重要インフラのレジリエンスを実現するアーキテクチャ

Stuart Phillips

2019年　5月29日

自己紹介

- Stuart Phillips, シニアコンサルティングエンジニア
  - Device as a Service (DaaS) 部門　セキュリティサービスリード
- HPプロフェッショナルサービスはお客様のテクノロジーの導入、OSの移行、サイバーセキュリティの脅威への対応をする際のサポートをするコンサルティングサービスを提供
- サイバーセキュリティ、ネットワーク、ユニファイド・コミュニケーションの25年以上の経験を持ち、特に世界各地で軍事、政府関連、制御システム、金融システム分野で高度なセキュリティソリューションを導入してきた経験を持つ。CISCOで働いていた際には、セキュリティ部門の責任を持ち、後にAP地域のセキュリティ―マーケティングの責任を持つ。その後、会社を興しロッキードマーチンを通じアメリカ空軍の仕事を委託。そこでは劣化した衛星ネットワークの下で、安全で最適化された通信を行うためのソフトウェアモデルの開発を行うセキュリティ研究プログラムの責任を持つ。
- コンピューターサイエンス学士、MBA – シンガポール
- アメリカ、コロラド在住

重要インフラでのレジリエンスの重要性

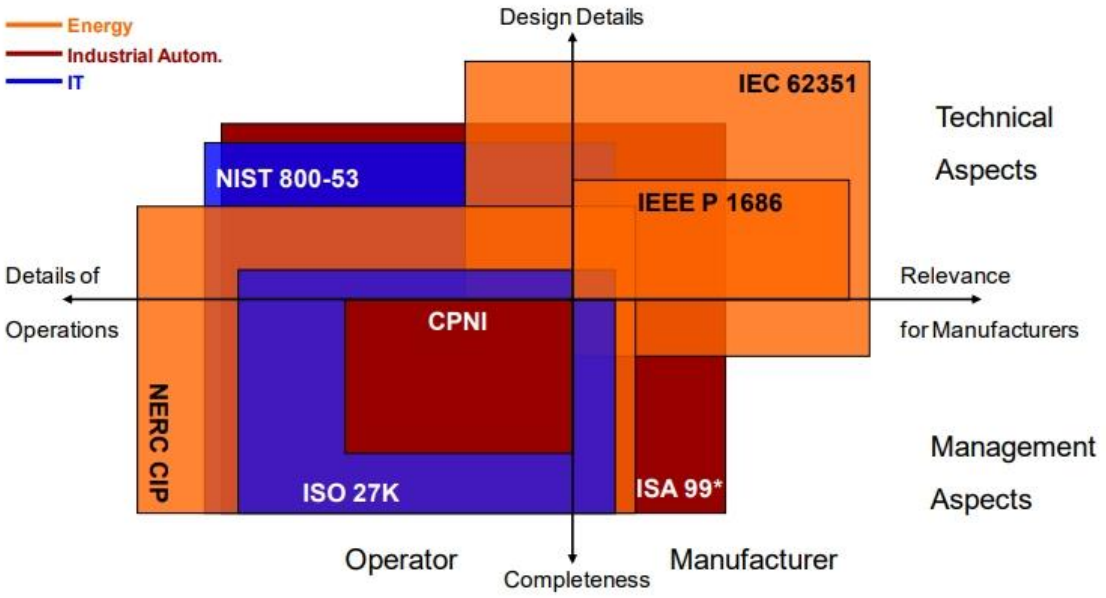
- 重要インフラ(CI)
  - 定義：社会や経済を機能させるための本質的な資産
- 運用技術(OT) 対 情報技術(IT)
  - 産業用制御システム（ICS）、SCADAとしても知られる
  - 電子的な方法で物理的なモノを操作する
    - 適切な時にバルブを開く
    - 必要な際に橋を閉じる
    - 適切な化学物質の割合で適切な時間の間飲料水を処理する
- CIは現代社会の基礎
  - 列車に安全に乗れますか？
  - 工場を操業するのに十分な電力が供給されますか？
  - 医者から処方された薬を信用できますか？
- CIはあらゆる経済の必須な要素のため保護する必要

日本での重要インフラの定義

- 14セクターが定義
  - 情報通信(Information and communication services)
  - 金融(Financial services)
  - 航空(Aviation services)
  - 空港(Airport)
  - 鉄道(Railway services)
  - 電力(Electric power supply services)
  - ガス(Gas supply services)
  - 政府・行政サービス（地方公共団体を含む）(Government and administrative services (including local public authorities))
  - 医療(Medical services)
  - 水道(Water services)
  - 物流(Logistics services)
  - 化学(Chemical industries)
  - クレジット(Credit card services)
  - 石油(Petroleum industries)
    - https://www.nisc.go.jp/active/infra/outline.html

NIST Cyber Security Framework と SP800-171/53

- https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
  - 民間企業のシステムと組織のCUI（機密情報以外の重要情報）の保護
- NIST標準は良く定義されており OT/ICSの場合にも有効
  - アクセス制御、意識向上と訓練、監査と責任追跡性、構成管理、識別と認証、インシデント対応、メンテナンス、メディア保護、人的セキュリティ、物理的保護、リスクアセスメント、システムと通信の保護、システムと情報の完全性

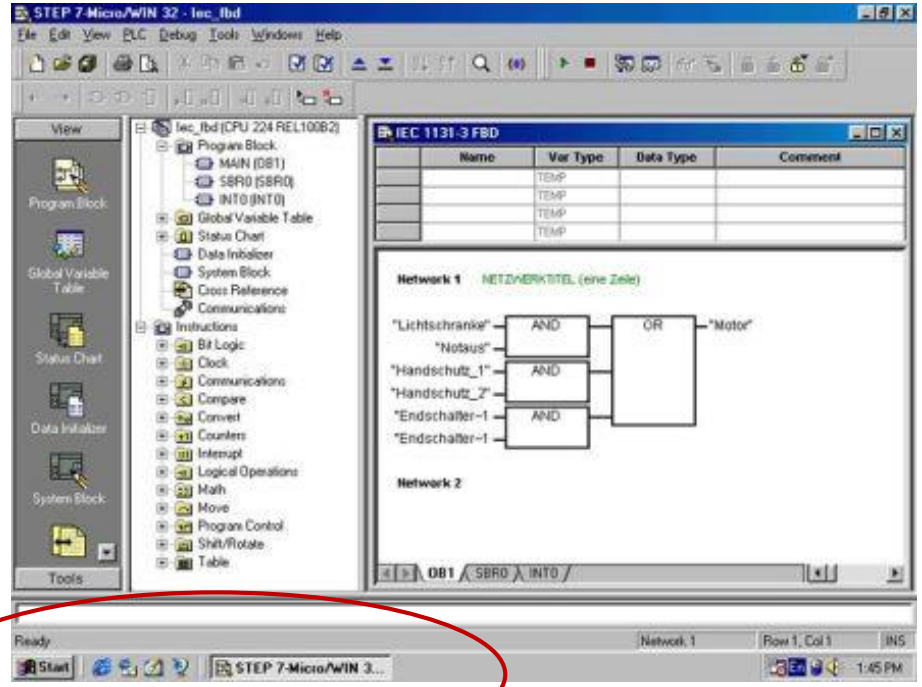


最近の重要インフラへの攻撃

- 産業スパイ
  - 計画、ノウハウ、顧客リスト、価格データ、入札情報を窃盗
- ランサムウェアと強奪
  - OTはより脆弱
  - Bitcoinにより可能となる
- 純粋な国家支援攻撃の出現
  - インフラへの政治的攻撃
    - 力の誇示
    - 将来はさらに悪化
    - 偽ランサムウェア (Not Petya etc.)

なぜ重要インフラ（CI）はそんなに脆弱なのか？

- 設置して終わりというアプローチ – CIシステムはアップデートするように設計されていない
  - 古いOSは攻撃が最も容易でランサムウェアの最大の犠牲者
- 好むと好まざるとに関わらずオペレーターの環境は変わる
  - 装置はこれまでになく複雑で多機能
  - 多くのデバイスは接続され、アップデートにインターネットを用いる
  - 分析のためにリアルタイムで収集データを見る要求の増加
- IT攻撃がCIシステムに侵入し始めている
  - 最近の研究によると攻撃の55%が人起点
    - マルウェアをインストールする悪意あるリンクのクリック
    - 感染したアップデートを含んだ家庭用USBの挿入
- CIオペレーターはサイバーセキュリティのトレーニングを受けていない
- ITセキュリティチームはOT/ITオペレーションのトレーニングを受けていない

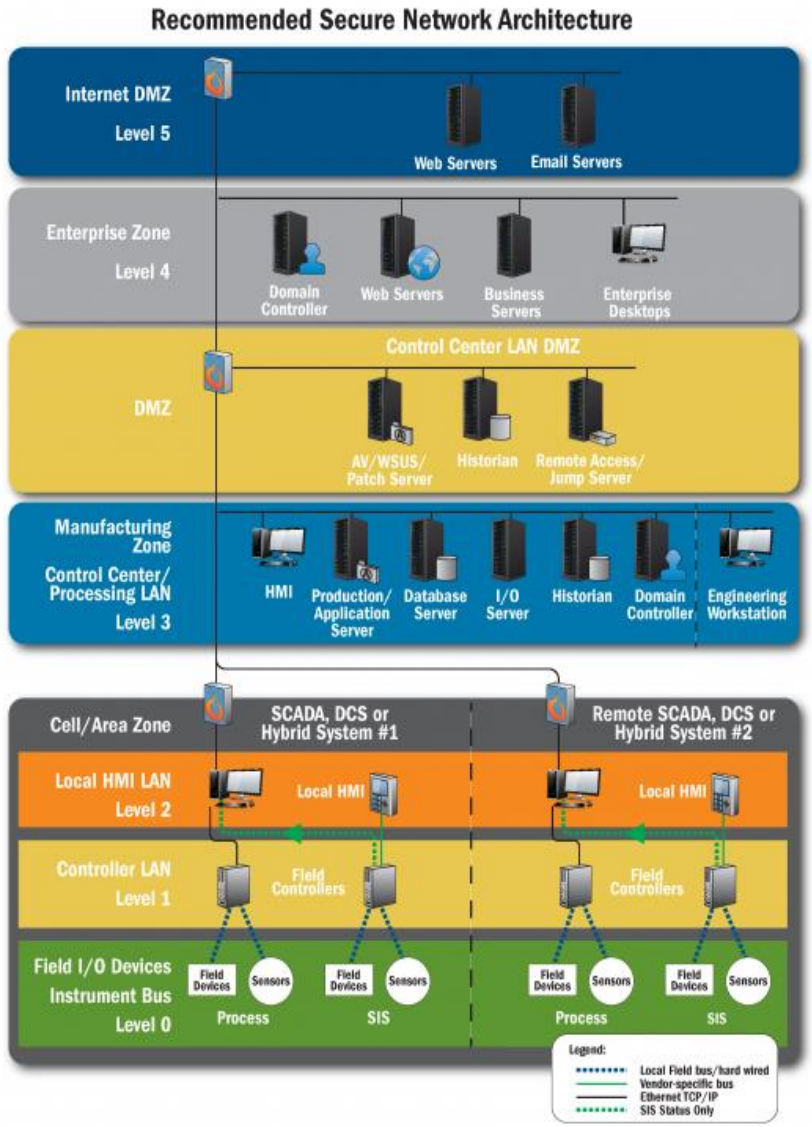


OTとITネットワークの統合

- ネットワーク統合は進む
- OTネットワークはよりスマート、より洗練
  - Webサーバーをビルトインしたplc
  - Wi FI接続の交通信号
  - 空港の携帯回線接続のビデオセキュリティカメラ
- 隔離（Air-gapped）あるいは閉域（Island）モード
  - 隔離された専用ネットワークですべての機器の管理
  - このネットワークを使いアップデート、管理
  - セキュリティを考慮してないため侵害が効果的に広がる傾向
    - USBを使った攻撃はこの目的のために作られた
- 2つの別のネットワークを維持していくコストが問題に
  - 2倍の帯域
  - 2倍の装置
  - 違うスキルの2つの要員チーム
- 統合ネットワークが急速に増えている

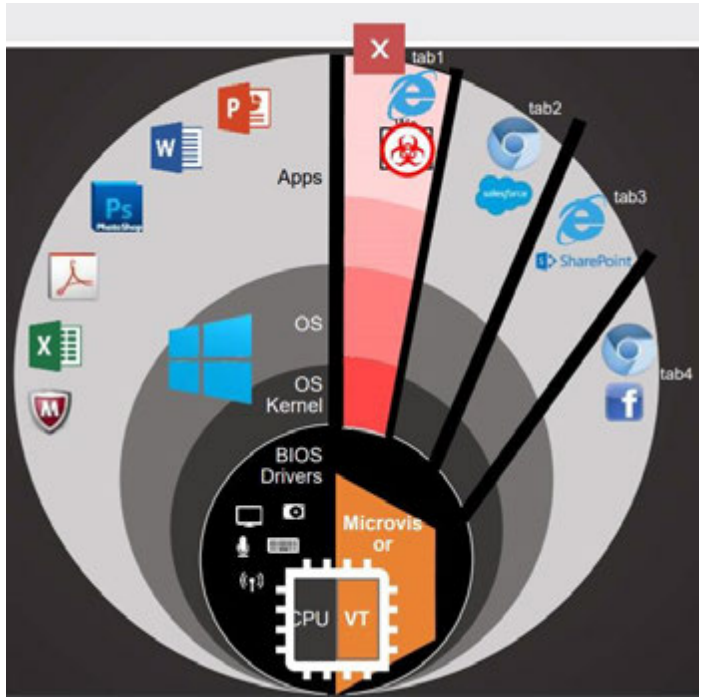
ベストプラクティス

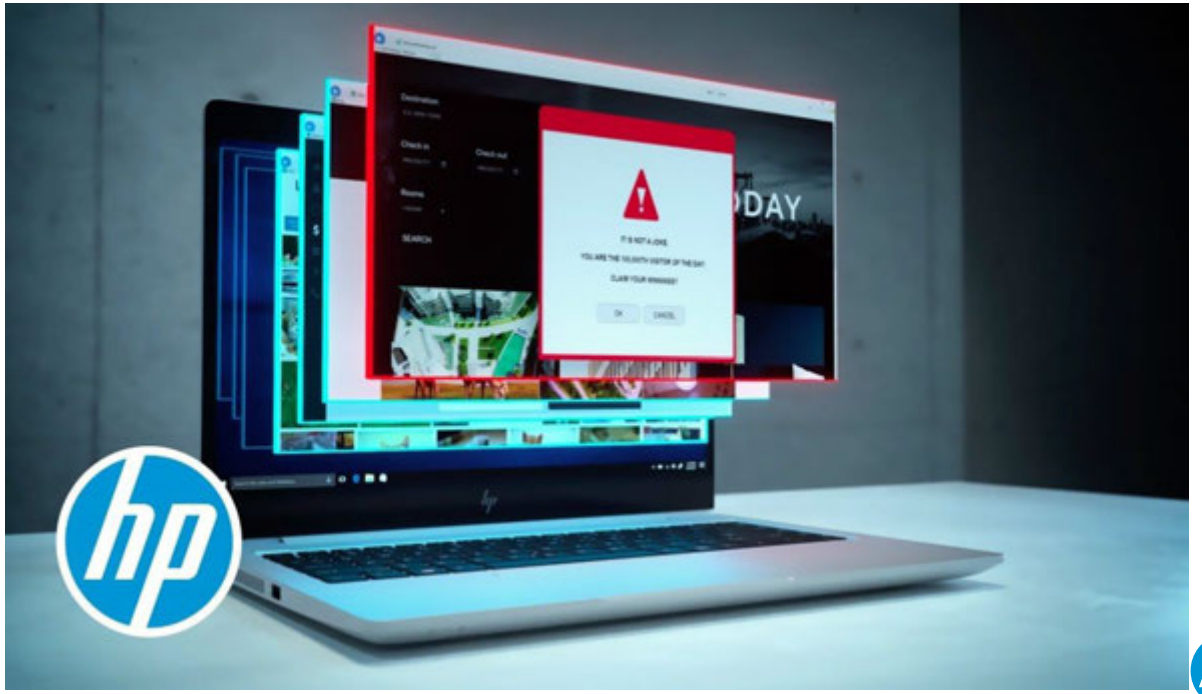
- ネットワークを適切にセグメンテーションする (ISA 99/Purdue Model)
- 補助的システムを含め全て最新のOSを導入する
  - エレベーター、エアコン、信号機
- テストを行う
  - 全てのシステムの脆弱性スキャンを実行する
- 定期的ソフトウェアのパッチ適用とアップデートをする
- 従業員のクロストレーニングを行う
- 従業員を“うっかり”事故から守る
  - 保護のないブラウジングやEメールの開封を制限する
- ネットワークの脆弱性を探す
  - 運用のためにユーザーが作ったオープンポートを探す



OT/ICSにおけるHP Sure Click Advanced

- マルウェアは特にOT/ICSシステムをターゲットにするように進化
  - Triton/Trisisはシュナイダーエレクトリックの 安全計装システムのロジックをマルウェアにより入れ替え、非常時に安全装置が動くことを妨げる
- Sure Click Advancedは対象システムにマルウェアが 侵入することをコンテナあるいはバーチャルマシンにより防ぐ
- ソフトウェアはバーチャルマシンで通常通りの動作をするが隔離される





HP DaaS アプローチの適用例 – 発電所の運用

- HP DaaSが短期間で現行OCのハードウェアを提供
  - 全てのOSをアップデート
- HPプロフェッショナルサービスがOSとアプリケーションのWindows 10移行をサポート
- HPマネージドサービスが定期的アップデート
  - ランサムウェアのリスクを削減
  - 安全なVPNもしくはフィルタリングされたファイヤーウォール経由で接続
- 資産管理の明確化
  - HP Tech Pulseがシステムの利用状況を追跡
- 偶発的な攻撃を制限
  - Sure Click advancedによりマルウェアとユーザー由来の攻撃をブロック

ありがとうございました