Security in industrial systems and its future

Kent Yoshida, Renesas Electronics Corporation

CIP Mini Summit, Lyon Convention Centre, October 31, 2019

Unstoppable cyber-attacks on the industry

***LockerGoga**, ransomware for encryption, 2019*

A huge aluminum plants hit by cyber-attacks, https://www.bbc.com/news/business-48661152

Loss scale:

- Forced to manually work until recovered after 3 months
- **Over 55 million US dollar**

Characteristic:

- Used legitimate credentials
- The purpose is not only demanding ransom, but **shutting down the target organization**

Increasing awareness of cybersecurity

- Most of the vulnerabilities released in the first half of 2019 are related software used for **the industrial control systems, ICS**.
- It is 36%* decreased from the second half of 2018.
- Increased security awareness due to cybersecurity laws like **NIS directive** contributed.
  NIS directive: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

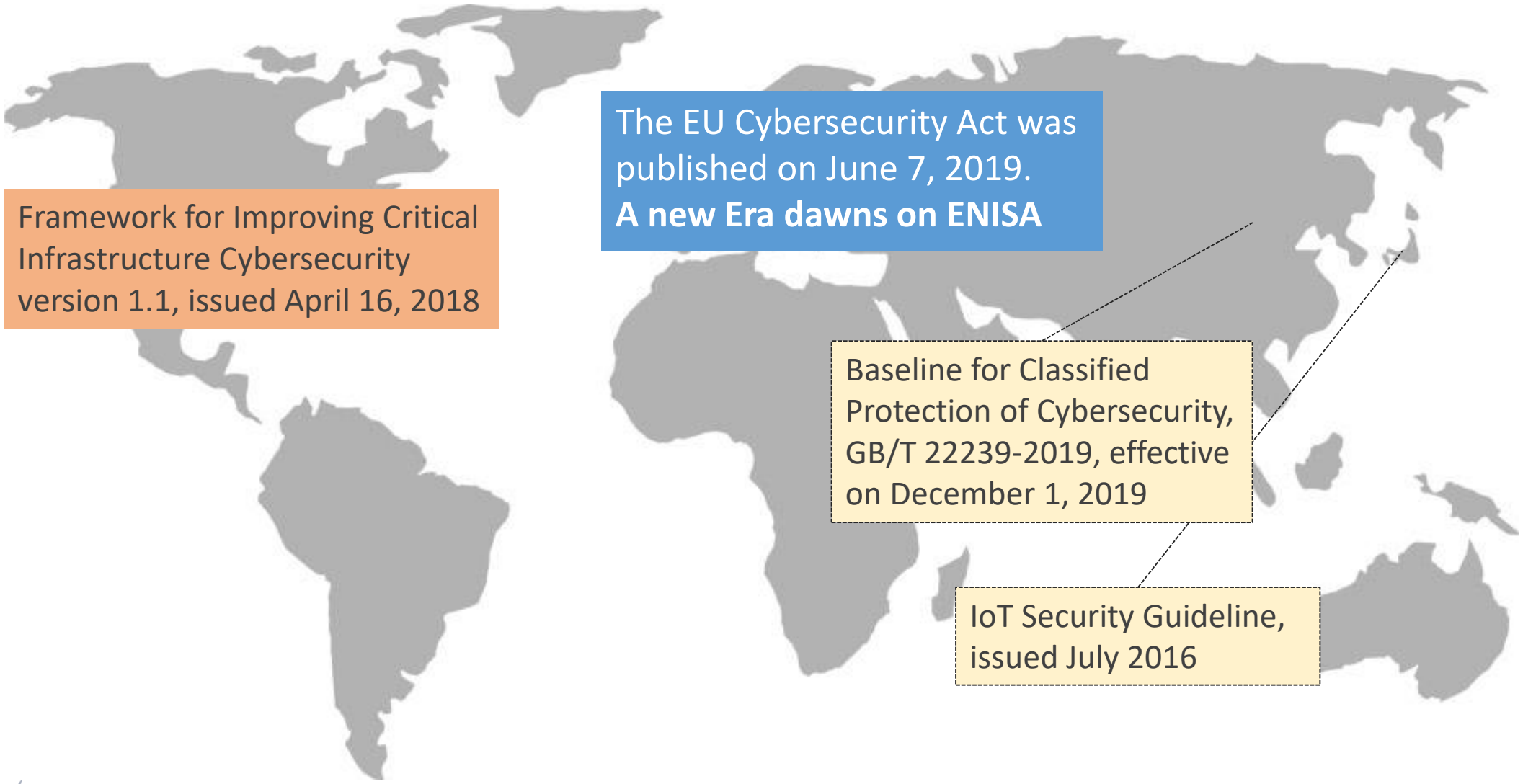
*The data from "Zero Day Initiative, ZDI" operated by TREND MICRO

ICS related vulnerabilities

ICS related Zero Day vulnerabilities

CIVIL INFRASTRUCTURE PLATFORM

Expectations of IEC 62443



Framework for Improving Critical Infrastructure Cybersecurity version 1.1, issued April 16, 2018

The EU Cybersecurity Act was published on June 7, 2019.
A new Era dawns on ENISA

Baseline for Classified Protection of Cybersecurity, GB/T 22239-2019, effective on December 1, 2019

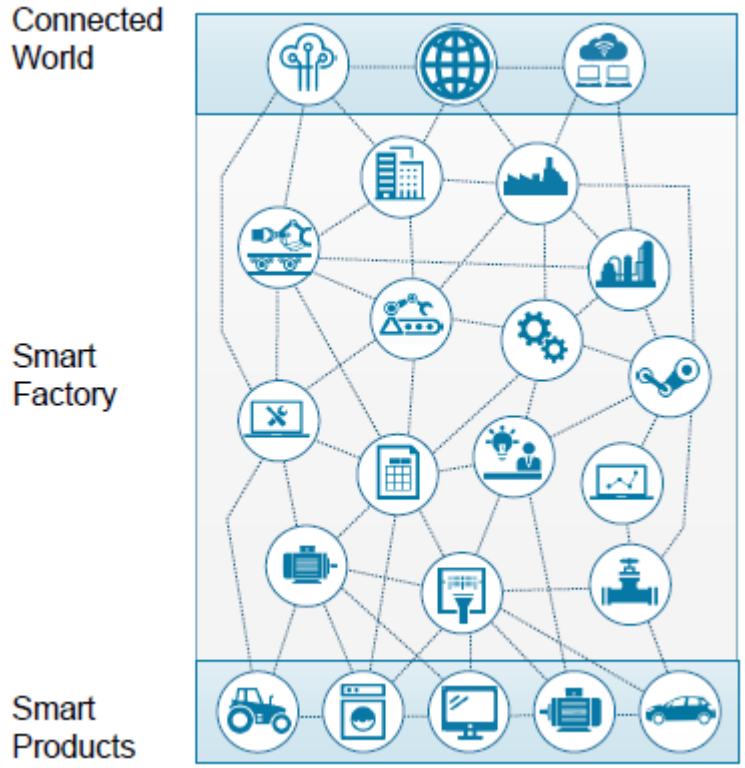
IoT Security Guideline, issued July 2016

Be standard and open

- In Industry 4.0, small IoT units connect to form a larger IoT.

Features of a larger IoT, i.e. system of systems (SoS):

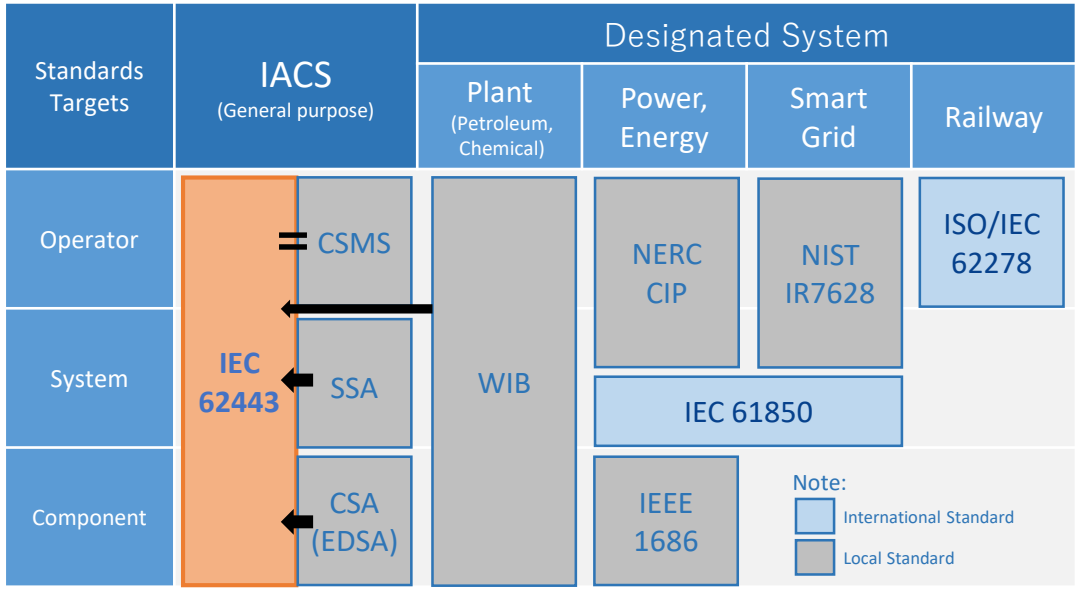
- **Evolving continuously** without perfection
- Realize **new purposes and functions** by connecting
- Geographically **distributed**

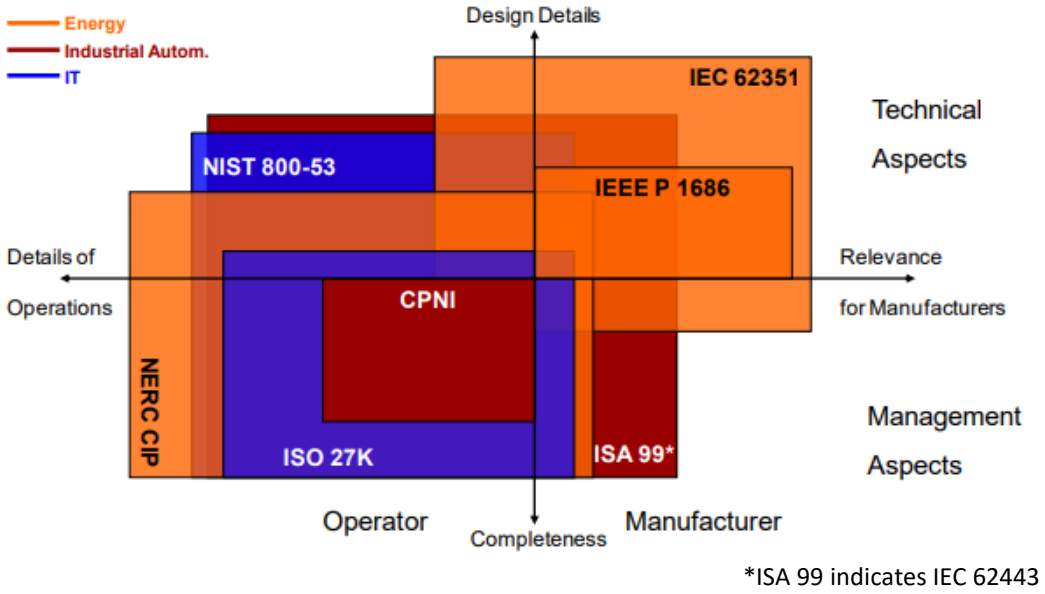


Cited from RAMI 4.0, Graphics © Anna Salari, designed by freepik

As integrated security standard for the industry

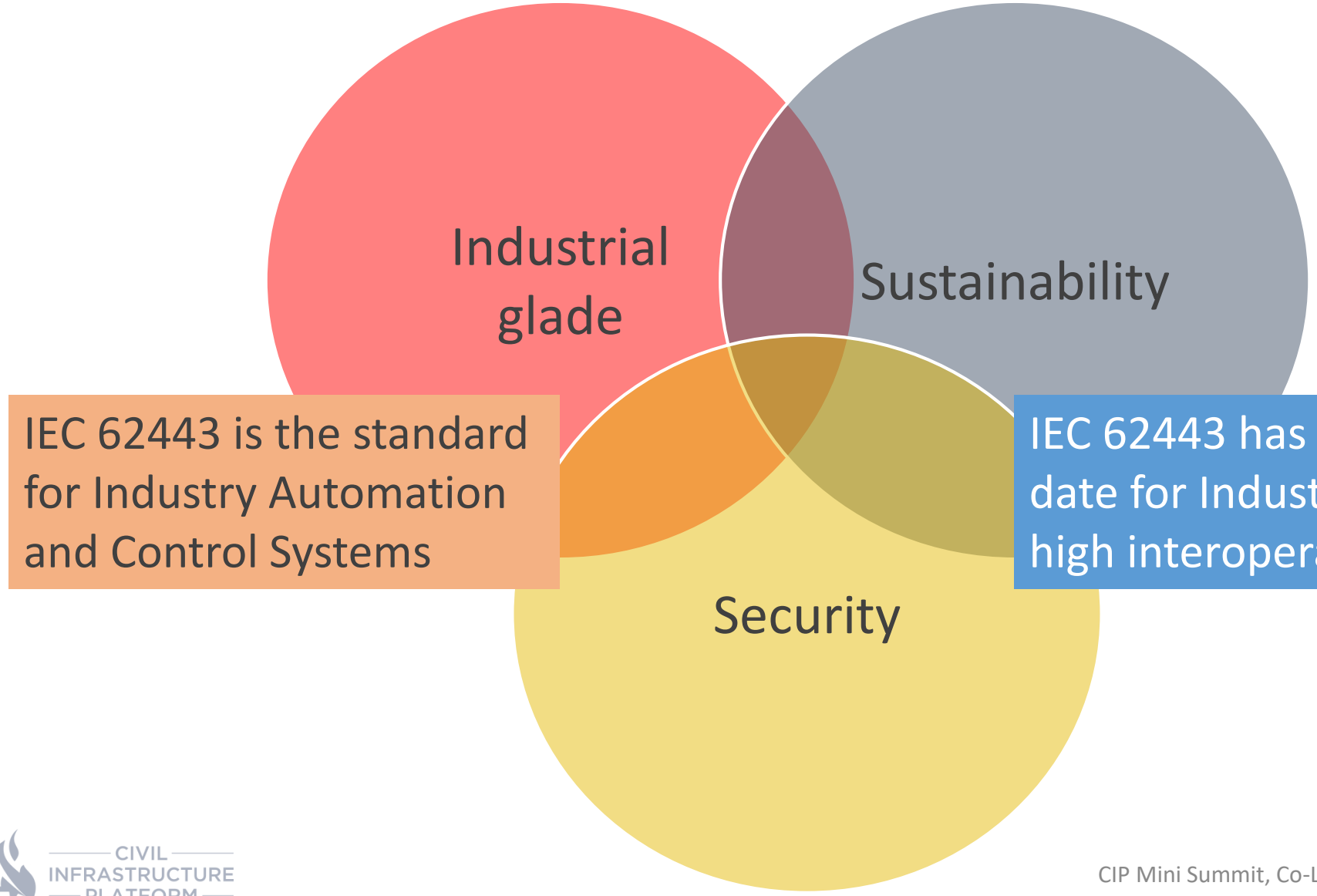
- **IEC 62443** is an international standard series that integrates major industrial security standards for each industry. And the series is **for all players** in the industrial automation and control systems, IACS.





*ISA 99 indicates IEC 62443

Comparison of IEC 62443 with CIP's key challenges



IEC 62443 is the standard for Industry Automation and Control Systems

IEC 62443 has been kept up to date for Industrie 4.0 and has high interoperability.

Target products of IEC 62443-4 series

- Linux is used for lots of target devices of IEC 62443-4 series.

Embedded device

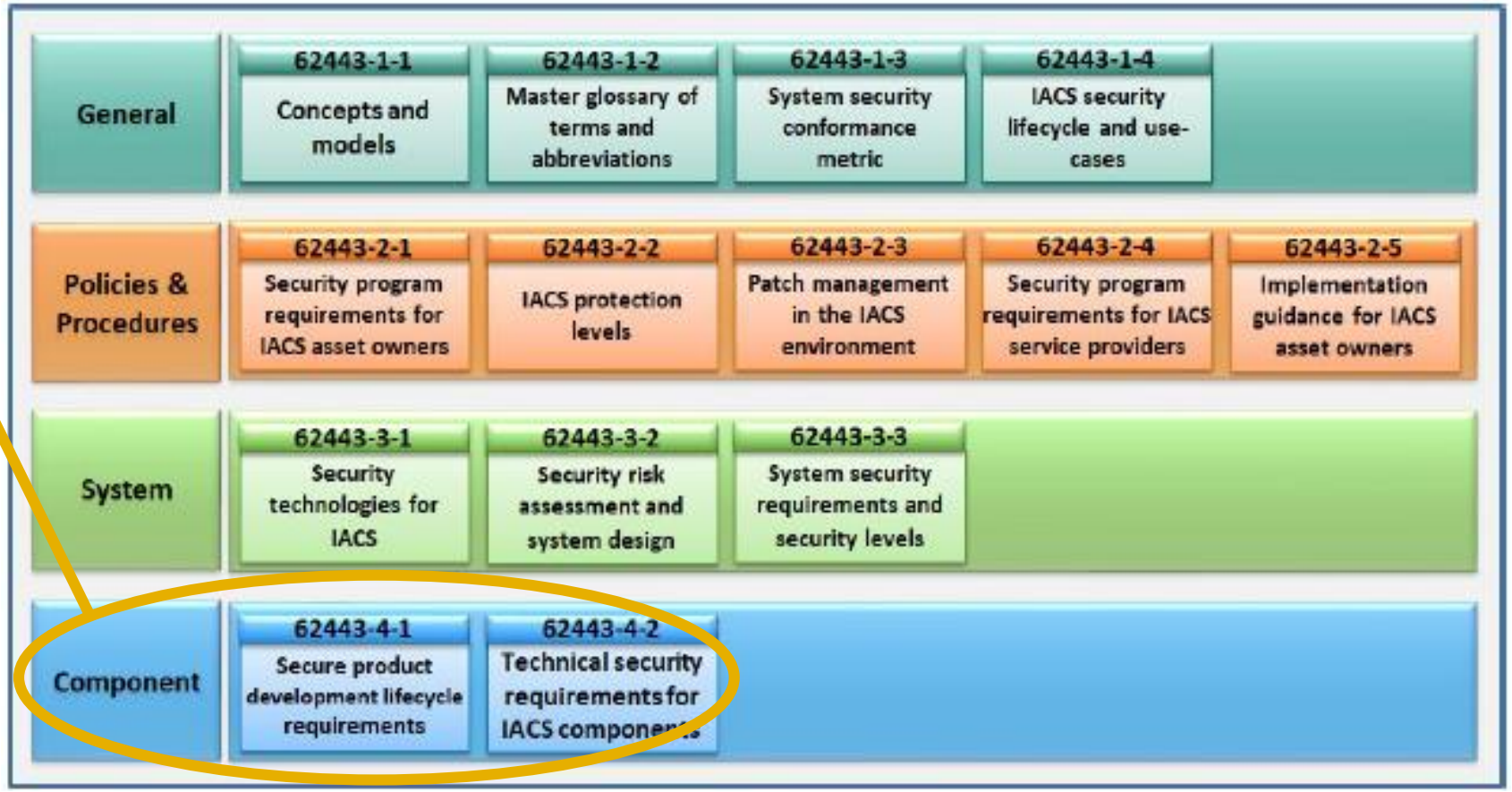
PLC, IED(with HMI), ...

Network device

Switch,
VPN terminator, ...

Host device/application

Operation workstation,
Data historian, ...



Mission and goal

- Security working group's mission:

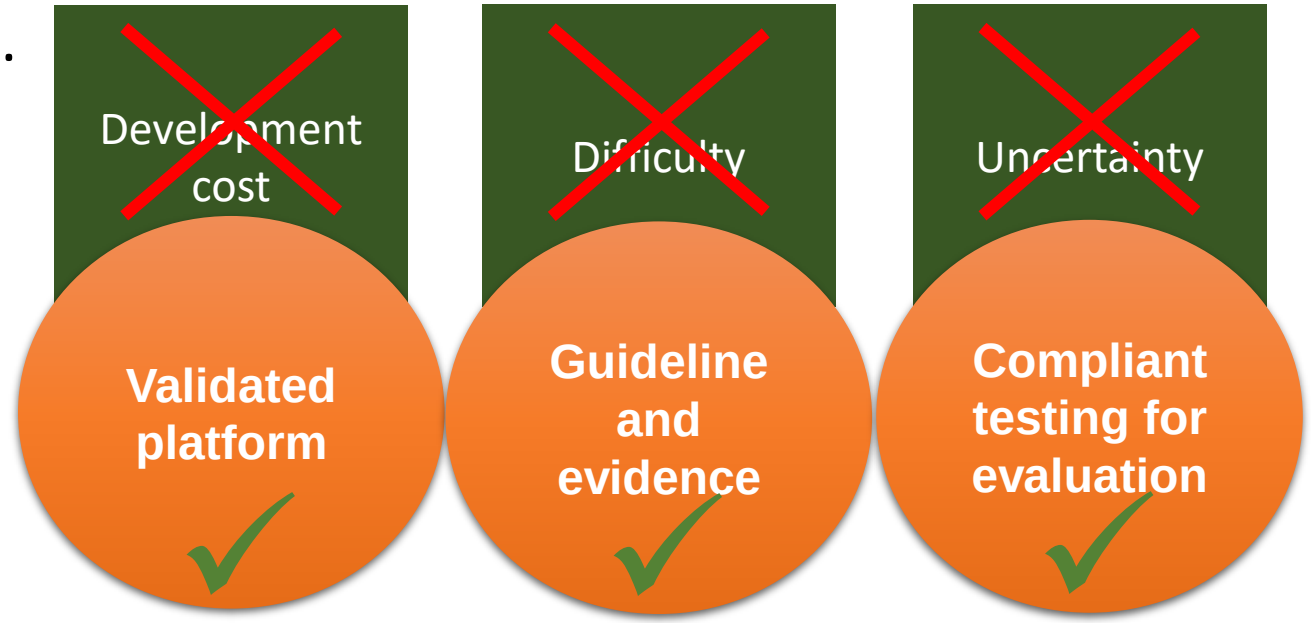
  Provide "Open source base layer - OSBL" needed for developing products compliant with IEC 62443-4-2 security requirements as well as to keep its security up to date.

- Goal:

  Get suppliers IEC 62443-4-2 certified.

  For that...

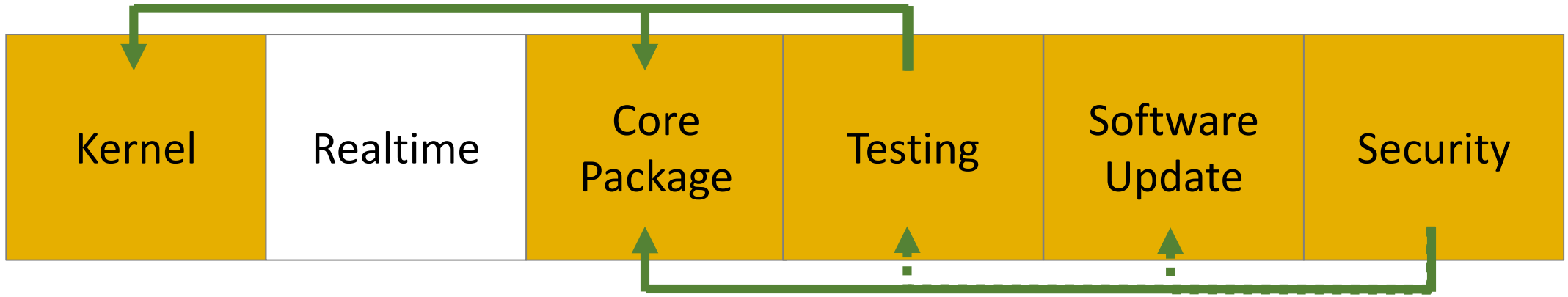
  Our solution makes certification easier!



CIP security implications

- What we do against the new upcoming vulnerabilities day by day?
  - To be maintained **whole life cycle** of products,
  - Software updating,
  - Testing, ...

CIP activities:



Current and future activity results

- Our solution makes certification easier:

  To reduce the development cost

  - Provide commonly required packages for IEC 62443-4-2 – **Package lists**
  - Maintain the common packages in collaboration with CIP-Core group
  - Manage the development process of the packages as per IEC 62443-4-1, *Under consideration*

  To clarify how to obtain certification

  - Define the user obligation – **Application rules/restricts**
  - Provide compliant testing environment for certification, *To be discussed*

Thanks you!

CIVIL
INFRASTRUCTURE
PLATFORM

Question?

CIVIL
INFRASTRUCTURE
PLATFORM

Thanks you!

CIVIL
INFRASTRUCTURE
PLATFORM