制御システムセキュリティセンター　ISASecure SSA/SDLA/EDSA認証 説明会

ISASecure EDSA説明
「制御システム認証のアセスメントについて」

SSA 2.0.0（FSA-S/SDLPA/SDA-S）

2015年5月14日（東京）、5月22日（大阪）
技術研究組合制御システムセキュリティセンター

研究員　奥村 剛 (CISSP)

目次

- SSA認証とは
- FSA-S/SDLPA/SDA-Sの位置づけ
- ドキュメント体系
- SSA/SDLA/EDSA認証対象と範囲
- ベースシステムの構成
- FSA-Sの規格と要求事項の概要
- SDA-Sの規格と要求事項の概要
- SSA認証判定基準一覧
- SSA認証取得のメリット
- 付録: EDSA/SSA/SDLAの比較

SSA認証とは

- ISCI (ISA Security Compliance Institute) により策定された、制御システムの特定のサブセットのためのセキュリティ認証[SSA-300 1.2より]
- ISA/IEC-62443-3-3 (制御システムの構築事業者向けのセキュリティ国際標準)に準拠

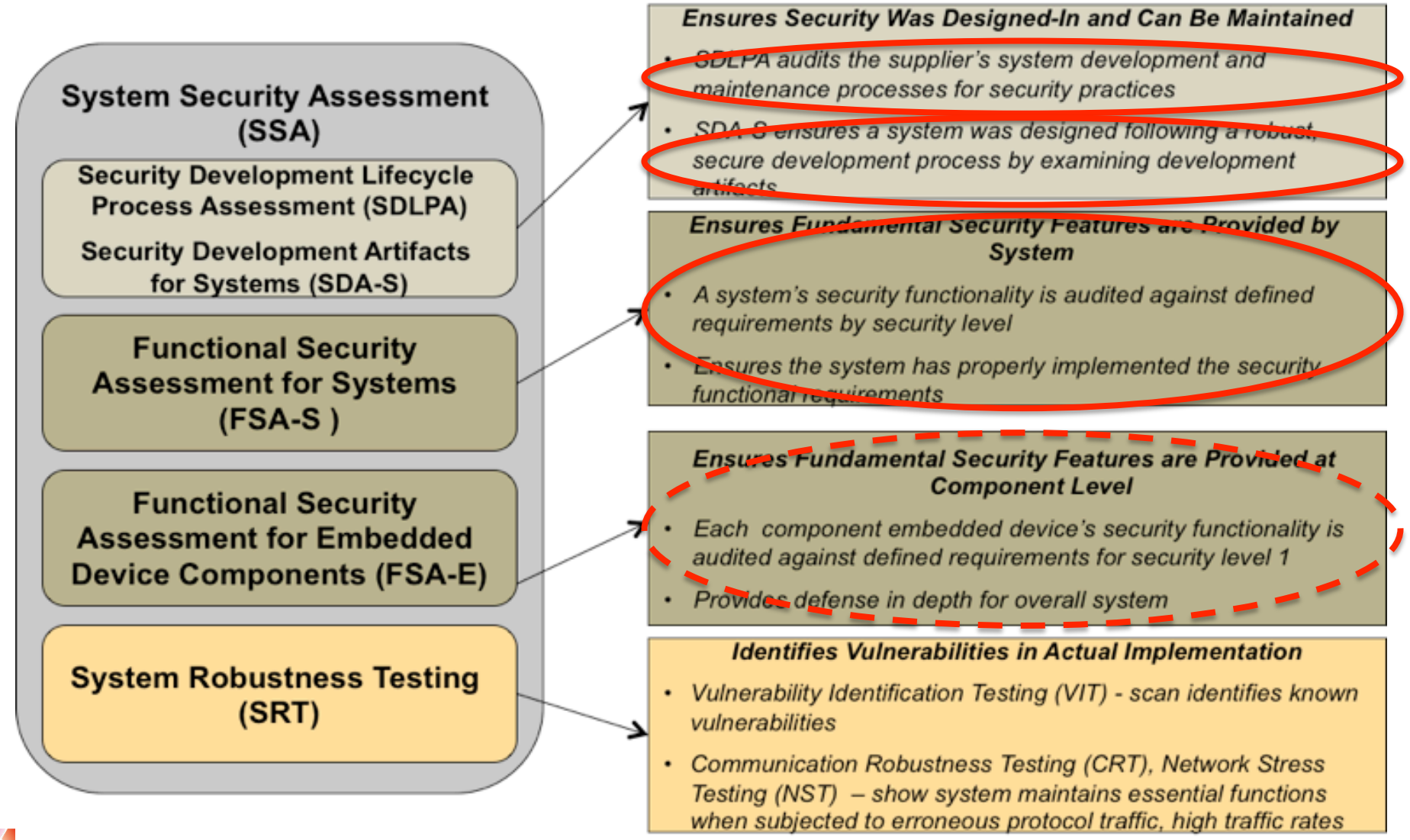
CSMS認証
（Cyber Security Management System）

SSA認証
（System Security Assurance）

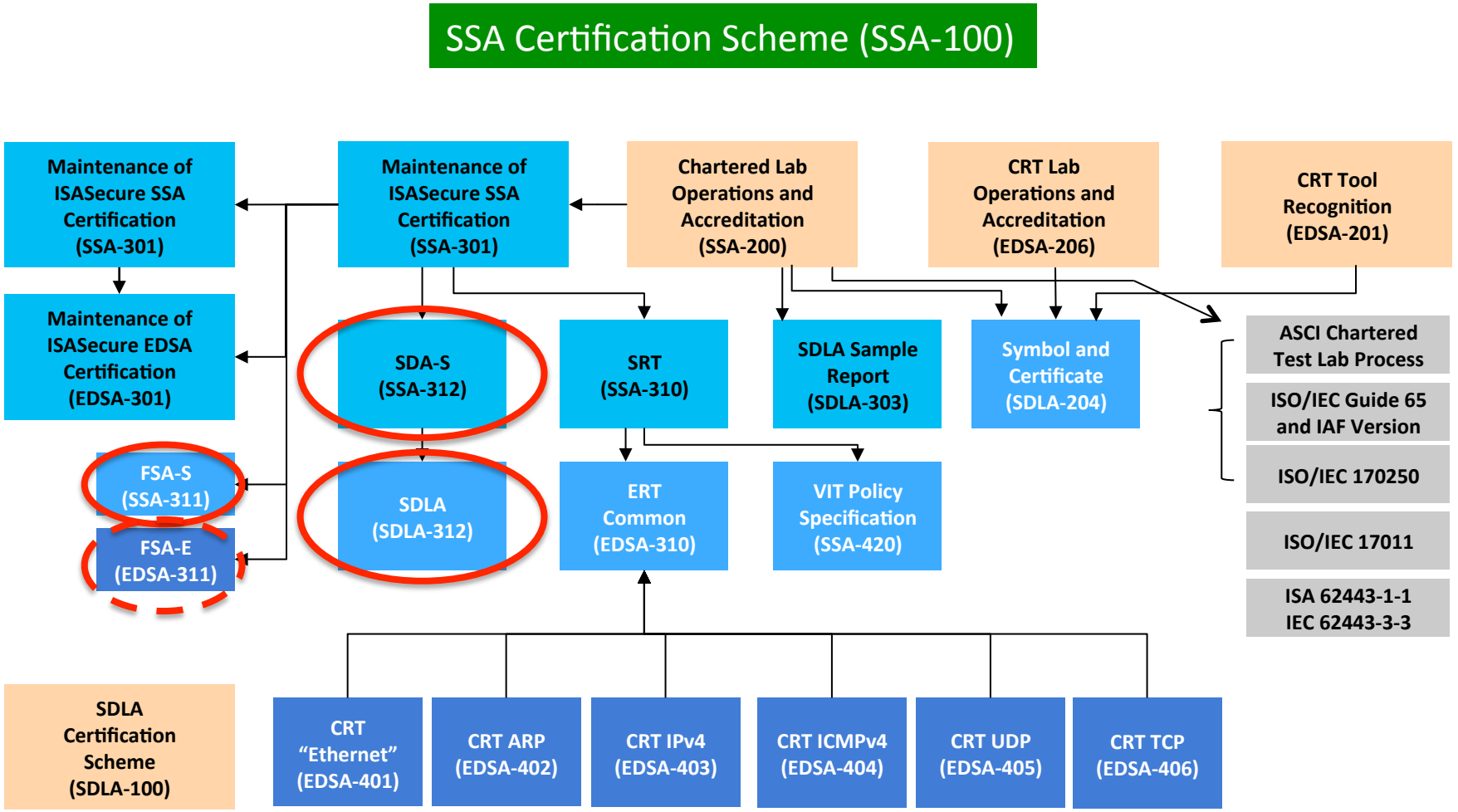
EDSA認証
（Embedded Device Security Assurance）

ISA Reference	IEC Reference	Title	Status
ISA-62443-1-1	IEC/TS 62443-1-1	Terminology, concepts and models	Published, Under Revision
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Under Development
ISA-62443-1-3	IEC 62443-1-3	System security compliance metrics	Under Development
ISA-62443-1-4	IEC/TR 62443-1-4	IACS security life cycle and use case	Proposed
ISA-62443-2-1	IEC 62443-2-1	IACS security management system – Requirements	Published, Under Revision
ISA-62443-2-2	IEC 62443-2-2	IACS security management system - Implementation guidance	Proposed
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch management in the IACS environment	Under Development
ISA-62443-2-4	IEC 62443-2-4	Requirements for IACS solution suppliers	Under development within IEC TC65 WG10
ISA-TR62443-3-1	IEC/TR 62443-3-1	Security technologies for IACS	Published
ISA-62443-3-2	IEC 62443-3-2	Security assurance levels for zones and conduits	Under Development
ISA-62443-3-3	IEC 62443-3-3	System security requirements and security assurance levels	Published
ISA-62443-4-1	IEC 62443-4-1	Product Development Requirements	Under Development
ISA-62443-4-2	IEC 62443-4-2	Technical security requirements for IACS components	Under Development

FSA-S/SDLPA/SDA-Sの位置づけ

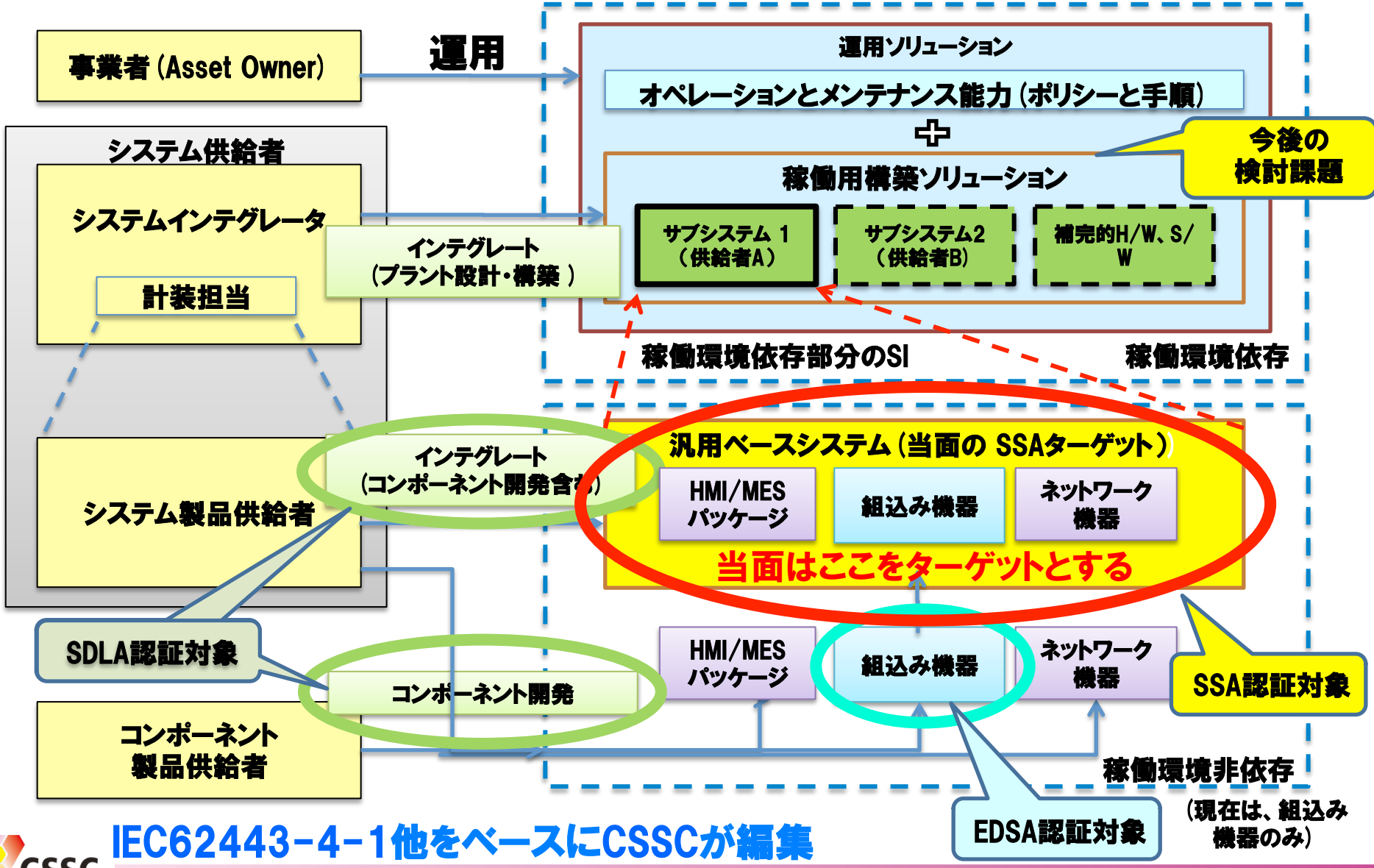


ドキュメント体系



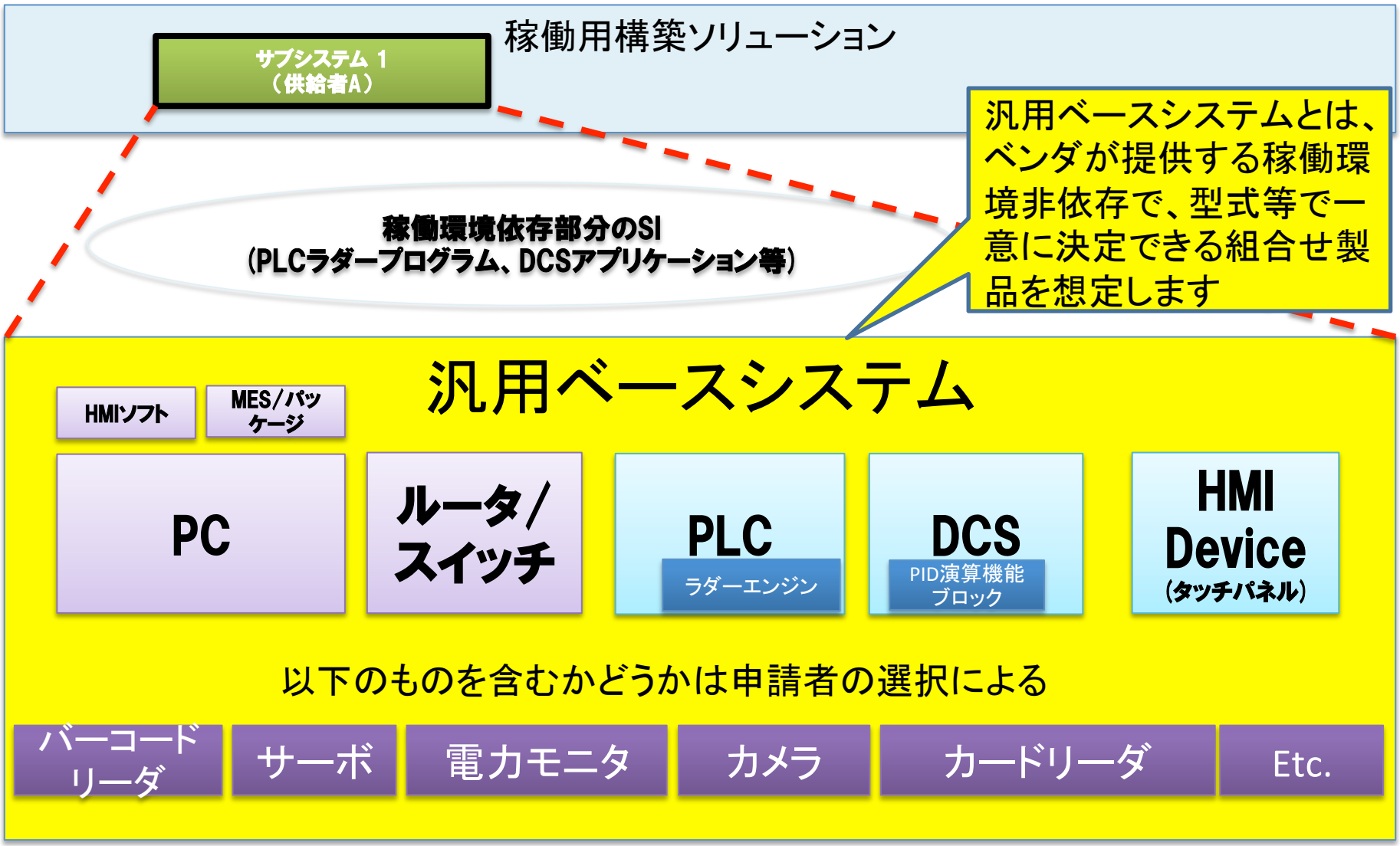
- SDAの要求事項は SDLAを利用している
- EDSA認証を取っていない機器は FSA-Eレベル1と同じ機能を持たなければならない

SSA/SDLA/EDSA認証対象と範囲



IEC62443-4-1他をベースにCSSCが編集

ベースシステムの構成


稼働用構築ソリューション
サブシステム 1
（供給者A）
稼働環境依存部分のSI
(PLCラダープログラム、DCSアプリケーション等)
汎用ベースシステムとは、ベンダが提供する稼働環境非依存で、型式等で一意に決定できる組合せ製品を想定します
汎用ベースシステム
HMIソフト
MES/パッケージ
PC
ルータ/スイッチ
PLC
ラダーエンジン
DCS
PID演算機能ブロック
HMI Device
(タッチパネル)
以下のものを含むかどうかは申請者の選択による
バーコードリーダ
サーボ
電力モニタ
カメラ
カードリーダ
Etc.

FSA-Sの規格と要求事項の概要

- SSA-311に規定された、下記内容に基づく
  - Identification & Authentication Control (識別及び認証制御)
  - Use Control (使用制限)
  - System Integrity (システム完全性)
  - Data Confidentiality (データ機密性)
  - Restricted Data Flow (制限されたデータフロー)
  - Timely Response to Event (事象への迅速な対応)
  - Resource Availability (リソース可用性)
- 対象システムの Zone毎に評価を行う
- 一部独立した試験(実システムによる試験)の実施も含まれる

SDA-Sの規格と要求事項の概要

- SSA-312に記載された要求事項(SDA-S.R1: SDA-Sの合格基準)により、実際には、SDLA-312の System に該当する要求事項について、評価を行う
- SDLA-312の要求事項は以下のとおり
  - Security Management Process (セキュリティ管理プロセス)
  - Security Requirement Specification (セキュリティ要求事項仕様)
  - Security Architecture Design (セキュリティアーキテクチャ設計)
  - Security Risk Assessment and Threat Modeling (セキュリティリスクマネジメントと脅威のモデル化)
  - Detailed Software Design (詳細ソフトウェア設計)
  - Document Security Guidelines (セキュリティ指針文書)
  - Module Implementation and Verification (モジュールの実装と検証)
  - Security Integration Testing (セキュリティ統合テスト)
  - Security Process Verification (セキュリティプロセス検証)
  - Security Response Planning (セキュリティ対応計画)
  - Security Validation Testing (セキュリティ妥当性検証テスト)
  - Security Response Execution (セキュリティ対応実行)

SSA認証判定基準一覧 [SSA-300 表1より]

トピック	要素	要求事項	参照文書
サプライヤによるセキュアな開発プロセス実施	SDLA	サプライヤは，当該システムのどのセキュリティゾーンに対しても規定された最高の能力セキュリティレベルと同等以上のSDLA認証レベルを有するISASecure SDLA認証を保有する。当該システムは，進行中の開発に対し，認証済プロセスの記載された適用範囲内である。 -又は- SDLAプロセス評価はSSA評価の一部として実施され，合格する。特に，当該システムのどのセキュリティゾーンに対しても規定された最高の能力セキュリティレベルと同等以上のSDLA認証レベルに適用可能な，すべてのSDLA基準が， 合格とアセスメントが実施される。検証基準は，[SDLA-312]内の「開発組織及びSDL検証活動」という題の欄内に列挙されている。	[SDLA-300] [SDLA-312]
セキュアな開発プロセスのシステムへの適用	SDA-S	システムは，SDA-S，セキュリティ開発アーティファクトのレビュー，に合格する。	[SSA-312]
システムのセキュリティ機能	FSA-S	各セキュリティゾーンに対する規定の能力セキュリティレベルへ適用可能なすべてのFSA-S基準は，そのゾーンに対してサポートされるか又は適用不可として，アセスメントされる。	[SSA-311]
システムの組込み機器コンポーネントのセキュリティ機能	FSA-E	システムの組込み機器コンポーネントに対して，レベル1に適用可能な，すべてのEDSA FSA基準は，SSA評価の一部として，サポートされるか若しくは割当可能として，アセスメントされるか，又は，組込み機器はISASecure EDSA認証を保有している(それは，この同じアセスメント結果がEDSA評価下で取得された) 割当可能とアセスメント実施された各組込み機器の要求事項は，評価中のシステムの展開時に，組込み機器がその要求事項を満たす方法で，他のシステムコンポーネントに，割当てられる。	[EDSA-311]
ネットワーク化環境内でのシステムロバストネス	SRT	システムはSRTに合格する。	[SSA-310]

SSA認証取得のメリット

- システム製品供給者
  - 自社が開発した製品(汎用ベースシステム)の認証を取得することにより、その製品の付加価値が上がる
  - SDLAも同時に取得することにより、個々の製品ではなく組織としてのセキュリティ対応力を証明できる
- システムインテグレータ
  - 自社が構築したシステム(プラントレベル)の認証を取得することにより、そのシステムの付加価値が上がる
  - SDLAも同時に取得することにより、個々のシステムではなく組織としてのセキュリティ対応力を証明できる
- 事業者のメリット(SSA取得済みシステム製品採用のメリット)
  - 自社で操業するシステムのセキュリティが高められる
  - ISMS取得のための地ならしができる

【参考1】EDSA/SSA/SDLAの比較

	EDSA	SSA	SDLA
認証対象	組込み機器	ベースシステム デザインソリューション	開発ライフサイクルプロセス
規格	EDSA-xxx (IEC 62443-4-1) (IEC 62443-4-2)	SSA-xxx (IEC 62443-3-1) (IEC 62443-3-2) (IEC 62443-3-3)	SDLA-xxx (IEC 62443-4-1)
想定される主な受審対象者	製品供給者	システム製品供給者(セットメーカー含む) システムインテグレータ	製品供給者 システム製品供給者(セットメーカー含む) システムインテグレータ
認証の範囲	組込み機器(型式とバージョンで指定)	システム(「システム名」、「構成機器の型式とバージョン」で指定)	組織(「組織名」と「開発ライフサイクルプロセス名」で指定)
認証の期限	無期限	無期限	期限あり(最大 36か月)

【参考1(続き)】EDSA/SSA/SDLAの比較

	EDSA		SSA	SDLA
評価内容	Ver.2010.1 (Ver.1)	Ver.2.0.0 (Ver.2)	SRT(ADT/CRT/NST/VIT) FSA-S SDA-S SDLPA(SDLA) (FSA-E)	SDLPA SDA-Eまたは SDA-S
	CRT FSA SDSA	ERT(CRT/VIT) FSA-E SDA-E SDLPA(SDLA)		
期待される効果の対象	組込み機器製品の付加価値		システム製品供給者(セットメーカ含む): システム製品や装置の付加価値 システムインテグレータ: セキュリティ対応力	組織のセキュリティ開発能力
認証の活用シーン(想定)	ベンダ: 他社製品との差別化 ユーザ: 製品調達要件		ベンダ: 機器の最小構成で取得実績 セットメーカ: 他社製品との差別化 ユーザ: システム調達要件	ベンダ: 実績 ユーザ: 製品/システム調達要件

【参考2】SSA 2.0.0 規格文書

FSA-S 規格文書（SSA-311）

原文（英語）：SSA-311 Functional Security Assessment for System

http://isasecure.org/en-US/Members/Download?PDF=SSA-311-Functional-security-assessment-for-systems

SDLPA, SDA-E 規格文書（SDLA-312）

原文（英語）：SDLA-312 Security Development Lifecycle Assessment

http://www.isasecure.org/Certification/Download-Request?PDF=SDLA-312-Sec-Dev-Lifecycle-Assess(v3_0)-(1)

ご清聴ありがとうございました。

セキュアな制御システムを世界へ未来へ

CSSCホームページ
http://www.css-center.or.jp/

CSSC説明ビデオ（日本語版）
http://www.youtube.com/watch?v=wbEiDQZU5sI&feature=youtu.be