「IEC62443とNIST SP800とISA-99におけるセキュリティベクトルについて」

株式会社ICS研究所
代表取締役社長
村上正志

本日のポイント

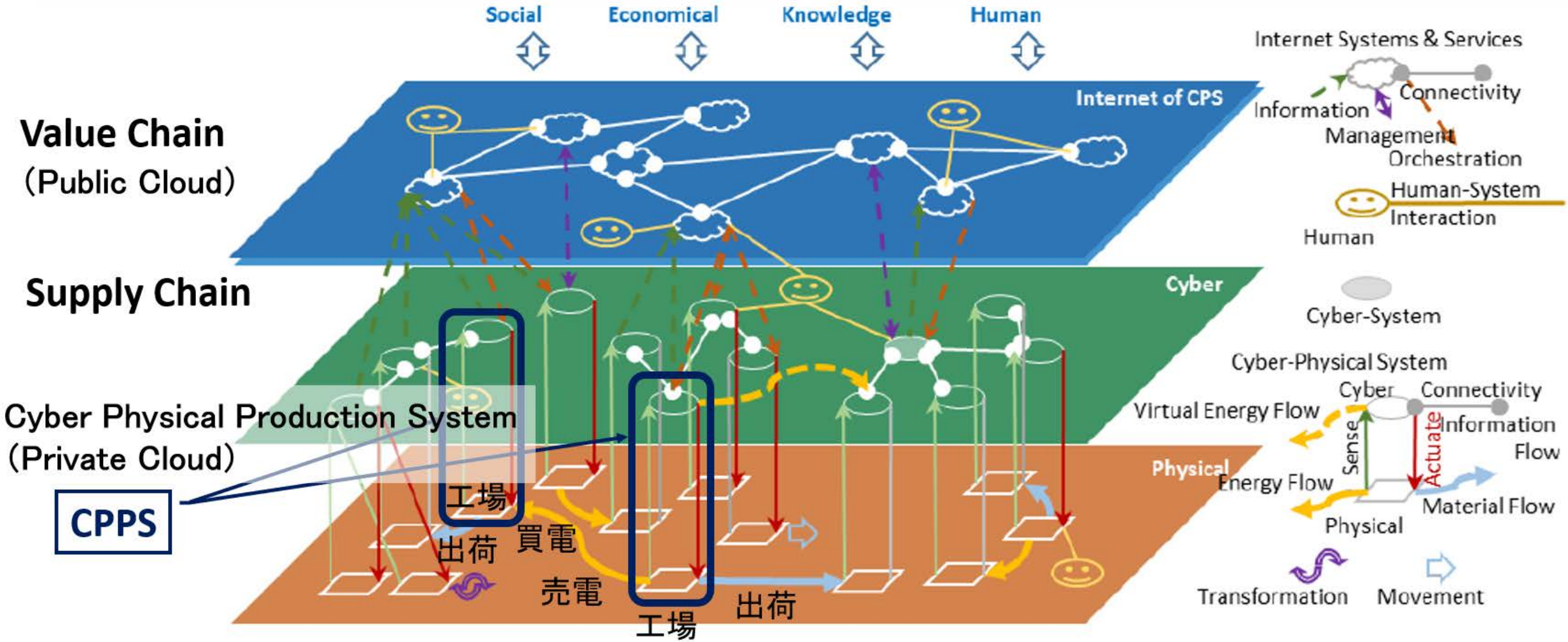
- IEC62443とNIST SP800及びISA-99に出てくるセキュリティ要件FRとシステム要件SRのセキュリティレベルでセキュリティベクトルを構成する話から、OPC UAがどのFRとSRをクリアするのかについてお話しします。
- 制御システム設計やシステムインテグレーションしていく上で課題となるスマートマニュファクチャリングやIndustry4.0／デジタルツイン／デジタルトランスフォーメーション／CPPS実現において当然実施しなければならない制御システムセキュリティ／制御セキュリティ／安全セキュリティ対策であるIEC62443-3-3／-4-2、NIST SP800、ISA-99／Secure認証の進め方及び設備の時刻合わせ実現のOPC UA TSNとフィールドバスの組み込み、セキュリティ監視システム設計及びシステムインテグレートしていく上で、広範囲の課題を解決していかなければならない課題解決にeICS講座をどのように活用して解決していくと良いかについてお話させていただきます。

Agenda

- IEC62443／NIST SP800／ISA-99 Secure認証のセキュリティレベルとEDSA認証のFSA
- IEC62443ベースのセキュリティレベル2から4に求められるサイバーセキュリティ監視システムの違い
- ログデータ解析機能の仕様と時刻合わせの重要性
- デジタルトランスフォーメーションやデジタルツインを実現する上でのセキュリティ対策のお話

CPS View：Systems of Systems

- それぞれのシステム層を連携させたCyber Physical Systemsで課題を解決
- 生産工場の高度化（AI活用）、供給連鎖、価値連鎖の構造化におけるHSEを保護するサイバーセキュリティ対策



出典：Industry4.0

Figure 9: A CPS View: Systems of Systems

CPPS：Cyber Physical Production System

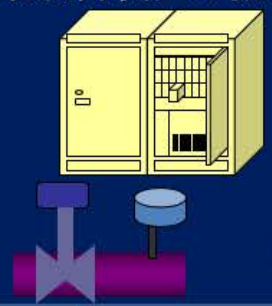
AI／ディープニューラルネットワーク／ディープラーニング

クラウドでAI（人工知能）を活用

① 安全操業の為の現場オペレーションナビ
② 熟練者の技術伝承が活かされる現場づくり
③ 現場の振る舞い監視情報と検知したインシデントを解析
④ プラントシミュレータと現場プラントを比較した振る舞い監視システム

③現場の振る舞い監視情報と検知したインシデントを解析

現場制御装置の振る舞い監視



インシデント検知

コントローラの振る舞い監視

現場

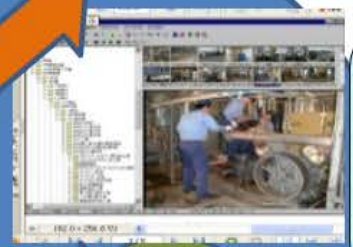
故障診断装置

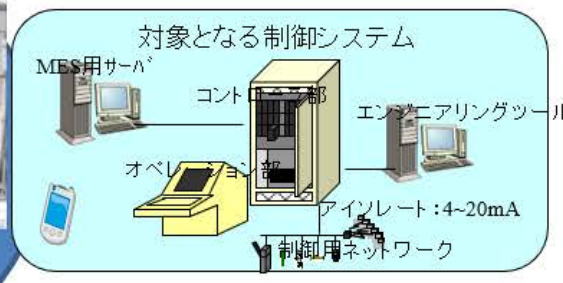
④プラントシミュレータを使った振る舞い監視システム

プラント異常検知

②熟練者の技術伝承が活かされる現場づくり

プラントの安全操業運転から、アラーム対応やメンテナンスまでのノウハウのデータベース構築

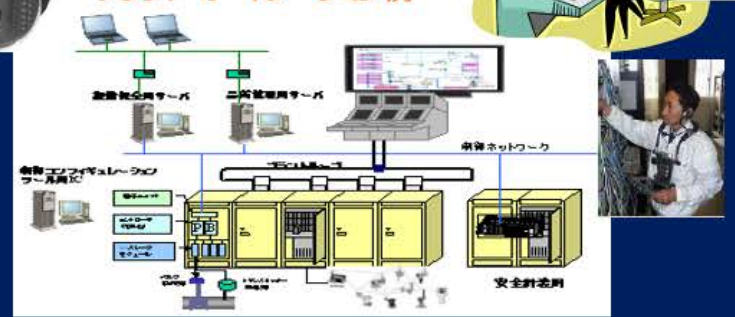




現場

Video Data Server

プラント・オートメーション例



Virtual Server

クラウド

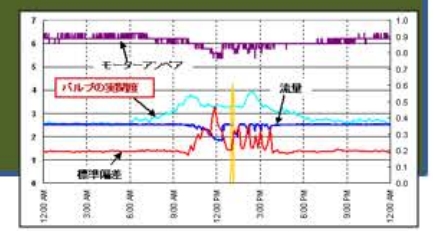
AI

①安全操業の為の現場オペレーションナビ

- ノウハウデータベースと事象に対するアクションオントロジーを構築
- 実用化テストを合格して、現場でダウンロード
- オペレーションナビの使用バージョンを管理

AIのサポートサービスセンター

オペレーションナビのオントロジー設計をする

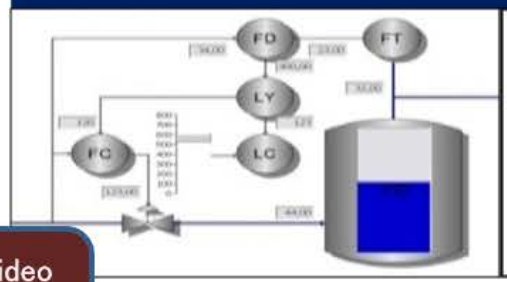


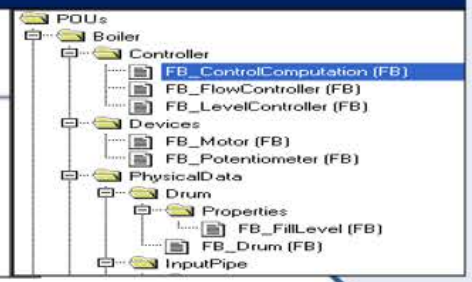
エンジニアリングサポート／オペレーションナビ

現場で使用している高度制御技術のエンジニアリングサポート

- 高度制御を使用する前の確認テスト
- シミュレータを利用したプラント制御チューニング事前テスト
- シミュレータを利用したオペレーションのナビゲーションシステム設計

セキュアな情報モデル通信プロトコルである OPC UAだからこそできるシミュレータ活用





Video Data Server

プラント・オートメーション例

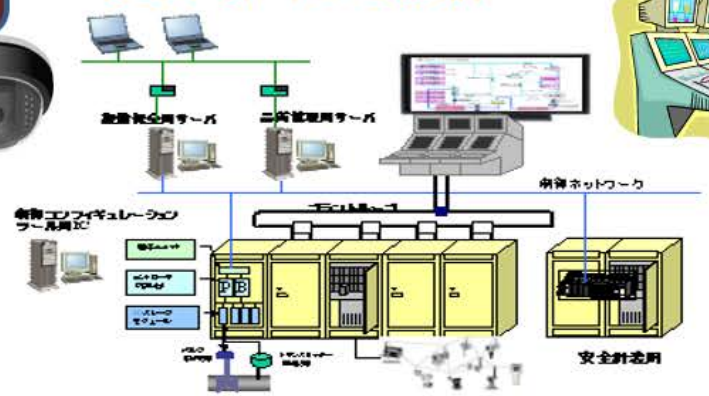


Figure 1: ARPM directly accesses the process and equipment data from the plant historian and extracts performance information

パートナー企業との設備管理と生産計画の連携

世界中の工場や施設の設備保全管理技術支援システム（AMTSS：Asset Management Technology Support System for User）
現場のノウハウを活かしたTBMとCBMを組み合わせてアセットマネージメントをセキュアに実現できる。それにより、部品購入計画ができ、その情報を受けた部品生産者の生産平準化と残業管理ができ、雇用安定につながる。

SCADAとHistorianを組み合わせて設計することができる

中近東

北米

東南アジア

国内A

国内B

Historian Server

Video Data Server

Historian View

SCM

消耗部品発注管理

部品生産計画管理

部品生産管理

部品生産計画

生産平準化

雇用安定

部品メーカー

SCADA

HMI／SCADA

CBM

TBM

TBM管理とCBM管理を組み合わせてアセット管理する。

現場

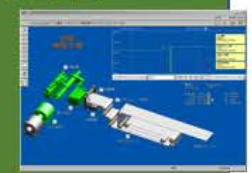
Asset

HMI／SCADA

各工場のCBMの検知仕組みを研究し、技術面で管理サポート

研究所

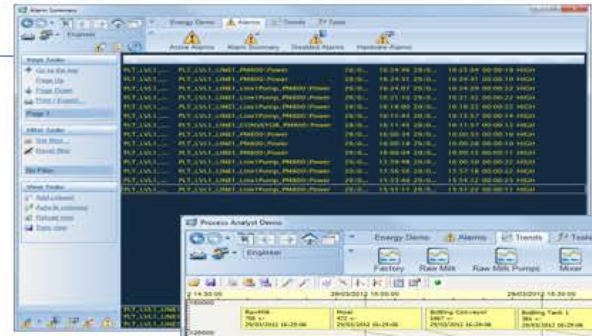
現場で必要な部品を欠かさないように適正在庫管理ができるように供給管理

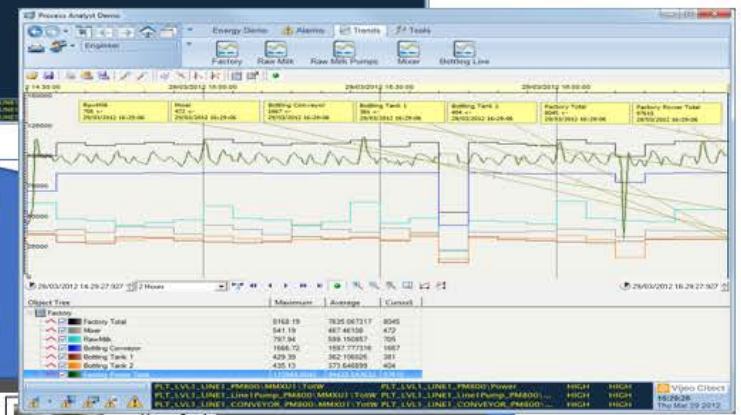


管理部門

BCP／BCMのインシデント監視・分析・回復

SCADA





サイバー攻撃から災害対策までを対処する現場サポート

- 地震、津波、集中豪雨、火山噴火などの防災対策サポート
- サイバー攻撃にも強い現場づくり⇒制御システムのセキュア改善支援
- 制御システムセキュリティ対策：現場インシデント検知 ⇒ 統合監視サーベイランスシステム
- 現場の制御システムのセキュア化の維持を目的としたセキュア改善研究を行って、現場改善を支援

SIEM

HMI／SCADA

Historian Server

プラントシミュレータ

Simulator

解析AI

プラント異常検知

サーベイランス監視画面イメージ

Video Data Server

インシデント検知

Gateway

高速データ収集

PI

DCS

現場

インシデント検知

故障診断装置

HMI／SCADA

攻撃研究システム
主要制御システムの防衛能力調査

シミュレータ

災害対策およびサイバー攻撃対策センター

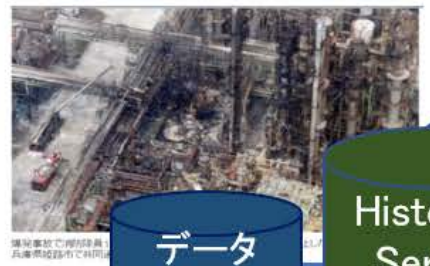
安全管理・事故解析・災害対策

爆発事故や火災事故発生時のプラントレコーダ

- プラントの制御モードや制御状況のデータを記録・バーチャル再現・分析
- 操作画面の状態や操作ログを記録・バーチャル再現・分析
- オペレータの配置や行動のビデオモニタを記録・再生・分析
- 現場作業者や連絡会話の記録・再生・分析

事故発生時の時系列状況をバーチャル再現して、事故の原因分析を可能にする検証システムを整備

現場のデータをリングバッファ形式で収集してトリガが入ったらフリーズしてバーチャル再現する機能



プラントレコーダ

データ解析

Historian Server

操作ログ

Video Data Server

高速データ収集

Gate way

DCS

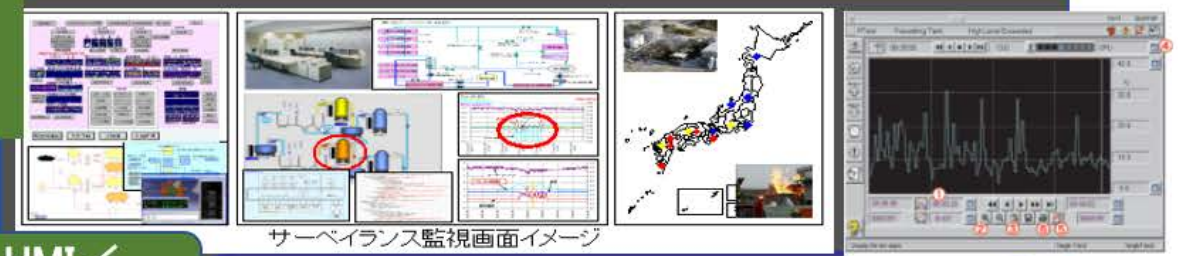
故障診断装置

時系列にバーチャル再現する機能

プラントシミュレータ

プラント再生・分析

Simulator

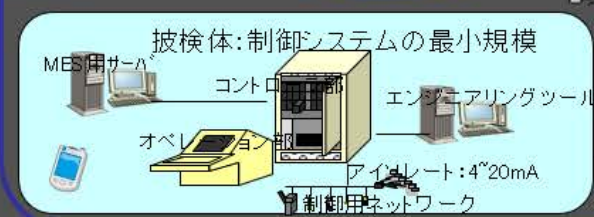


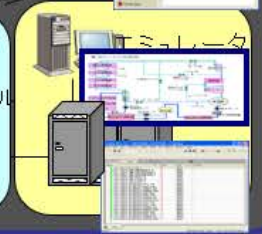
サーベイランス監視画面イメージ

HMI／SCADA

事故解析データベース

シミュレータ





事故解析及び対策研究センター

災害時対応サーベランス監視システム

サイバー攻撃から災害対策までを対処する現場サポート

- 地震、津波、集中豪雨、火山噴火などの防災対策サポート
- 被災工場の生産製品を別の工場で生産する場合の支援
- 調達から納品配送までの現場支援
- サイバー攻撃にも強い現場づくり⇒制御システムのセキュア改善支援
- 制御システムセキュリティ対策：現場インシデント検知 ⇒ 統合監視サーベイランスシステム
- 現場の制御システムのセキュア化の維持を目的としたセキュア改善研究を行って、現場改善を支援

AI技術利活用のシステム構造について

プライベートクラウド

分析

モデリング

検証

AI／ディープラーニング

再学習情報

改善提案

AI

ディープニューラルネットワーク／ディープラーニング

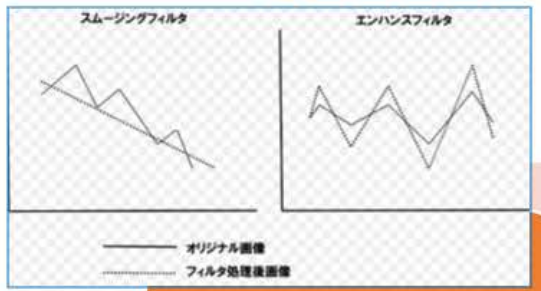
学習

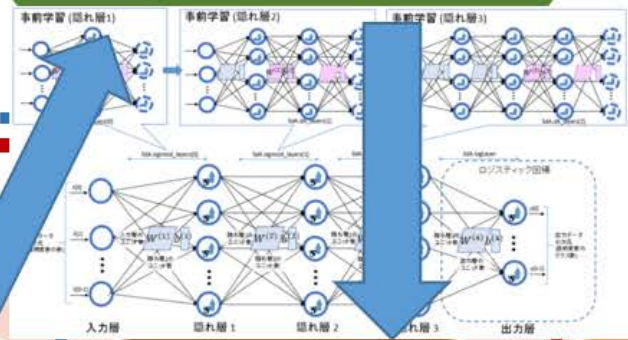
成果評価

サンプル収集

Edge-computing

Data Preparation





入力処理

センシング

ランタイム

前処理

プロセス

エンベデッドニューロ

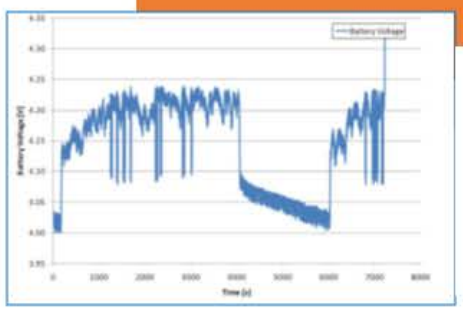
データ

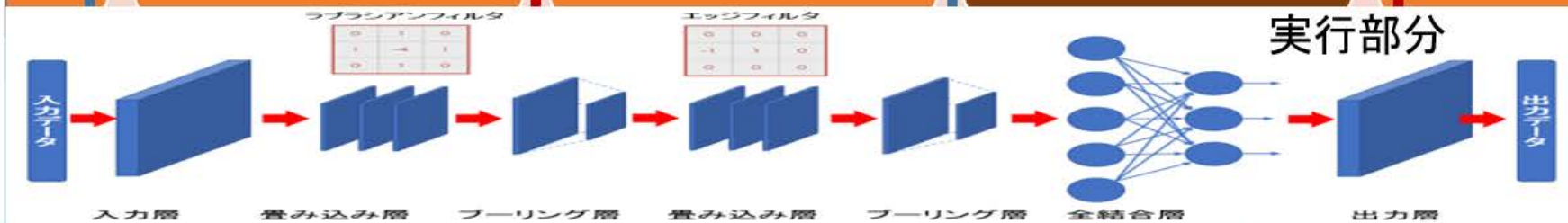
マイニング

AI／ディープラーニング

ランタイム／フィルタ

出力処理

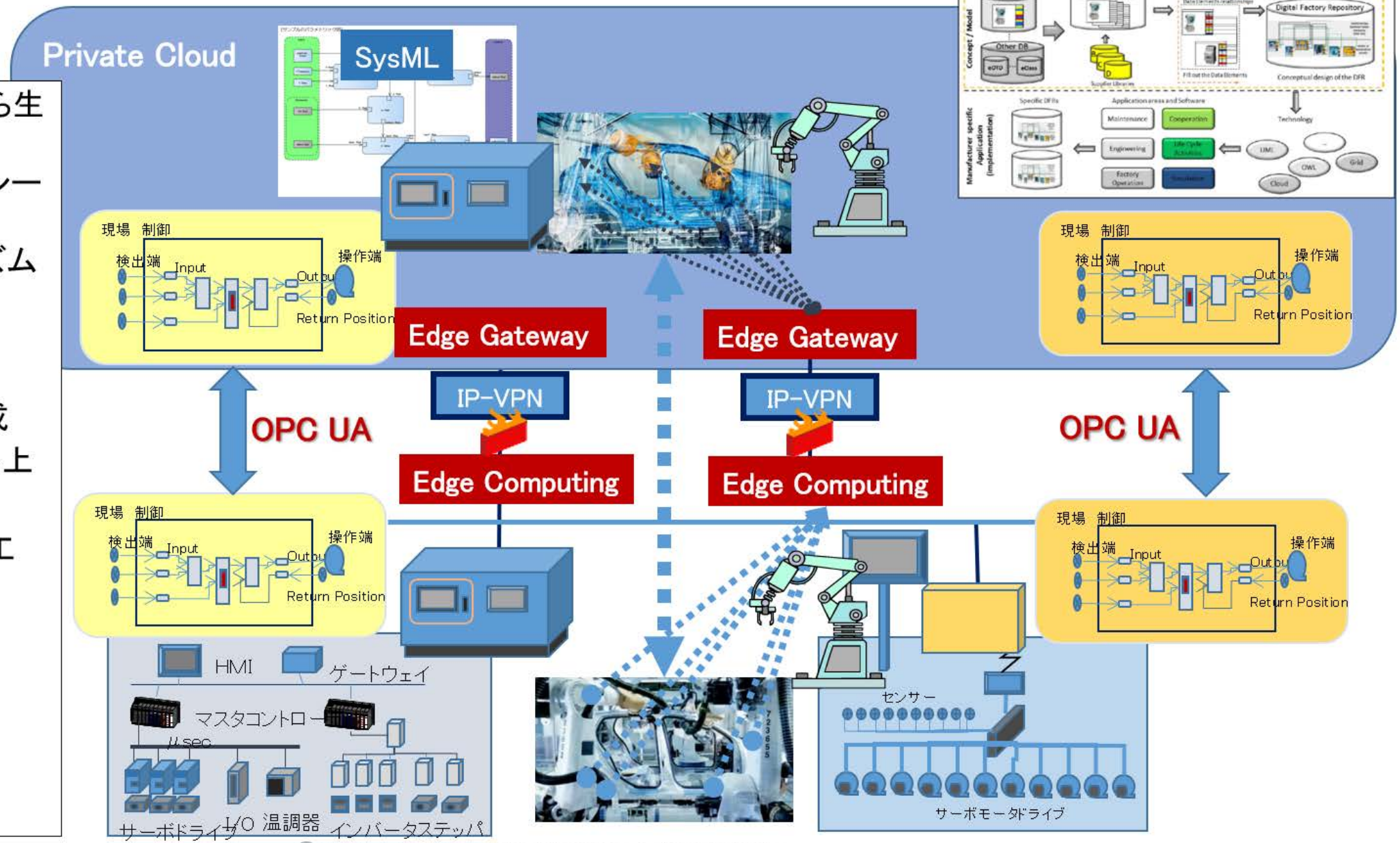




実行部分

Product Lifecycle ManagementとCPPSとセキュリティ

- 生産計画の段階から生産プロセスにおける
  - 製造手順プロシージャー作成
  - 制御アルゴリズムの確認
  - BCP
  - Cybersecurity Framework作成
  - 生産ライン立ち上げ期間短縮
- 生産工場での生産工程での振舞い監視
  - 生産品質管理
  - BCM
  - Cybersecurity Framework Management



今後、５Ｇが導入されるとどうなるか？

当日お話します。

国内外のサイバーセキュリティ法規制

米国
2002年：米国連邦情報セキュリティマネジメント法
（Federal Information Security Management Act：FISMA）
2013年2月：米国「大統領令 第13636号」
2015年：サイバーセキュリティ法
2017年5月11日：サイバーセキュリティに関する大統領令

米国は、NISTのガイドラインが基本となっています。

EU
2015年：EU「EUデータ保護指令（95/46/EC）」
（NIS（Network and Information Security）指令）
2016年8月8日　EU　NIS指令発行
2018年5月25日：EU一般データ保護法
2018年5月：EU参加国サイバーセキュリティ法法制化

中国
2017年6月：中国版サイバーセキュリティ法
2017年10月：国家情報法

注：中国のサイバーセキュリティ法は、罰則が厳しい。
注：中国国内の工場のリモートサポートは中国国内で対応が基本です。

日本
2014年11月：日本「サイバーセキュリティ基本法」
2017年4月18日：「重要インフラの情報セキュリティ対策に係わる第4次行動計画」
2017年10月：経済産業省「サイバーセキュリティ経営ガイドライン　V2.0」
2018年4月4日：「重要インフラにおける情報セキュリティ確保に係る 安全基準等策定指針（第5版）」
2018年「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引（第 1 版）」
2018年：「サイバーセキュリティ基本法」を改正
2019年：サイバーセキュリティ協議会

2016年8月8日　EU　NIS指令発行

欧州委員会は，世界同時サイバー攻撃をふまえて対策を強化すべく，2017年9月，サイバーセキュリティ規則案を提出

- **EUサイバーセキュリティ認証制度**の設立
  - 重要なインフラ施設や新しい消費者機器においてIoT製品・サービスの信頼性を確保するためのEU cybersecurity certification framework を設立。
  - 認証は任意のものであるが，日本企業も，認証の取得を取引先である欧州企業から取引条件として求められる可能性⇒サイバーセキュリティ対策の強化は，取引先や顧客の維持の観点からも重要。
- **EUサイバーセキュリティ庁**の設置
  - 現存するEuropean Agency for Network and Information Security(ENISA)を発展させて，European Union Cybersecurity Agencyを設置することを提案。

2018年5月9日までに　**EU各国がサイバーセキュリティ法法制化完了**

2018年11月6日までに　事業者の対応期限

どのような制御製品が求められるか？
どのような制御システムを設計すれば良いか？

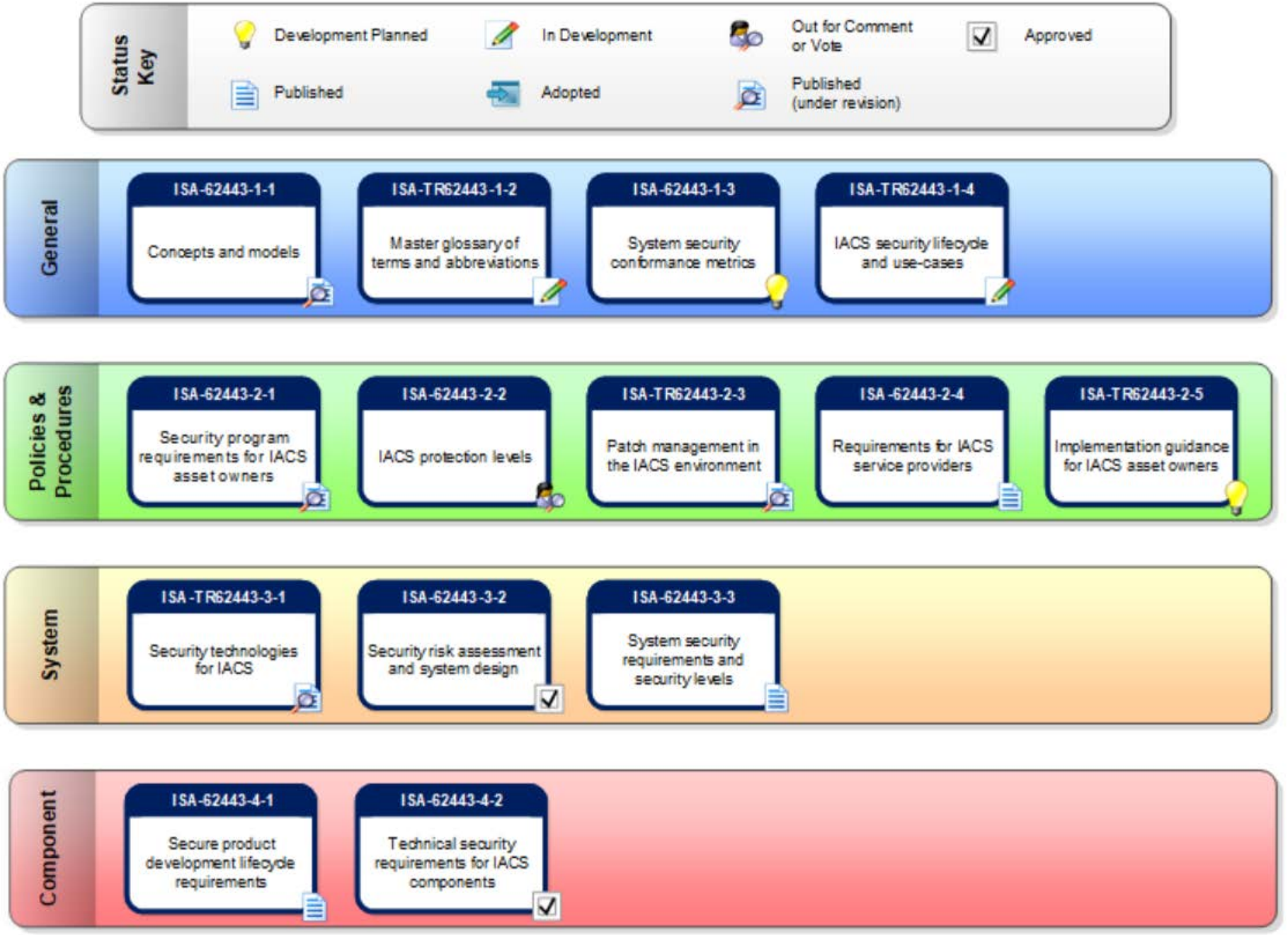
当日お話します。

どのようなセキュリティ対策ソリューションが求められるか？

当日お話します。

IEC62443

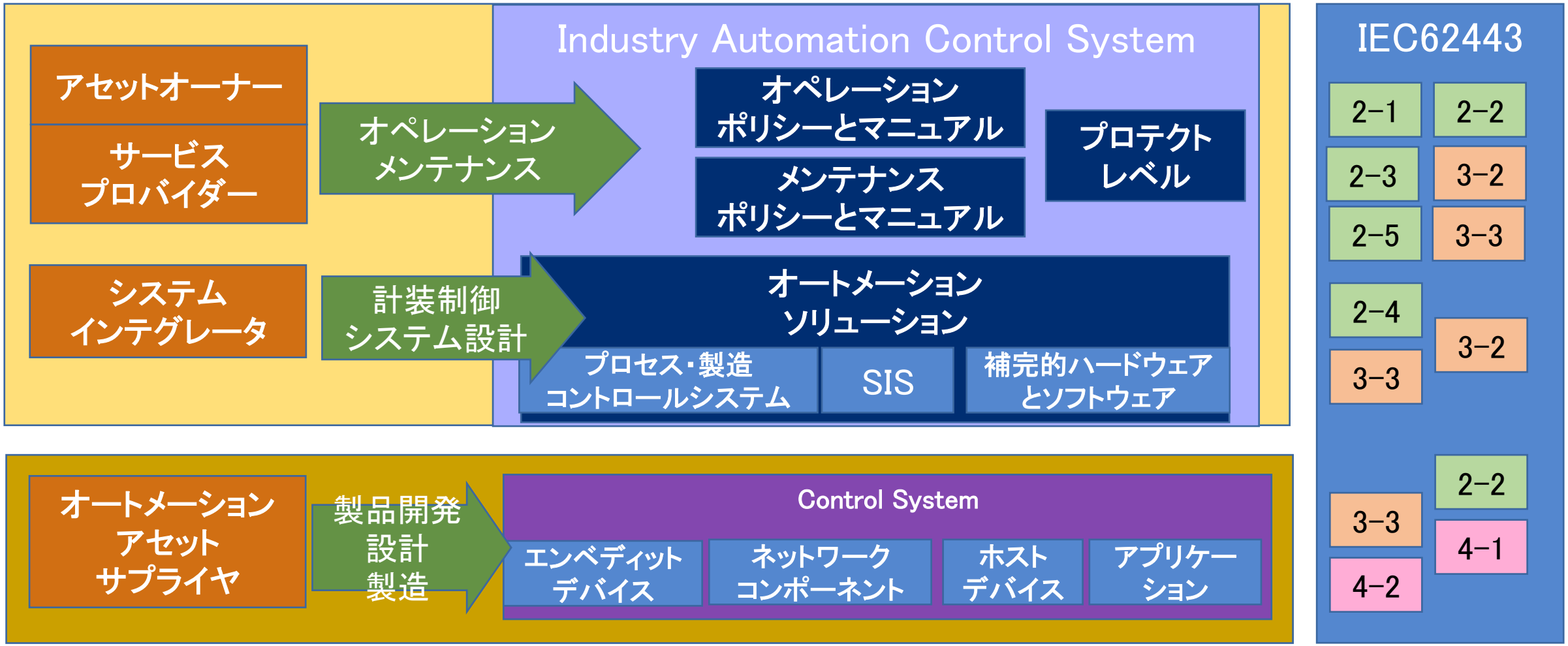
- 2011年に一度決まりましたが、その後のサイバー攻撃手法の高度化、法整備、産業別ガイドラインの整備、対策技術の進歩などで、レベルを向上
- -3-3を基準に、サイバーセキュリティレベルの照合作業を実施
- IEC62443の内容に新しい要素を追加し、各項目の整合性を確認して、全体的に更新されています。
- IEC62443では、HSE対策機能を妨げてはならないし、その機能を保護するセキュリティ対策実施となります。



https://www.isa.org/isa99/

IEC62443の対象範囲

IEC62443の各規格内容がどこを対象にしているかが解ります。



IEC62443のセキュリティ基本要件（FR：foundational requirements）

No.	セキュリティ要件	概要
1	認証 ：IAC(Identification and authentication control)	成りすましの防止 制御システムへのアクセスを許可する前に、すべての利用者（人、ソフトウェアプロセス、デバイス）を識別し、認証すること
2	アクセス権のコントロール UC（Use control）	特権の昇格の防止 認証済みユーザに与える権限を限定して、システムやリソースへの制限されたアクションを実行させるようにしたり、権限の監視をすること
3	データの完全性 ：DI（Data integrity）	改竄の防止 未認証のユーザーまたは不測の挙動によってデータが変更、破損、喪失しないこと
4	データの機密性 ：DC（Data confidentiality）	情報漏えいの防止 利用可能でないまたは開示されていない情報を未認証のシステムエンティティ（未認証の個人、エンティティ、プロセスを含む）が利用できないこと
5	データフローの制約 ：RDF（Restricted data flow）	影響範囲の局所化 不必要なデータフローを制限するために、ゾーンまたは経路を部分分けすること
6	イベントへのタイムリーな応答 ：TRE（Timely response to events）	迅速な復帰 適切な権限所持者への通知、違反の証拠を含むレポートの作成、問題発生時のタイムリーな調整アクションによるセキュリティ違反への応答
7	リソースの可用性 ：RA（Resource availability）	サービスダウンの防止 必須のサービスが使用不能に陥らないよう、システムまたはリソースの可用性を保証すること

Table B.1 – Mapping of SRs and REs to FR SAL levels 1-4

SRs and REs	SAL 1	SAL 2	SAL 3	SAL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user, process and device identification and authentication		✓	✓	✓
RE (1)		✓	✓	✓
RE (2)			✓	✓
SR 1.2 – Account management	✓	✓	✓	✓
SR 1.3 – Identifier management	✓	✓	✓	✓

出典:IEC62443-3-3

IEC62443-3-3
システム要件

- IEC62443では、セキュリティレベルでシステム要件が明確になっている。
- 基本設計の段階から、制御システムゾーン区分とセキュリティレベル定義を実施する。 それにより、ゾーン内の制御ネットワークや制御機器に要求されるセキュリティ要件が明確になる。

サイバー攻撃に強い制御システムを設計するにはどうしたら良いか？

当日お話します。

Schematic of correlation of the use of different SL types

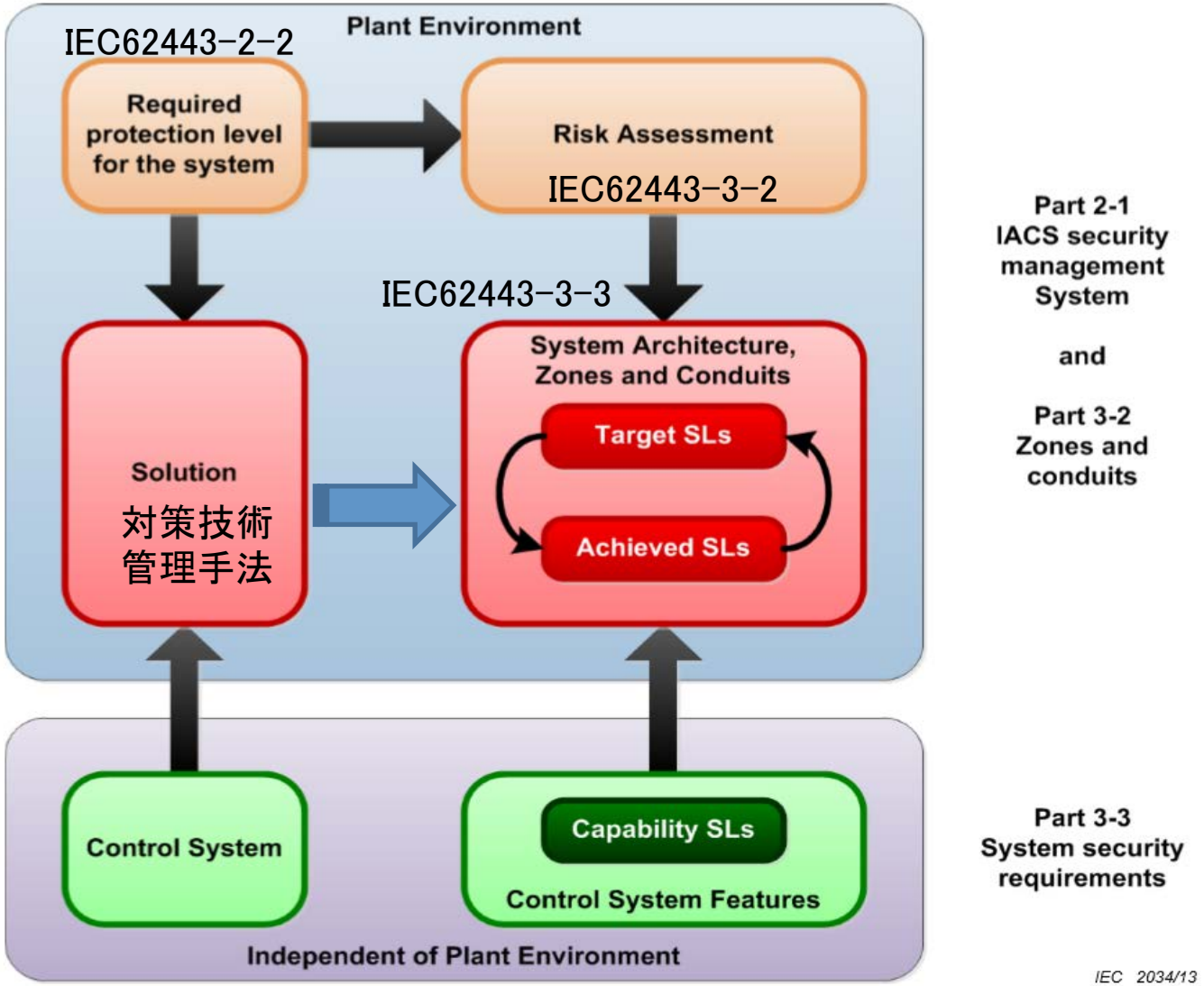


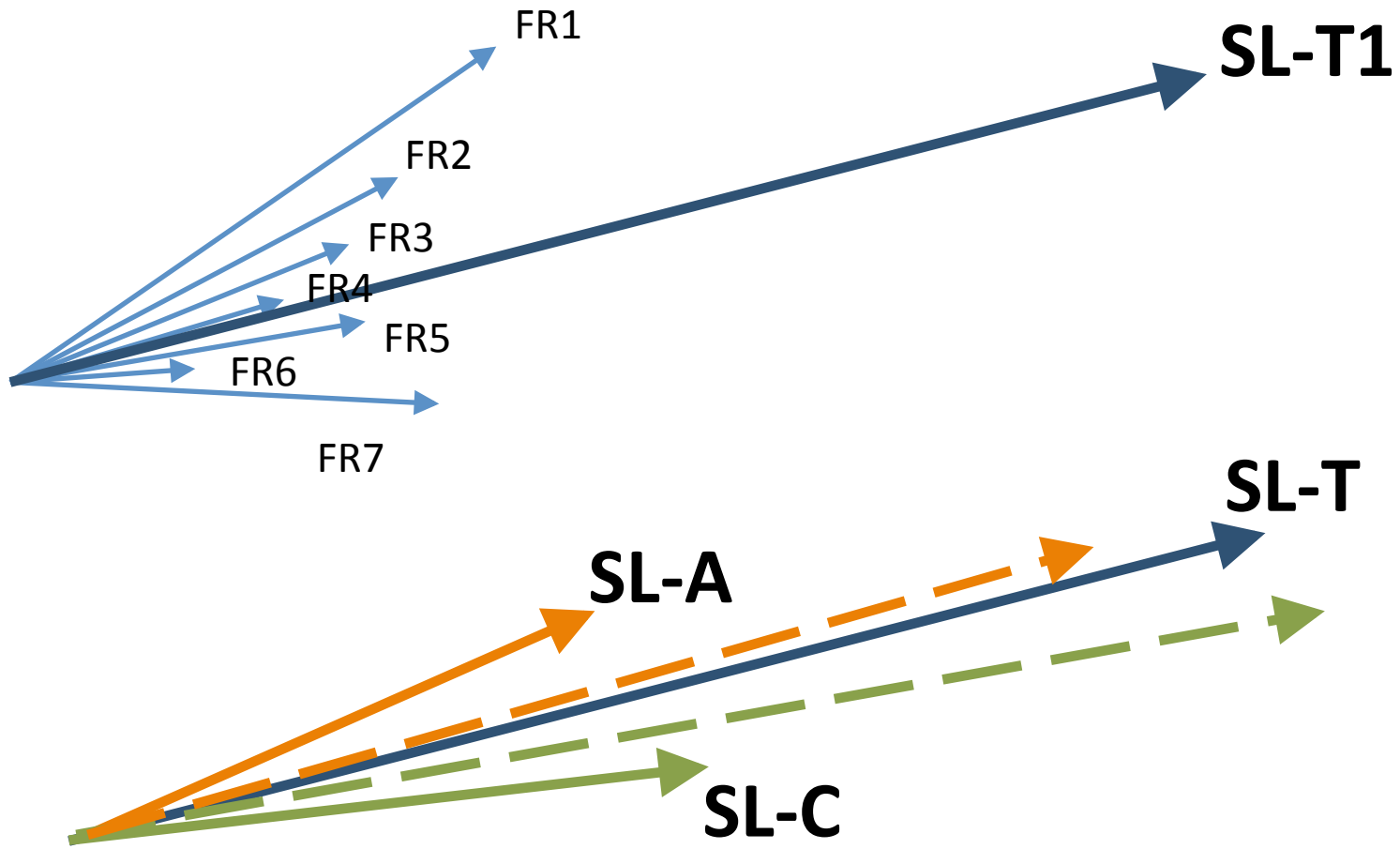
Figure A.3 – Schematic of correlation of the use of different SL ty

出典：IEC62443-3-3

セキュリティ要件とセキュリティベクトル

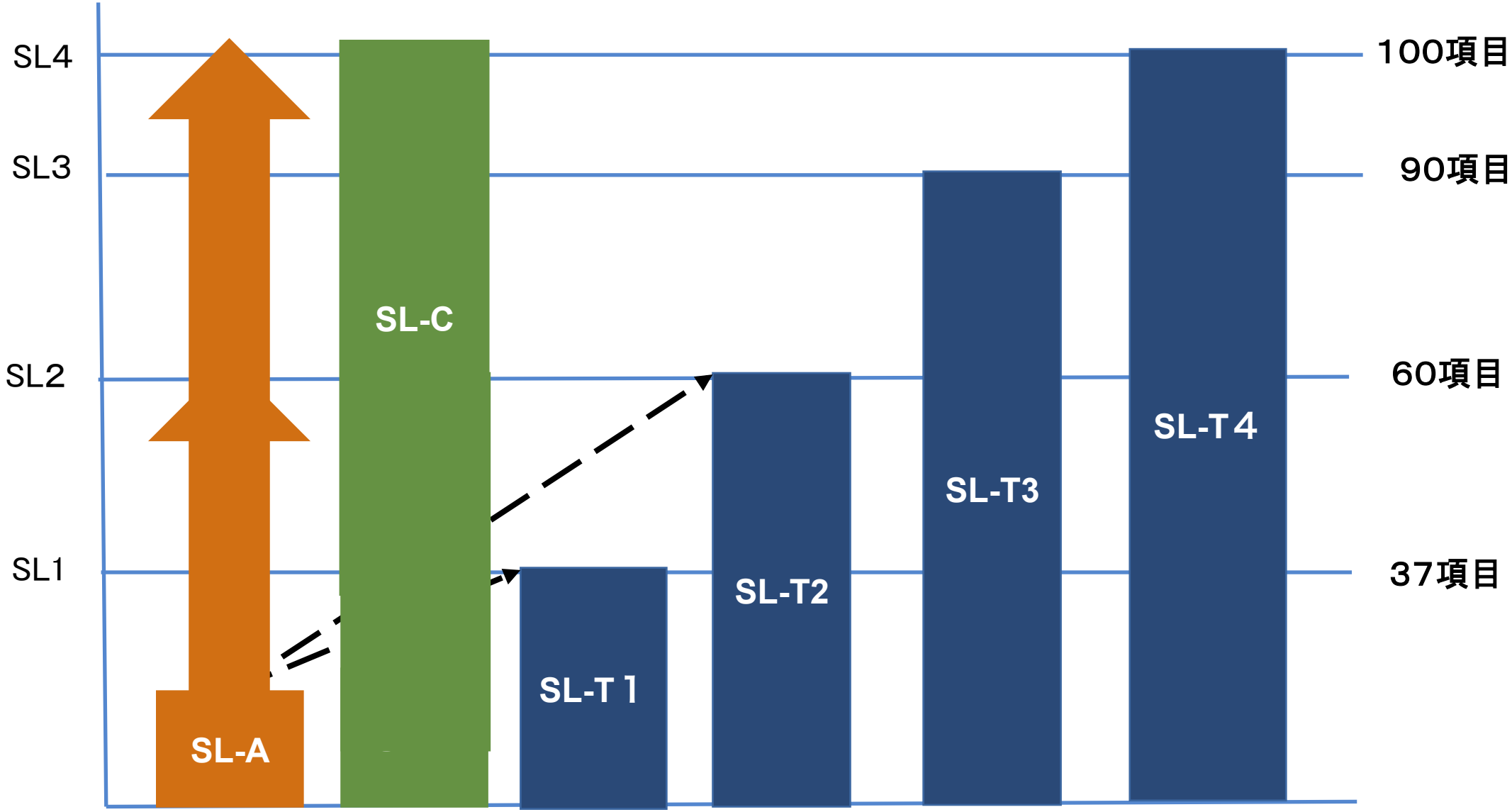
セキュリティ要件のシステム要件数

FR 項目	SL-A	SL-T			
		SL-1	SL-2	SL-3	SL-4
FR1	4	10	16	22	24
FR2	3	8	12	21	24
FR3	3	5	10	16	19
FR4	1	2	4	5	6
FR5	2	4	6	10	11
FR6	1	1	2	3	3
FR7	4	7	10	13	13

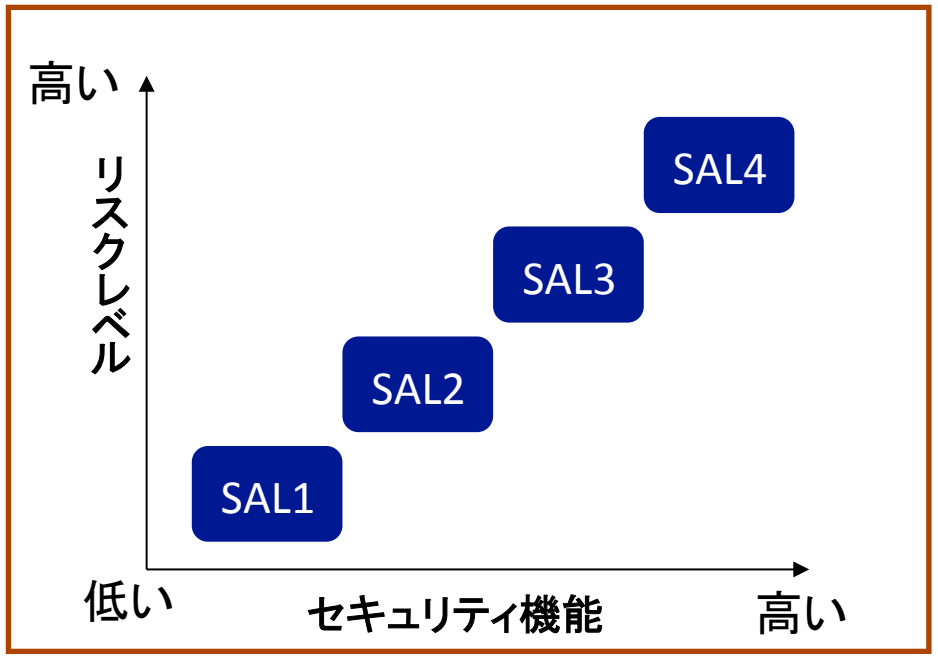


SL-T：セキュリティレベルの目標値
SL-A：現在の制御システムの実力値
SL-C：能力値（コンポーネント、マネージメント、インテグリティなど）

サイバーセキュリティレベル

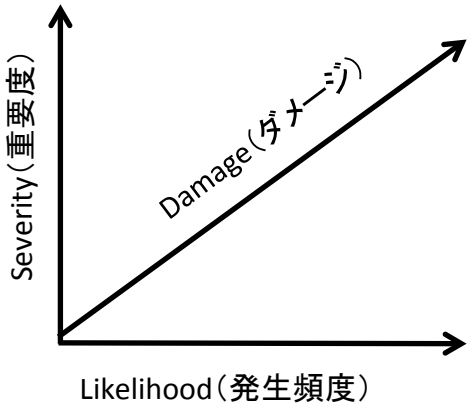


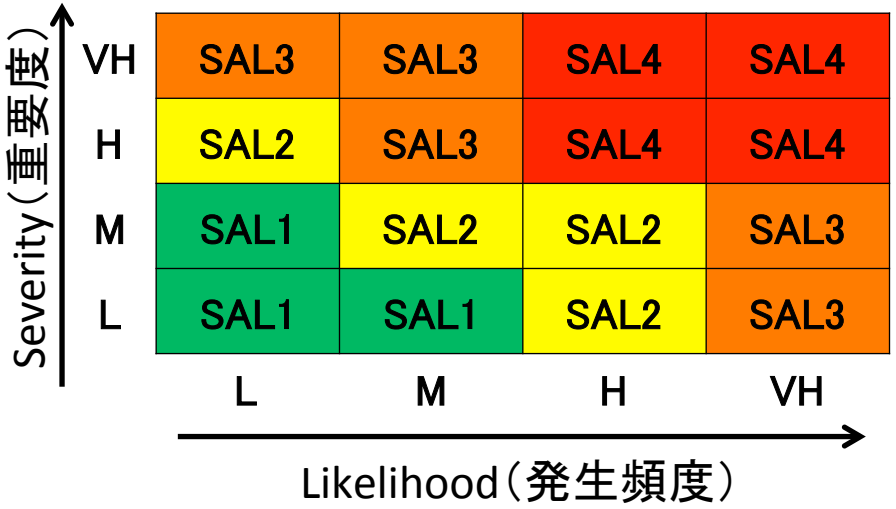
SL：セキュリティレベル1から4について

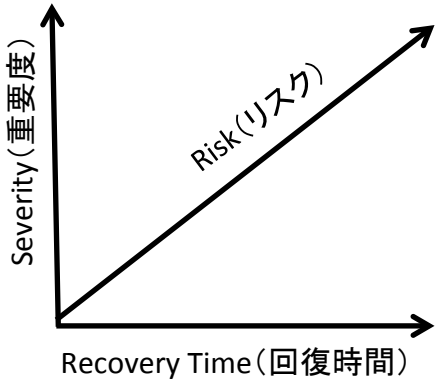


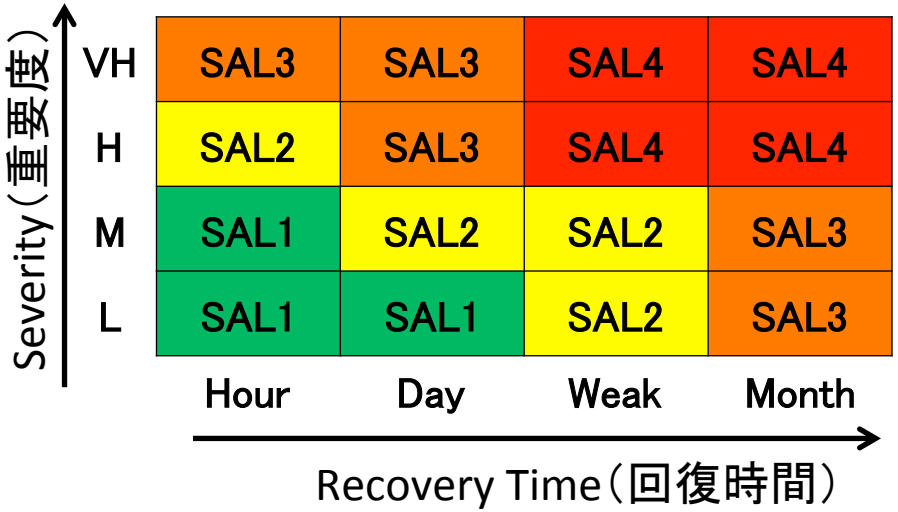
SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)					
SR 1.1 – Human user identification and authentication	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				✓

出典：IEC62443-3-3









本文は、IECよりご購入ください。 eICSジャーナルの「 IEC62443-3-3 解説」を必ずお読みください。対策技術はeICS講座で確認してください。

IEC62443-4-1 Example scope of product life-cycle & Defence in depth strategy is a key philosophy of the secure product life-cycle

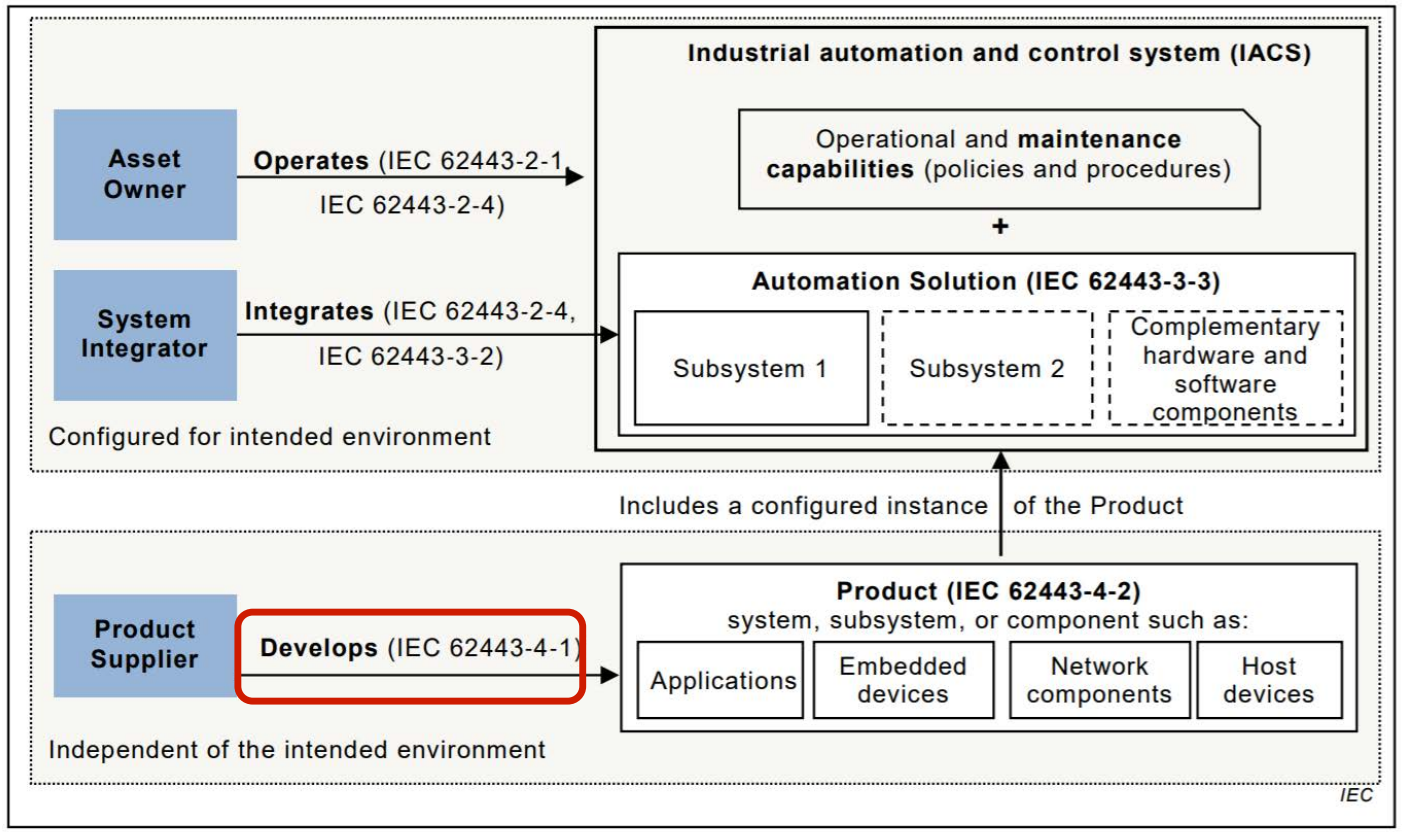


Figure 2 – Example scope of product life-cycle

出典:IEC62443-4-1

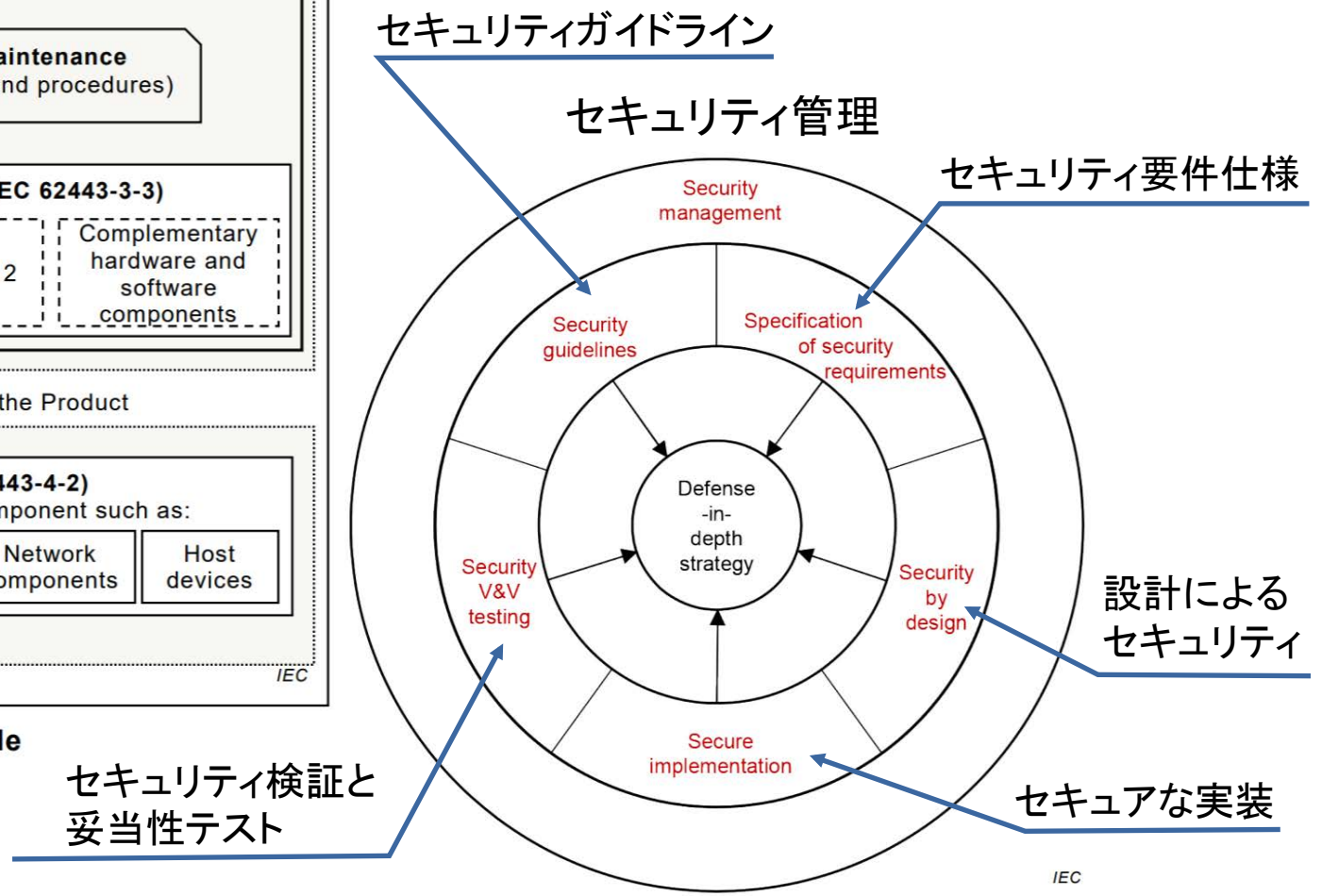


Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle

当日お話します。

CSMS認証とISA Secure認証

CSMS認証：Cyber Security Management System Certification

- IEC62443-2-1
- サイバー攻撃に対するリスクアセスメントを基準にしたセキュリティ管理能力の評価

SDLA認証：Security Development Lifecycle Assessment

V2.0：13 February 2018

- SDLPA：Security Development Lifecycle Process Assessment （セキュリティ開発ライフサイクルプロセス評価）
- SDA-S：Security Development Artifacts for System （システム設計品の開発評価）
- SDA-E：Security Development Artifacts for Embedded Devices （組み込みコンポーネント対象の開発評価）

SSA認証：System Security Assessment Certification

V2.1：13 February 2018

- System Security Assessment （システムセキュリティ評価）：SDLPA＋SDA-S
- FSA-S：Functional Security Assessment for System（システム対象の機能セキュリティ評価）
- FSA-E：Functional Security Assessment to Embedded Devices Components（組込みコンポーネント対象の機能セキュリティ評価）
- SRT: System Robustness Testing（システムロバストネス試験）

EDSA認証：Embedded Device Security Assurance Certification

V2.1：13 February 2018

- SDSA：Software Development Security Assessment（ソフトウェア開発セキュリティ評価）
- FSA：Functional Security Assessment（機能セキュリティ評価）
- VIT（Vulnerability Identification Testing ：脆弱性識別テスト）
- CRT：Communication Robustness Testing（通信ロバストネス試験）

これは、ISASecure プログラムが 制御システムセキュリティのための開発標準 ISA 62443 をサポートし、整合するための目標です。[EDSA100] ISASecure と ISA 62443 の間の関係について説明します。

EDSA-300

EDSA-300

ISA Security Compliance Institute - Embedded Device Security Assurance - ISASecure® certification requirements

Evaluation Elements for ISASecure EDSA Certification

- ERT（Embedded Device Robustness Testing）には、脆弱性識別テスト（VIT）と通信堅牢性テスト（CRT）という二つの主要な要素があります。VITは、既知の脆弱性の存在確認のためにデバイスをスキャンします。CRT は、正常なネットワークプロトコルトラフィックと、通常のトラフィック速度（flood conditions）の両方に対応しながら、デバイスが必要な機能を適切に維持する機能を検討しています。

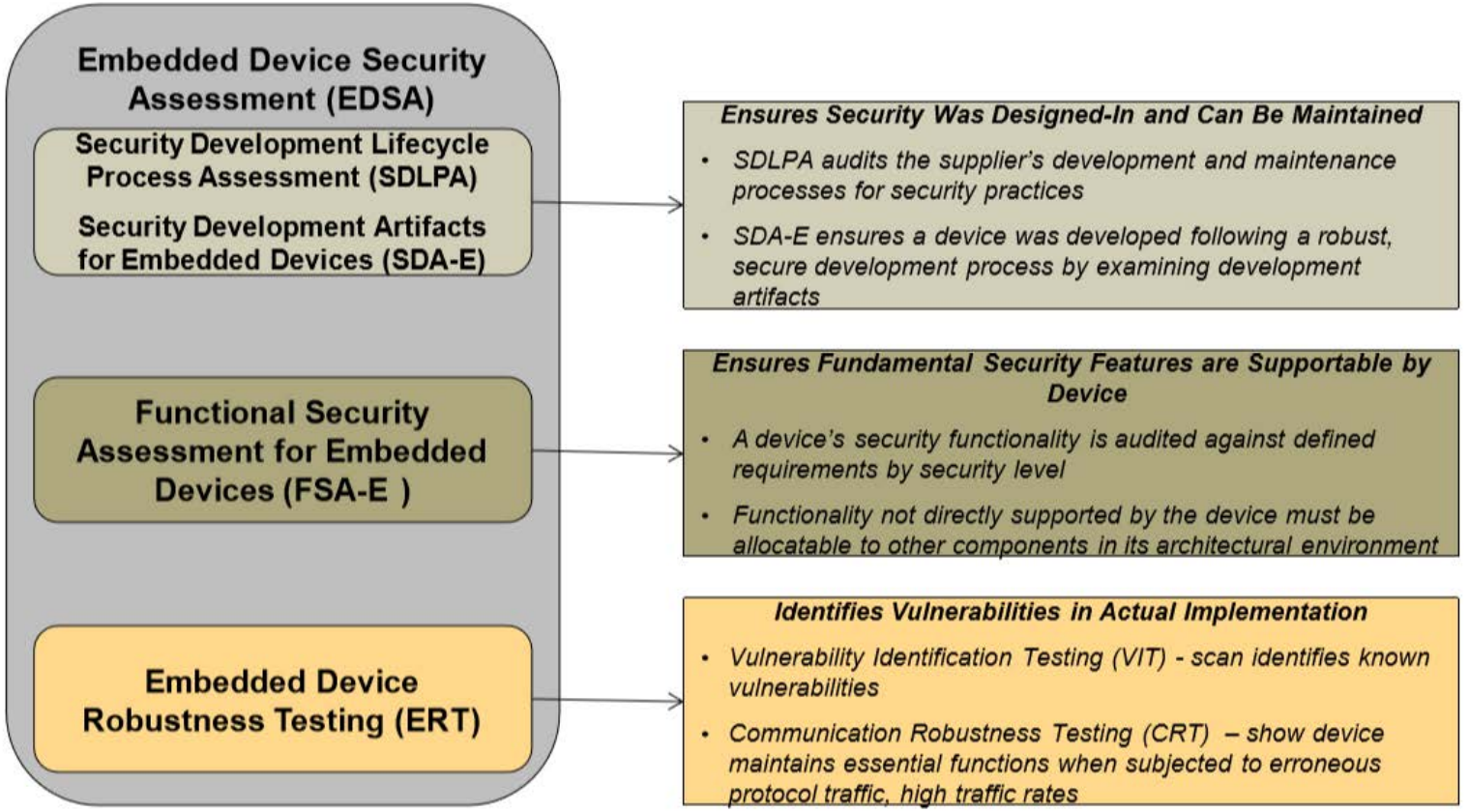


Figure 1 - Evaluation Elements for ISASecure EDSA Certification

出典：EDSA認証　EDSA 300　V3.2

VITの試験ツールはNessusです。
CRTの試験ツールはAchilles、Defensicsです。

Structure of EDSA Certification

- ·組込み機器用セキュリティ開発成果物（SDA-E);
- ·組込み機器のセキュリティ機能評価（FSA-E）
- ·組込みデバイスのRT（Robustness Testing：堅牢性テスト）
- EDSAV2.1ではRT（Robustness Testing）が、VIT（Vulnerability Identification Testing ：脆弱性識別テスト）とCRT（Communication Robustness Testing：通信堅牢性テスト）の二つになっています。

EDSA認証取得製品（ISASecure Certified Devices）：43製品（2019年5月現在）

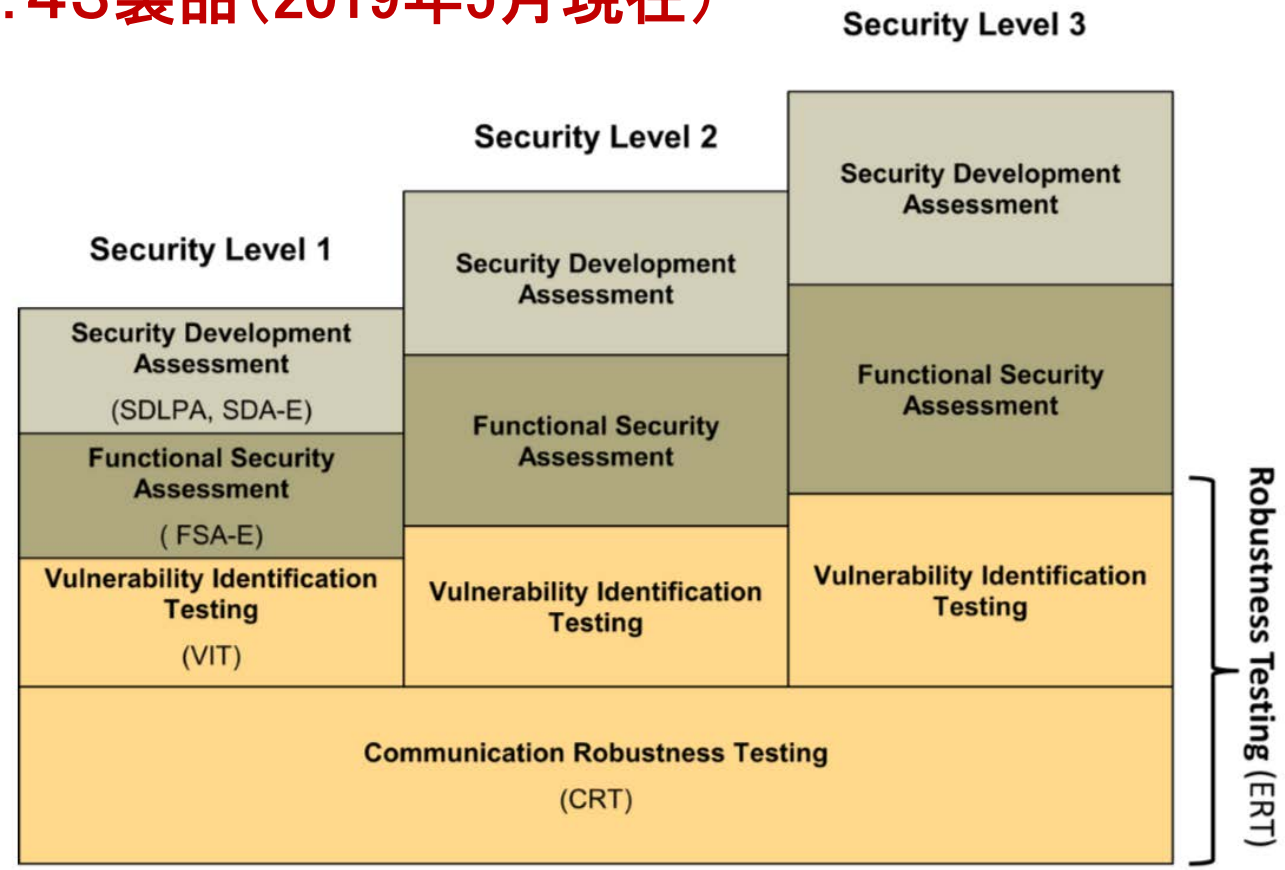


Figure 1 - Structure of EDSA Certification

VITの試験ツールはNessusです。

出典：EDSA-100 ISA Security Compliance Institute – Embedded Device Security Assurance – Version 3.3 February 2018

EDSA310

EDSA-310

ISA Security Compliance Institute - Embedded Device Security Assurance - Requirements for embedded device robustness testing

EDSA310

- IP ベースのプロトコルの組み込みデバイスの実装の堅牢性を調べ、既知の脆弱性について埋め込みデバイスをスキャンします。これらのトピックに対応した組み込みデバイスの堅牢性テスト（ERT）は、それぞれ、通信の信頼性テスト（CRT）と脆弱性識別テスト（VIT）と呼ばれます。

CRT：Communication Robustness Test Tool

Achillesの概要

- Achillesは、二種類の製品タイプを持ちます。
  - Achilles Test Platform
    - LANインターフェースを搭載した制御製品に対して、さまざまな不正トラフィックを与え、通信ロバスト性・通信断・フリーズなどの潜在的脆弱性の有無をテストする機能を有するBOXタイプのハードウェア製品
    - 決められたテスト項目を決められた手順で固定的に確認評価する仕様になっている。
  - Achilles Test Software
    - 汎用PCのVM workstation上にインストールして使用する柔軟性と可搬性に優れた低価格のソフトウェア製品
    - 制御製品開発時のセキュア性テストに向いている。

SSA-420

SSA-420

ISA Security Compliance Institute — System Security Assurance - Vulnerability Identification Testing Policy Specification

Vulnerability Identification Testing (VIT)の内容

- 当日お話します。

Tenable Network Security

Nessusは、次のタイプの脆弱性を検知するためのスキャンを行う

- クラッカーが遠隔でシステムの極秘データをコントロールするかアクセスすることを可能にする脆弱性
- 不良コンフィギュレーション（例えば、メールリレーやミッシングパッチなど）
- システムアカウント上のデフォルトのパスワードや共通のパスワード、ブランク/アブセントのパスワード、さらに辞書機能に攻撃するヒドラ（外部ツール）をコール
- 無効パケットの使用によるTCP/IPスタックのサービス妨害
- PCI DSS（Payment Card Industry Data Security Standard）監査の準備

EDSA311

EDSA-311

ISA Security Compliance Institute - Embedded Device Security Assurance - Functional Security Assessment (FSA)

EDSA311

Access Control

Reference ID and Name	*ISASecure*™ Level
Access Control	
└ FSA-AC-1 Access Control Authorization	NA
└ FSA-AC-1.1 Role Based Access	>1
└ FSA-AC-1.2 Dual Approval Access	>1
└ FSA-AC-1.3 Least Privilege Default Access	>1
└ FSA-AC-1.4 Administrator User Role	>1
└ FSA-AC-1.5 Administrator Support Functions	>2
└ FSA-AC-2 User Authentication	NA
└ FSA-AC-2.1 Authentication by User ID and Password	NA
└ FSA-AC-2.1.1 User Management of Password	All
└ FSA-AC-2.1.2 Monitor Unsuccessful Login Attempts	All
└ FSA-AC-2.1.3 Record Successful Logins	All
└ FSA-AC-2.1.4 Display Previous Login History	>2
└ FSA-AC-2.1.5 Password Modification Reminder	>2
└ FSA-AC-2.1.6 Password Strength Enforcement	>2
└ FSA-AC-2.1.7 Action for High Number of Unsuccessful Login	All
└ FSA-AC-2.1.8 Minimum Password Capability	All
└ FSA-AC-2.1.9 Clear Text Passwords	All
└ FSA-AC-2.1.10 Cryptographic Password Protection	>2
└ FSA-AC-2.1.11 Access Control for All Exposed Services	All
└ FSA-AC-2.2 Other Authentication Methods	Not required
└ FSA-AC-2.3 Two Factor Authentication (local network)	>2
└ FSA-AC-2.3 Two Factor Authentication (remote)	All
└ FSA-AC-2.5 Authentication Feedback	All
└ FSA-AC-3 System Use Notification	All
└ FSA-AC-4 Local Session Locking Timeout	>1
└ FSA-AC-5 Remote Session Termination Timeout	>1

Use Control

Reference ID and Name	*ISASecure*™ Level
Use Control	
└ FSA-UC-1 Wireless Access	NA
└ FSA-UC-1.1 Physical Disable Wireless Access	All
└ FSA-UC-2 Device Authentication	NA
└ FSA-UC-2.1 Failures in Cryptology Services	All
└ FSA-UC-2.2 Basic Device Authentication	>1
└ FSA-UC-2.3 Cryptographic Device Authentication	>2
└ FSA-UC-3 Creation of Audit Trail	NA
└ FSA-UC-3.1 Configuration of Audit Events	>2
└ FSA-UC-3.2 Content of Audit Record	NA
└ FSA-UC-3.2.1 Time Stamp for Audit	>1
└ FSA-UC-3.2.2 Information for Non-repudiation	>2
└ FSA-UC-3.2.3 Additional Content for Audit Record	>2
└ FSA-UC-3.3 Protection of Audit Information	NA
└ FSA-UC-3.3.1 Audit Fault Warning	>2
└ FSA-UC-3.3.2 Basic Protection of Audit Information	>1
└ FSA-UC-3.3.3 Crypto Protection of Audit Information	>2
└ FSA-UC-3.4 System Wide Audit	>2
└ FSA-UC-3.5 Audit Report Generation	>1

IEC62443との違いは、当日お話します。

出典：EDSA認証　EDSA311

EDSA311

Data Integrity

Reference ID and Name	*ISASecure*™ Level
Data Integrity	
└ FSA-DI-1 Integrity of Data in Transit	NA
└ FSA-DI-1.1 Insertion of Data Packets	>1
└ FSA-DI-1.2 Deletion of Data Packets	>1
└ FSA-DI-1.3 Excessive Delay of Data Packets	>1
└ FSA-DI-1.4 Re-sequencing or Replay of Data Packets	>1
└ FSA-DI-1.5 Basic Modification of Transmitted Data	>1
└ FSA-DI-1.6 Crypto Modification of Transmitted Data	>2
└ FSA-DI-1.7 Point to point Communications	NA
└ FSA-DI-1.7.1 Session Creation	>1
└ FSA-DI-1.7.2 Basic Session Protection	>1
└ FSA-DI-1.7.3 Crypto Session Protection	>2
└ FSA-DI-1.7.4 Session Closure	>2
└ FSA-DI-1.7.5 Session Timeout	>2
└ FSA-DI-1.8 Multicast / Broadcast Communications	NA
└ FSA-DI-1.8.1 Multicast Restrictions	>2
└ FSA-DI-1.8.2 Multicast Reception Protection	>2
└ FSA-DI-1.8.3 Multicast Transmission Restrictions	>2
└ FSA-DI-1.9 Verify Input Data Syntax	>1
└ FSA-DI-1.10 Handling Error Conditions	>1
└ FSA-DI-2 Integrity of Data at Rest Measures	>1
└ FSA-DI-2.1 Protection of Static Data	NA
└ FSA-DI-2.1.1 Disable Unused Ports	All
└ FSA-DI-2.1.2 Write Protection	>2
└ FSA-DI-2.2 Detection of Unauthorized Changes	NA
└ FSA-DI-2.2.1 Executable Code Basic Mod Protection	>1
└ FSA-DI-2.2.2 Executable Code Crypto Mod Protection	>2
└ FSA-DI-2.2.3 App Configuration Basic Protection	>1
└ FSA-DI-2.2.4 App Configuration Crypto Protection	>2
└ FSA-DI-2.2.5 Verify Application Specific Syntax	>1
└ FSA-DI-2.2.6 OS Basic Configuration Protection	>1
└ FSA-DI-2.2.7 OS Crypto Configuration Protection	>2
└ FSA-DI-2.2.8 Basic Executable Code Insert Protection	>1
└ FSA-DI-2.2.9 Crypto Executable Code Insert Protection	>2
└ FSA-DI-2.2.10 Non Execution of Data	>2
└ FSA-DI-3 Auto Verify Security Functions	>2

Data Confidentiality

Reference ID and Name	*ISASecure*™ Level
Data Confidentiality	
└ FSA-DC-1 Confidentiality of Data in Transit	NA
└ FSA-DC-1.1 No Clear Text in Data Transit	All
└ FSA-DC-1.1 Cryptographic Protection for Data Confidentiality	>1
└ FSA-DC-1.2 Cryptographic Key Management	>2
└ FSA-DC-2 Confidentiality of Data at Rest	NA
└ FSA-DC-2.1 Basic Confidentiality of Data at Rest	>1
└ FSA-DC-2.2 Crypto Confidentiality of Data at Rest	>2
└ FSA-DC-3 Cryptographic Mechanisms	>1

出典:EDSA認証　EDSA311

EDSA311

Restrict Data Flow

Timely Response to Event

Network Resource Availability

Reference ID and Name	*ISASecure*™ Level
Restrict Data Flow	
└— FSA-RDF-1 Information Flow Enforcement	All
└— FSA-RDF-2 Application Partitioning	>1
└— FSA-RDF-3 Security Function Isolation	>2
└— FSA-RDF-4 Shared System Resources	>2
Timely Response to Event	
└— FSA-TRE-1 Incident Response Support	>2
Network Resource Availability	
└— FSA-NRA-1 Denial of Service Protection	All
└— FSA-NRA-1.1 Data Flooding Protection	>2
└— FSA-NRA-1.2 Protocol Fuzzing Protection	All
└— FSA-NRA-1.3 Deterministic Loss of Comm	All
└— FSA-NRA-1.4 Notification of Attack	>1
└— FSA-NRA-1.5 Preservation of Essential Services	All
└— FSA-NRA-2 IACS Backup	All
└— FSA-NRA-3 IACS Recovery	All

出典：EDSA認証　EDSA311

EDSA312

EDSA-312

ISA Security Compliance Institute — Embedded Device Security Assurance – Security development artifacts for embedded devices

EDSA312

- 当日お話します。

産業界連携サプライチェーン

空港設備管理システム

国土交通省
「空港分野における情報セキュリティ確保に係る安全ガイドライン」　第1版

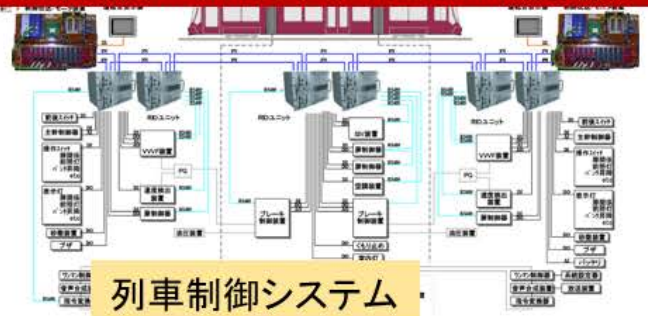
航空機製造工場

国土交通省
「航空運送事業者における情報セキュリティ確保に係る安全ガイドライン」第4版

航空機メンテナンス

列車・車両製造工場

国土交通省
鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第3版）



列車制御システム

米国国防省
調達品のサイバーセキュリティにNISTのSP800-171を指定

防衛兵器製造工場

工作機械製造工場
NC／CNC／ロボット

制御製品製造工場

コンピュータボード
製造工場

半導体製造工場

ClassNK Technical Information
Amendment to the ClassNK Rules and Guidance related to computer based systems

港湾安全監視システム

船舶製造工場

Guidelines on Cyber Security Onboard Ships Version 2.0
Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI

自動車製造工場

ACEA（欧州自動車工業会）
Principles of Autombile Cybersecurity

交通管制システム

ソフトウェアベンダ

National Highway Traffic Safety Administration
Cybersecurity For Modern Vehicles

SAE INTERNATIONAL米国自動車技術会(Society of Automotive Engineers)
“CYBERSECURITY GUIDEBOOK FOR CYBER-PHYSICAL VEHICLE SYSTEMS”

産業界連携サプライチェーン

製造した製品の安全

医薬品製造工場

医療品製造工場

FDA

医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律

薬事法

GAMP

バイオ医薬品製造工場

バリデーション
トレーサビリティ
コントロール・モニタ
プロダクション・ログ

装置・機械・ロボット製造工場
医薬製造装置、秤量器
打錠機、コーティング機械

制御製品製造工場

コンピュータボード
製造工場

食料品製造工場

食品衛生法

HACCIP

半導体製造工場

FDA：販売前申請における医療機器のサイバーセキュリティ管理に関するガイドライン：2016年12月28日
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff

DOD（国防総省）：STIG（Security Technical Implementation Guide）

精密医療機器製造工場

IEC 62304
Medical device software – Software life cycle processes
（医療機器ソフトウェア—ソフトウェアライフサイクルプロセス）

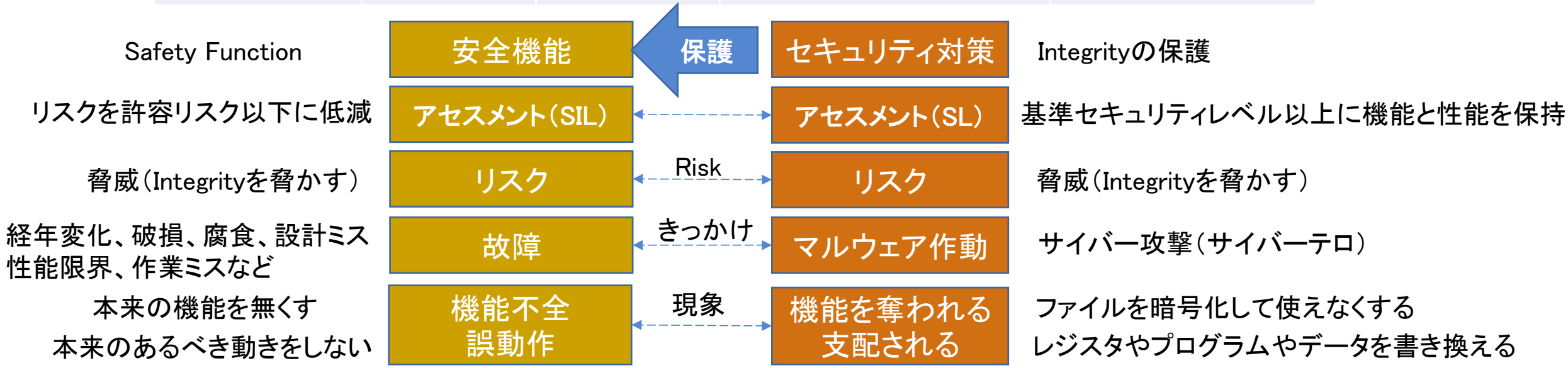
IEC 80001-1:2010
Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities
（医療機器を含むITネットワークへのリスク管理の提供）

ソフトウェアベンダ

厚生労働省
「医療機器におけるサイバーセキュリティの確保について」

機能安全／機械安全と制御セキュリティ

分野	機能安全	機械安全	安全・セキュリティ規格	セキュリティ規格
プロセス産業	IEC 61508		IEC TR 63069	IEC 62443
FA機械	ISO 13849 IEC 62061	ISO 12100	IEC TR 63074	IEC 62443
原子力	IEC 61513		IEC 62859	IEC 62645
自動車	ISO 26262		ISO 26262	J-3061
航空	DP-178C			DO 326A
鉄道	IEC 62278			IEC 62280



さあ、どうする？
いったい、自分に何が足らないのか？
これからの我が社に何が必要か？

当日までに考えてみてください。