CSSC認証ラボラトリー　ISASecure EDSA認証 説明会

ISASecure EDSA CRT説明

2014年1月15日

CSSC認証ラボラトリー 評価員
田中　貴志

目　次・・・ ISASecure EDSAのCRT説明

1. CRT試験とは
2. CRT試験の内容
3. CRT試験の準備
4. まとめ

1．CRT試験とは ･･･ CRT試験の位置づけ

ISASecure

◆SDSA、FSA、CRTの3つを評価することで、想定脅威に対する対策のカバー範囲が十分であることを認証

EDSA

ソフトウェア開発セキュリティ評価（SDSA）

体系的な設計不良の検出と回避

- ベンダのソフトウェア開発とメンテナンスのプロセス監査
- 堅牢（robust）で,セキュアなソフトウェア開発プロセスを当該組織が守っていることを評価する。

※3段階のセキュリティレベルにより評価項目数が決まる

機能セキュリティ評価（FSA）

実装エラー / 実装漏れの検出

- セキュリティ機能要件について、目標とするセキュリティレベルに対応する全要件が実装済みであるかどうかを評価

※3段階のセキュリティレベルにより評価項目数が決まる

通信ロバストネス試験（CRT）

デバイスの堅牢性を評価する試験

- コンポーネントのロバストネス（堅牢性）について試験
- 奇形や無効な形式のメッセージを送り、脆弱性等を分析

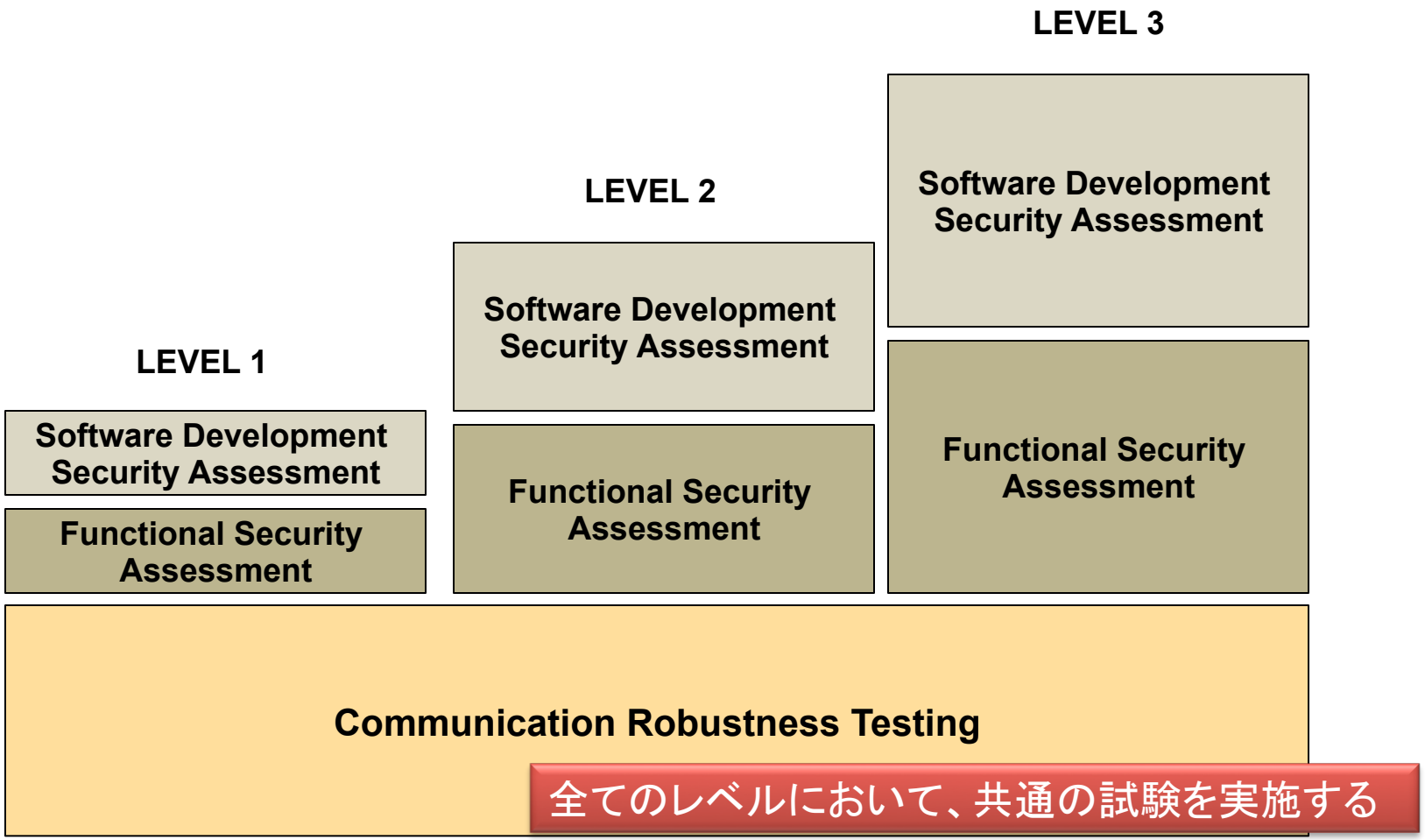
※セキュリティレベルによらず、評価項目数は同一

EDSA：Embedded Device Security Assurance

Communication Robustness Testing(CRT), Functional Security Assessment (FSA), Software Development Security Assessment(SDSA)

出典:「ISA Security Compliance Institute （ISCI） and ISASecure™及びhttp://www.css-center.or.jp/sympo/2013/documents/sympo20130528-article.pdf

1．CRT試験とは ・・・ ISASecureレベルとCRT試験



出典：ICSJWG Spring 2011, (ASCI)
「Validating the Security Assurance of Industrial Automation Products」

1．CRT試験とは ・・・ 試験の目的と要件

■ CRT試験とは

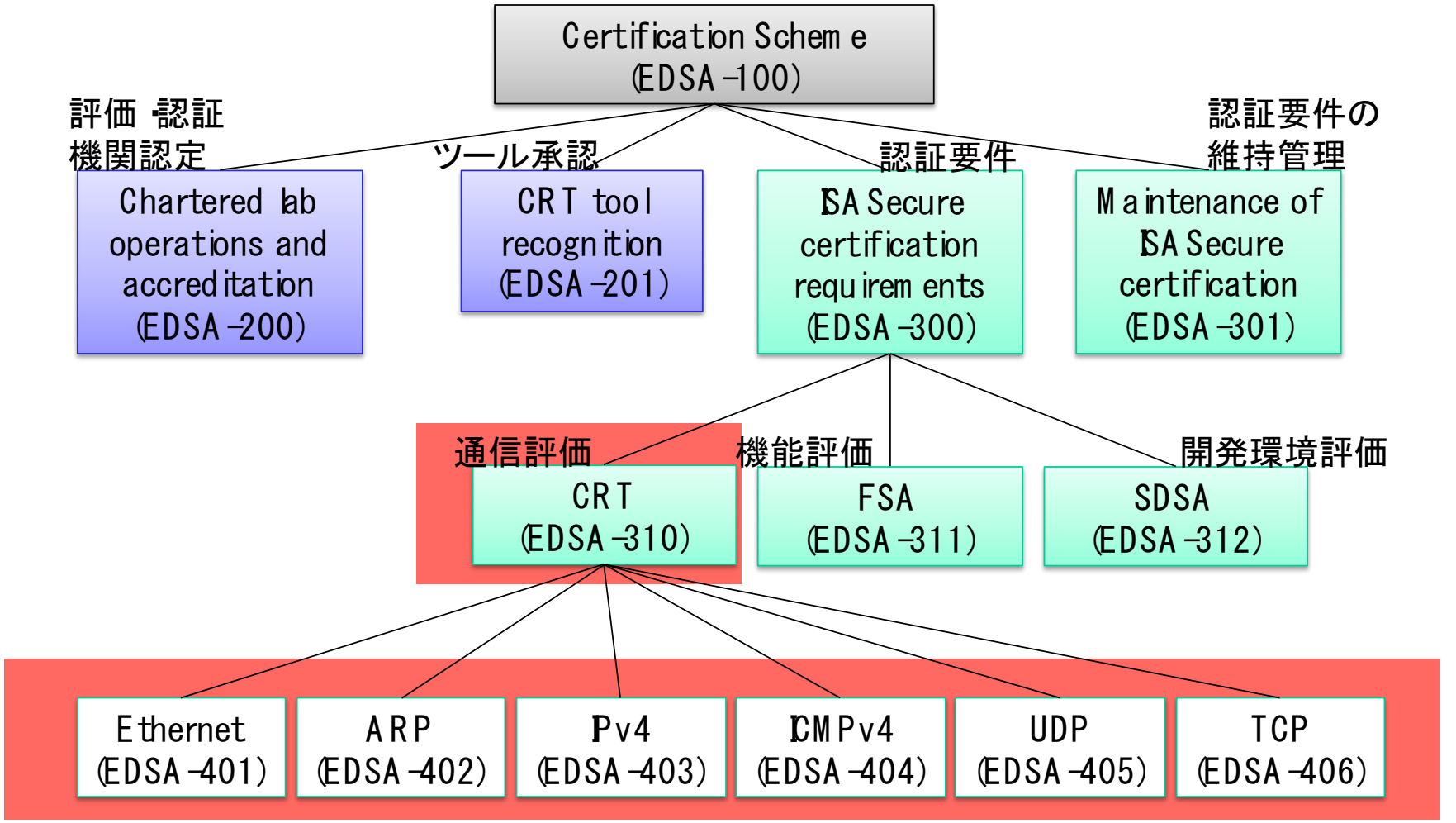
組込み機器へのネットワークプロトコル実装が,ネットワークから受信した異常な又は意図的な悪意のトラフィックに対して,自分自身及び他のデバイス機能を防御する程度を測定する。

不適切なメッセージ応答,又はデバイスが重要サービスを適切に実行継続できないと,デバイス内部の潜在的なセキュリティ脆弱性の存在を示している。

- ●CRT 要件
  - –EDSA-310
    - ◆IPベースのプロトコル実装用のCRT共通要件
  - –EDSA-401～406
    - ◆コアプロトコルに対する要件

出典:ICSJWG Spring 2011, (ASCI)
「Validating the Security Assurance of Industrial Automation Products

1. CRT試験とは ・・・ EDSA規格のドキュメント体系とCRT要件



◇ IPAにより翻訳されたEDSA規格の対訳版はISCIウェブサイトにて公開。
http://isasecure.org/ISASecure-Program/Japanese-ISASecure-Program.aspx

1．CRT試験とは ・・・ 試験対象プロトコル

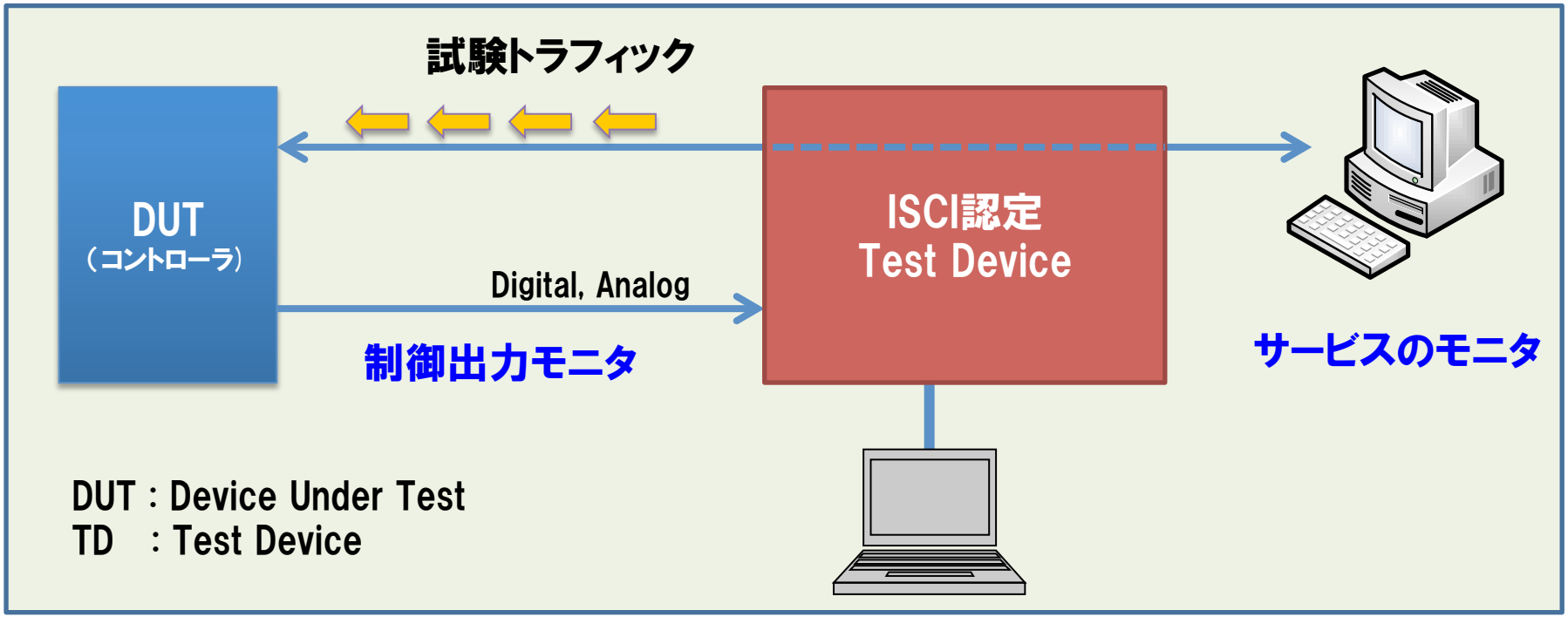
- Group 1 に該当するプロトコルに対する要件は、EDSA 401～406で規定
- Group 2～Group 5 については、ISASecure EDSA認証プログラムで用意されていく予定

Group 1	Group 2	Group 3	Group 4	Group 5
• IEEE 802.3 • (Ethernet) • ARP • IPv4 • ICMPv4 • TCP • UDP **コアプロトコル**	• BOOTP • DHCP • DNS • NTP, SNTP • FTP, TFTP • HTTP • SNMPv1-2 • Telnet	• HTTPS • TLS • Modbus/TCP	• IPv6 • OPC • Ethernet/IP/CIP • PROFINET • FFHSE • Selected wireless protocols/stacks with elements such as: - IEEE 802.11 - ISA100.11a - WirelessHART	• SNMPv3 • SSH • Server • OPC-UA • MMS • IEC • 61850 • SMTP

Protocols for ISASecure Communications Robustness Testing

2. CRT試験の内容 ・・・ CRT試験機器構成

- **ISCI認定の試験デバイス**により試験パケットをDUTに対して送信し、サービスの維持を確認
- **6つの必須サービス**の維持が合否判定基準
  ⇒コントローラだけではなく、事実上HMI側の用意も必要
- コントローラは、エンドユーザ文書で推奨されている最大の負荷下で試験を実施する



図：CRT試験環境のイメージ

2. CRT試験の内容 ・・・ ISCI認定 試験デバイス

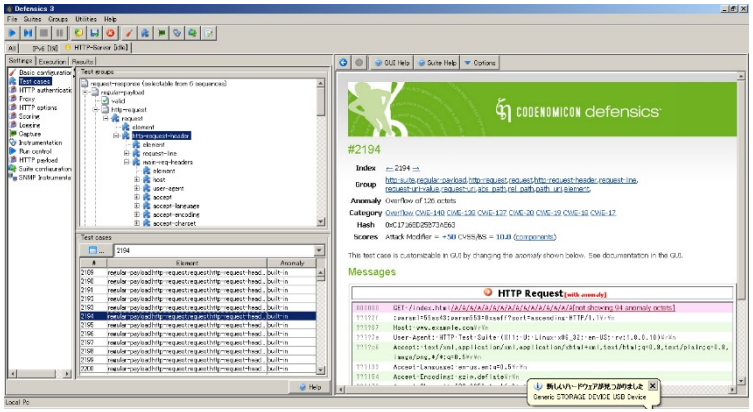
CRT試験には、ISCI の認定した試験デバイスを用いる。
ISASecure : Recognized Test Platforms for CRT
http://www.isasecure.org/Supplier-Resources/Recognized-Test-Platforms-for-CRT.aspx

●Wurldtech 社 Achilles Test Platform

http://www.wurldtech.com/product_services/discover_analyze/achilles_test_platform/

●Codenomicon社 DEFENSICS

http://www.codenomicon.com/defensics/



2. CRT試験の内容（参考）・・・ EDSA認証(CRT試験)とAchilles認証

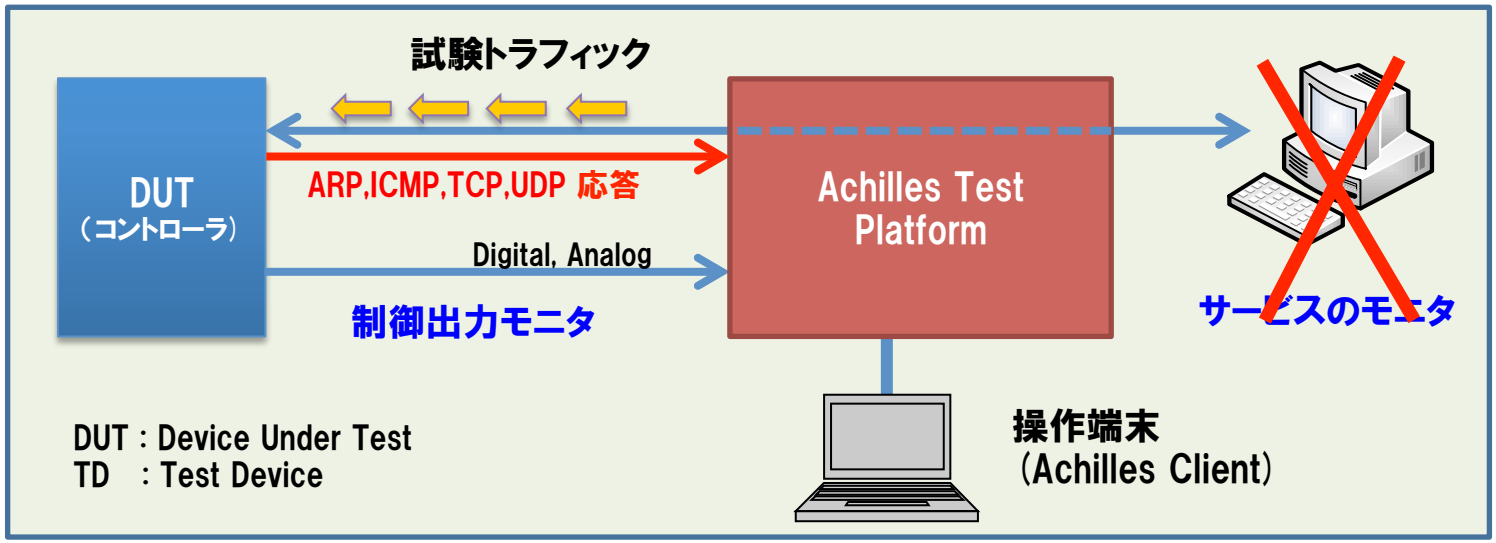
■ Wurldtech社 Achilles 認証（Achilles Communication Certification）との差異

●試験トラフィックの内容は、試験デバイスにAchilles Test Platformを利用した場合、Achilles Level 2とほぼ同一内容

●判定基準

A)制御出力モニタに関する判定基準は、ほぼ同一

B)Achilles 認証では、通信機能の維持が判定基準となっているが、EDSA認証では、サービスの維持が判定基準となっている

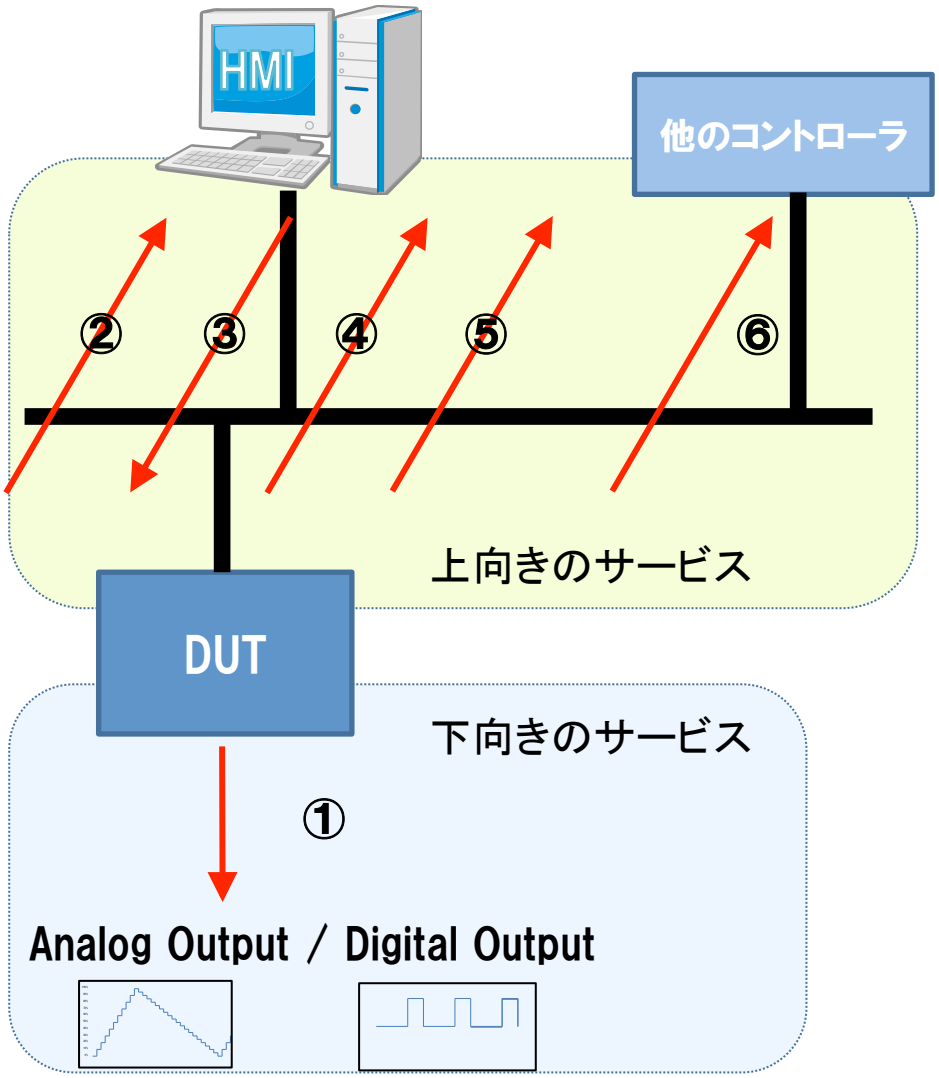


図：Achilles認証試験環境のイメージ

2. CRT試験の内容 ・・・ 6つの必須サービス

■ 6つの必須サービス

次の機能を用いたサービスが適切に維持されていることを確認する



2. CRT試験の内容 ・・・ 6つの必須サービス

■ 6つの必須サービス

次の機能を用いたサービスが適切に維持されていることを確認する

上向きのサービスは、申請者が設計に基づき定義する

- 「サービス」の具体的内容
- 「サービスの維持」とはどのような状態なのか、定量的に判別する方法

試験所と合意

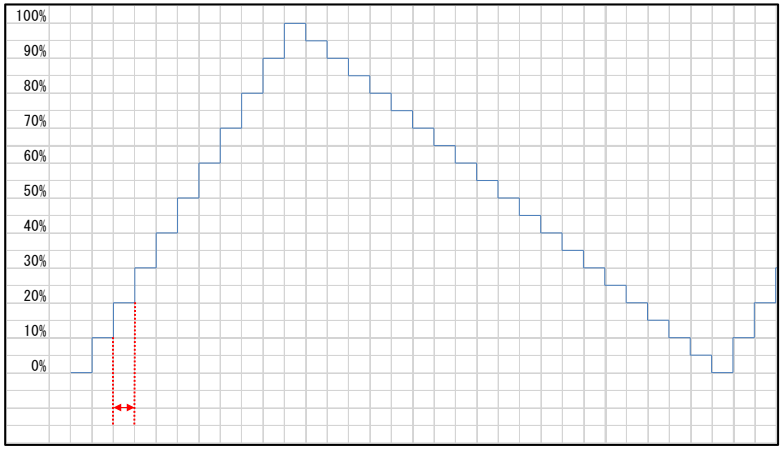
「上向きの必須サービスを適切に維持する」の判定基準

2. CRT試験の内容 ・・・ 下向きのサービス（制御ループ）の定義と維持

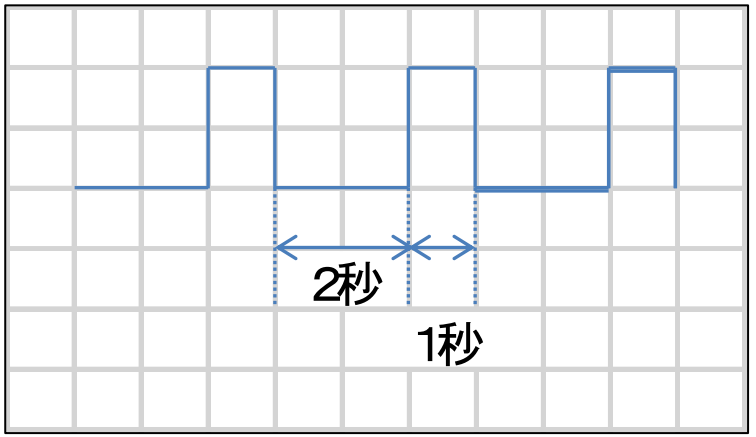
■下向きの必須サービスの定義

①制御ループ

- 出力する信号は、EDSA-310に定義されている
- 下向きのサービスは、常に維持されている必要がある



アナログ信号



デジタル信号

項目	値
制御ジッタ	1秒±100ms

試験対象のコントローラのスペックから定義

2. CRT試験の内容 ・・・ 上向きの必須サービスの定義

■上向きの必須サービス

② プロセスのビュー
例:「プロセス制御・安全ループ」で出力しているデジタル信号・アナログ信号のトレンド表示・記録

③ コマンド(設定値の変更など)
例:HMIからプロセスパラメータを一定周期で自動的に変更し、その結果がわかるログを記録

④ プロセスアラーム
例: :「プロセス制御・安全ループ」で出力しているアナログ信号出力にたいして、50%以上でアラームが発生するように設定。そのアラームを記録。

⑤ 必須履歴データ
例:一定周期でプロセスパラメータ変更操作をおこない、その操作履歴が発生するようにし、ログに記録

⑥ ピアツーピア制御通信
例:一定周期で、他のコントローラ間に対して制御通信(コマンド送信)が発生するようにし、その結果がわかるログを記録

- **フラッディングによる干渉が原因でサービスが失われることは許容される**
- **ただし、仕様(タイミング等)にもとづき復帰する必要がある。**

2. CRT試験の内容 ・・・ 試験の流れ

評価機器情報シート

準備・計画

- CRT評価の実施に必要な環境準備
- 実施プランの作成

試験実施計画書

実施

- 認定評価装置を用いて、試験の実施
  - 試験環境セットアップ
  - インタフェースサーフェステスト
  - 基本的なロバストネステスト
  - 負荷ストレスロバストネステスト

試験結果

レポート

- 試験結果のまとめ

CRT試験報告書

2. CRT試験の内容 ・・・ 試験環境

●試験の実施場所
- –CSSC東北多賀城本部

<u>試験対象機器を持ち込んで試験</u>

●試験可能機器
- –10/100/1000Base-T I/F
- –サイクルタイム 100ms 以上
- –電源 100V/50Hz

条件は変更される可能性があります。最新の条件は、お問い合わせください。

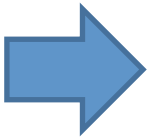
3. CRT試験の準備 ・・・ CRT試験実施に向けて

① 「コントローラ」の定義
② 通信条件の仕様整理
  – アクセス可能なネットワークインタフェース
  – 通常のトラフィック
  – 防御機能と回復条件
③ 上向きの必須サービスの定義
④ 6つの必須サービスの実現と監視基準の定義

3. CRT試験の準備 ・・・ CRT試験実施に向けて

① 「コントローラ」の定義

- 認定の対象とする「コントローラ」の範囲を定義する
  - 一つの製品として定義可能であること
  - 物理的に単体であることは必須ではない。
    （外付けFirewall等との組み合わせでも可）
- 製品としてとりうる、CPU、ネットワークインタフェースの冗長構成を整理



どのインタフェースに対して、どういう状態で試験を実施するかが決まる

3. CRT試験の準備 ・・・ CRT試験実施に向けて

② 通信条件の仕様確認

●アクセス可能なネットワークインタフェース一覧の作成

i. ①で作成したそれぞれの構成に対して、インタフェース一覧を作成する

ii. その中から、対象となるインタフェース、対象外のインタフェースを決める
対象外となるインタフェースには、その除外理由を申請する必要がある
例:「メンテナンス用のインタフェースで、通常はロックされている」
「イーサネットインタフェースではない」

●通常のトラフィックの定義

どのような通信が行われても、必須サービスが維持されるトラフィック量を仕様化
例:1Mbps 以下

●防御機能と回復条件

特定の条件下で防御機能が働く等により上向きのサービスが一時的に停止または提供できなくなる場合、その機能と発動条件、および回復条件を定義。

3. CRT試験の準備 ・・・ CRT試験実施に向けて

③ 上向きの必須サービスの定義
④ 6つの必須サービスの実現と監視基準の定義

製品の持つ機能のうち、なにが「必須サービス」に該当し、「期待された動作」なのかを申請者は申請する必要がある。

まとめ　～ CRT 試験に当たって～

- CRT 試験環境の理解
- 「6つの必須サービス」という概念の理解
- 受験にむけての準備のポイント
  - 「コントローラ」の定義
  - 通信条件の仕様整理
  - 上向きの必須サービスの定義
  - 6つの必須サービスの実現と監視基準の定義
- セキュアな製品設計と実装
  - 期待しない通信相手の存在を想定する（脅威の存在）
  - 境界でのパラメータのチェック
  - ネットワーク通信に対するファジング試験の導入

ご清聴ありがとうございました