THE LINUX FOUNDATION PROJECTS

CIVIL INFRASTRUCTURE PLATFORM

The international effort to establish OSBL of cyber security for IACS

Kento Yoshida, Renesas Electronics Corporation,
Security working group chair of the CIP project

@OSS/ELC EU, Oct. 28, 2020

The CIP project and security working group

What is the “CIP” project

CIVIL
INFRASTRUCTURE
PLATFORM

To establish a “base layer” of industrial-grade tooling

using the Linux kernel and other open source projects

The key challenges

- Apply IoT concepts to industrial systems.
- Ensure quality and longevity of products.
- Keep millions of connected systems secure.

Industrial grade

- Reliability
- Functional Safety
- Real-time capabilities

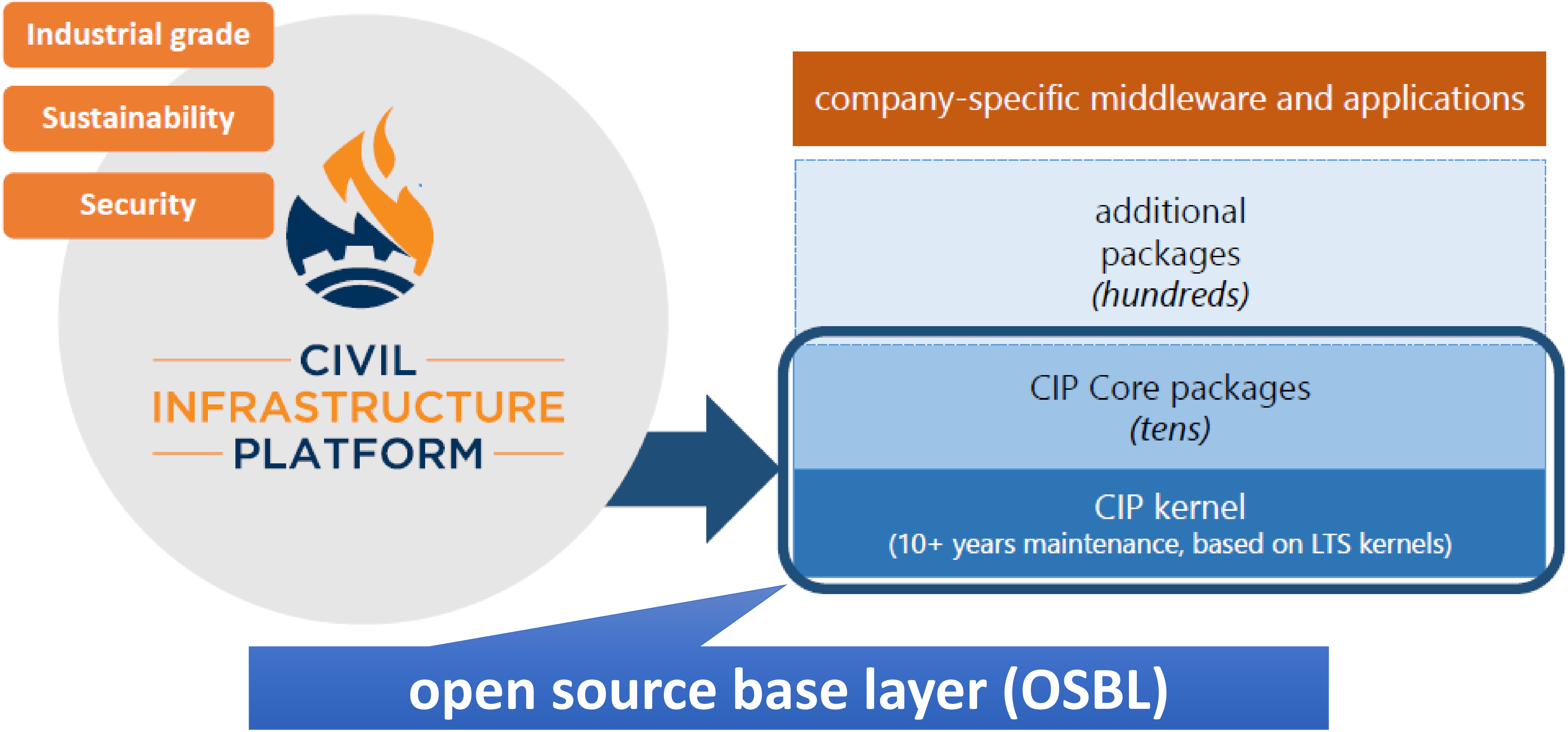
Sustainability

- Product life-cycles of decades
- Backwards compatibility
- Standards

Security

- Security & vunerability managment
- Firmware updates
- Minimize risk of regressions

What is “OSBL”



Industrial grade

Sustainability

Security

company-specific middleware and applications

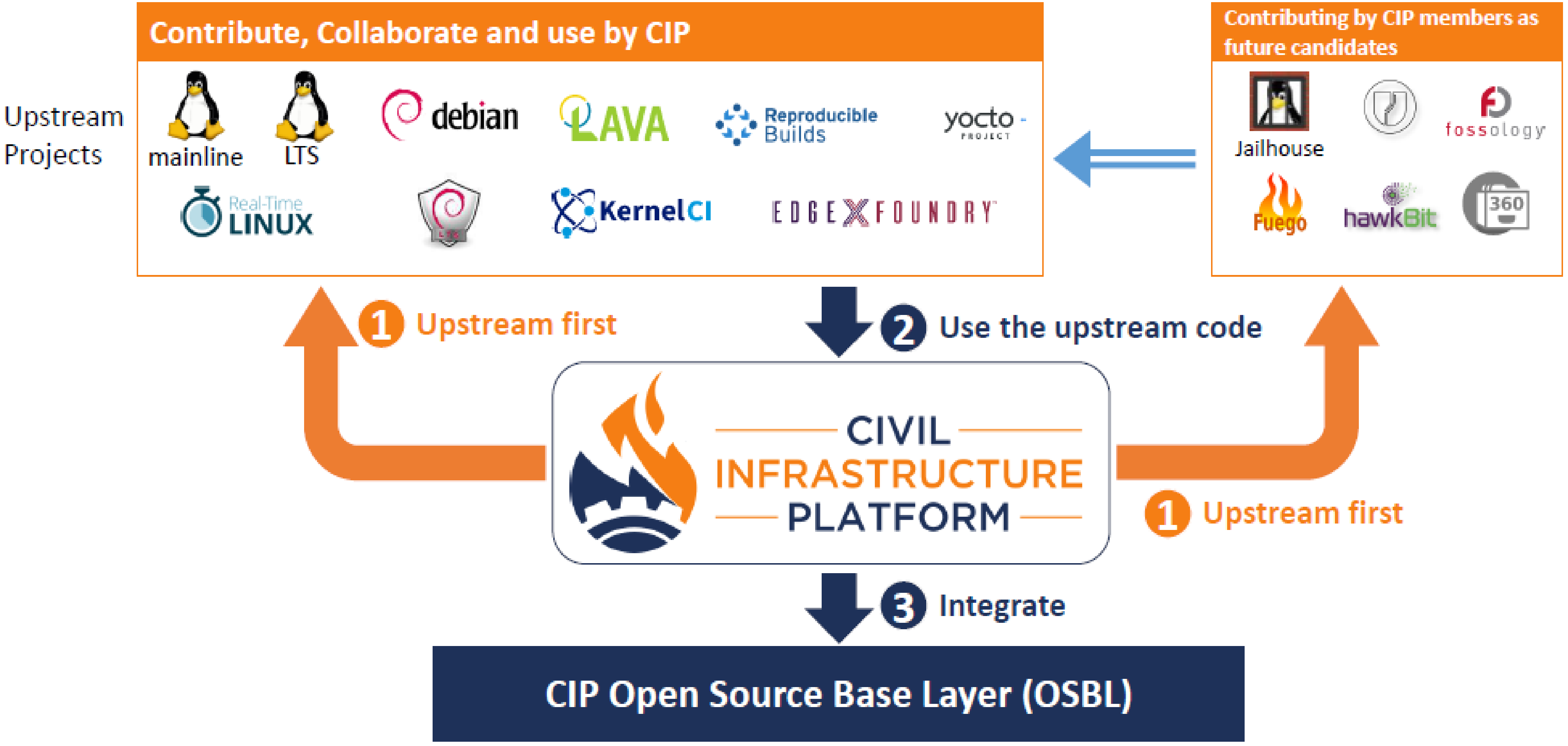
additional packages *(hundreds)*

CIP Core packages *(tens)*

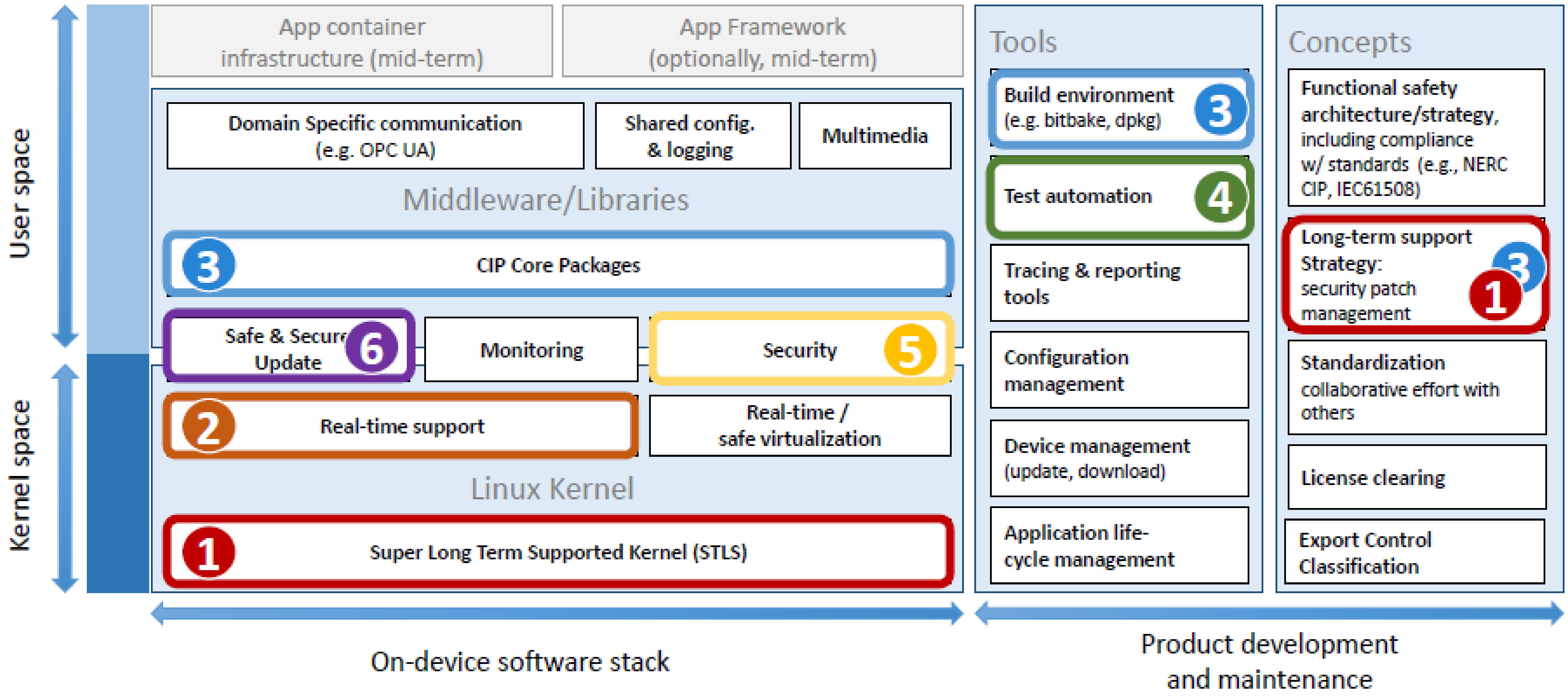
CIP kernel
(10+ years maintenance, based on LTS kernels)

open source base layer (OSBL)

Collaborative development with other OSS projects



Scope of activities



User space

Kernel space

App container infrastructure (mid-term)

App Framework (optionally, mid-term)

Domain Specific communication (e.g. OPC UA)

Shared config. & logging

Multimedia

Middleware/Libraries

3 CIP Core Packages

Safe & Secure Update 6

Monitoring

Security 5

2 Real-time support

Real-time / safe virtualization

Linux Kernel

1 Super Long Term Supported Kernel (STLS)

Tools

Build environment (e.g. bitbake, dpkg) 3

Test automation 4

Tracing & reporting tools

Configuration management

Device management (update, download)

Application life-cycle management

Concepts

Functional safety architecture/strategy, including compliance w/ standards (e.g., NERC CIP, IEC61508)

Long-term support Strategy: security patch management 3 1

Standardization collaborative effort with others

License clearing

Export Control Classification

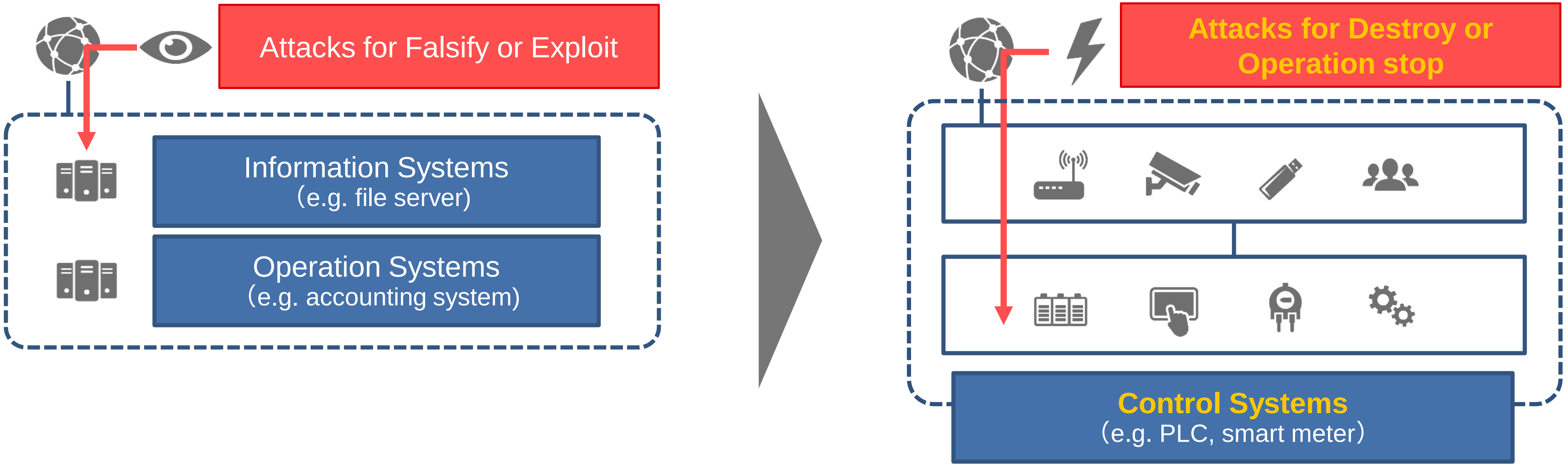
On-device software stack

Product development and maintenance

IEC 62443 certification

Growing threats of cyber-attacks

Targets have been changed to control systems

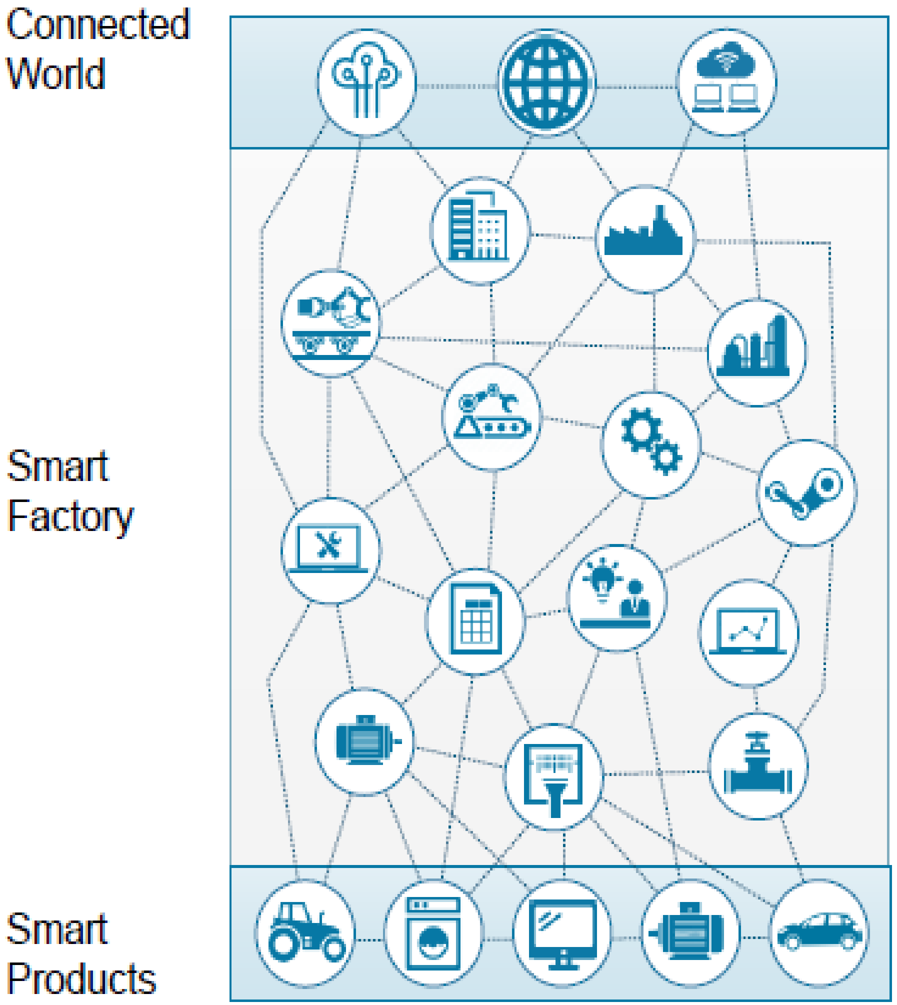


New shape of industry

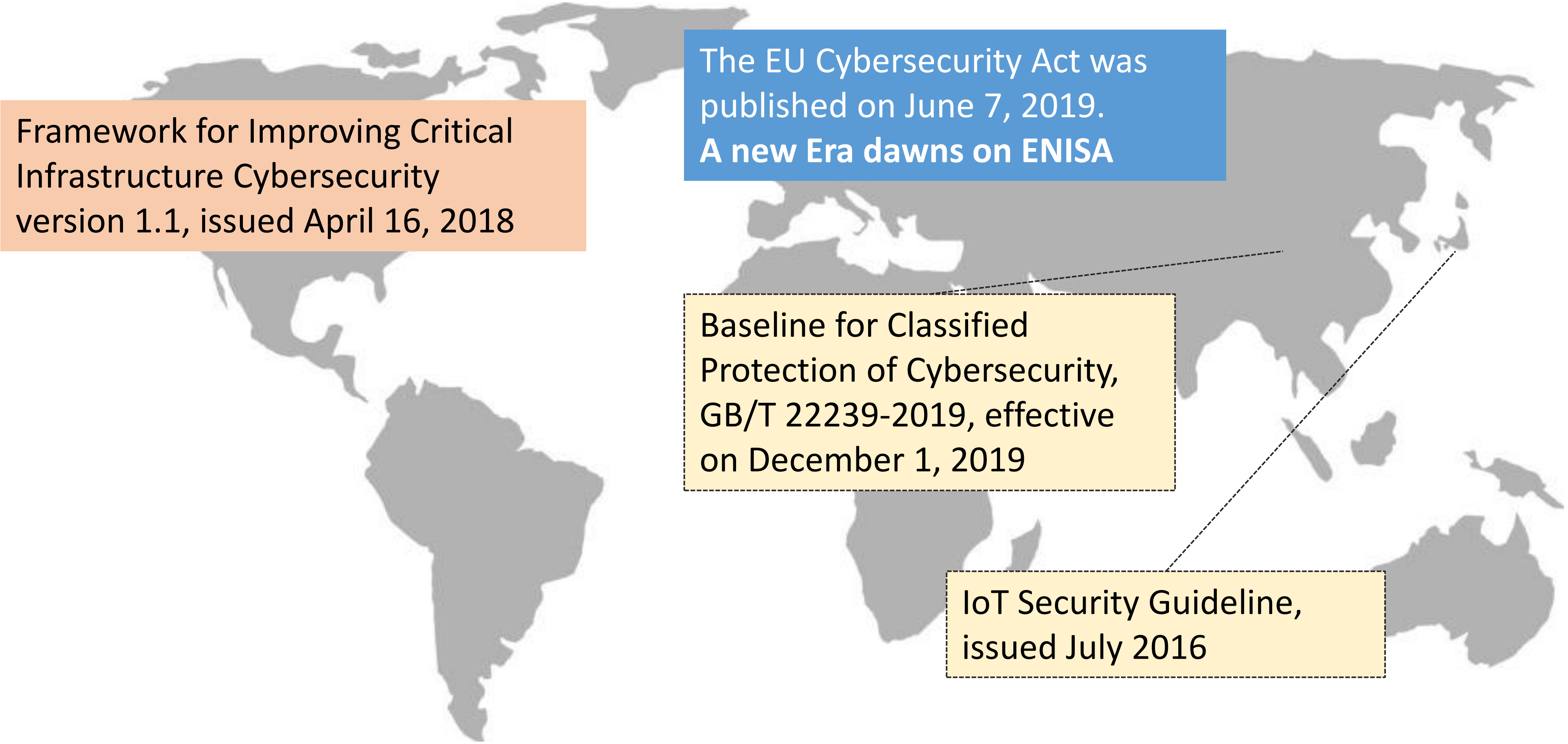
Be standard, be open
for cyber security in industry 4.0

Features:

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



Advances in cyber security



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

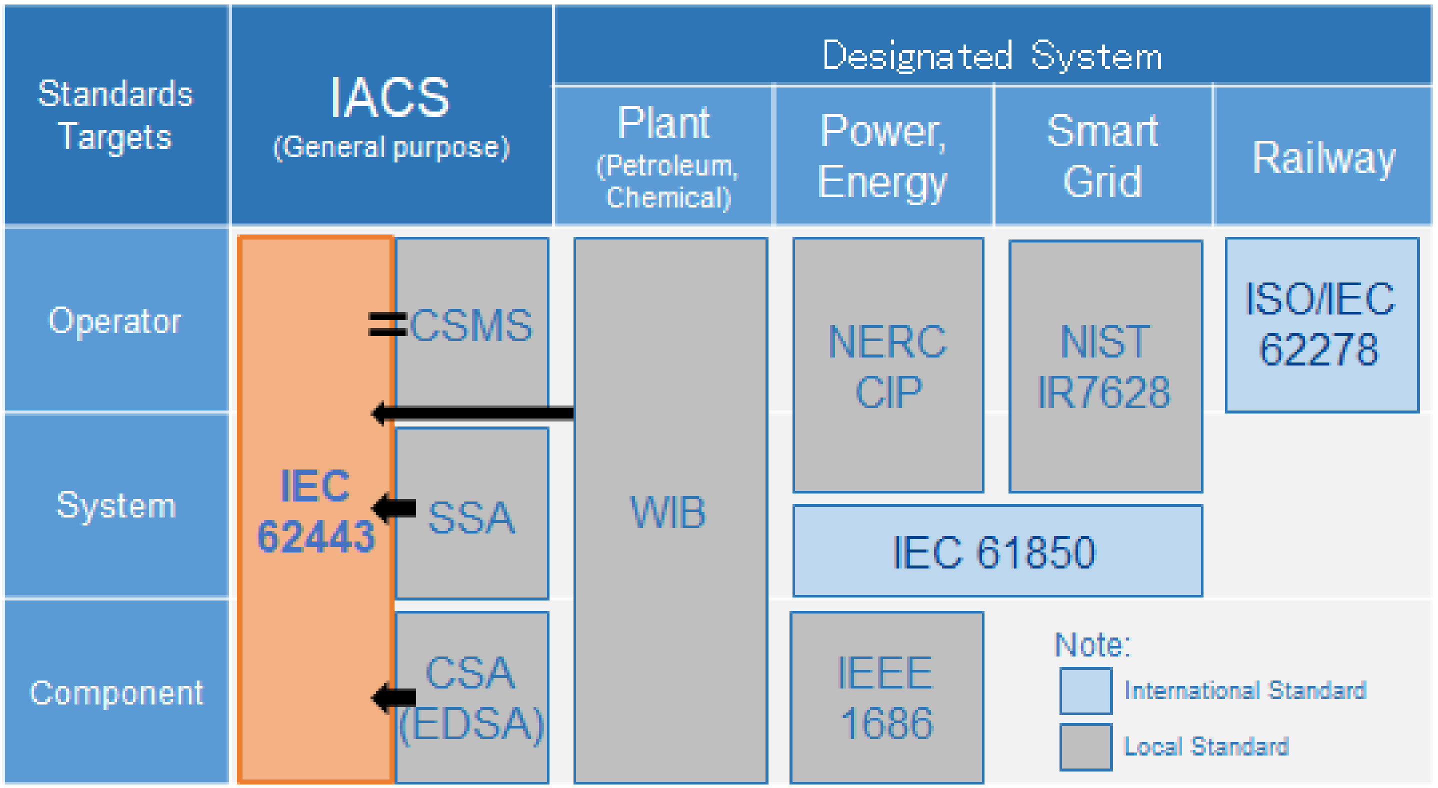
The EU Cybersecurity Act was published on June 7, 2019.
A new Era dawns on ENISA

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

IoT Security Guideline, issued July 2016

Why IEC 62443

IEC 62443 series are integrated cyber security standards



Standards Targets

IACS (General purpose)

Designated System

Plant (Petroleum, Chemical)

Power, Energy

Smart Grid

Railway

Operator

System

Component

IEC 62443

=CSMS

SSA

CSA (EDSA)

WIB

NERC CIP

NIST IR7628

ISO/IEC 62278

IEC 61850

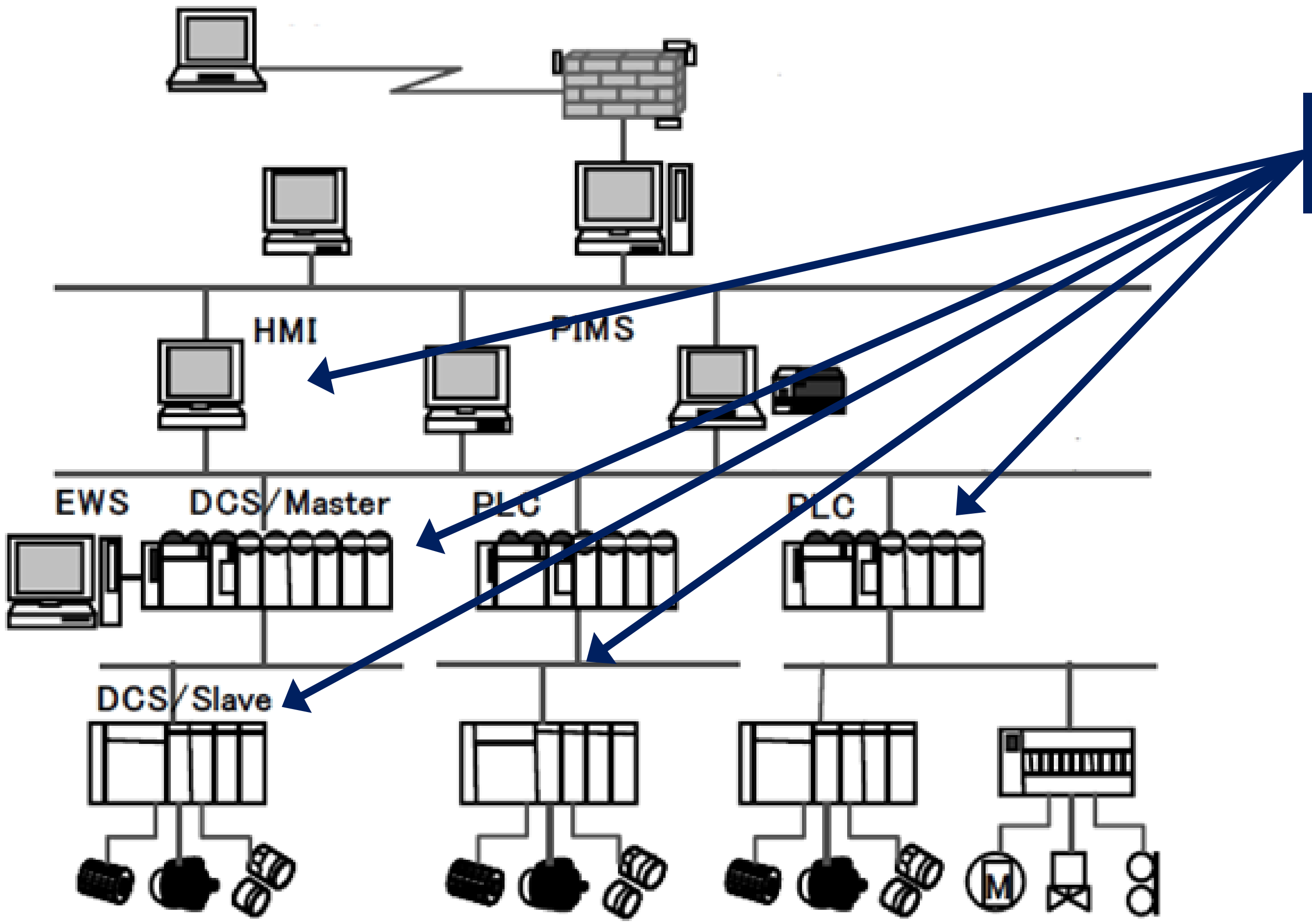
IEEE 1686

Note:

International Standard

Local Standard

Linux is acting on many components for IACS



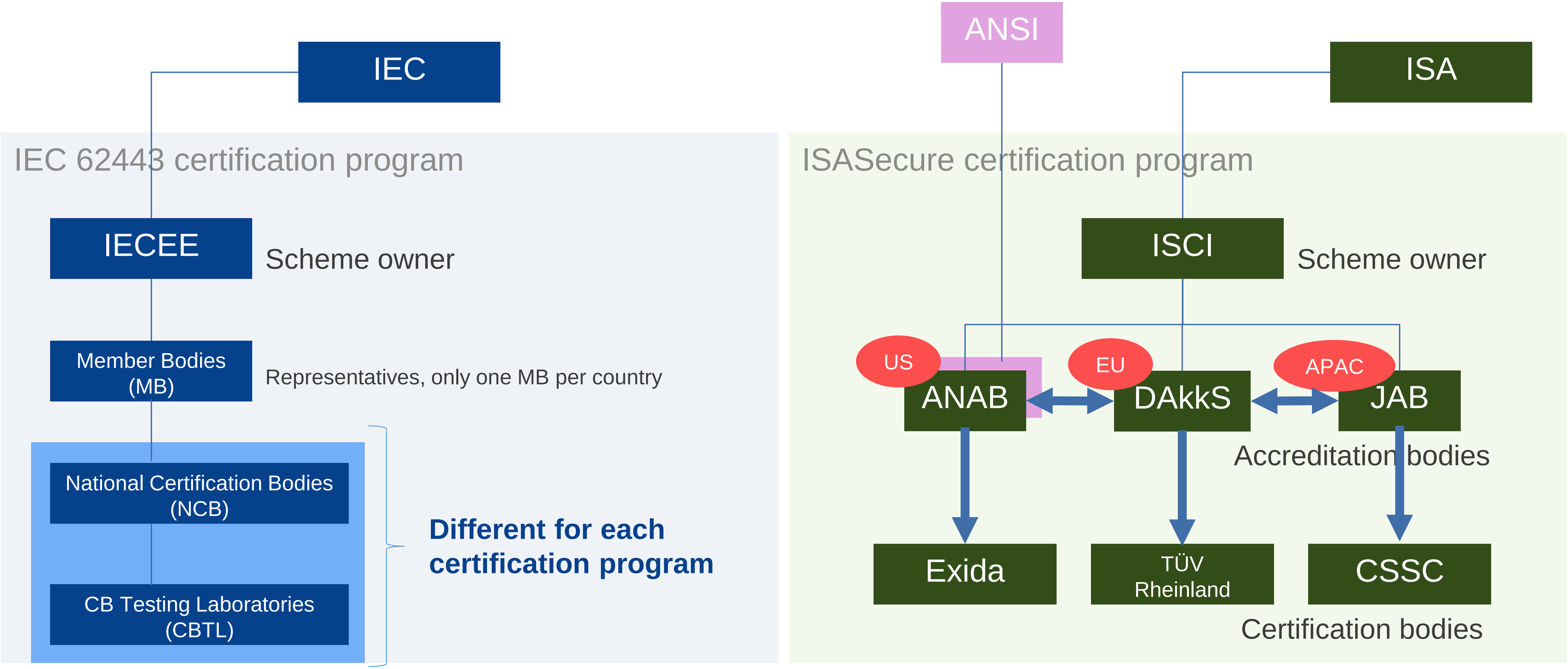
IEC 62443 Part 4

IEC 62443-4-1:
secure product development lifecycle requirements

IEC 62443-4-2:
technical security requirements for IACS components

Target devices, level:
Embedded and network device, level-3

Structure for IEC 62443 certification

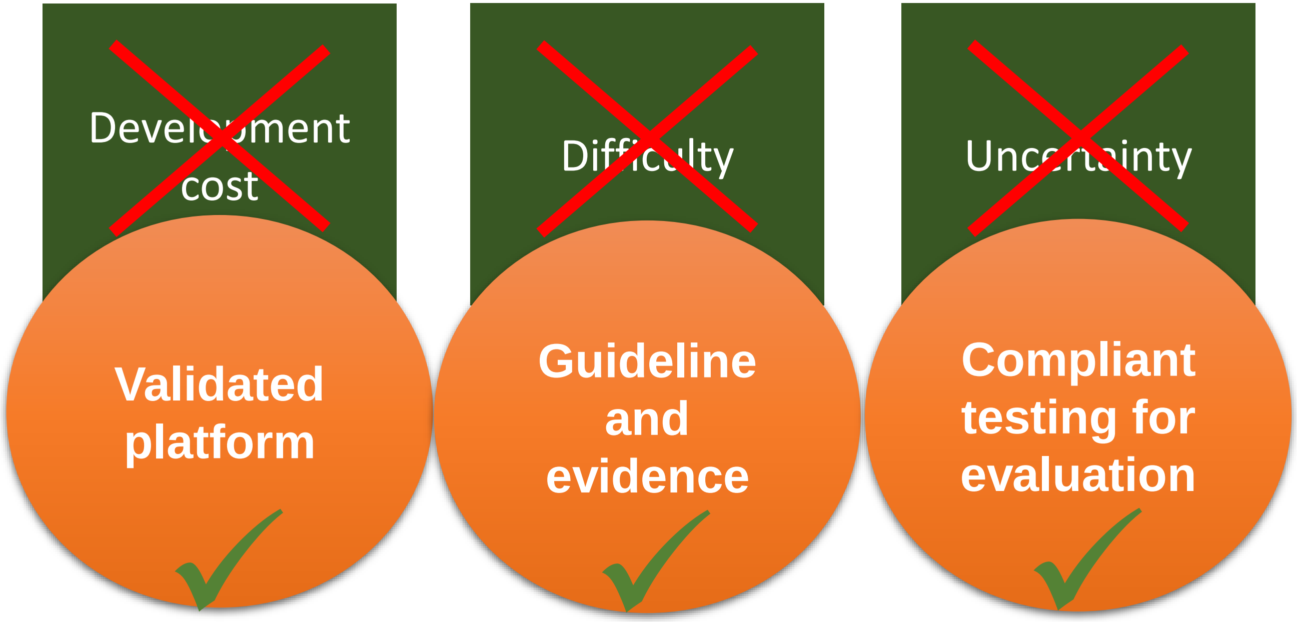

IEC
IEC 62443 certification program
IECEE
Scheme owner
Member Bodies (MB)
Representatives, only one MB per country
National Certification Bodies (NCB)
CB Testing Laboratories (CBTL)
Different for each certification program
ANSI
ISA
ISASecure certification program
ISCI
Scheme owner
US
ANAB
EU
DAkkS
APAC
JAB
Accreditation bodies
Exida
TÜV Rheinland
CSSC
Certification bodies

CIVIL INFRASTRUCTURE PLATFORM

Activity updates

Security working group’s mission and goal

Provide OSBL compliant with IEC 62443 certification



~~Development cost~~

Validated platform ✓

~~Difficulty~~

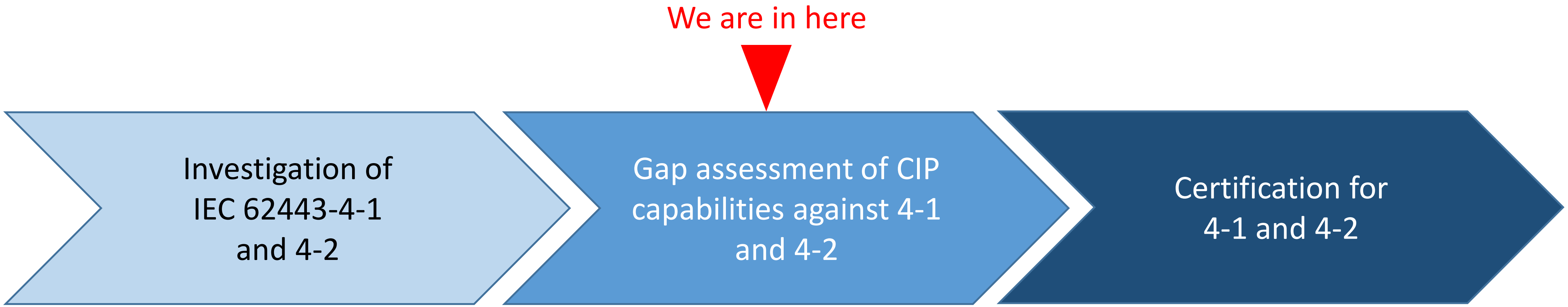
Guideline and evidence ✓

~~Uncertainty~~

Compliant testing for evaluation ✓

progress of the CIP assessment for IEC 62443 part 4

Completed the gap assessment for IEC 62443-4-1, and started the gap assessment for IEC 62443-4-2


We are in here
Investigation of IEC 62443-4-1 and 4-2
Gap assessment of CIP capabilities against 4-1 and 4-2
Certification for 4-1 and 4-2

Key challenges to meet IEC 62443-4-1 requirements

Needed special consideration caused not being a product

Development environment security	Following secure design principles	Defence in depth measures	Security implementation review	Defining Threat Model
• In OSS development , many developers contribute, making sure all stages of development are secured is the challenge	• OSS components are designed by many people and organizations, ensuring secure design is challenging	• Ensuring defence in depth measures will be supported by environment where product is deployed is bit challenging	• Reviewing all changes or implementation to confirm security measures is challenging	• CIP being a platform poses challenge to define Threat Model since it’s boundaries are not known

Approach to address key challenges

To achieve as much support as possible as a platform

Development environment security	Following secure design principles	Defence in depth measures	Security implementation review	Defining Threat Model
• Re-use existing OSS infrastructure such as combination or private and public repos • Exploit merge feature to control software modifications	• CIP plans to document how to protect open interfaces, restricted access based on roles • Few secure design principles depend upon type of product and it's use cases	• The overall objective is to reduce attack surfaces • Document general measures for defence in depth • Product specific measures have to be taken by product suppliers	• CIP team reviews each security fix before applying to CIP • Plans to closely track CVEs of critical issues and regularly release security fixes	• It is planned to define a generic threat model to meet this requirement

Preparing user friendly documents now

Documents compliant with IEC 62443-4-1

User Manual

- How to build CIP kernel and core packages
- Configuration

Security Capabilities

- List of all security packages to meet IEC 62443-4-2 security features requirements
- details of security features which are supported by security packages

development process documents

- Version controlling
- Review policy/cycle
- Records

Can be reused by user certification

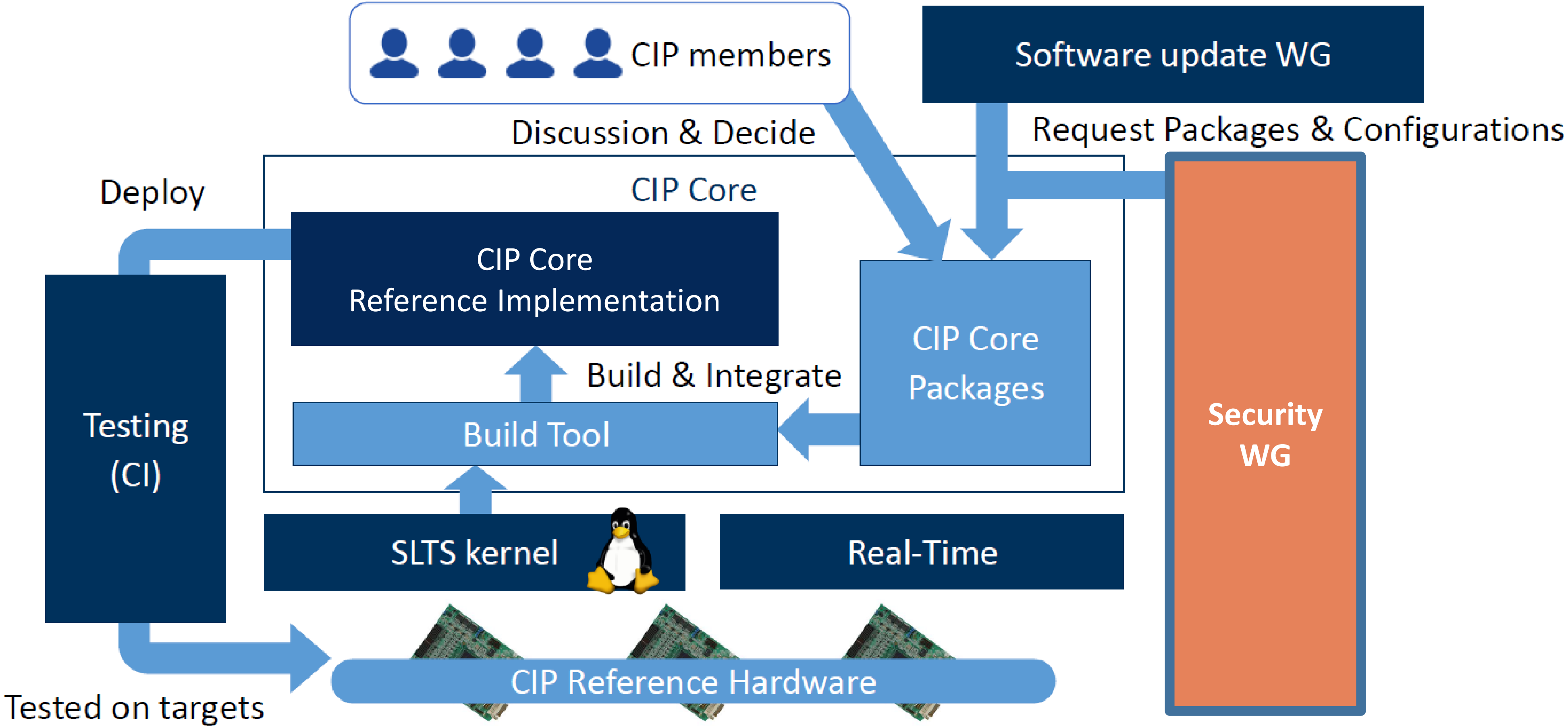
Essential packages to meet IEC 62443-4-2

Started the gap assessment of security packages

	Selected package examples:
FR 1 – Identification and authentication control (IAC)	shadow, pam, openssl, openssh, fail2ban
FR 2 – Use control (UC)	acl, audit, syslog-ng, chrony
FR 3 – System integrity (SI)	openssl, aide
FR 4 – Data confidentiality (DC)	openssl, util-linux(ipcrm, ipcs), shred
FR 5 – Restricted data flow (RDF)	-
FR 6 – Timely response to events (TRE)	acl, audit, syslog-ng, bro
FR 7 – Resource availability (RA)	nftables

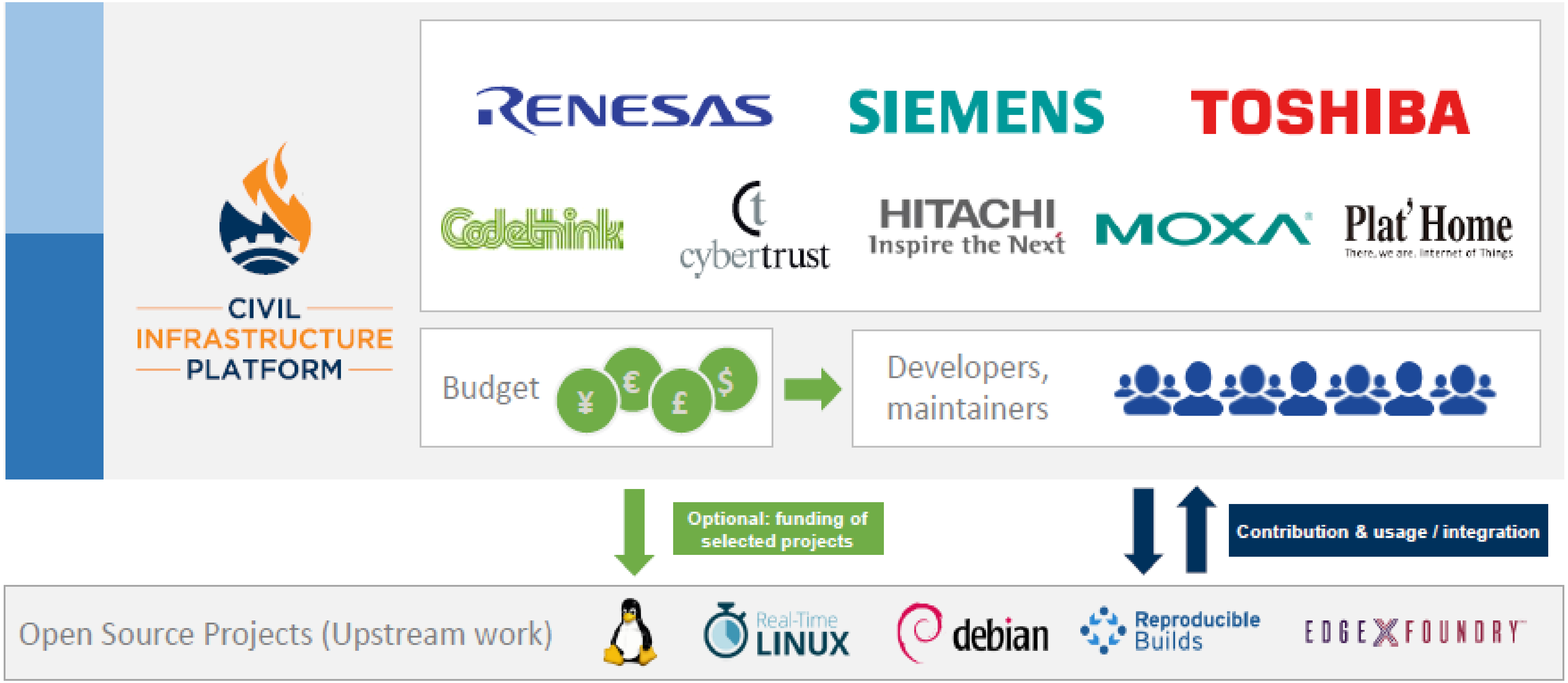
CIVIL INFRASTRUCTURE PLATFORM

Considering > Packaging > Testing



To close

The backbone of CIP are the member companies



Budget

Developers, maintainers

Optional: funding of selected projects

Contribution & usage / integration

Open Source Projects (Upstream work)

Join us

CIP for sustainable Smart Cities with Open Source Software

CIVIL
INFRASTRUCTURE
PLATFORM

RENESAS SIEMENS TOSHIBA

Codethink cybertrust HITACHI Inspire the Next

MOXA Plat'Home There, we are, Internet of Things

Contact information and Resources

- To get latest information:
  - Contact to our mailing list: cip-dev@lists.cip-project.org
- Other resources:
  - Twitter: @cip_project
  - CIP Web Site: https://www.cip-project.org
  - CIP wiki: https://wiki.linuxfoundation.org/civilinfrastructureplatform/
- Upcoming session
  - CIP mini-summit, **Friday, Oct. 30, 11:00 GMT**: https://sched.co/eDiQ

Thanks you!

CIVIL
INFRASTRUCTURE
PLATFORM

Q&A

CIVIL
INFRASTRUCTURE
PLATFORM