providers deliver proper security.

**Today -> Future**

- Fully interconnected systems across locations and companies
- Public/private cloud services for ICS
- Operator models/Admin Asset Shells
- Remote OTA-Software-Update
- Remote Device Management
- Less non-critical infrastructure Crypto agility and PQC

# Threats associated with ICS

01
- **Denial of service**

02
- **Breach of trade secrets**

03
- **Shortage of supply**

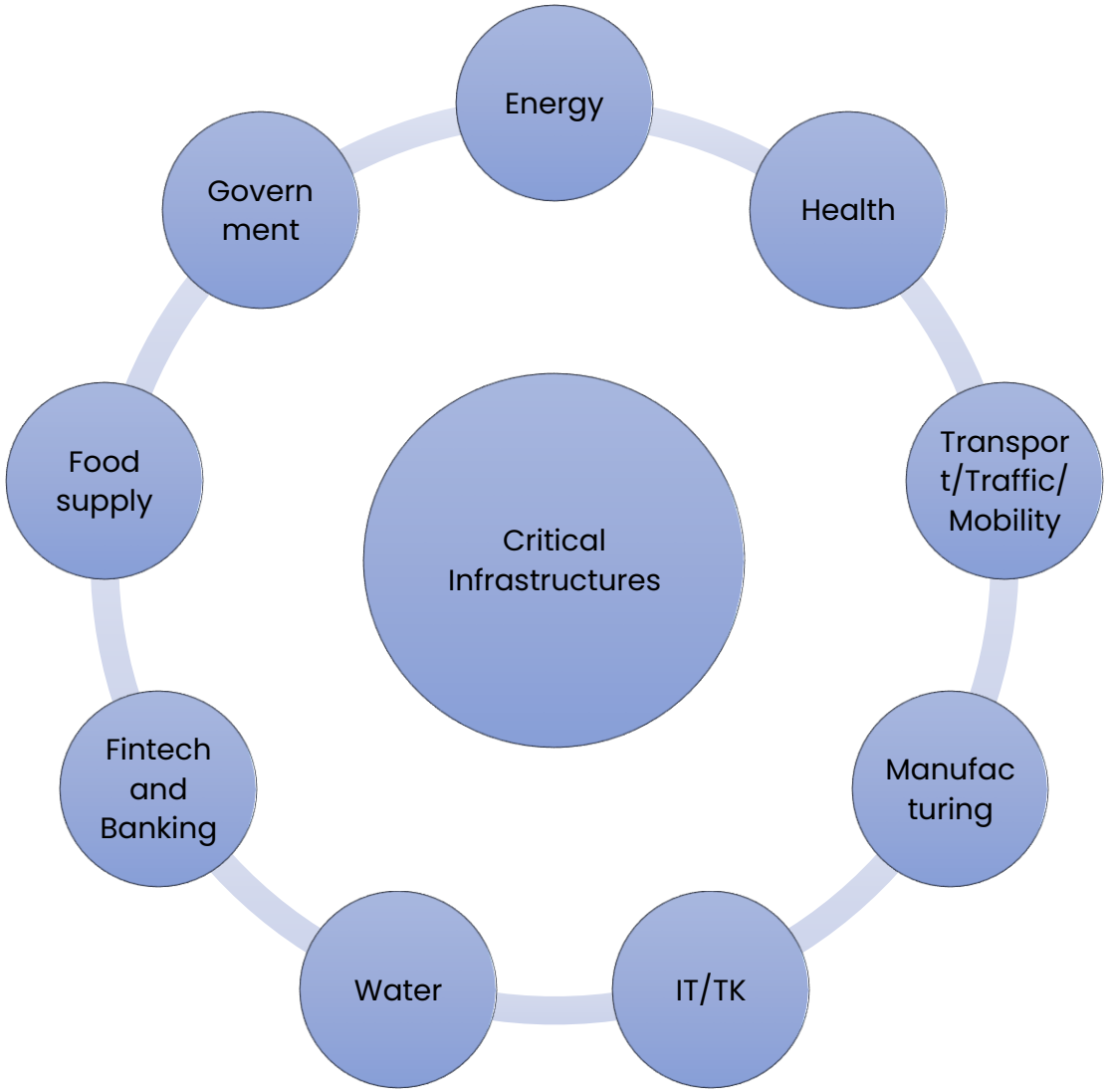
04
- **Environmental damage**

05
- **Damage/loss of life**

06
- **Loss of production**

07
- **Regulatory violations**

08
- **Image damage**



# Secure Update Management

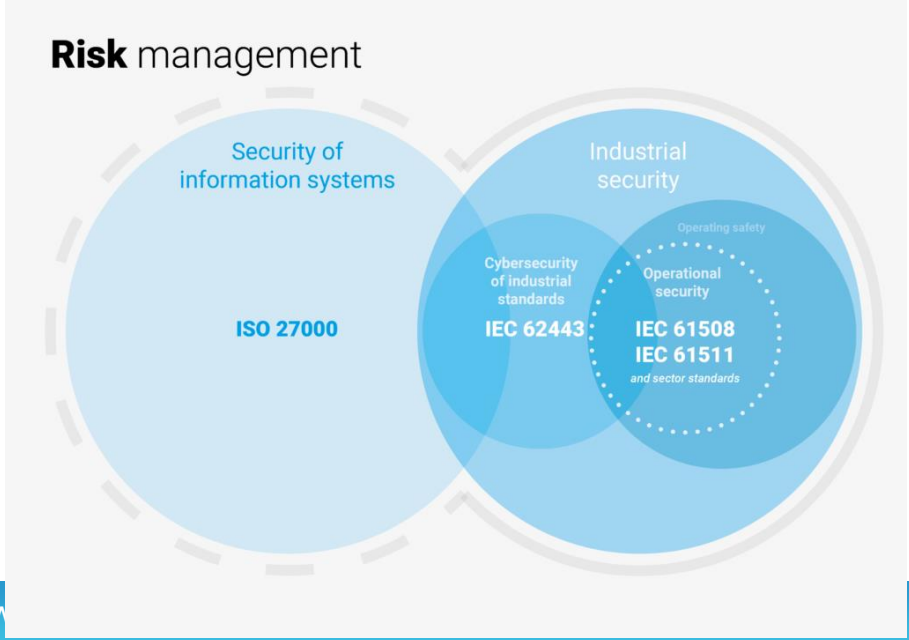
Signed firmware-updates

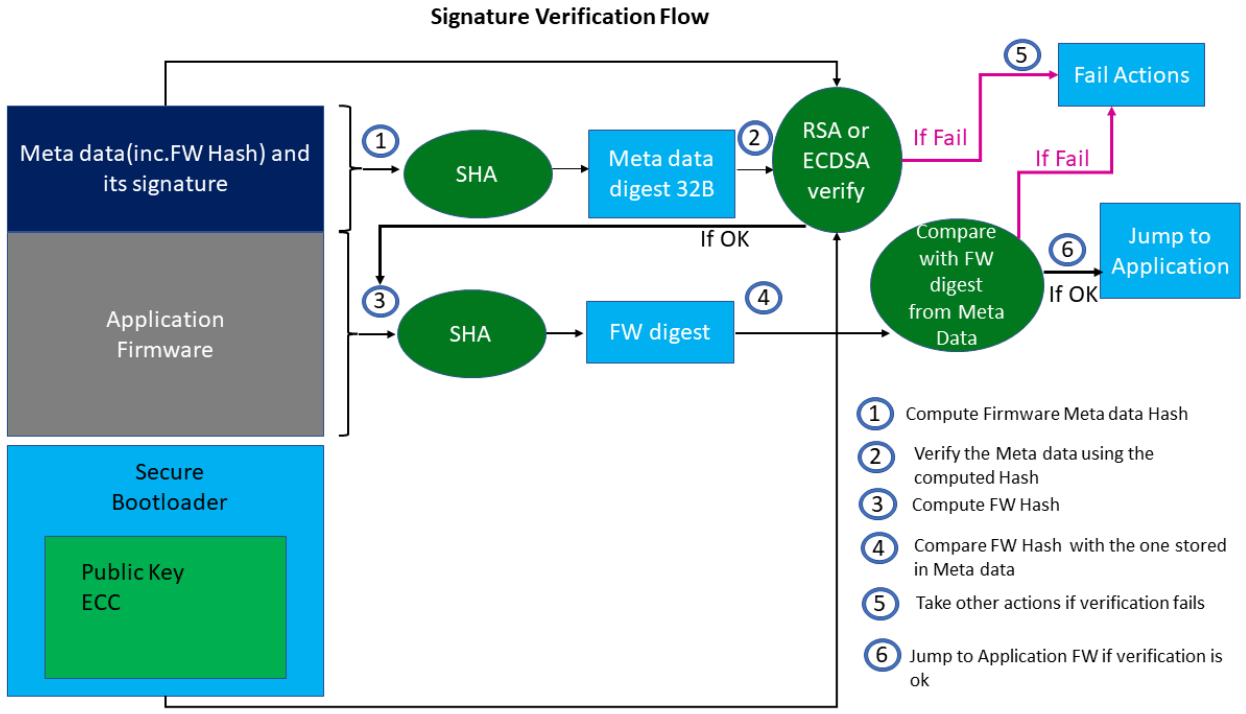
Protection against malware and software modifications

Verification of the software's authenticity before performing the update

Authorization

- Activation of functionality/features
- Acceptance of 3rd party software



# IEC 62443

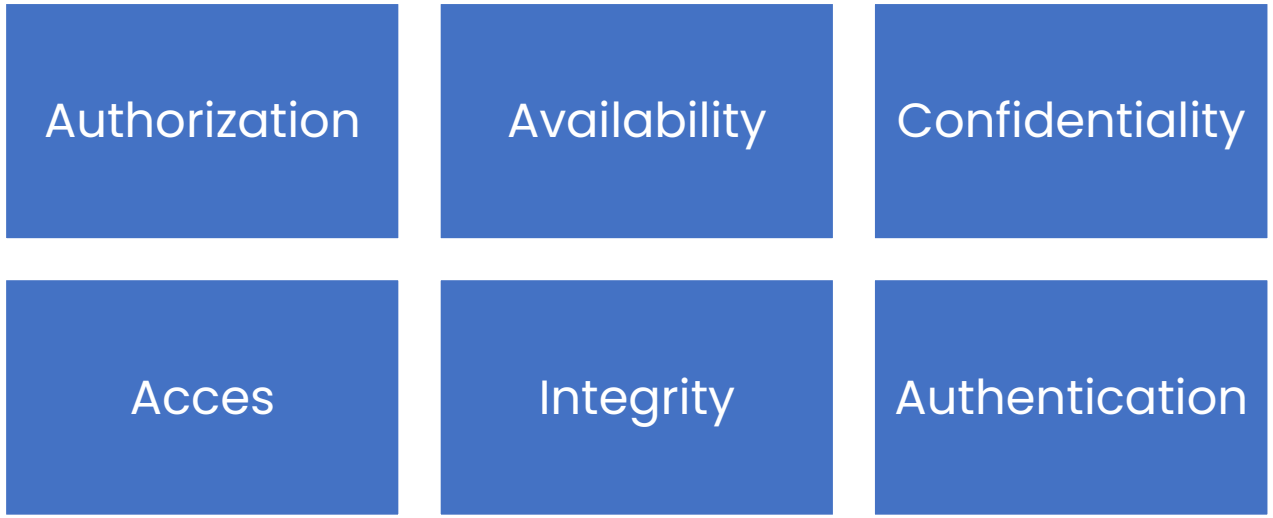
## Industrial Automation & Control System

| General | Policy & Procedure | System | Component |
|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **General** | **IEC 62443-1-1**<br>Terminology, Concepts and Models | **IEC TR-62443-1-2**<br>Master Glossary of Teams and Abbreviations | **IEC TR-62443-1-3**<br>System Security Conformance Metrics | **IEC TR-62443-1-3**<br>IACS Security Lifecycle and Use-Cases | |
| **Policies & Procedures** | **IEC 62443-2-1**<br>Establishing an Industrial Automation and Control System Security Program | **IEC TR-62443-2-2**<br>IACS Protection Levels | **IEC TR-62443-2-3**<br>Patch Management in the IACS Environment | **IEC TR-62443-2-4**<br>Requirement for IACS Service Providers | **IEC TR-62443-2-5**<br>Implementation Guidance for IACS Asset Owners |
| **System** | **IEC TR 62443-3-1**<br>Security Technologies for IACS | **IEC TR-62443-3-2**<br>Security Risk Assessment and System Design | **IEC TR-62443-3-3**<br>System Security Requirments and Security Levels | | |
| **Component** | **IEC 62443-4-1**<br>Product Development Requirements | **IEC 62443-4-2**<br>Technical Security Requirments for IACS Components | | | |

# IEC 62443

The assets to be protected are defined in a broad framework, suitable for each specific case. IEC 62443 establishes the assets and capacities to be protected as follows:




The 2 most important aspects or definitions of the measures found throughout the legislation are:

•**Security zones:** A group of physical or logical assets that share common security requirements. A zone clearly delimits the whole by defining a logical or physical border that separates internal and external parts.

•**Gateways:** These are communication paths between two security zones. They provide the security features that allow two zones to communicate securely. All communication between different areas must be performed through a gateway.

# Secure Update Management

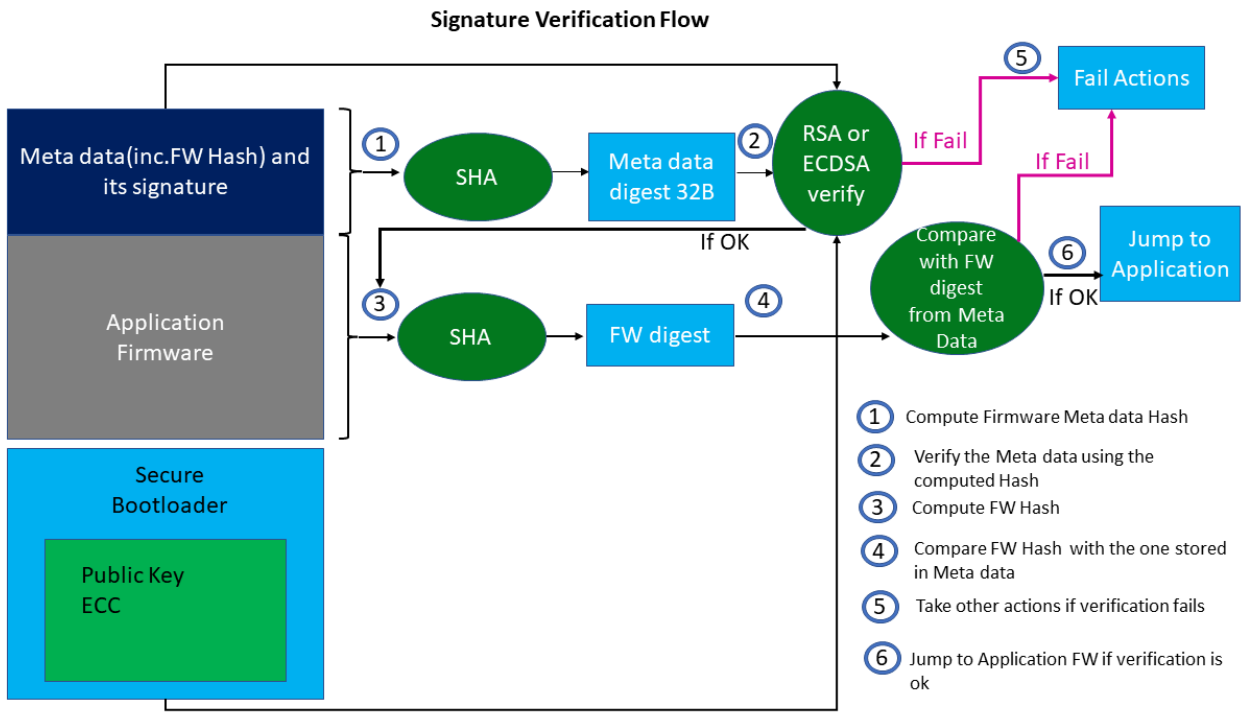
Signed firmware-updates

Protection against malware and software modifications

Verification of the software's authenticity before performing the update

Authorization

- Activation of functionality/features
- Acceptance of 3rd party software



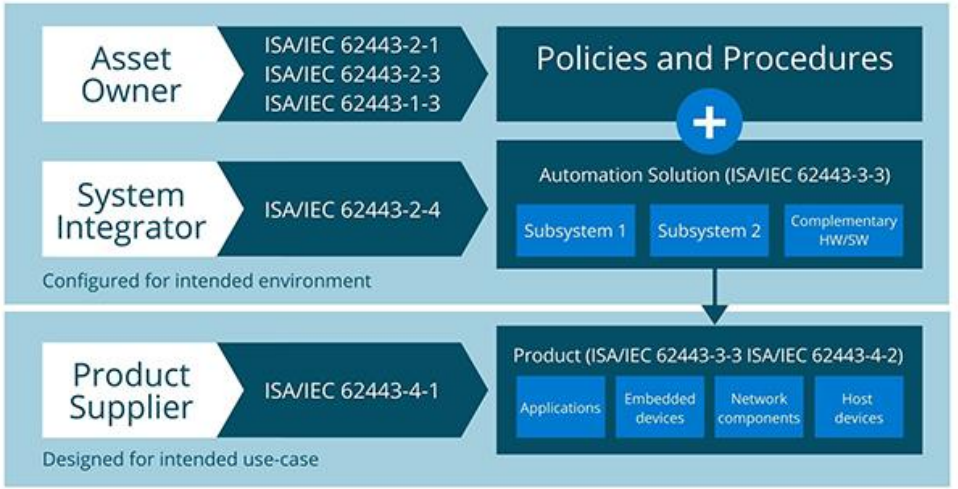
# Public key infrastructure (PKI) certificates

| Security Level | Node | Switch | Forwarder | Gateway | Border Gateway |
|---|---|---|---|---|---|
| 1 | Not Applicable | | | | |
| 2,3,4 | Requirement: ISA-62443-4-2 CR 1.8 When public key infrastructure (PKI) is utilized, use of PKI shall be according to ISA-62443-3-3 SR 1.8 | | | | |
| | Test: Verify that certificate expirations dates are acceptable. | | | | |

# IEC 62443 Methodology

The different stages of the methodology are as follows:

- Understanding and breakdown of the system or product under study, its functionalities, and the most critical assets to protect.
- Analysis of vulnerabilities.
- Segmentation of the system or product under study into security zones; identification of its access points and the interactions between zones; marking the assets to be protected.
- Study of external attack scenarios; identification of possible threats.
- Scenario cross-checking between the system or known product and external attack options. Assessment of the impact on security; initial conclusions on the cybersecurity of the system.
- Mitigation measures and attainment of SL levels (1-4).



# Risk Assessment IEC 62443 vs Other Standards

## Not every system is equally critical

- The interest of this first analysis is to assess the likelihood of threats while taking into consideration the degree of impact.
- This also allowed them to deduce the level of risk, wich gives a clear idea of the most harmful vulnerabilities.
- The threats identified exploit the fact that the security level of the FR under study (IAC) is limited to SL0.
- The impact assessment takes the following factors into consideration:
  - The mission of the system or the business processes involved.
  - The criticality of the system, derived from the value of the data to the organization.
  - The sensitivity of the system and its data.

| | TOE | Product | Assess Process | Design | Quality Test | Level | #req |
|---|---|---|---|---|---|---|---|
| **IEC 62443-4-1** | I S | | (X) | (X) | (X) | - | 48 |
| **IEC 62443-4-2** | I S | X | | (X) | | SL | 88 |
| **ISO/IEC 11889** | S | X | | X | | - | N/A |
| **ISO/IEC 27402** | D | (X) | (X) | | | - | 13 |
| **GP SESIP** | S | X | (X) | X | | EAL | 53 |
| **ETSI EN 303645** | C D | X | X | | | o | 67 |
| **ETSI TS 103701** | C D | (X) | X | | X | | 109 |

# Understanding ISA/IEC 62443 Standards for IoT Manufacturers

Practitioners and customers often ask if we “comply” with ISA/IEC 62443.

This is a bit of a misnomer, as 62443 is not a regulation mandated by a government or industry agency, such as NERC-CIP is for the energy industry.

***Instead, 62443 is a set of recommended standards that can help companies with industrial automation and control systems protect and secure those systems.***

Industry seek to confirm compliance as they have adopted 62443 as a corporately mandated cyber security standard That said, their products *security capabilities and features meet the foundational and security level requirements of* the relevant 62443 standards and fulfill the compliance requirement.

# Reaching IEC 62443 Compliance By Using Certified Components

The NXP security primitives can help engineers find a security solution that fits their projects' needs. However, every project is unique, and so is the security solution needed.

Engineers can choose from various powerful yet efficient SoCs with integrated security solutions, dedicated secure elements, or a combination of both—whichever best meets their requirements.

2 prominent examples of MCUs with enhanced integrated security features include selected devices from the LPC5500 family of MCUs and i.MX RT1180 crossover MCU.

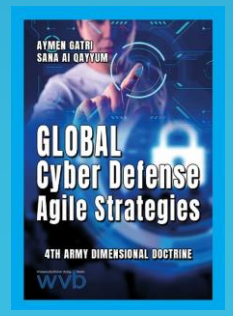
For example, specific models of the Arm® Cortex®-M33-based LPC5500 MCUs integrate security features such as Arm TrustZone®, a PRINCE block cipher module for real-time encryption and decryption of data written to and read from the flash memory, AES-256 encryption/decryption engine, and SRAM PUF-based unique key storage. These features allow the LPC5500 series to be used in secure edge devices in both consumer and industrial settings. Some devices in the LPC5500 family are certified for SESIP Assurance Level 2.


# TEAM

## Dr. Ing Aymen Gatri, MBA

Co-Founder CEO, Neuss

- PhD Telecommunications, UK, MBA USA-Japan Entrepreneurship
- 13+ Digitalization transformation and Cyber security Experience with : Daimler AG, Siemens, NAVTEQ, NOKIA, Metso Outotec
- Alumni of Warsaw security Forum, MSC, DAG




## Dipl. Ing Hamza Ben Ammar

Co-Founder CTO, Karlsfeld

- Dipl. Ingenieur Cybersecurity
- 9+ offensive Cyber Security Experience
- Certified Ethical Hacker V10
- Senior Cyber security Expertise with HypoVereinsbank, Orange Telecom, Brain loop, etc..

C|EH™
Certified Ethical Hacker

## David Venable

Advisory Board Member Dallas, USA

- VP Masergy Group, USA
- Founder Vanda Security
- Adjunct faculty at the National Cryptologic School "NSA".
- Former intelligence professional with the U.S. National Security Agency NSA cryptography.

Most Influential People in Security 2019

**David Venable**
*Vice President of Cybersecurity*
*Masergy*
CYBERSECURITY

## Philip Sparks

Advisory Board Member Frankfurt

- CEO and Co-founder of ICanDo52.
- Professor of innovation/business execution and management consultant
- Executive Experience in government, military and private sector.
- Author over 15 programs in Risk Management, Cyber Security, Executive Development, Innovation and ICT.

Deutsche Bank

# CONTACT US

Thanks for your commitment to Privacy, Safety & Security!
Thank you for your attention!


+49-21315328428

info@teligenica.com

https://www.teligencia.com/

Engelbertstraße 19, 41462
Neuss, Germany