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 SSA説明
「制御システム認証のテスティングについて」

SSA 2.0.0（SRT）

2015年5月14日（東京）、5月22日（大阪）

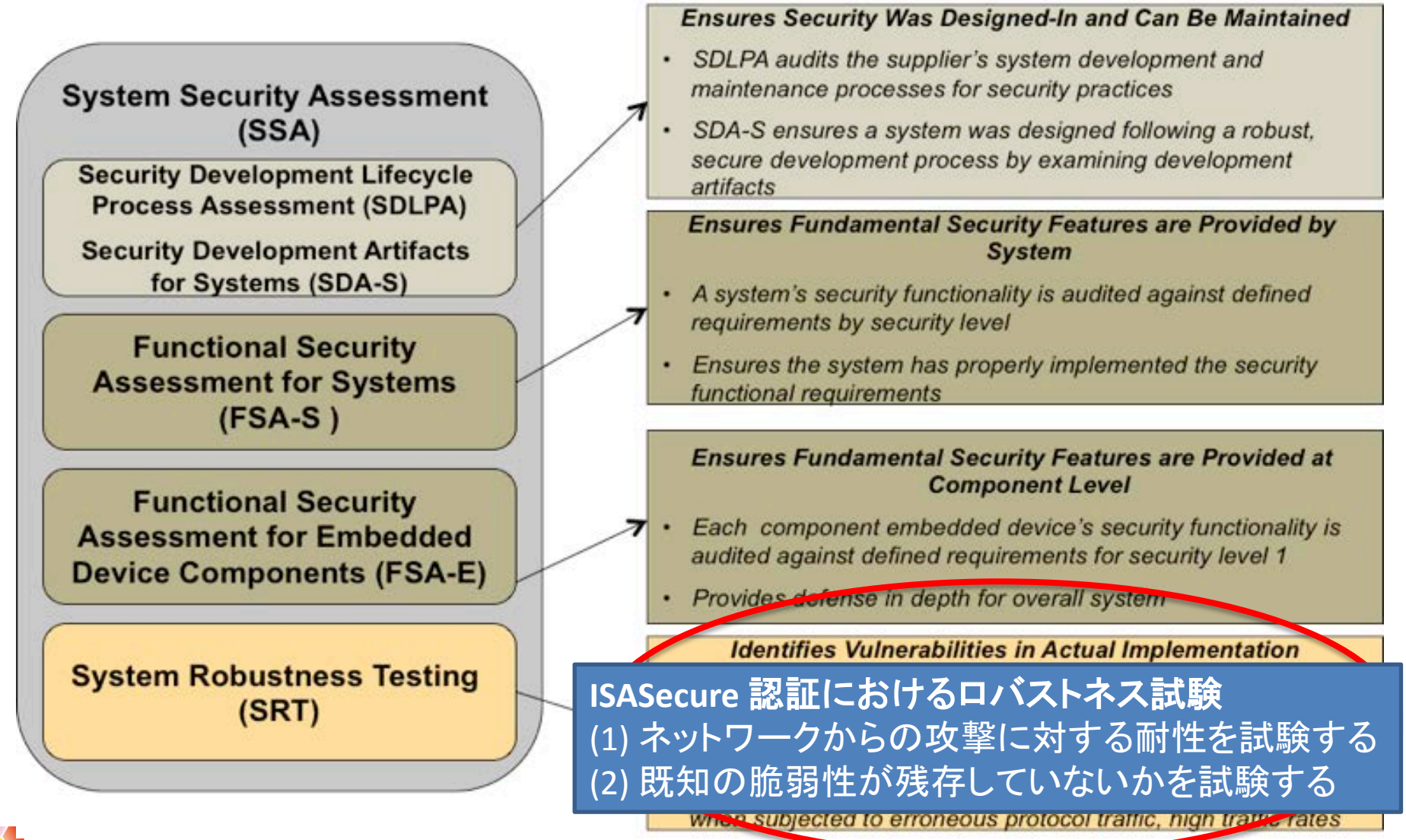
技術研究組合制御システムセキュリティセンター

研究員　田中　貴志

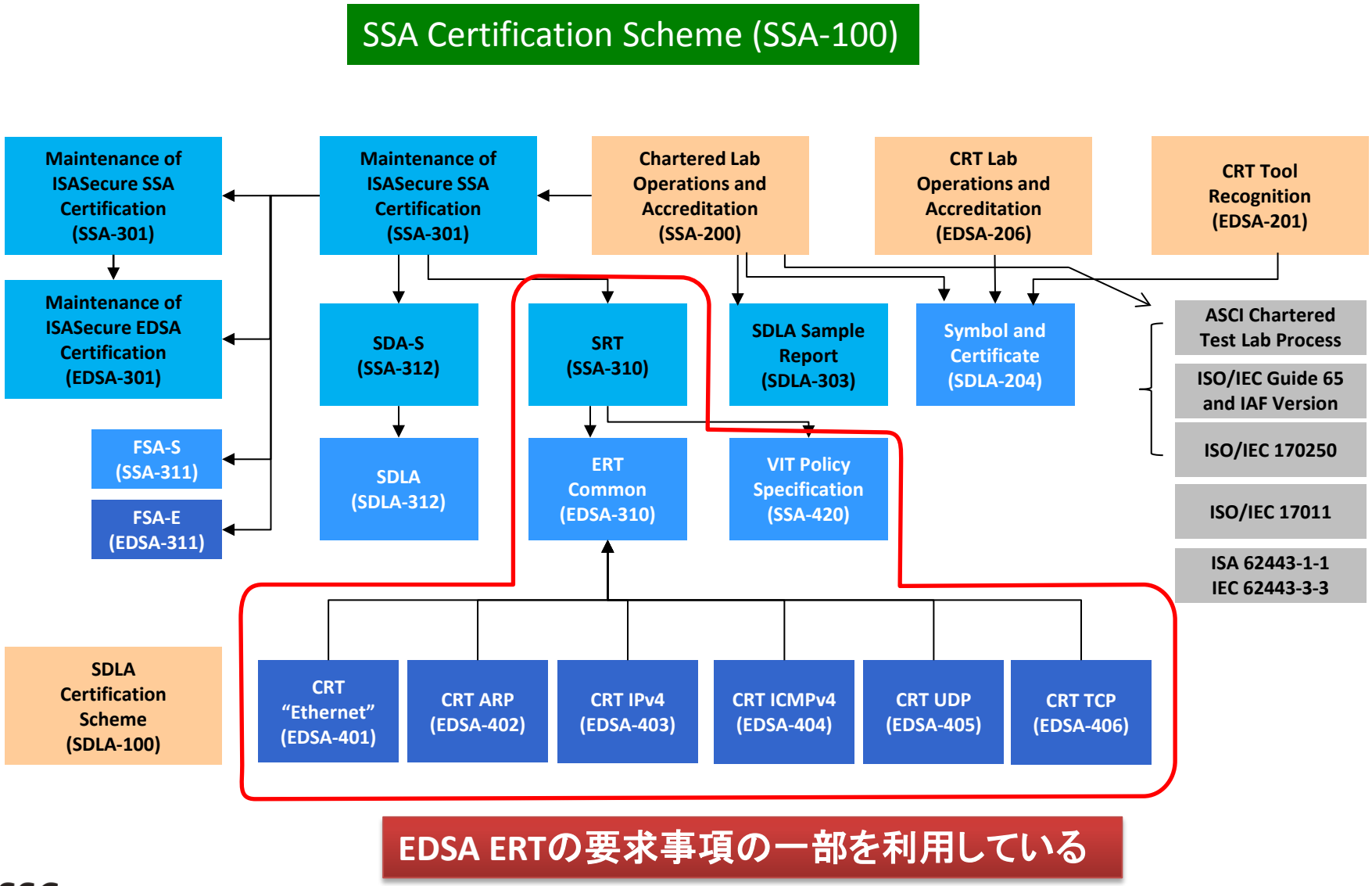
目次

1．SRT試験の位置づけ

SRT試験の位置づけ：SSA認証とSRT



SSA 認証プログラム　ドキュメント体系とSRT



基本的な合否判定

■ＳＲＴの合格条件

システムにとってのEssential Function（必須機能）を定義し、想定されるネットワーク経由の攻撃を受けてもそれを**維持できる**こと

Essential Function（必須機能）の分類

1. 制御機能 (The control function)
2. 安全計装機能 (The safety instrumented function)
3. プロセスビュー (Process view)
4. プロセスコマンド (Process command)
5. プロセスアラーム (Process alarm)
6. プロセス履歴 (Process history)
7. 外部通信 (External communications)
8. 任意の必須機能 (Any additional essential functions)

申請者の準備

- SUTの持つEssential Function は何かを定義する
- Essential Function が、**適切に維持されているとはどういう状態か**を定義する

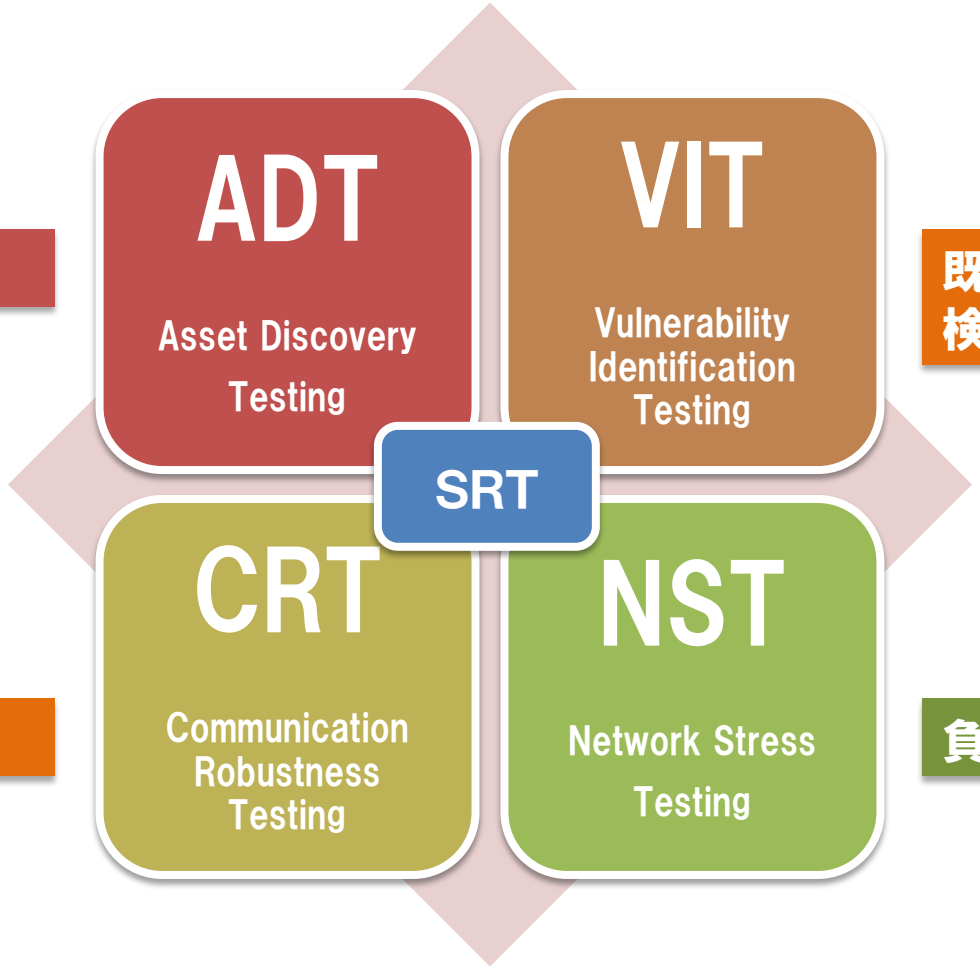
１～５は、該当する機能がある場合は、評価対象とする
６～８は、申請者が必要だと考えていれば、試験対象に追加することができる

2. 試験の概要

試験の概要：4種の試験カテゴリ

- ４つのカテゴリで試験を実施
- 全てのカテゴリで合格するとＳＲＴに合格

利用ポートの特定

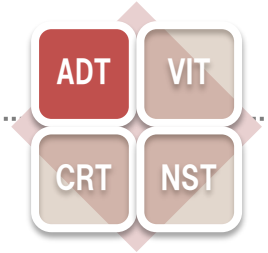


既知の脆弱性の残存を検査

ファジング試験

負荷試験

試験の概要：SSA-ADT (Asset Discovery Testing)



■試験内容

ポートスキャン、IPプロトコルスキャンをおこなう。

CSSC-CLでは、Nmapを用いて、ポートスキャンを実施する。
(Nmap：http://www.nmap.org/)

■試験対象

SUT中のコンポーネントが持つ、全てのIPアドレスに対して実施する

■合否判定

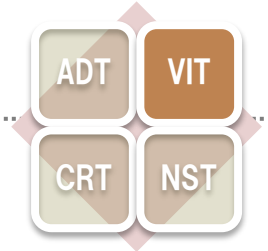
●開きポートが設計通りであること

●スキャン中に必須機能が維持できていること

■注意事項

すべてのモード、インタフェースに対して試験を実施する

試験の概要：SSA-VIT (Vulnerability Identification Testing)



■試験内容

既知の脆弱性がSUTに残っていないかを脆弱性スキャンツール (Nessus) を用いて検査する

(Nessus http://www.tenable.com/products/nessus-vulnerability-scanner)

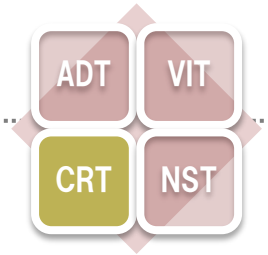
■試験対象

SUT中のコンポーネントが持つ、全てのIPアドレスに対して実施する。

■合否判定

- 必須機能が維持できていること
- Highリスクの脆弱性がないこと
- 対応策のないMediumリスクの脆弱性がないこと
- FSA-E の要求事項に違反するLowリスクの脆弱性がないこと

試験の概要：SSA-CRT (Communication Robustness Testing)



■試験内容

ネットワークからの攻撃に耐性のあることをISCI承認ツールを用いて評価する
EDSA ERT試験のうち、Basic Robustness Test 相当の試験を実施する

■試験対象

1. 全てのアクセス可能なインタフェース
   ただし、EDSA認証を取得しているEmbedded Device は、除く。
2. SUTの外部からアクセス可能なインタフェース。
   ただし、外部と接続しているFirewallの外側のI/Fは除く。

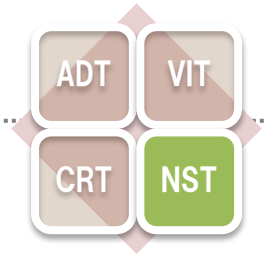
■合否判定

●必須機能が維持できていること

■注意事項

制御機能が動作する全てのモードで試験する

試験の概要：SSA-NST (Network Stress Testing)



■試験内容

ネットワークの負荷（攻撃）に耐性のあることをISCI承認ツールを用いて評価する
EDSA ERT試験のうち、Load Stress Testing 相当の試験を実施する

■試験対象

すべてのアクセス可能なインタフェース
ただし、外部と接続しているFirewallのインタフェースは除く

■合否判定

●必須機能が維持できていること

■注意事項

すべてのネットワーク機器が対象となる

EDSA 2.0.0 ERT と SSA SRT

	EDSA-ERT	SSA-SRT			
	Embedded Device	Embedded Device	Component ※1	Component (Visible) ※2	External Firewall ※3
SSA-ADT (Interface Surface Test)	✔	✔	✔	✔	✔
SSA-CRT (Basic Robustness Test)	✔	✔		✔	
SSA-NST (Load Stress Test)	✔	✔	✔	✔	
VIT	✔	✔	✔	✔	✔

- 個々の試験の内容は、EDSA ERTで実施する試験内容と同一
- 合否判定条件が異なる

※1 Component: Embedded Device 以外のアクセス可能なネットワークインタフェースを持つ機器
※2 Component (Visible) : コンポーネントのうちSUTの外部からアクセス可能なネットワークインタフェースを持つ機器（Firewall経由等を含む）
※3 External Firewall : SUT の外部と接続されたFirewall

3. 試験にむけて

試験とその準備

SUTの定義

- 試験対象システム構成の決定
- Essential Function とその「維持」を定義

必須機能の維持を確認するための環境を含むこと

SUT情報の提出

- 構成物一覧
- システム構成図
- ネットワーク構成・設定の説明

試験の実施

- ADT
- CRT/NST
- VIT → VITで脆弱性が発見された場合の対策の提出

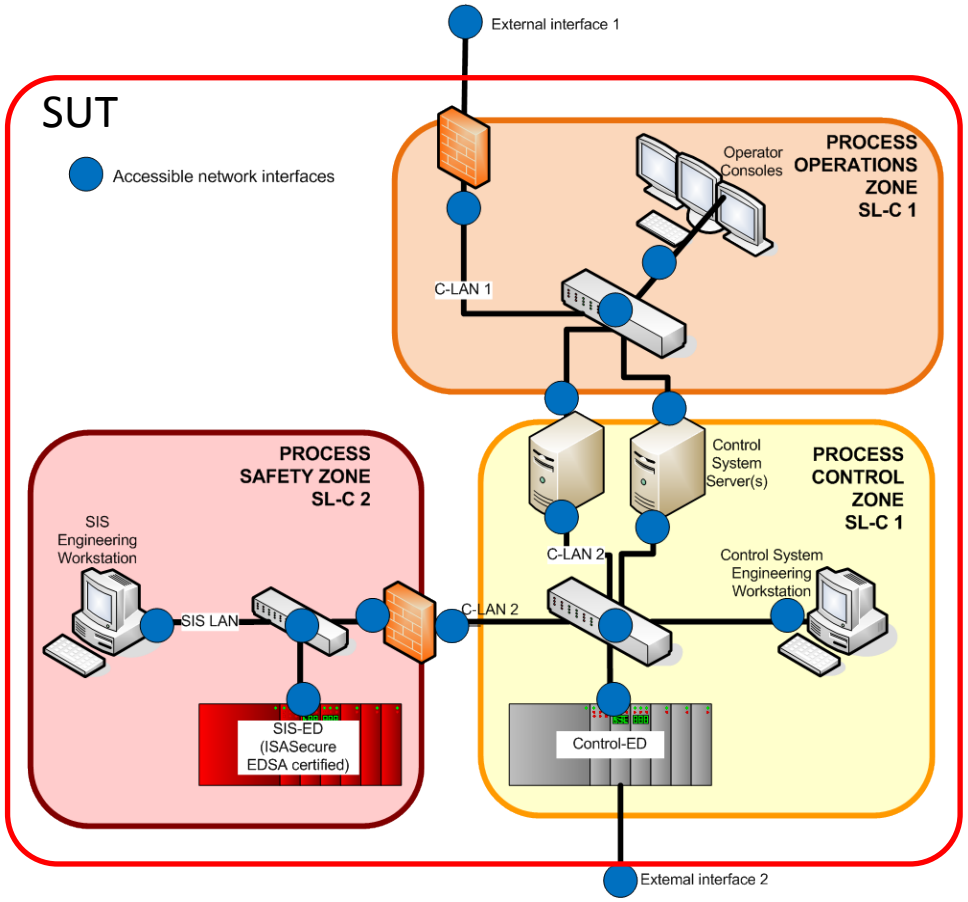
申請者の立ち合いの元、試験を実施

レポートの発行

- 申請者の申告内容にもとづく試験条件と試験結果を報告書にまとめる

試験対象の定義

SSA-301 で例示されているSUTの例



Keywords:

- SUT
- Zone
- Bill of Materials
  - Embedded devices
  - Hosts
  - Application
  - Network components
- Network Interfaces
  - External Interface
  - Accessible Network Interface
    - Internal access
    - Visible from External Interface

試験対象の定義：Example SUTの部品表

Process Operations Zone

Device	Manufacturer	Model Number	Software/Firmware	Version(s)
POZ Firewall	ABC	123	Firmware	V3.5.12345
Operator Consoles	XYZ	W321	Windows 7	SP2
			HMI Client Software	V5.6.213
			Java	Version 7.51
			Name of antivirus solution 1	3.6
C-LAN 1 Switch	ABC	1121	Firmware	V1.2

Process Control Zone

Device	Manufacturer	Model Number	Software/Firmware	Version(s)
Control System Servers	XYZ	S321	Windows Server 2008	SP2
			HMI Server Software	V5.6.210
			...	
Control System Engineering Workstation	XYZ	W321	Windows 7	SP2
			Engineering Software	V5.6.250
			...	
C-LAN 2 Switch	ABC	1121	Firmware	V1.2
Control-ED	AAA	A11	Firmware	V5.1.231

Process Safety Zone

Device	Manufacturer	Model Number	Software/Firmware	Version(s)
SIS Firewall	ABC	123	Firmware	V3.5.12345
SIS LAN Switch	ABC	1121	Firmware	V1.2
SIS-ED	AAA	S11	Firmware	V5.1.231
SIS Engineering Workstation	XYZ	W321	Windows 7	SP2
			Engineering Software	V5.6.250

Essential Function とその「維持」を定義

Essential Function（必須機能）の申請

1. 制御機能 (The control function)
2. 安全計装機能 (The safety instrumented function)
3. プロセスビュー (Process view)
4. プロセスコマンド (Process command)
5. プロセスアラーム (Process alarm)
6. プロセス履歴 (Process history)
7. 外部通信 (External communications)
8. 任意の必須機能 (Any additional essential functions)

- １～５の機能は、該当機能の有無を申請
  （該当機能が存在すれば評価対象となる）
- ６～８の機能は、申請者の申請により、試験対象に追加することができる

Essential Functionの定義

大きく2つに分類される

–概念は、EDSA のEssential Functionと同じ

■Downward Essential Function

Embedded Device のうち、制御機能を持つデバイスが対象
規定の信号を出力する機能を試験用に用意する(EDSAと同一）

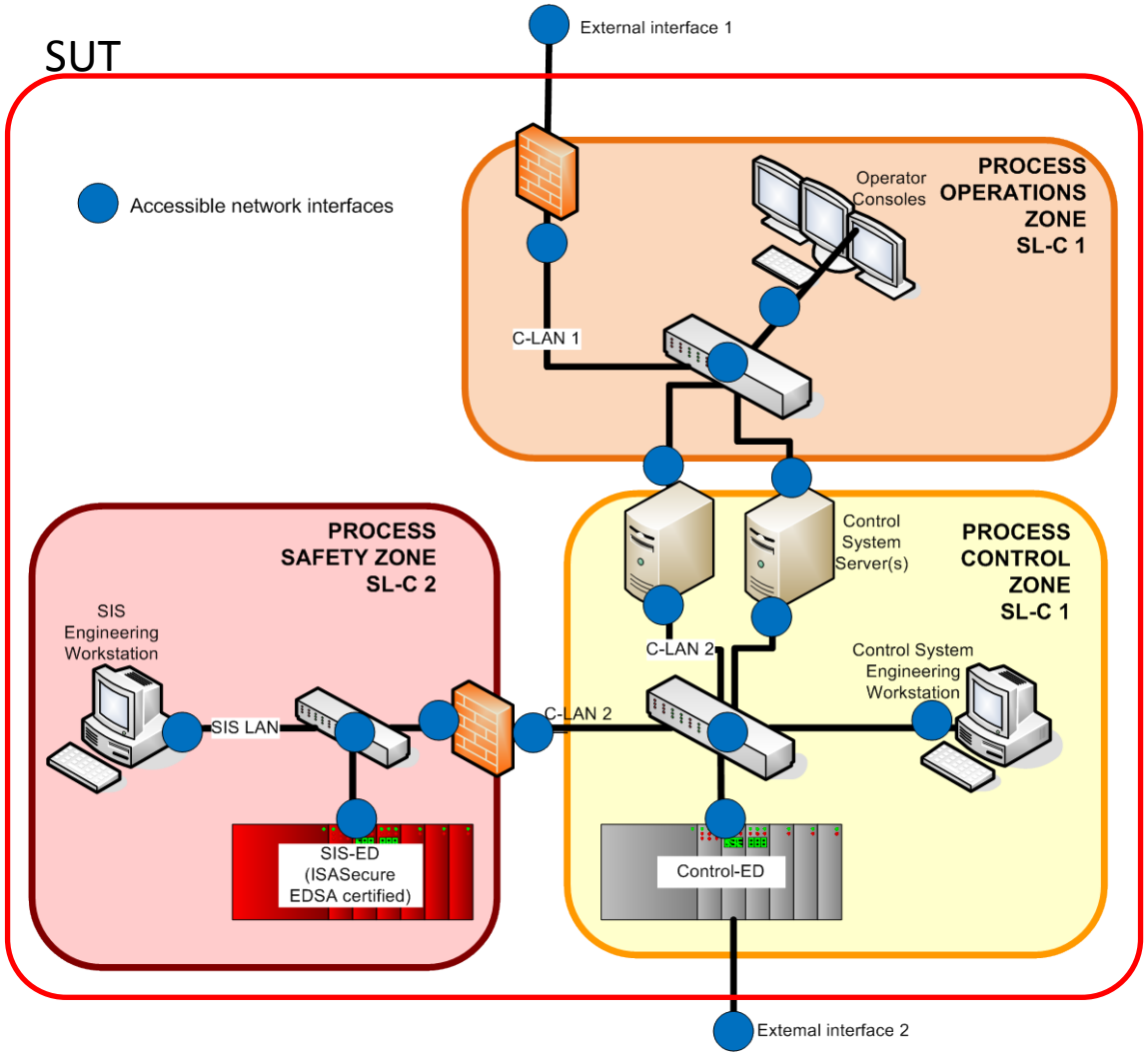
■Upward Essential Function

- EDSA の場合は、Embedded Device を中心に定義される機能であるが、SSAでは、**システムとして**該当する機能を定義する必要がある。
- それぞれのEssential Functionに関して、一部について具体的な要求がある

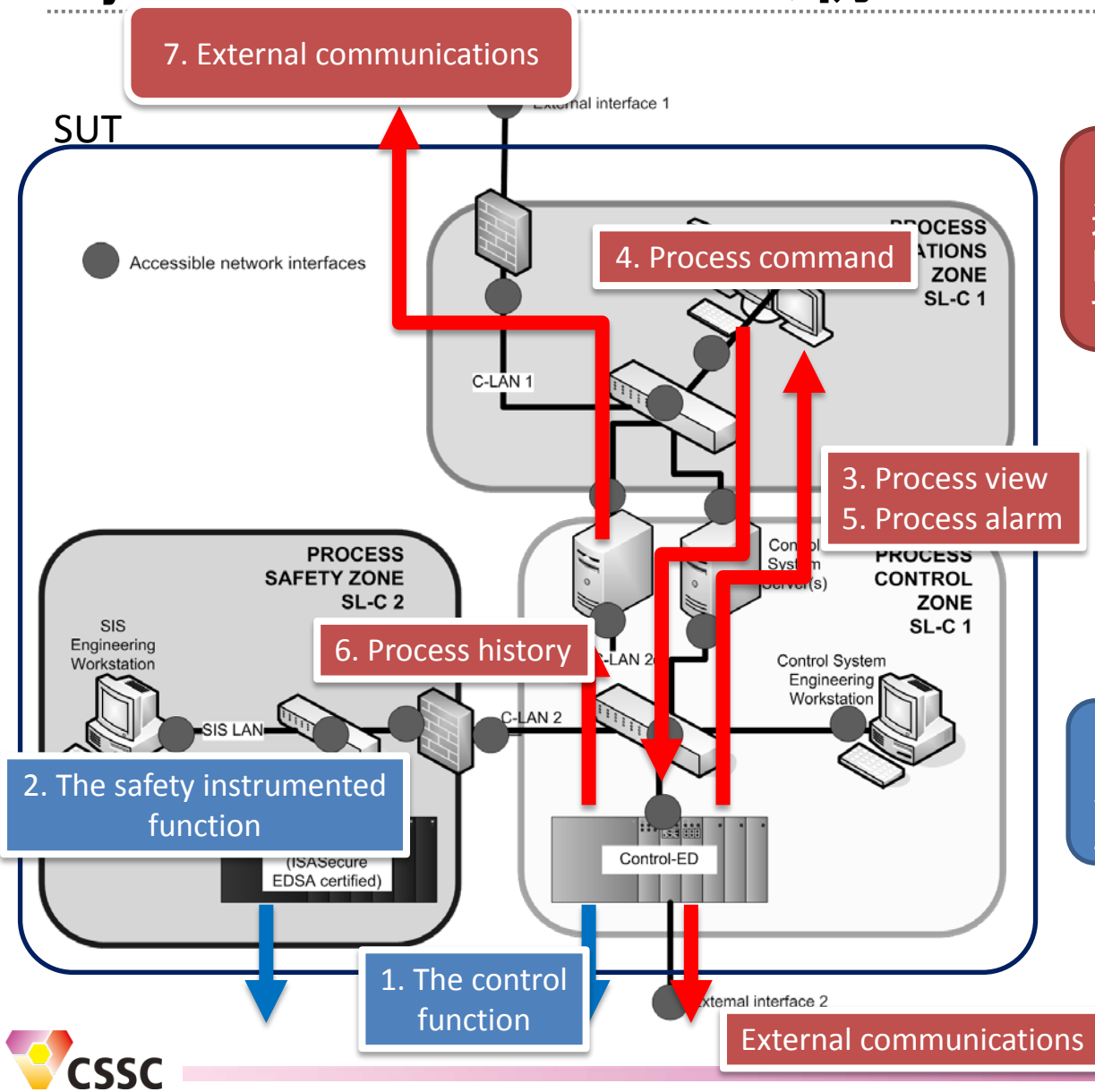
例:

- 適切に:時間軸で定義
- サービスが中断してもよい条件
- 中断後の復帰条件

System Essential Function の例



System Essential Function の例



■Upward Essential Function
通信経路も重要
同一Essential Function が複数存在する場合は、全てが試験対象

■Downward Essential Function
規定の信号を出力する機能を試験用に組み込む

4. まとめ

4. まとめ

- 内容
  - SRT試験の位置づけ
  - 試験の概要
  - 試験に向けて
    - 試験対象システム構成の決定
    - Essential Function（必須機能）の理解

- 対象システムのEssential Functionとその維持の監視がキーポイント
- 基本的に試験の中身は、EDSA ERTと同一。ただし、どのインタフェースに、どの試験を実施するかを試験機関と検討するが必要ある

【参考1】SSA 2.0.0 規格文書

SRT 規格文書（SSA-310）

原文（英語）：SSA-310 Requirements for System Robustness Testing (SRT)

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dSSA-310-System-robustness-test-spec(v2_0))

VIT 規格文書（SSA-420）

原文（英語）：SSA-420 Vulnerability Identification Test (VIT) Policy Specification

http://www.isasecure.org/Members?returnurl=%2fen-US%2fMembers%2fDownload%3fPDF%3dSSA-420-Vulnerability-Identification-Test-Policy-S

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

技術研究組合
制御システムセキュリティセンター
Control System Security Center

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