THE LINUX FOUNDATION PROJECTS

CIVIL INFRASTRUCTURE PLATFORM

【Case study2】 オープンソースプロジェクトにおける 産業向けサイバーセキュリティ に対する取り組み

Kento Yoshida, CIP security working group chair
from Renesas Electronics Corporation

OSAKA NDS Embedded Cross Linux Online Forum #12

Feb. 12, 2021

Self introduction

31st October 2019 at CIP mini-summit, Lyon, France

～ 2016/12
独立系ソフトウェアハウスにてAE・PL・PMとして次世代スマホ向けプロトコルスタックの開発など多種プロジェクトに従事

2017/1～
ルネサスにてネットワーク検索エンジン（NSE）のソリューション開発に従事
現部署（MPUプロダクト部）に異動後、RZ/Gシリーズのセキュリティ・ソリューション開発に従事
2018年12月のセキュリティWG発足を機にCIPに参画
2020年1月より同WG議長

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

CIVIL INFRASTRUCTURE PLATFORM

company-specific middleware and applications

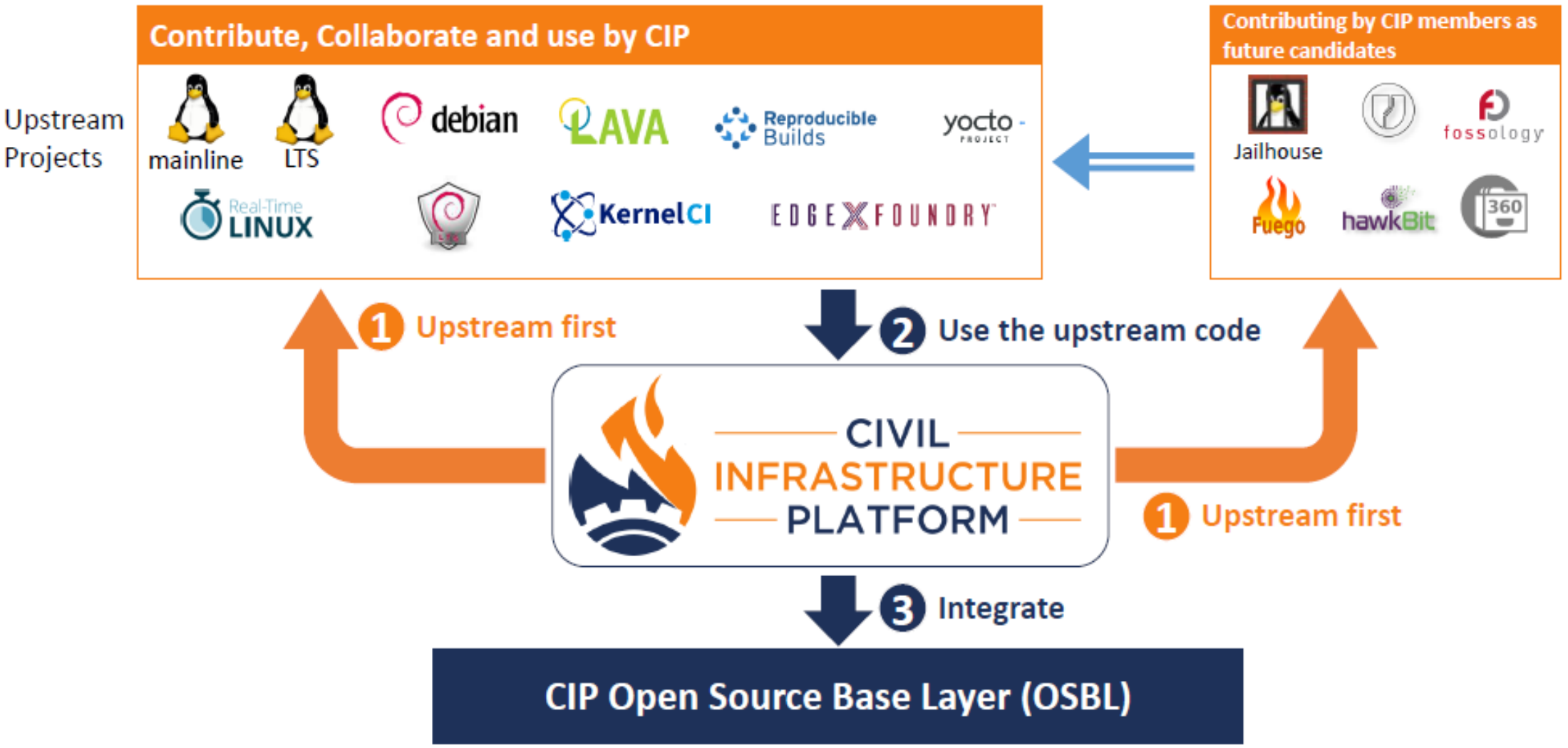
additional packages *(hundreds)*

CIP Core packages *(tens)*

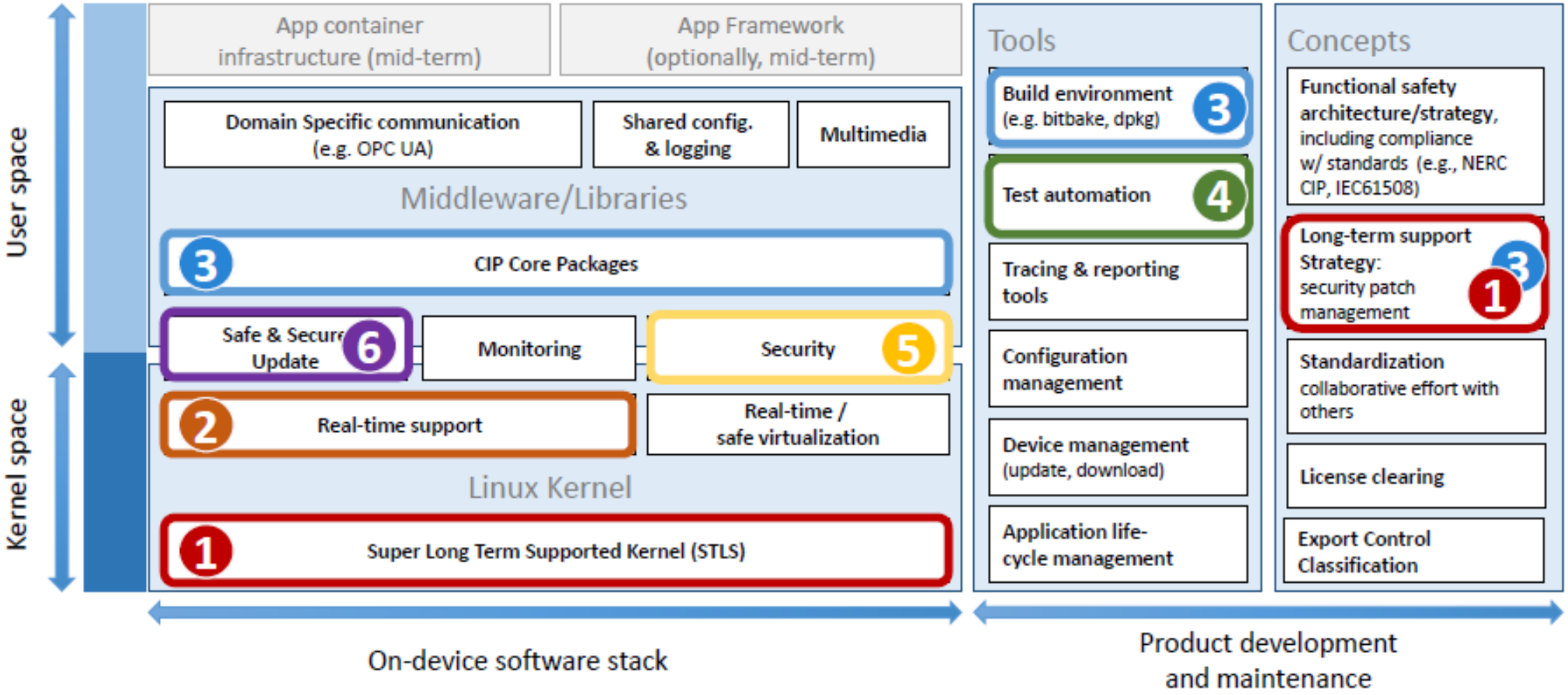
CIP kernel
(10+ years maintenance, based on LTS kernels)

open source base layer (OSBL)

Collaborative development with other OSS projects



Scope of activities

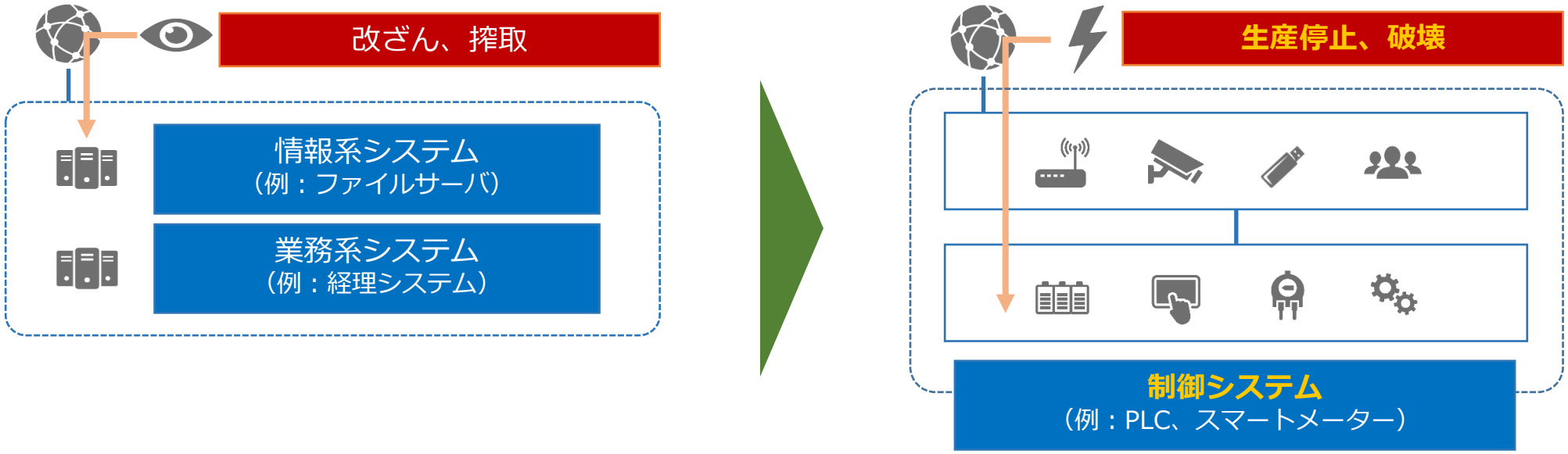


IEC 62443 certification

拡大するサイバー攻撃の脅威

サイバー攻撃の標的は情報資産から制御システムへ

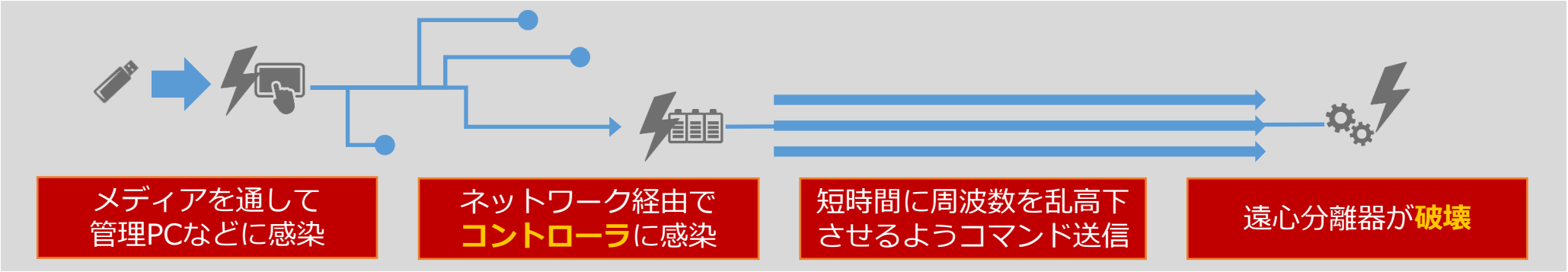
- **IoTの進歩を背景**にいままではスタンドアローン型ネットワークであった制御システムがサイバー攻撃の対象に
- 攻撃者の目的も生産停止やシステムの破壊など**物理的な影響**に及び、被害規模が拡大
- 情報資産を守るセキュリティマネジメントから、**システムそのものを守る**セキュリティマネジメントへ



参考：重要インフラの制御システムへの攻撃例

「Stuxnet」2010年

- イランにある**核施設**の遠心分離器9,000台のうち、約1,000台が破壊された
- 遠心分離器の制御システムに侵入し、**周波数をコントロール**してダメージを蓄積させた



巧妙化するマルウェアの脅威

- Stuxnetは、**Windows**のショートカットファイルの脆弱性を狙ったマルウェア
- 複数の技術者が数か月から数年かけて**入念に準備**（コード量50倍以上）
- 制御システムの構成を把握して**特定の機器**をターゲットに絞り込み
- 感染機器の**監視機能を停止**させ、強制的に異常操作を実行

運用・保守のみの課題ではない！

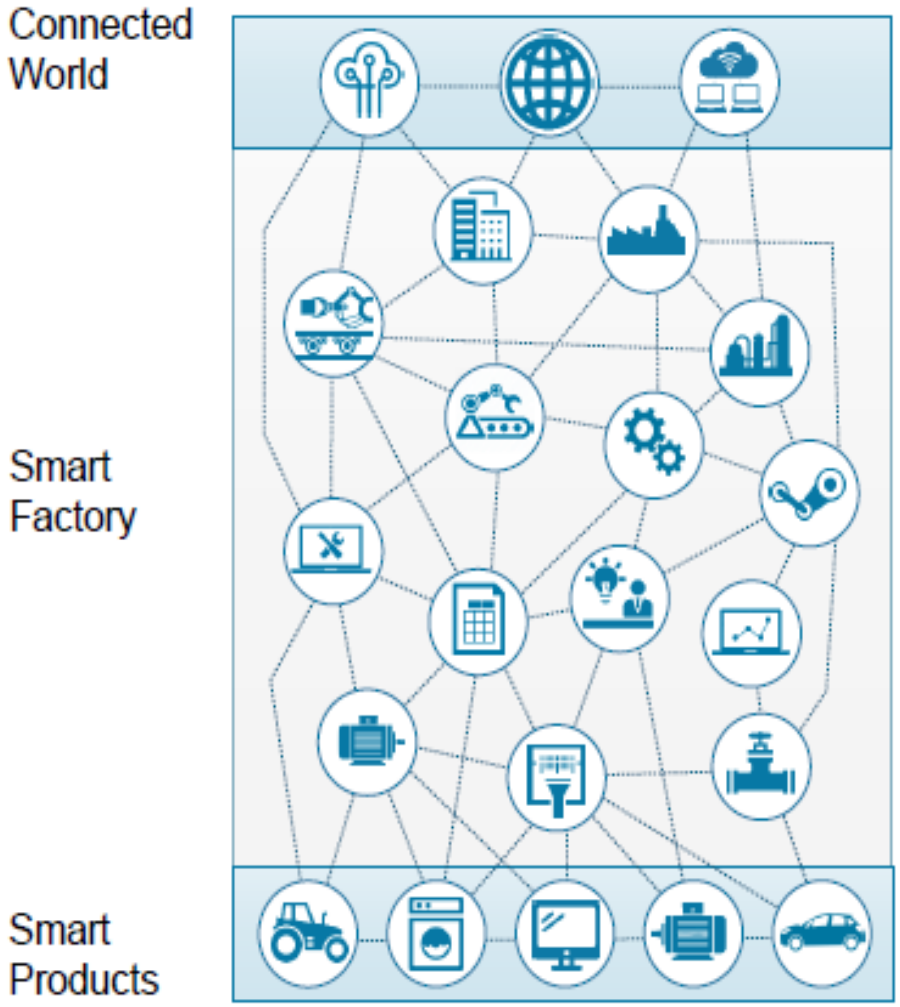
機器、システム自体の
セキュリティ機能も重要

New shape of industry

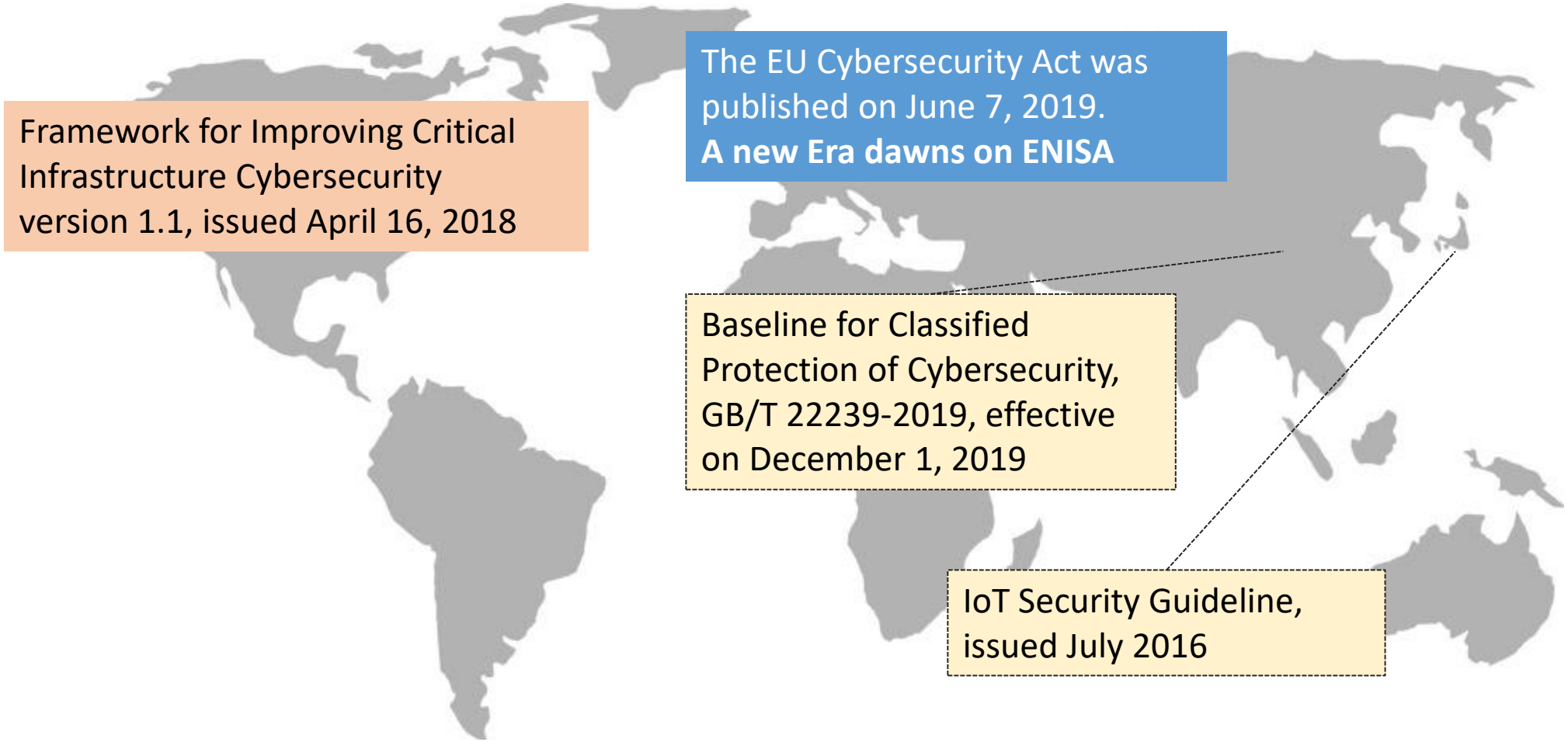
Be standard, be open
for cyber security in industry 4.0

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

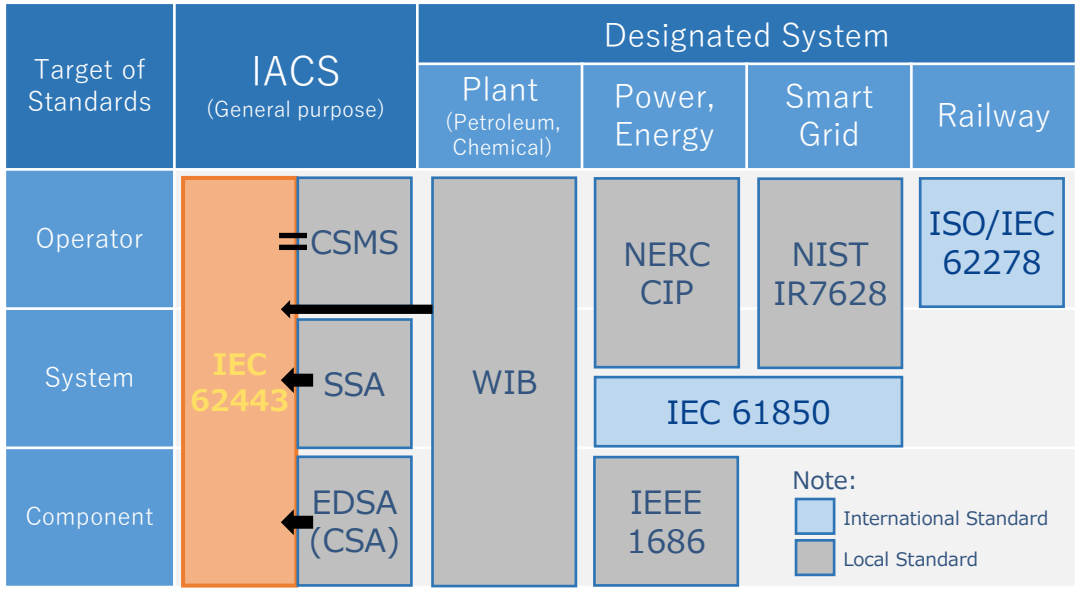
セキュリティ統一規格として注目を集めるIEC 62443

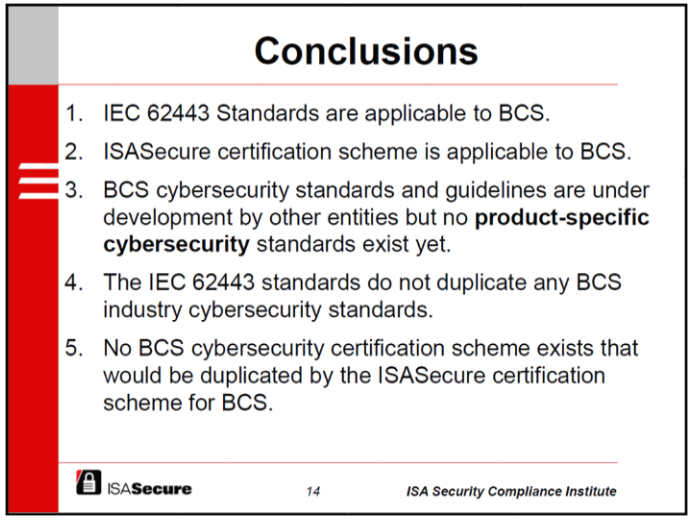
IEC 62443 に欧米が注目

- 異なる事業体のFA向けセキュリティ規格を統合した汎用規格としてIEC 62443シリーズが整備・拡大中
- 米国ISAが制定した規格を**ANSI・IEC**が制御システム（IACS）向けのセキュリティ統一規格として採用

FA業界のみでなくBA業界も IEC 62443 に注目

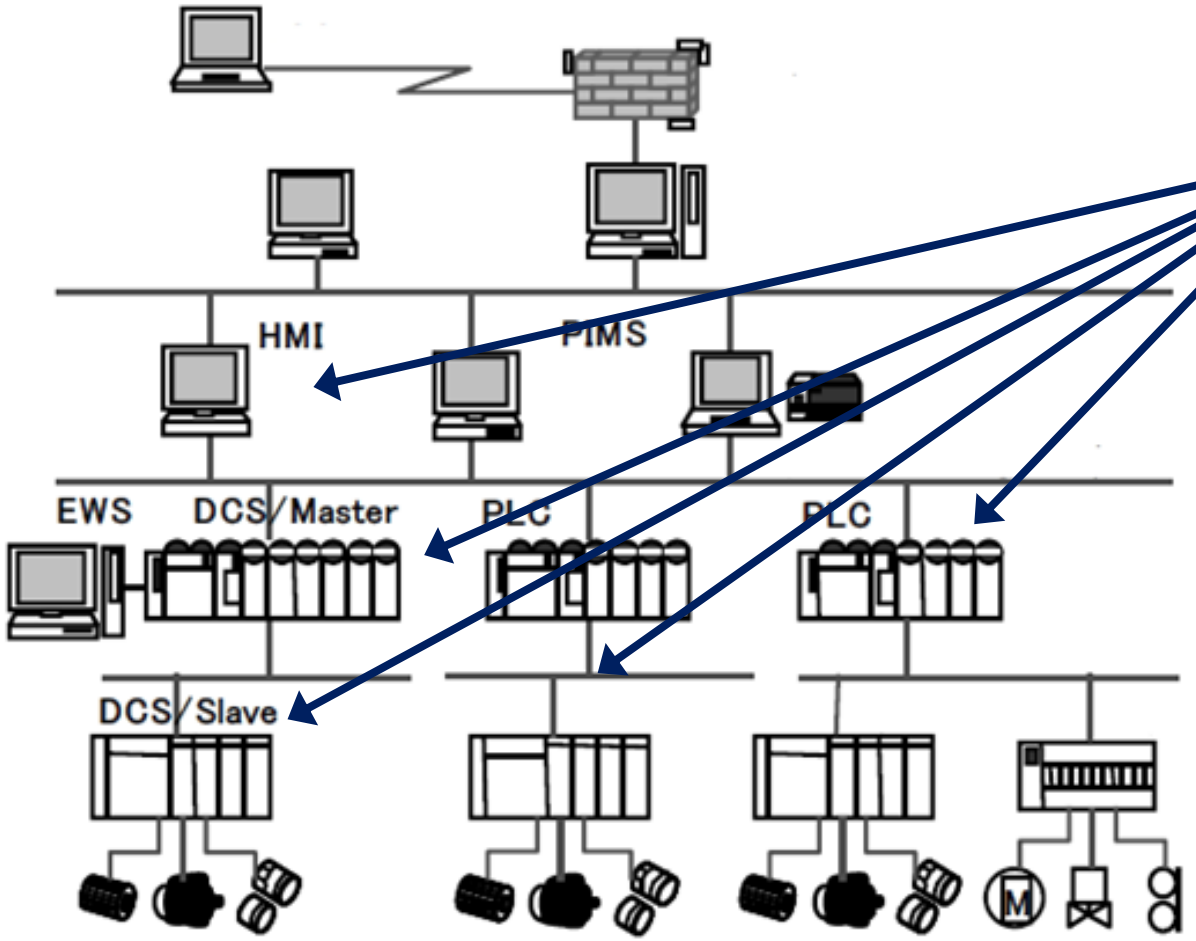
- Building Control System (BCS) のサプライヤを中心にISASecureのWGがIEC 62443の有効性を検証・確認





Cited from "ISA/IEC 62443 STANDARDS AND ISASECURE® CERTIFICATION: APPLICABILITY TO BUILDING CONTROL SYSTEMS" in https://www.isasecure.org/en-US/

Linux is acting on many components for IACS



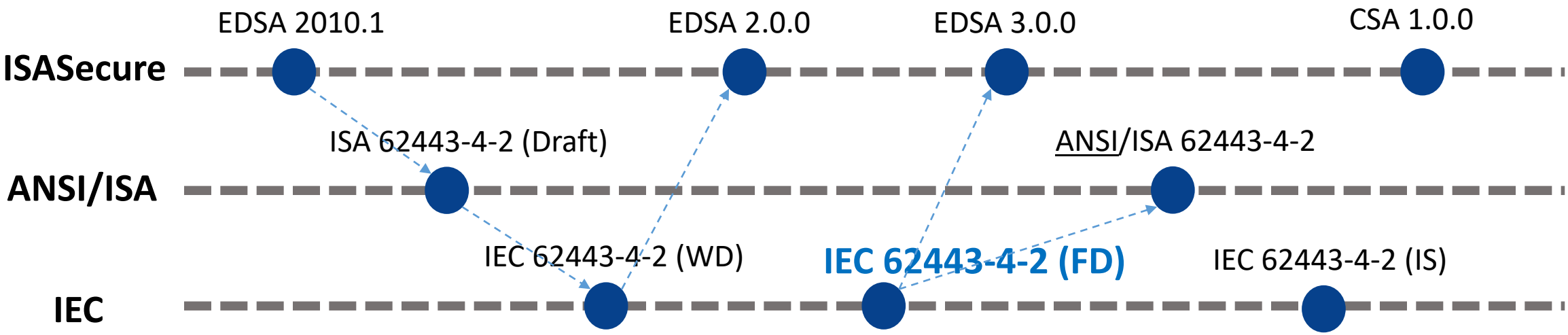
IEC 62443 Part 4

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

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

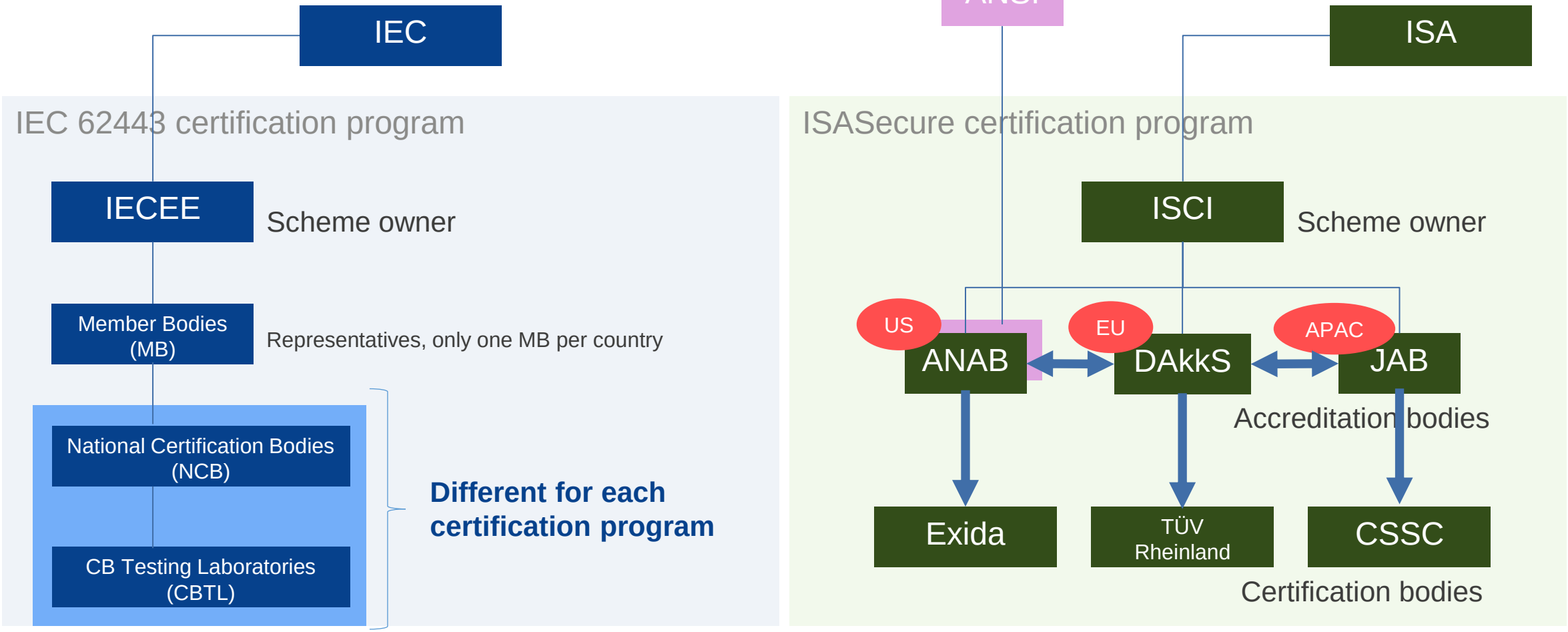
Target devices, level:
Embedded and network device, level-3

Specification history



- IEC 62443-4-2 (Final Draft) is adopted ISASecure certification program and ANSI/ISA standard.
- IEC 62443-4-2 International Standard version was issued in March 2019.
- ISASecure certification program changed the program name from EDSA to CSA.
- CSA program is available now.

Structure for IEC 62443 certification



Activity of Security working group towards IEC 62443

Issues to be solved

Security is non-competitive, but cost excessive

- Certification requires special work such as implementation/evaluation specifications
- Certification requires **necessary and sufficient** measures

Insufficient	Sufficient	Excessive
▪ Risk of **re-certification** ▪ Development schedule delay	▪ Adequate cost ▪ Adequate schedule	▪ Excessive development cost ▪ Market introduction delay

Certification requires a unique how-to

- To avoid compromising product availability, it is impossible to **specifically describe** security-related standards
  - **Implement** what and how much?
  - Provide **evaluation environment** in what way? Evaluate what?

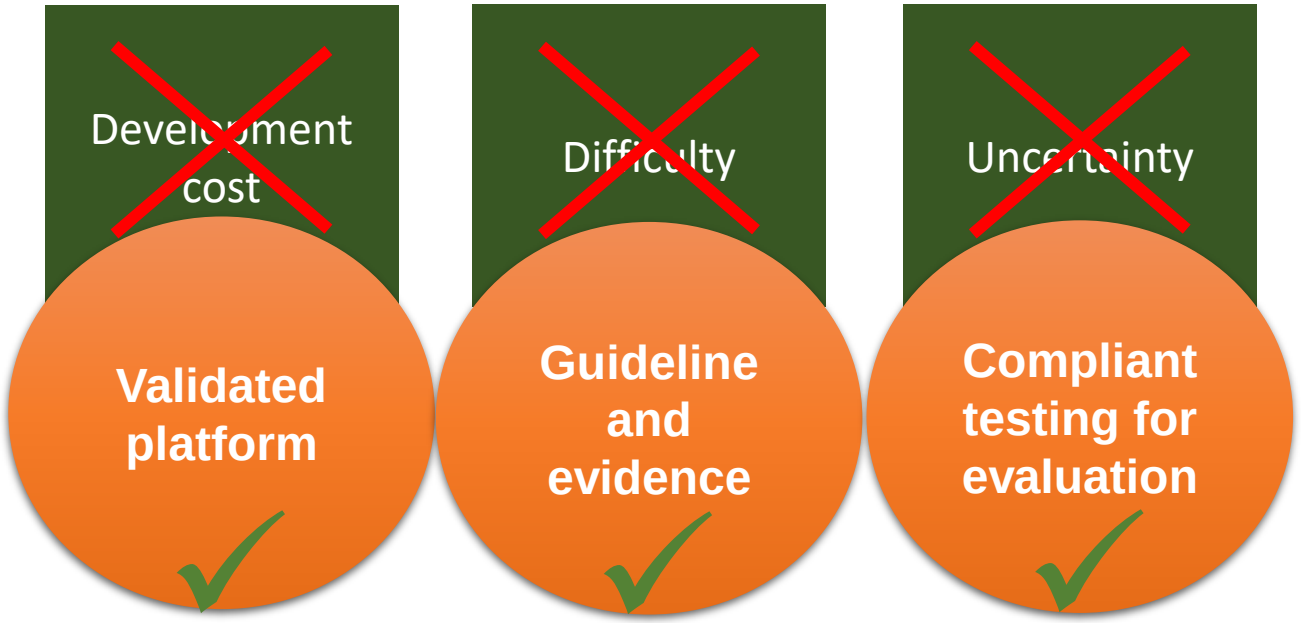
Development Cost

Difficulty

Uncertainty

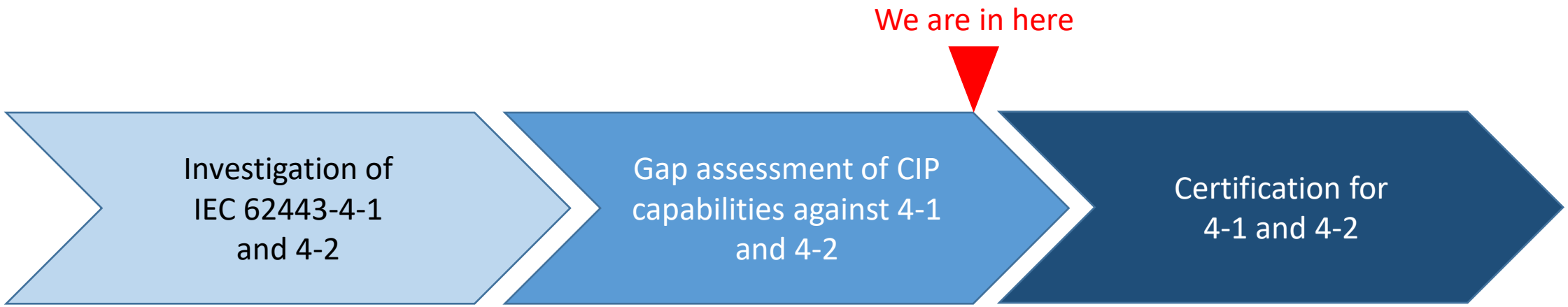
Security working group’s mission and goal

Provide OSBL compliant with IEC 62443 certification

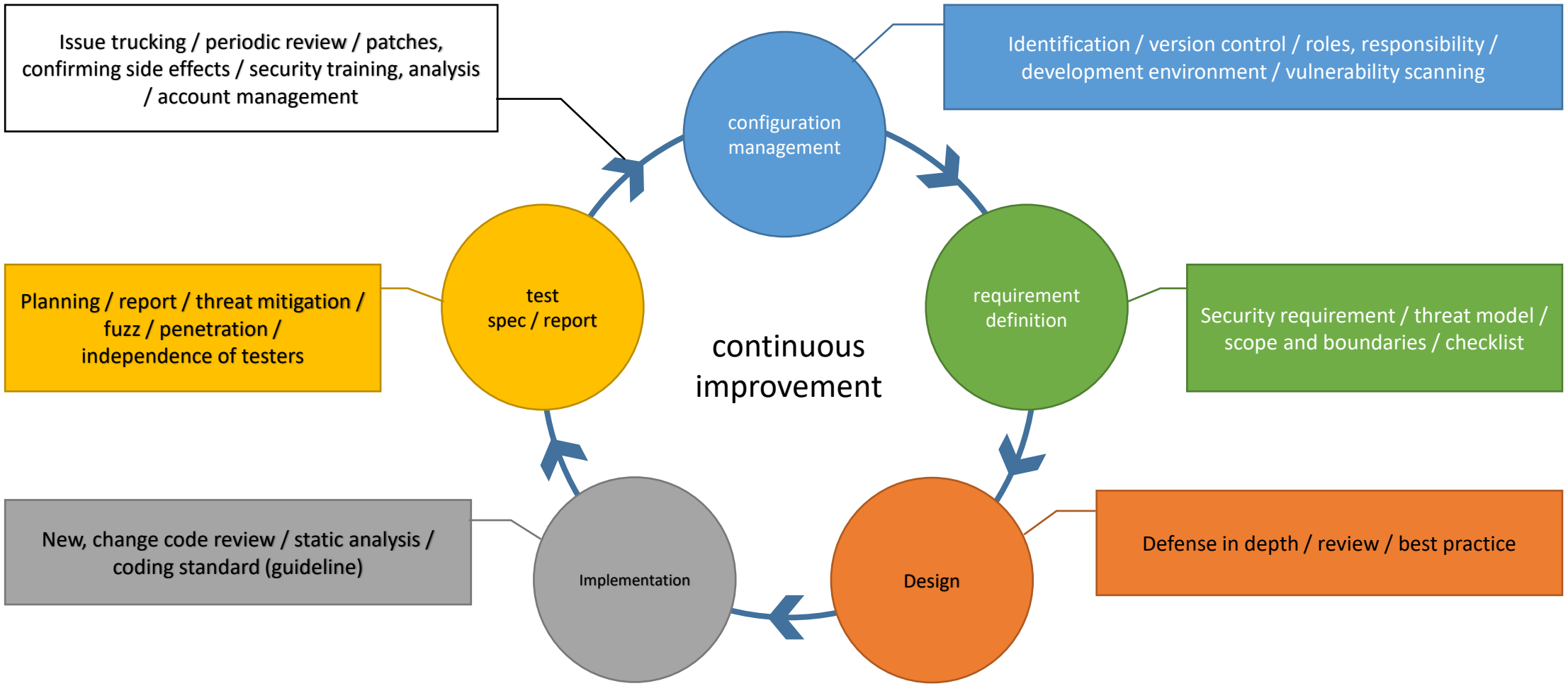


Progress of the CIP assessment for IEC 62443 part 4

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



The gap analysis for IEC 62443-4-1



Key challenges to meet IEC 62443-4-1 requirements

Needed special consideration caused not being a product

Configuration management	Requirement definition	Design	Implementation	Testing
• Version control with a snapshot of lists of packages • Risk assessment to ensure fixing open CVEs	• Create a threat model for generic requirements • Scope the capabilities CIP intend to implement	• Define open interfaces which security packages have, general measures how to ensure security for a product supplier	• Considering to use static analysis tool when integration and reporting the results • Review security fixes and notify them	• Cyclic running automated test in LAVA lab • Define the product supplier obligation to run threat mitigation, fuzz and penetration

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
- Test report

Can be reused by user certification

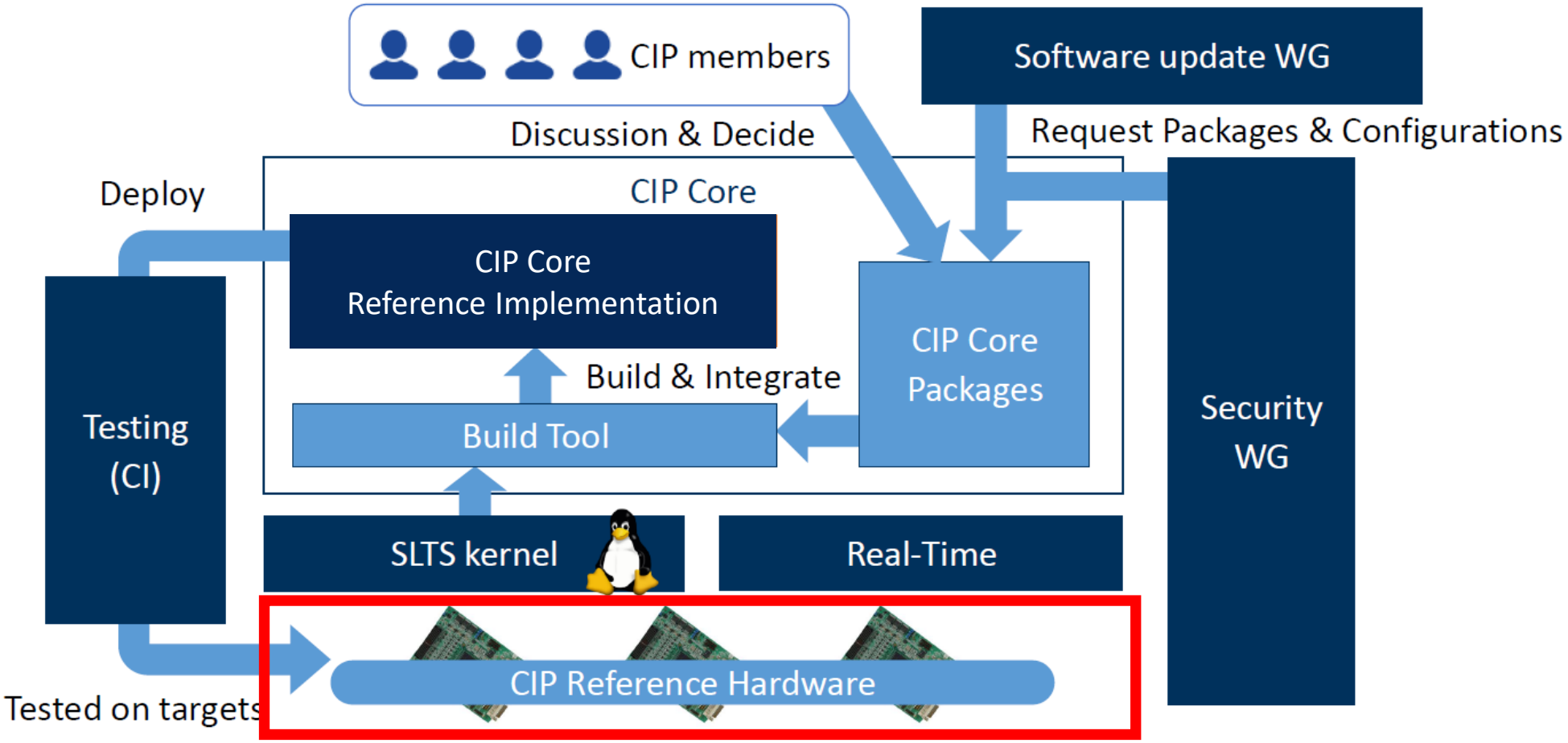
CIVIL INFRASTRUCTURE PLATFORM

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

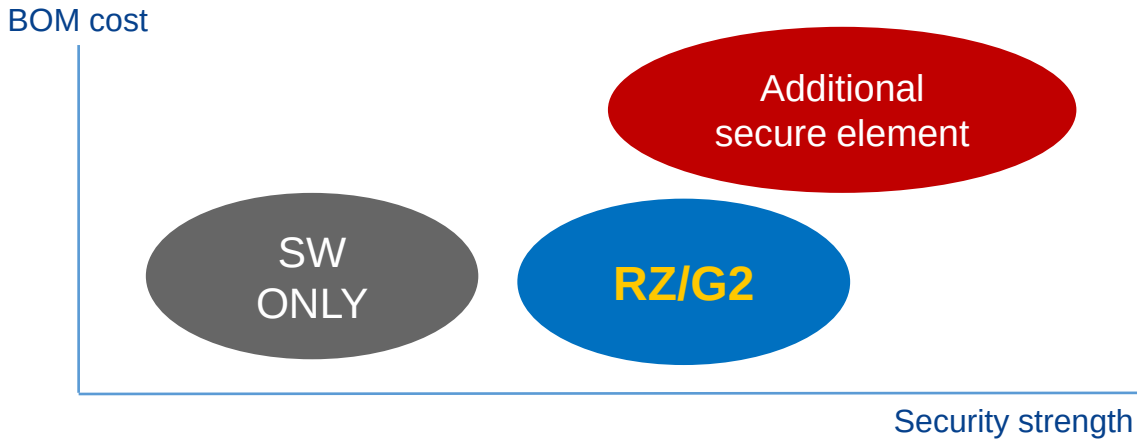
Considering > Packaging > Testing



HARDWARE要件への対応

RZ/G2は産業制御機器向けの高性能な機能に加え、
IEC 62443-4-2のSL-3相当の ハードウェアセキュリティをMPU単体で実現。

必要十分なセキュリティ機能を有するRZ/G2でBOMコストを最適化



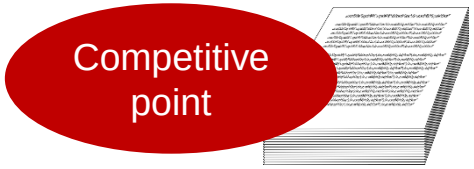
INSUFFICIENT	SUFFICIENT	EXCESSIVE
SL-3への適合には HWセキュリティが必須	**RZ/G2はSL-3への適合に必要な HWセキュリティを単体で搭載**	セキュリティ専用チップは BOMコストを押し上げる

RZ/G IEC 62443 READY ソリューション提供物

ユーザのセキュリティ開発および認証コストを削減するための３つの提供物

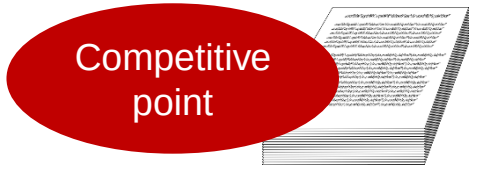
Verified Linux Package（VLP）
& セキュリティパッケージ

IEC 62443-4-2のSL-3への適合性をISCI認定の第三者認証機関にて評価したセキュリティソフトウェアパッケージ（ライブラリ、ツールなど）でセキュリティ要件の多くをカバー。アプリケーションのセキュリティ開発を強力にサポート。



適合性評価レポート

ISCI認定の第三者認証機関が発行した、RZ/G2 Linux向けセキュリティパッケージのIEC 62443-4-2適合性評価レポートを提供。
アプリケーションが対応すべきセキュリティ要件が一目瞭然であり、調査・設計工程の工数を大幅に削減。



実装ガイドライン
（CIP SWG 認証ドキュメント）

アクセス制御の実行やバックアップなど、アプリケーションおよび上位システムにて対応しなければならない多数の要件について、どのような機能が求めらているのか、ルネサスが適合性評価を通して得た分析結果を実装ガイドとして提供。

Advantages comparison CIP vs Non-CIP(OSS) distributions

Items	CIP	Non-CIP (OSS)
Dedicated kernel maintainers for SLTS up to 10 years	✓	✗
IEC-62443-4-x assessed platform by accredited Certification Body	✓	✗
Close monitoring of CVEs at user and kernel level	✓	✗
Extended support from Debian ELTS for specific packages	✓	✗
Regular automated testing on multiple SOCs with published test results on KernelCI	✓	✗
Strong support from big players of embedded system industry	✓	✗

Maintaining IEC-62443-4-x certification for long term

Final certification for IEC-62443-4-x

CB defines change control process along with certification

Modifications after IEC-62443-4-x certification

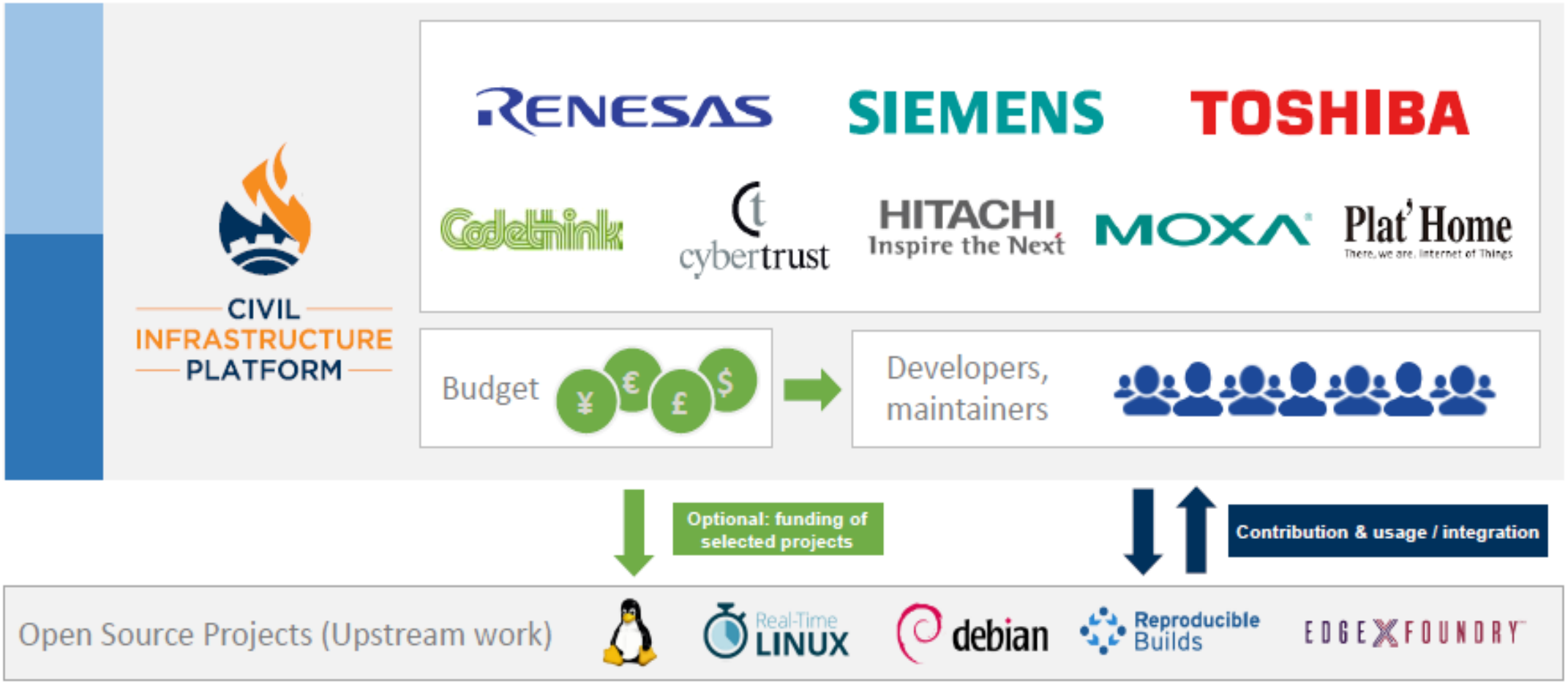
Follow change control process and modify/update certified product

After 3 years CB audits all the past changes

If all changes are found in accordance with change control process, certification is renewed/invalidated

To close

The backbone of CIP are the member companies



Join us

CIP for sustainable Smart Cities with Open Source Software

RENESAS SIEMENS TOSHIBA

Codethink cybertrust HITACHI Inspire the Next

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

Thank you!