LINUX FOUNDATION
COLLABORATIVE PROJECTS

CIVIL INFRASTRUCTURE PLATFORM

Two Years Experience of Industrial-grade Open Source Base Layer Development and its Future

Takehisa Katayama, CIP Board/TSC Representative
from Renesas Electronics Corporation

OSAKA NDS Embedded Linux Cross Forum #8

Feb. 5th, 2019

CIPとは？

CIPとは？

- Linux Foundationの中で、最も保守的なProjectの一つ
  - 現代社会を支える最も重要なProjectの一つ

- CIPのねらいは
  - 産業機器が求める要件を満たすLinuxの提供
    - 高い信頼性・安定性・長期間のメンテナンス
    - **Open Source Base Layer（OSBL）**
  - Upstream Communityと密に連携して開発すること

- OSBL ≠ 新ディストリビューション

CIVIL INFRASTRUCTURE PLATFORM

現代社会はLinuxの上で成り立っている

https://www.airpano.com/360Degree-VirtualTour.php?3D=San-Francisco-USA

Transport

Rail automation

Vehicle control

Automatic ticket gates

Energy

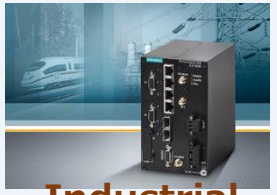
Power Generation

Turbine Control

Industry

Industry automation

CNC control



Industrial communication

Others

Healthcare

Building automation

Broadcasting

解決しなければならない課題は…

https://www.airpano.com/360Degree-VirtualTour.php?3D=San-Francisco-USA

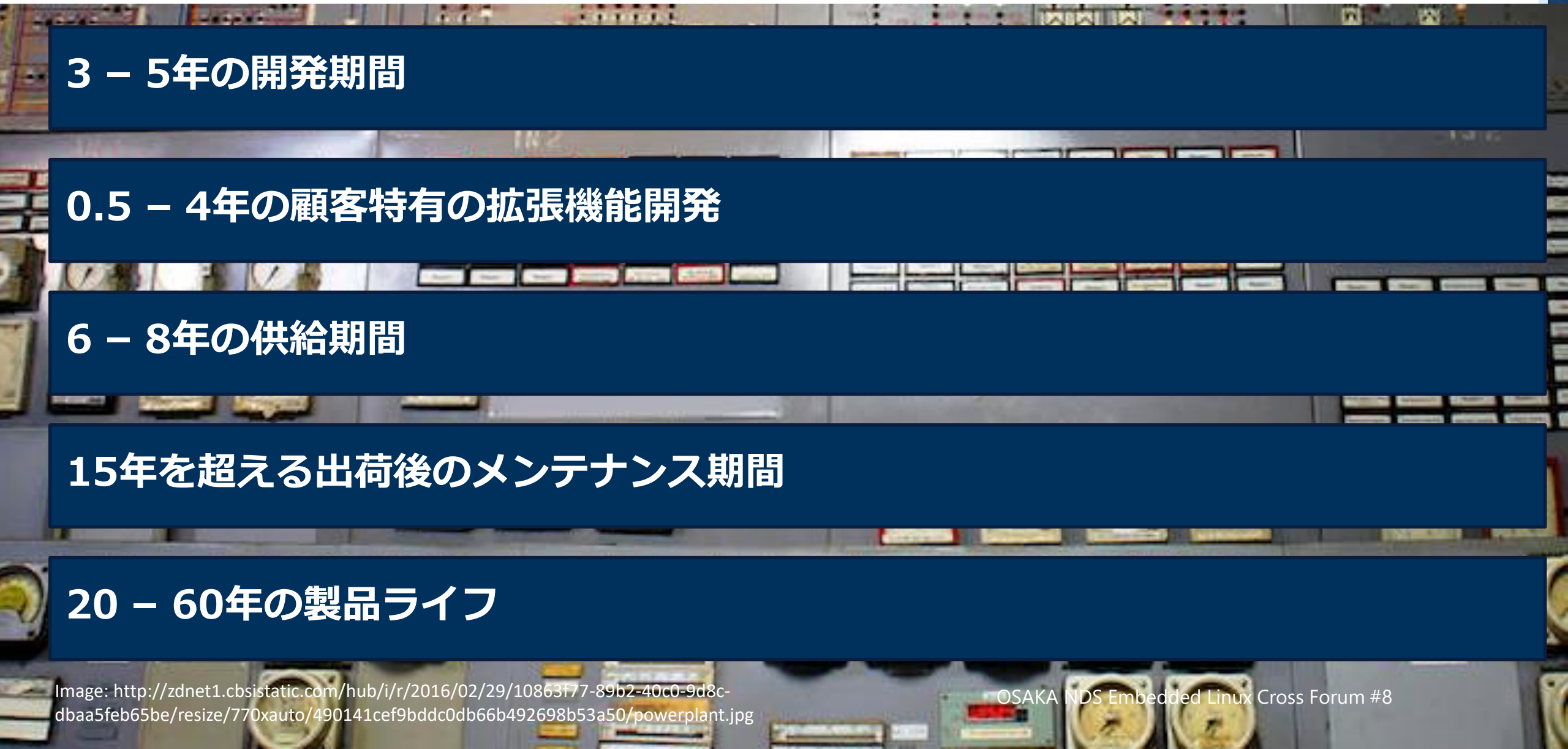
発電所の制御システム:

25-60 年という製品ライフ

ハードウェアの改良やソフトウェアの更新など、アップデートを実施したくないシステム

Image: http://zdnet1.cbsistatic.com/hub/i/r/2016/02/29/10863f77-89b2-40c0-9d8c-dbaa5feb65be/resize/770xauto/490141cef9bddc0db66b492698b53a50/powerplant.jpg

例：発電所の制御システム



3 – 5年の開発期間

0.5 – 4年の顧客特有の拡張機能開発

6 – 8年の供給期間

15年を超える出荷後のメンテナンス期間

20 – 60年の製品ライフ

Image: http://zdnet1.cbsistatic.com/hub/i/r/2016/02/29/10863f77-89b2-40c0-9d8c-dbaa5feb65be/resize/770xauto/490141cef9bddc0db66b492698b53a50/powerplant.jpg

ユーザーが直面している課題は・・・

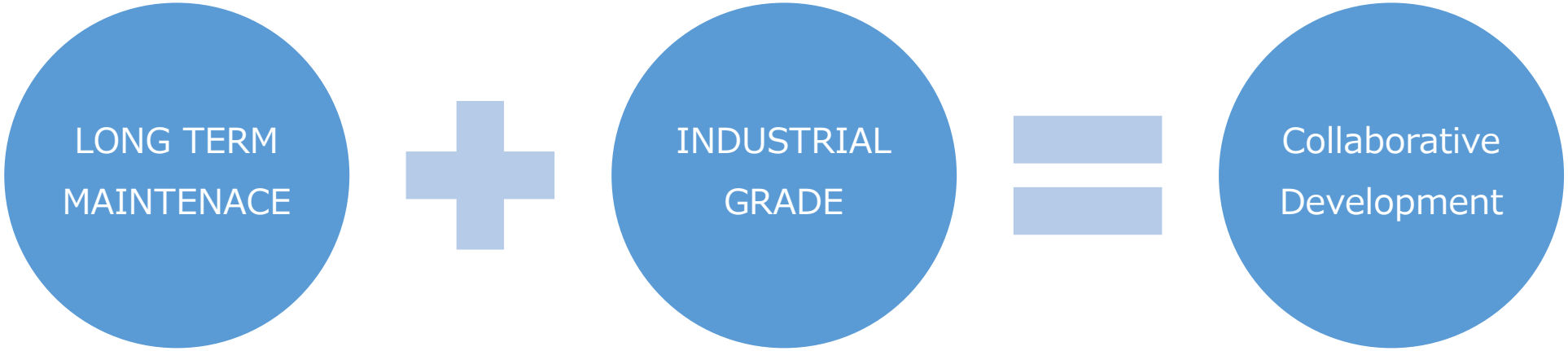
- 現代社会を支えるシステムの特徴
  - **長期運用**
  - **産業グレード**（堅牢性、セキュア、信頼性やリアルタイム性能）

- 課題
  - **各企業が負担**してきたメンテナンスコスト
  - 長期運用と**最新のテクノロジートレンドへの**追従の両立

→ どの企業も**同じ課題**を持つ

CIVIL INFRASTRUCTURE PLATFORM

課題解決に必要なソリューションは…



- 各企業共通課題 → Open Sourceで連携して解決
  - 超長期メンテナンス
  - セキュア、堅牢性、高信頼性など
- **Upstreamコミュニティ**にて共同で行う事が最も重要
  - 各社がローカルで行う事はメンテナンス性を低下させる

CIP is our solution...

CIPは、社会インフラシステムなどの高い信頼性が必要な産業機器に共通して利用可能な *Open Source Base Layer* (OSBL) を提供する

https://www.cip-project.org/

CIVIL INFRASTRUCTURE PLATFORM

since April 2016

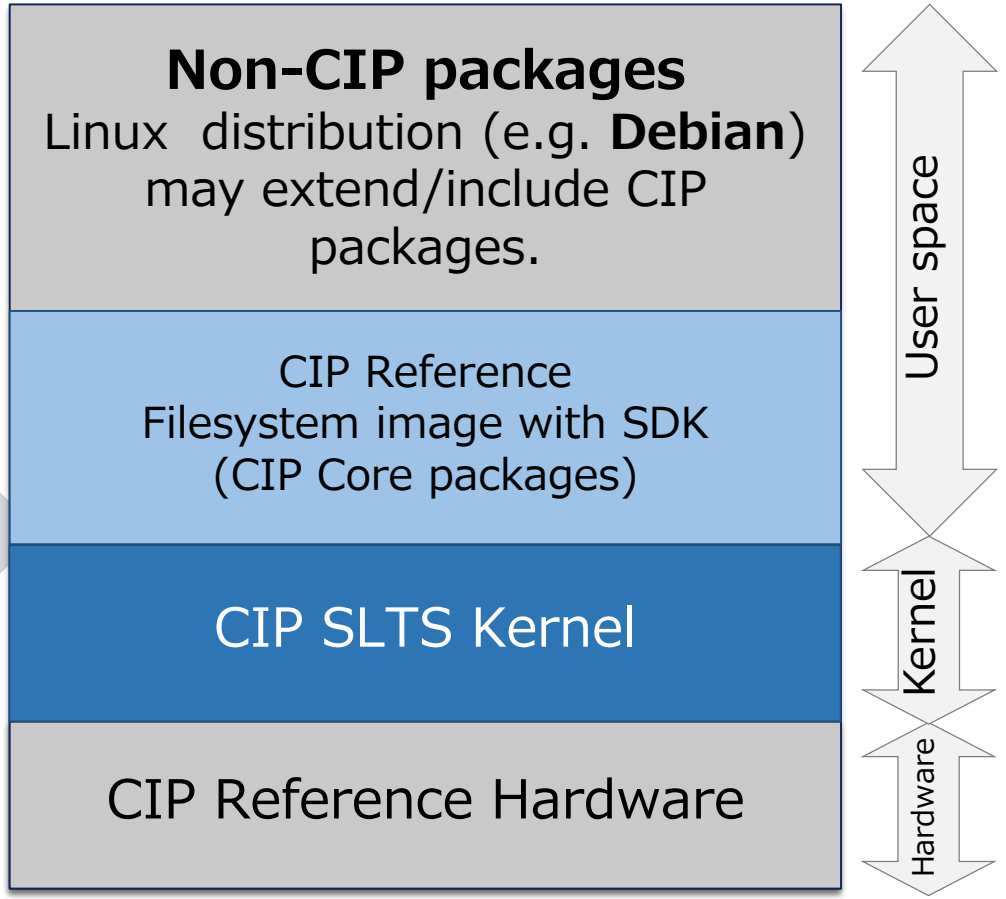
“Open Source Base Layer (OSBL)”とは?

OSBL

- 産業グレードのOpen Source コアコンポーネント、ツール、およびメソッドのセット

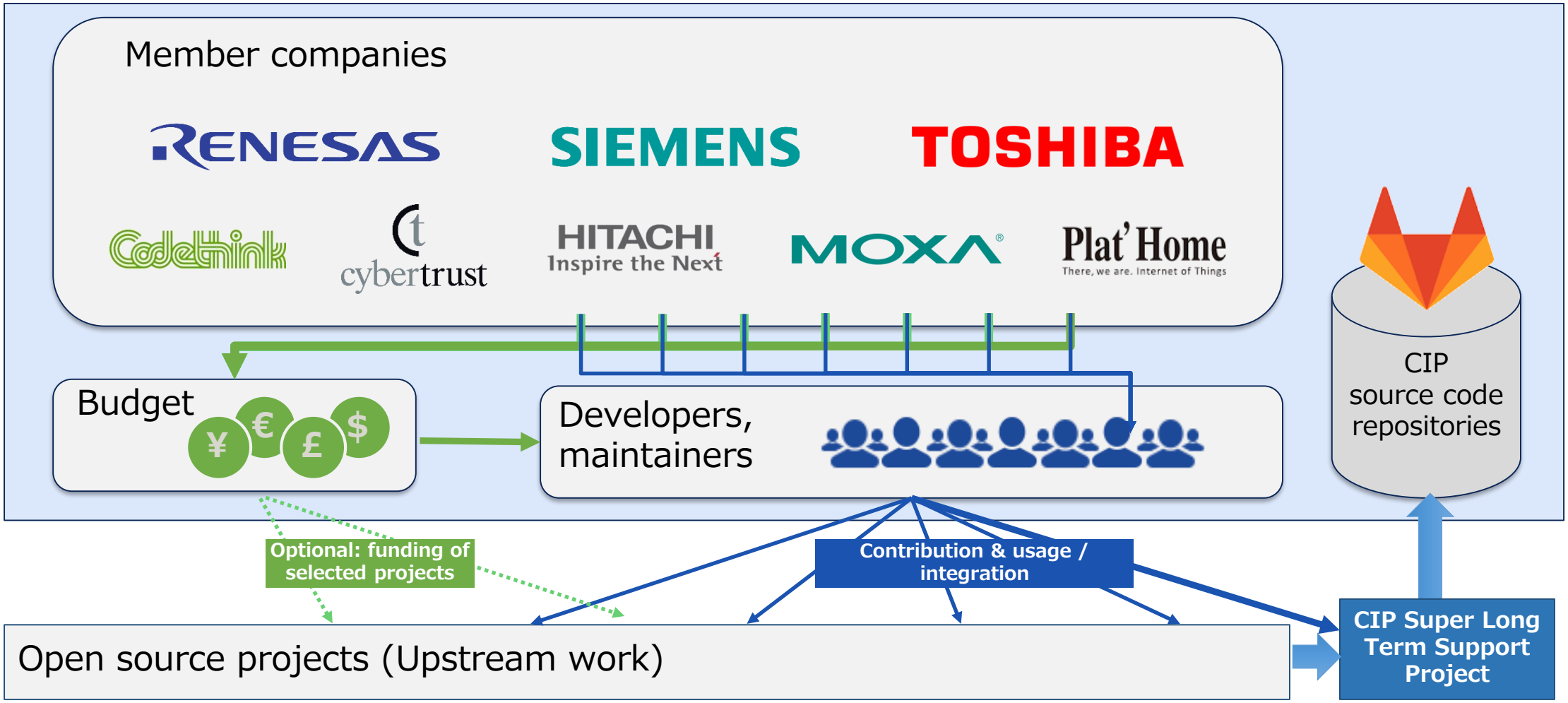
Open Source Base Layer (OSBL)

- **Open sourceベースのリファレンス実装**
- **産業グレードシステムの制御機器用の最小セットからスタート**



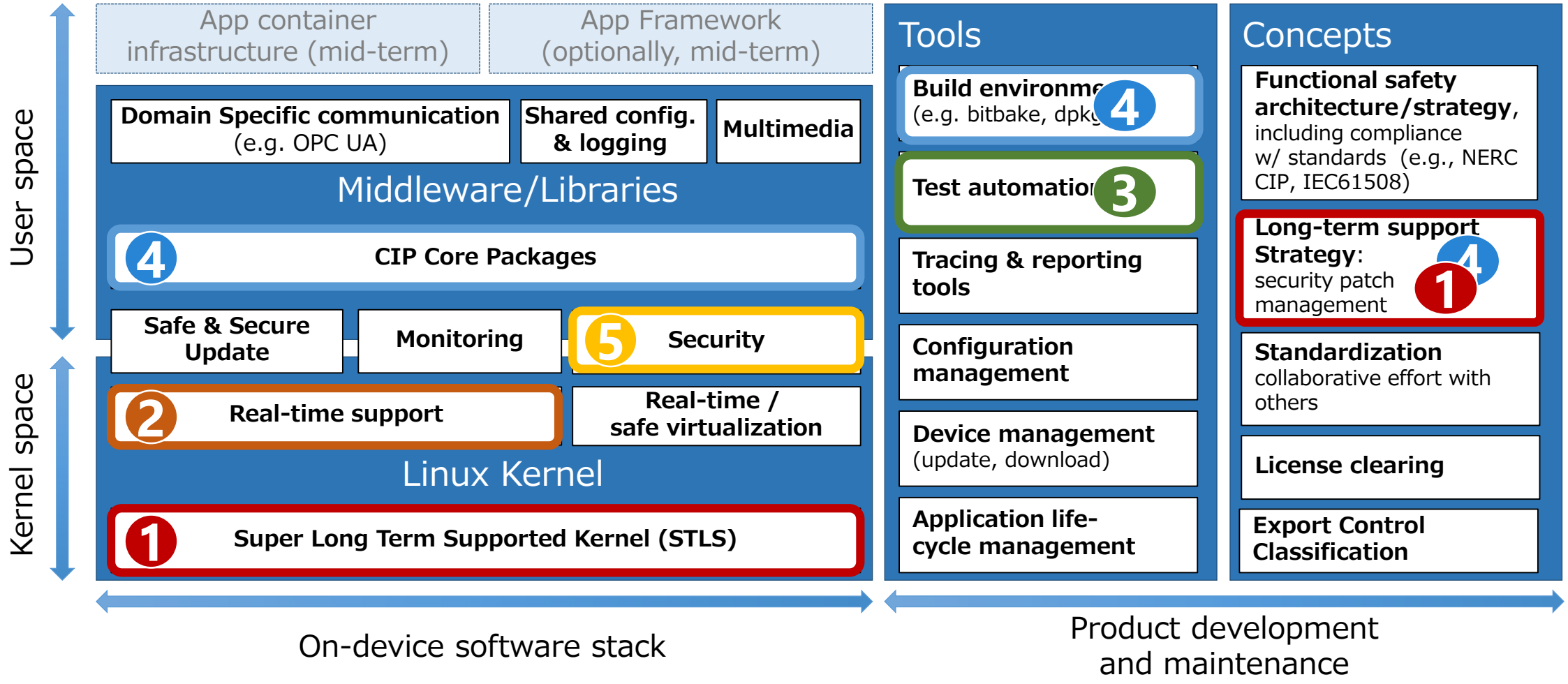
CIVIL INFRASTRUCTURE PLATFORM

CIPの活動はメンバー企業によって支えられている



CIPの取り組みとステータス

CIPのスコープ



CIVIL INFRASTRUCTURE PLATFORM

CIPの取り組み

❶ Kernel メンテナンス

- CIPプロジェクト最初のアクティビティ。SLTS Kernelを選定し、超長期にメンテ

❷ Real Time Support

- PREEMPT_RT PatchをCIP Kernelへ適用し、CIP-RTとして超長期にメンテナンス

❸ Testing

- 社会インフラシステムや産業機器が求める高い安定性、信頼性、セキュリティ標準への準拠のため、CIPプラットフォーム全体評価を行うTest Labを開設。

❹ CIP Core

- CIP Coreは、超長期間のメンテナンスが要求される産業グレードのコンポーネントを評価するため、最小のFileSystemイメージを開発するプロジェクト。

❺ Security Working Group

- ユーザーが、サイバーセキュリティ標準IEC62443の取得をサポートするガイドライン、テスト環境、テストケースを

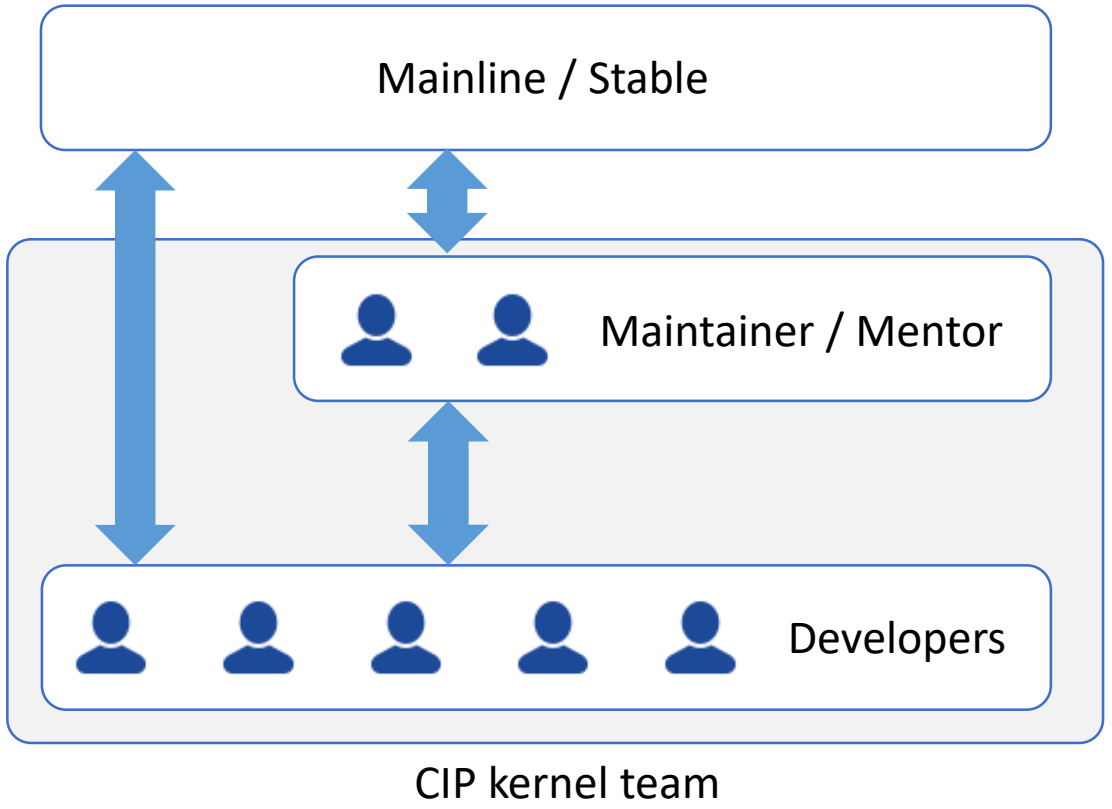
CIVIL INFRASTRUCTURE PLATFORM

❶ CIP Kernel team

CIP内にkernelメンテナンスチームを構成

- CIP Kernel Maintenance Team
  - Maintainer / Mentor
  - Developers
- CIP Kernel teamの役割
  - stable kernel用Patchのレビュー
  - Test
  - Upstreamへのフィードバック

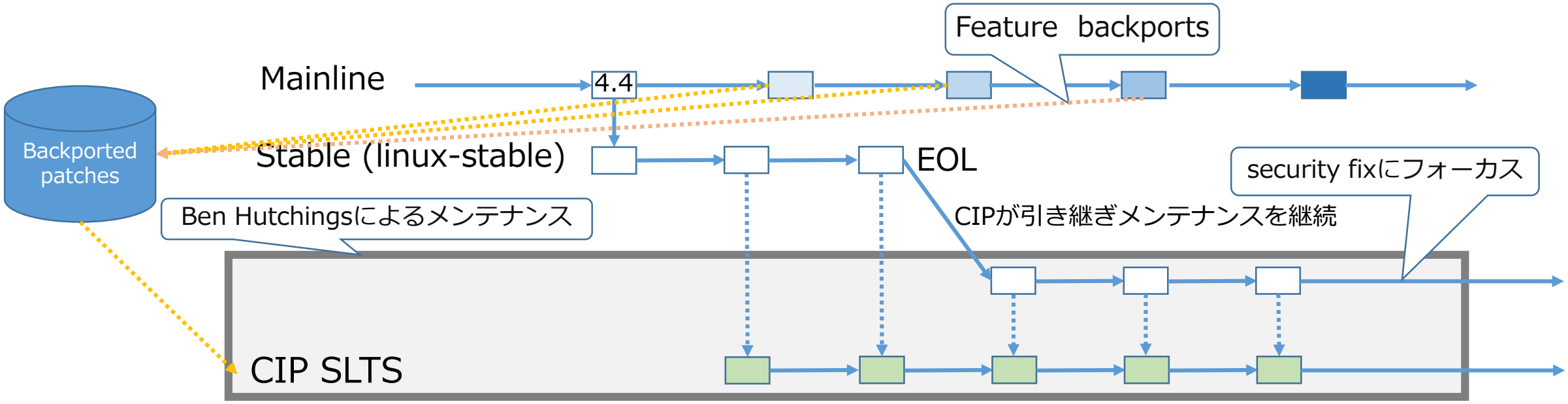
- **Upstream first**



❶ CIP SLTS Kernel開発

CIP SLTS：メンテナンス期間は10年超

- linux-stable.git のオフィシャルCIP SLTS kernel tree
  - https://git.kernel.org/cgit/linux/kernel/git/bwh/linux-cip.git/
- Maintainer: Nobuhiro Iwamatsu（Cybertrust社）



❶ CIP SLTS Kernel開発

linux-4.4.y-cip

- 最初のCIP kernel (Linux 4.4.42-cip1)　を2017/1/13 にリリース
- 最新のCIP kernel (Linux 4.4.171-cip30) を2018/2/1　にリリース
- 32bit Kernelのみ

Kernel maintenance policy※

- **Upstream first**
  - Renesas RZ/G1M 搭載のCIPリファレンスボード（Rainbow G20D - RZ/G1M）用BSPは、全てUpstreamし、CIP Kernelへバックポート済み
- Feature backportも実施（～5年）
- ValidationはCIP Testインフラ、もしくはメンバー企業で実施

※：https://wiki.linuxfoundation.org/civilinfrastructureplatform/cipkernelmaintenance

CIVIL INFRASTRUCTURE PLATFORM

❶ CIP SLTS Kernel開発

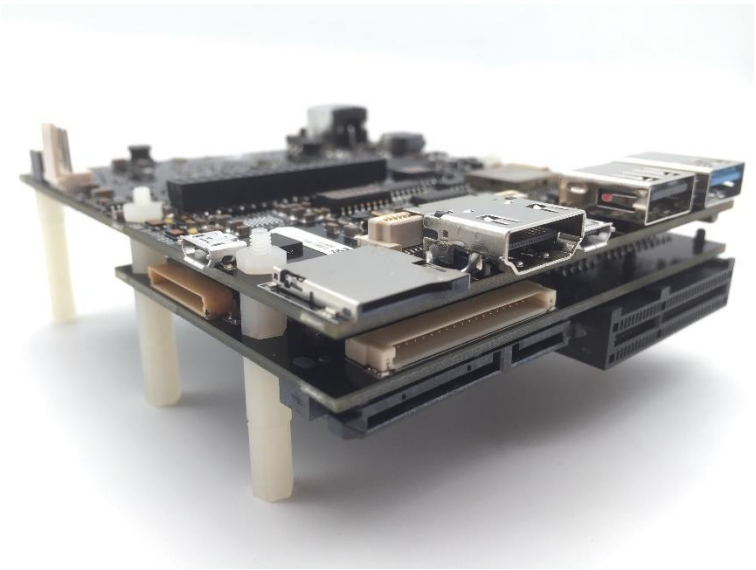
4.19

CIVIL INFRASTRUCTURE PLATFORM

❶ CIP SLTS Kernel開発

New CIP Kernel

- ”Linux 4.19.13-cip1” を2019/1/11にリリース
- 32bit/64bitサポート
- ルネサス製RZ/G2M搭載ボード（HiHope RZG2M）がCIPリファレンスボード



Linaro 96Board CE Extended Version互換

CIVIL INFRASTRUCTURE PLATFORM

サイバーセキュリティ

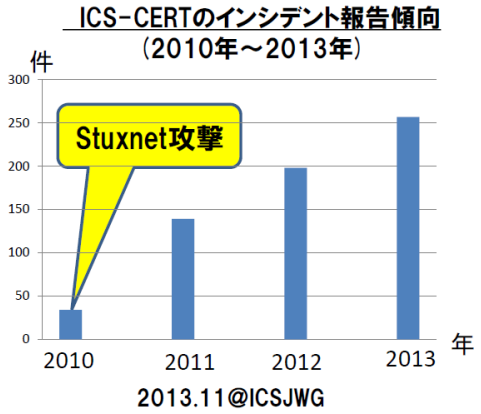
⑤ サイバーセキュリティ対策の動向

制御システムへのサイバー攻撃

- 2010年のStuxnet攻撃を皮切りに増加傾向。
- サイバーセキュリティ認証では、事業者（オペレーター）向けの規格だけでは足りず、制御システムの脆弱性やリスクアセスメントの規格も必要。
- それをカバーした汎用標準規格 **IEC62443** が注目されている。

Back ground

引用：Embedded Technology 2013 / 組込み総合技術展ＩＰＡブースプレゼン



近年、サイバー攻撃による制御システムのセキュリティインシデント件数が飛躍的に増大

Factory operator's situation

Risk!
信頼失墜

Risk!
品質悪化
生産停止

Risk!
装置・設備
の破壊

制御システムなど全てのセキュリティ対策が不可避

汎用規格 IEC62443 に注目

CIVIL INFRASTRUCTURE PLATFORM

⑤ サイバーセキュリティ対策の動向

従来のサイバーセキュリティ（情報セキュリティ）

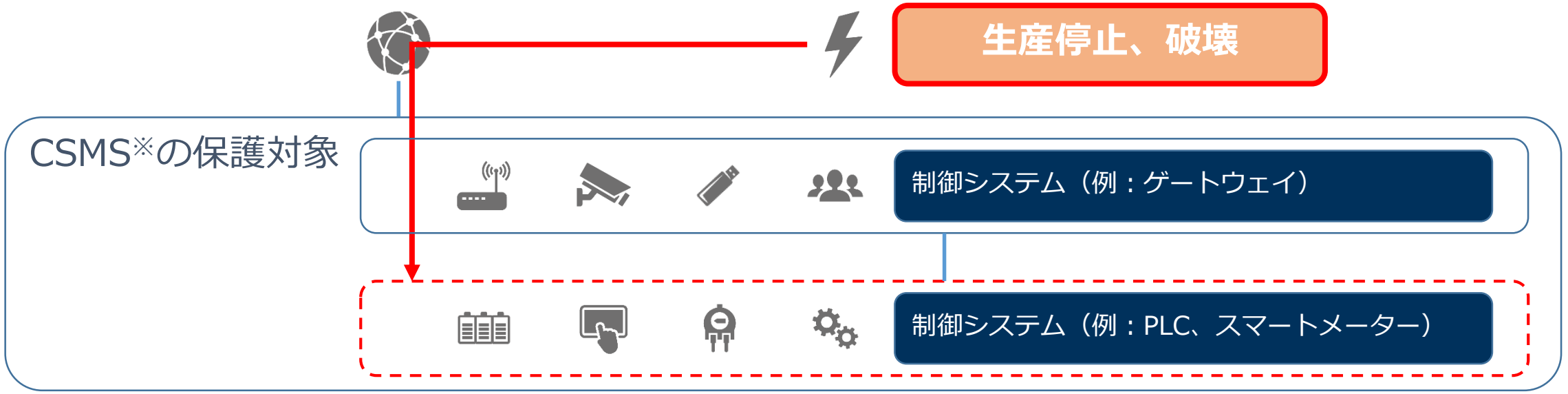
- ISMS認証制度により、情報資産のセキュリティ対策を実施
- 攻撃者の目的は、データの改ざんや搾取

※： Information Security Management System, 情報セキュリティマネジメントシステム

⑤ サイバーセキュリティ対策の動向

サイバーセキュリティ対策

- IoTの進歩を背景に制御システムがサイバー攻撃の対象
  - 攻撃者の目的も生産停止やシステムの破壊など、被害規模が拡大
- 制御システムの保護を目的としたCSMS※で対策を実施
- 制御システムの保護は、運用管理だけで無くシステム全体での対策が必須



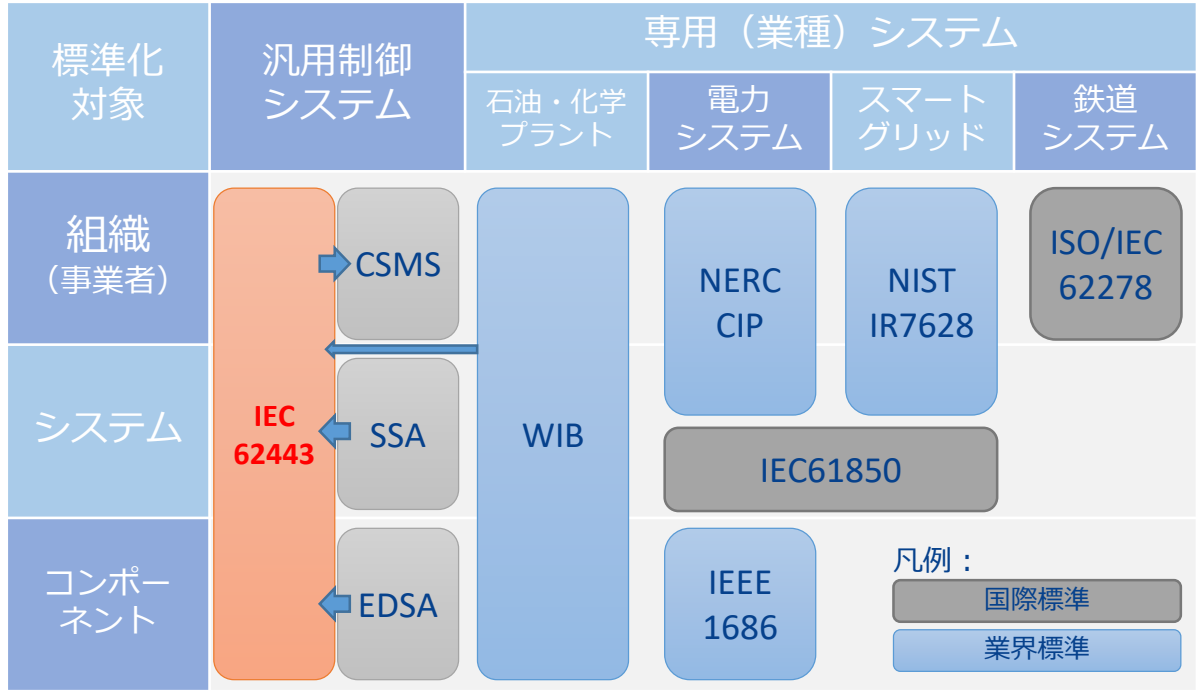
※： Cyber Security Management System, サイバーセキュリティマネジメントシステム

❺ サイバーセキュリティ対策の動向

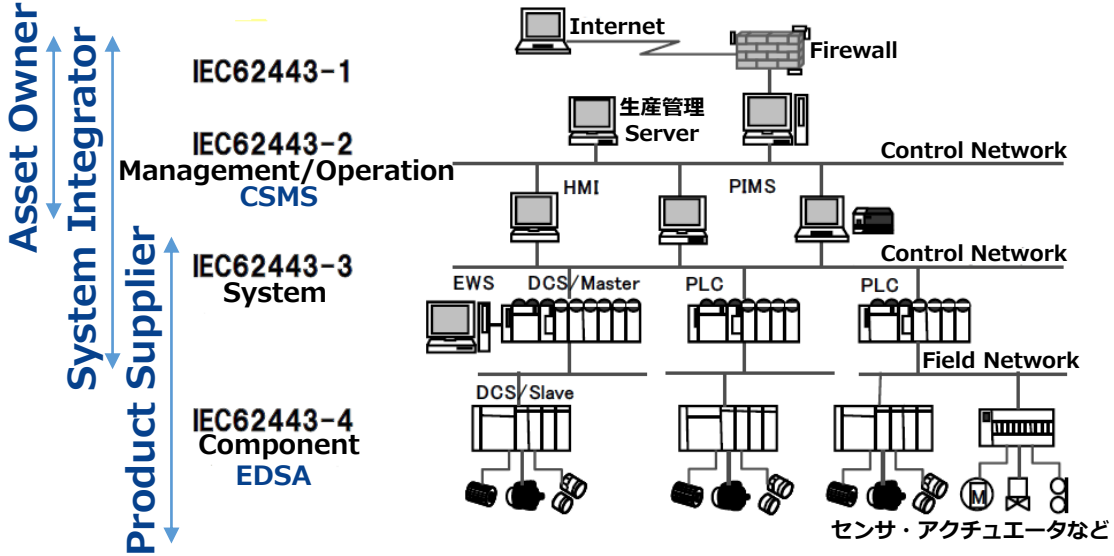
汎用サイバーセキュリティ規格 IEC62443

- 制御システムへのサイバー攻撃が増加。制御システムの**全レイヤ/プレイヤー**をカバーした汎用の標準規格 **IEC62443** への注目が日米欧で高まっている。

Standard integration



IEC 62443 overall image



参照：https://www.ipa.go.jp/files/000066499.pdf

CIVIL INFRASTRUCTURE PLATFORM

❺ サイバーセキュリティ対策の動向

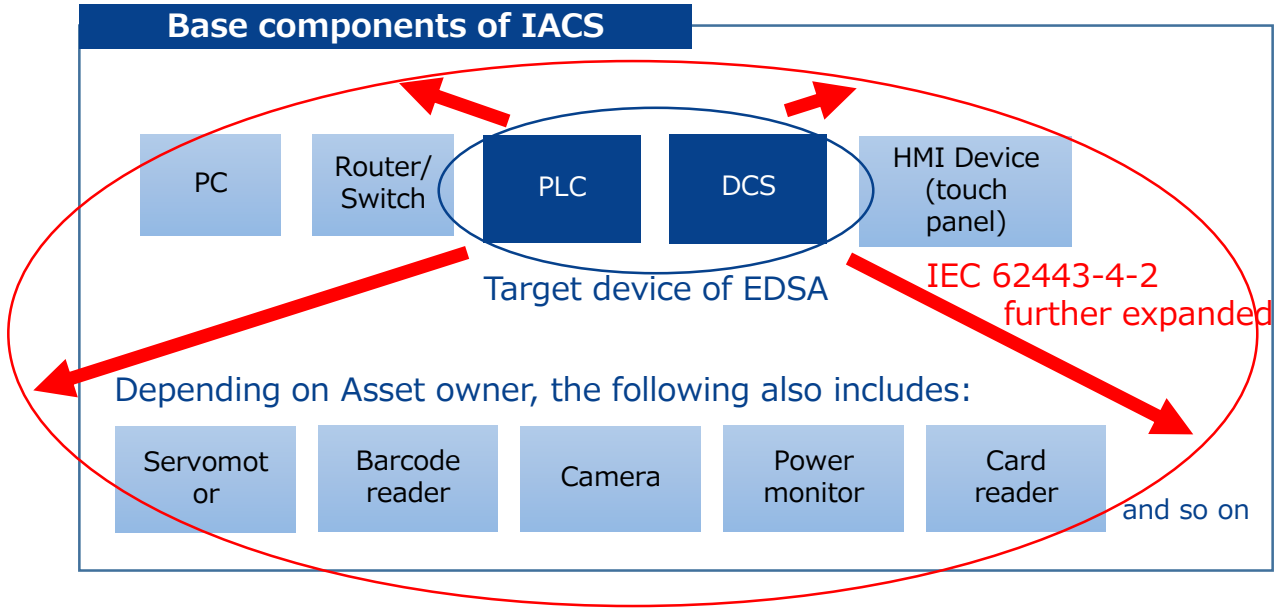
62443の拡大（米国）

- ISASecure※が、すでに運用中のEDSA認証を拡張してIEC62443-4に提案
  - 制御システムの所有者やコンポーネント機器サプライヤの多くがISASecureに参加
- 対象機器が、PLC/DCSなどの組み込み機器からネットワーク機器、HMI機器に拡大
- 2018/8/13に、ANSI/ISA62443-4-2が策定された

ISASecure members (extract)

Chevron	ExxonMobil	Honeywell
Schneider Electric	Shell	Synopsys
WisePlant	YOKOGAWA	YPF

Referred from https://www.isasecure.org/en-US/



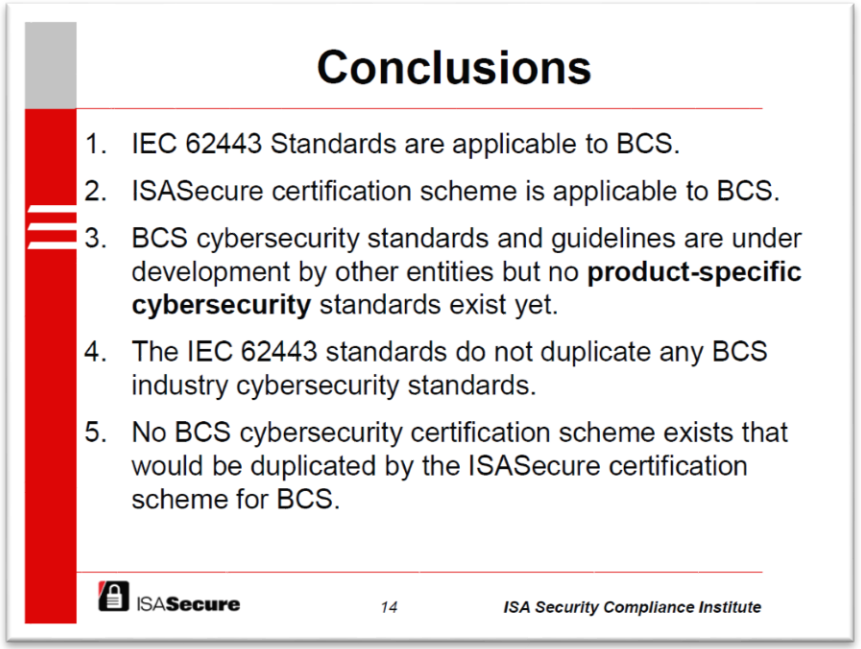
※ISASecure：認証スキームを策定するグループ、ISCI：ISAの下部組織で、認証スキームのオーナー、ISA：制御システムに係る規格の標準化活動を行う国際計測制御学会

CIVIL INFRASTRUCTURE PLATFORM

⑤ サイバーセキュリティ対策の動向

制御システムからビル制御システム（BCS）への拡張（米国）

- ISASecureのWorking Groupと大手BA機器メーカーが IEC62443のBCS向けの適用性を評価し、適用できるとの見解を示した。
- これにより、今後IEC 62443はFA業界のみでなくBA業界でも国際標準として扱われる。

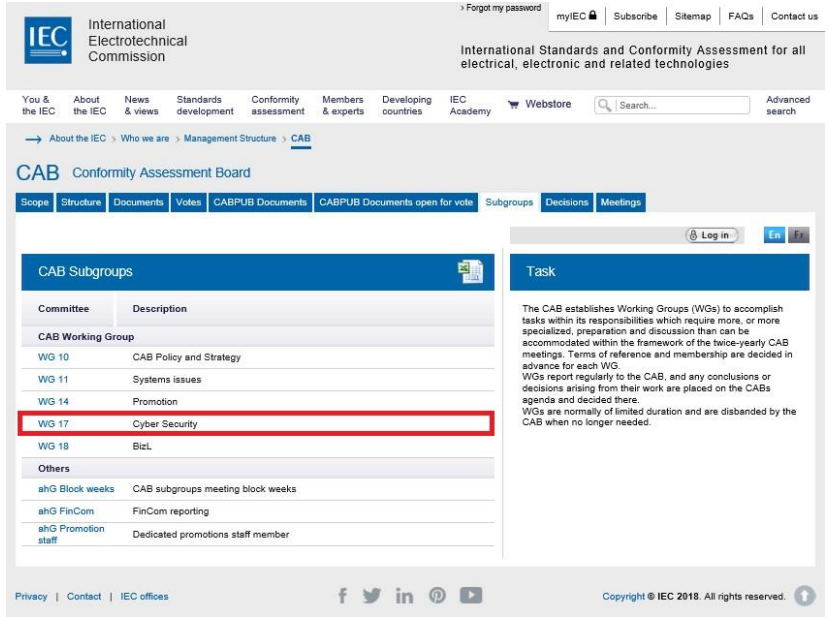


※：引用：“ISA/IEC 62443 STANDARDS AND ISASECURE® CERTIFICATION: APPLICABILITY TO BUILDING CONTROL SYSTEMS” in https://www.isasecure.org/en-US/

⑤ サイバーセキュリティ対策の動向

62443の拡大（欧州）

- ENISAはEUのサイバーセキュリティ規格を策定中
- IEC CAB WG17※ からENISAにIEC62443を提案中



引用：https://www.iec.ch/dyn/www/f?p=103:89:10516232197512::::FSP_ORG_ID,FSP_LANG_ID:3250,25

IECはIEC62443をEUの
セキュリティ統一規格として提案

※: IECのCAB（Conformity Assessment Board）に設置されたサイバーセキュリティの適用性を検討するWorking Group

CIVIL INFRASTRUCTURE PLATFORM

IEC62443認証取得における課題

❺ サプライヤーの抱える課題

IEC62443認証を取得するための費用

- セキュリティ要件を満たすための開発費
- 認証取得のためのドキュメント作成費

IEC62443認証を取得するための期間

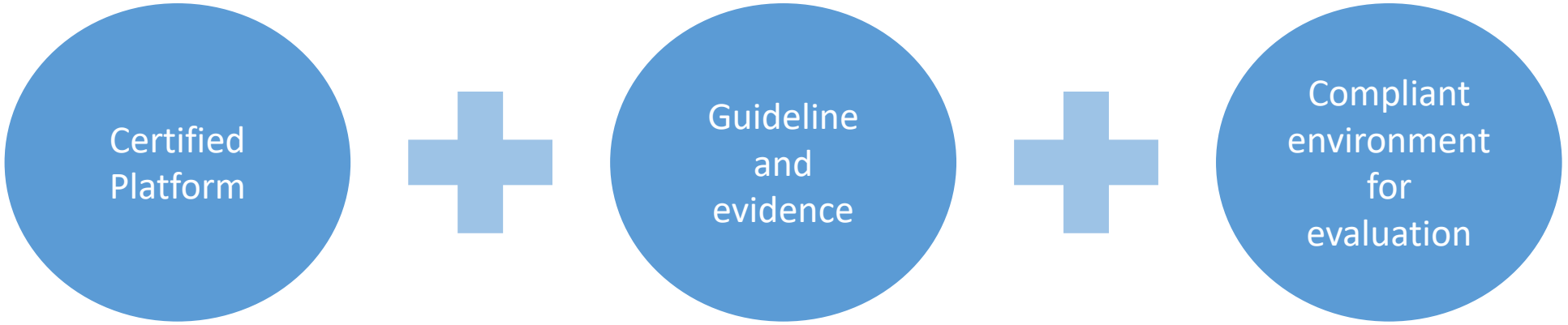
- セキュリティ規格の解釈
- 認証取得のための独特なノウハウ

→ **非競争領域だがコストが過大**

CIVIL INFRASTRUCTURE PLATFORM

❺ CIPの考えるソリューション

負担削減のための３つの対策



- 認証された共通のプラットフォームで開発費を削減
- 認証取得に必要なドキュメントを予め準備
  - 認証に必要なセキュリティ機能のエビデンスを転用
  - 実装ガイドラインで開発期間を短縮
- 認証に対応した評価ツールで確実な評価

CIP Security WGの取り組み

❺ CIP Security Working Group

CIP Security Working Groupを発足

- 2018/12/5にキックオフ
- OSSベースで、IEC62443取得をサポート
- Linuxベースのシステムで認証を取得するための：
  - ガイドライン
  - リファレンス環境
  - テストケースの開発・メンテナンス

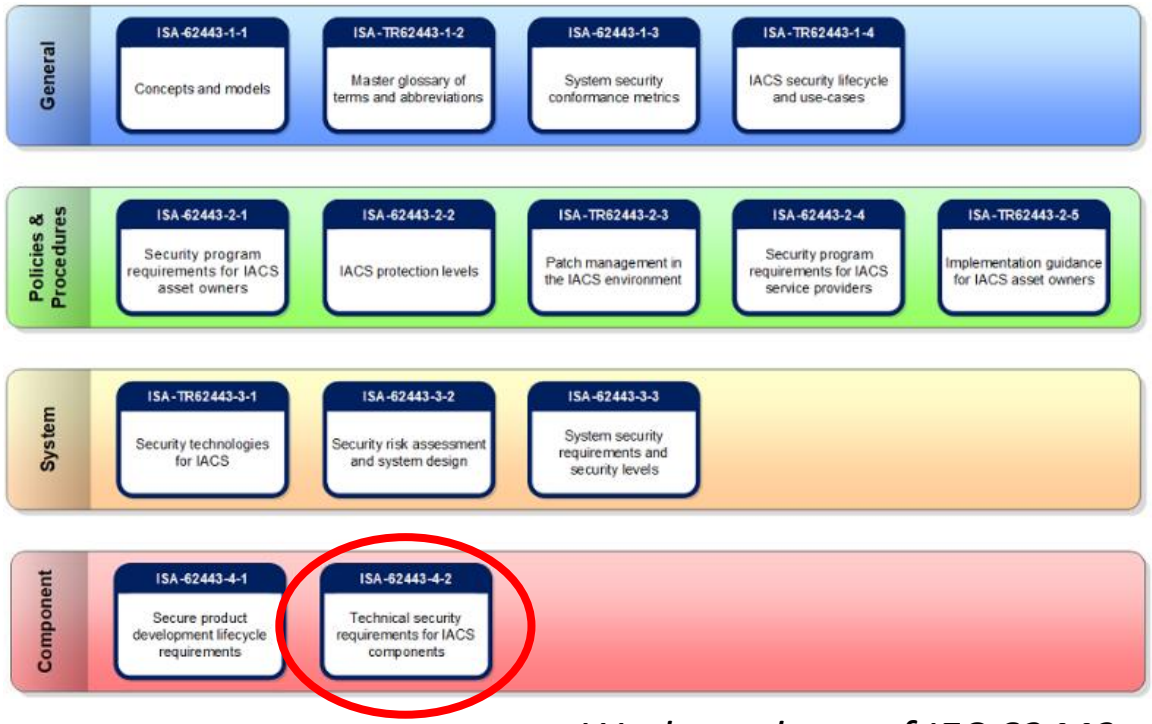
CIPは、OSSをベースにすることで、
世の中広くセキュアになる事に貢献

CIVIL INFRASTRUCTURE PLATFORM

❺ CIP Security Working Group

CIP Security WGのターゲット

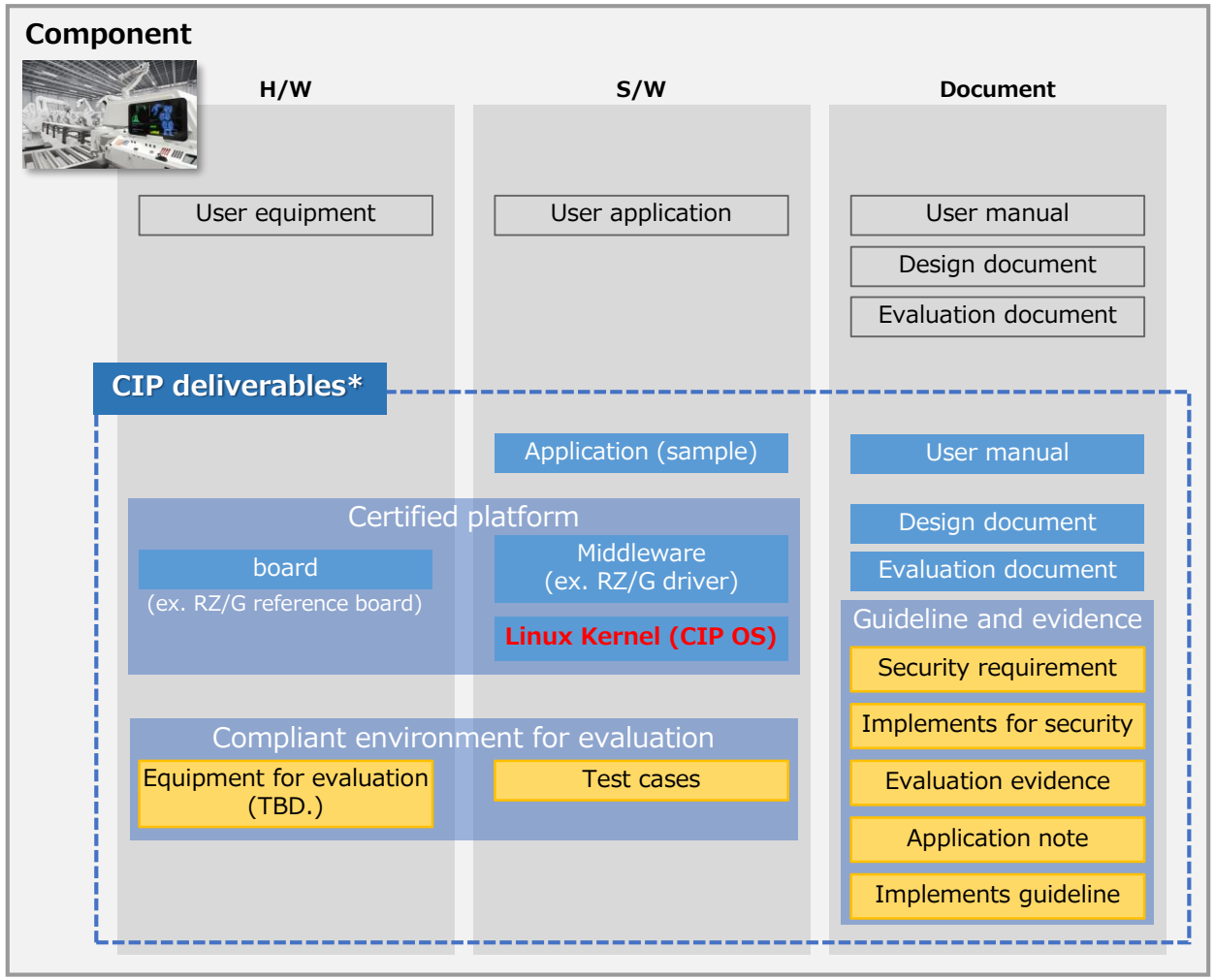
- IEC62443-4-2
  - 産業用自動制御システム（IACS）用コンポーネント向けセキュリティ技術要件



Work products of IEC 62443

CIVIL INFRASTRUCTURE PLATFORM

❺ CIP Security WGのスコープと成果物（暫定）



- 認証された共通のプラットフォーム
  - 評価ボード
  - Linux Kernel
  - Middleware

  セキュリティ要件の一部を共通プラットフォームでカバー

- 認証取得に必要なドキュメント
  - セキュリティ機能要件
  - セキュリティ実装仕様
  - セキュリティ機能評価仕様
  - セキュリティアプリケーションノート
  - 設計支援ガイド

  evidence

  エビデンスはそのまま流用可能
  さらにガイダンスでユーザのセキュリティ機能開発を支援

- 認証に対応した評価ツール
  - 評価用装置（TBD.）
  - テストケース

  評価環境の提供によりユーザ自身で事前に認証評価を実施

*: Noted that this image is under planning and for only illustrative purposes.

CIVIL INFRASTRUCTURE PLATFORM

まとめと結論

まとめ

CIPプロジェクトは

- Linux Kernelメンテナンス：
  - Linux kernelを超長期（10年超）にメンテナンス。
  - v4.4（32bit）に加え、v4.19（32/64bit）Kernelのメンテナンスを開始
  - 産業機器に求められるReliability（Testing）、Real Timeもスコープ

- Security Working Group：
  - サイバーセキュリティ標準規格の認証取得をサポート
  - OSSベースシステムの認証取得をサポートする事で世の中広くセキュアに

- 上記以外の活動も実施・検討中

結論

- この社会には産業グレードのOpen Source Base Layerが必要
  - CIPはLinuxを用いて、これを提供
- 以下によりOSBLを持続する
  - 産業分野の企業・半導体企業の支援
  - 成熟したオープンソースプロジェクトとの緊密な協力関係を構築 (Debian, PREEMPT_RT, kernelci, …)
  - 適切なツールチェーンの提供
  - 徹底的なテストの実施
  - セキュリティ要求にも積極的に貢献

コントリビューションとコラボレーションがCIPの重要な要素

Thank you!