

ビッグデータ活用の為の ネットワークセキュリティ化装置

2020年11月

名古屋工業大学 社会工学専攻

経営システム分野

教授 橋本 芳宏

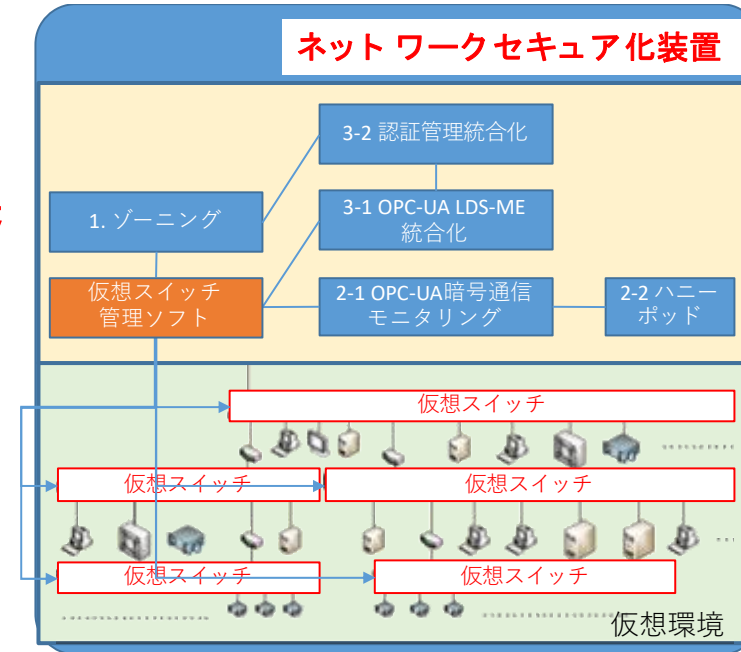
従来技術とその問題点

- 製造現場におけるネットワーク環境
 - 制御機器は、ベンダー独自のフィールドバスで連携され、ベンダーが工事するため、接続は整然と整理・管理されていた。しかしながら、ベンダーが独自ハードからWindows PCとEthernetの利用へと方針変更した。
 - 汎用ネットワーク機材を使用し、ユーザ主体で接続した結果、混沌としたスパゲッティ構造が現出した。
 - 結果、セキュリティを考慮したとは言い難い状況となっている。
- 製造企業はIoT/AI/DXによる経営効率化を進めている。
 - その結果、**外部とのネットワーク接続が開かれ、サイバー攻撃に晒されること**となった。
- 製造系ネットワークのセキュア化は必須である。
 - しかしながら、常時稼働の可用性が重視される現場での大々的な**ネットワークの再構築(アドレス設定変更、LANケーブル再配線)**は**困難**な状況にある。



新技術の特徴・従来技術との比較

- 新技術: ネットワーク構造の変更管理システム
 - 制御機器とネットワークスイッチの接続を、**仮想スイッチとの接続に置換**
 - 管理マシンの実環境上の管理ソフトから、**仮想環境上の仮想スイッチを一元管理し、これを切替えることで動的にゾーンを切替**
 - **シンプル、低コスト**で実現(超小型IoT機器を使用)



- 従来技術:
 - 物理的なケーブルの差し替え、設定変更
 - ・ 物理的にネットワーク構成を変更するには、LANケーブルの抜き差しや引き回し変更等の**手間のかかる物理作業**やルータ、
 - ・ スイッチ、Firewall等を1つ1つ**手作業で設定変更**する必要がある。
 - 高価なSDN(Software Defined Network)機材への取り替え
 - ・ 一般のネットワークスイッチより**大変高額(8万円vs140万円)**
 - ・ 専門家による**高額**のサポートが必要



取替



武器となる研究シリーズ：動的ゾーニング

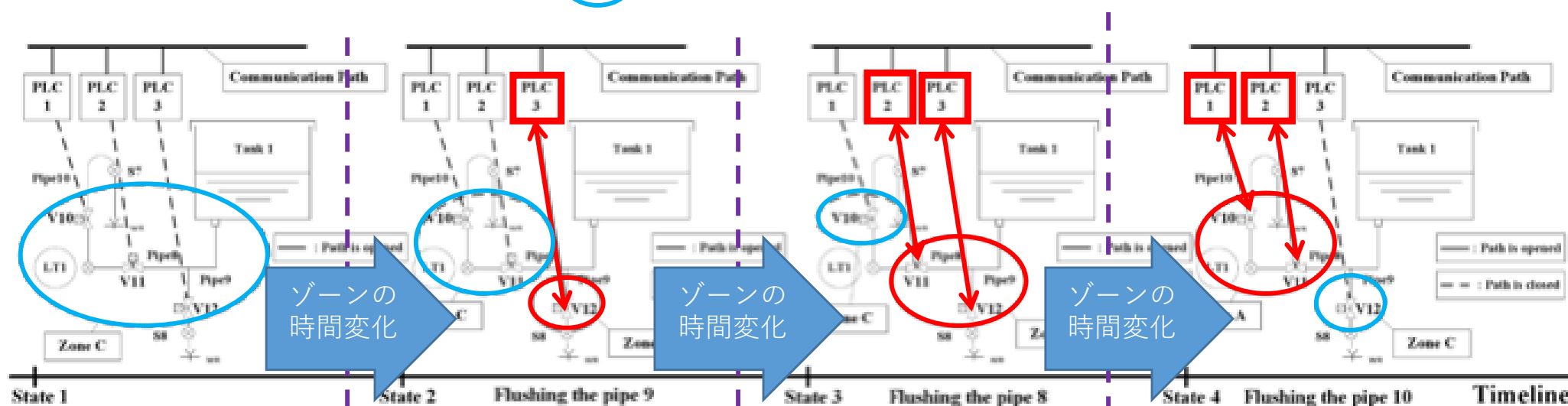
時間ゾーニング手法

- 製造装置の運転スケジュールに合わせて通信必要箇所をゾーン分け

空間ゾーニング手法

- 製造装置の物理的・論理的接続関係に合わせて通信必要箇所をゾーン分け

○ 通信が必要な空間ゾーン ○ 通信が不要な空間ゾーン ↔ 制御のために必要な通信



時間 1
通信不要

時間 2
制御器PLC3から
バルブV12への
通信が必要

時間 3
制御器PLC2, PLC3
からバルブV11, V12
への通信が必要

時間 4
制御器PLC1, PLC2
からバルブV10, V11
への通信が必要

想定される用途・実用化イメージ

- 製造現場で、IoTやAIが使いこなすためにも、
 - まずは製造現場のネットワークをなんとかしたい
 - しかし、工場の運転が長時間停止は避けたいし、費用も抑えたい。
- 我々が、製造系ネットワークを最新・高セキュリティのネットワークに変身させる。
 - 仮想化で、配線構造を自由に再構成
 - セキュリティ規格IEC62443が求めるゾーニングに容易に対応
 - 加えて、IoTやIndustry 4.0に対応したOPC-UAを導入
- 愛知県産業界に、セキュリティの高い産業用ネットワーク環境を低コストで提供する。

実用化に向けた現状と課題

- テーマ1:ゾーニング装置
 - 運転条件を考慮したゾーニング(開発済み)
 - データ保護(ブロックチェーン)を考慮したゾーニング(開発中)
- テーマ2:監視装置
 - 攻撃監視ハニーポッド(開発済み)
 - OPC-UA暗号通信モニタリング(開発済み)
- テーマ3:統合認証装置
 - OPC-UA LDS-ME:OPC-UAクライアントがサーバを発見する仕組の統合化(開発中)
- テーマ4:セキュアサーバ装置
 - 上記テーマ1から3を組み込んだ管理サーバ(要開発:一部開発済み)
- テーマ5:テスト環境
 - 上記テーマ用のテストベッド(開発済み)
 - 上記テーマをテストできる実環境(要開発:企業より提供を希望)

求める連携先とメッセージ

- セキュリティ関連技術のため、
 - 研究チームが責任を持って管理できる、大学内の実験室を主たる開発の場として使用する。
 - 本研究でテストベッドが完成するまで、大学内の既存テストベッドを使用するため
 - サイバー攻撃を模擬する等の実験を行うため、封鎖・管理されたネットワーク環境を確保するため
 - テストベッドは連携企業に無償開放する。
 - 企業内、各界へのサイバー攻撃デモンストレーションに使用可能とする。
- 実際の現場で、**プロトタイプ**のテストを受けていただける企業を募集中
 - 開発済みのゾーニング装置プロトタイプのテスト
 - 現場での実績なし
 - 開発済みの監視装置プロトタイプのテスト
 - 現場(大手製造企業)での実績あり

<http://www.manage.nitech.ac.jp/Security/>

本技術に関する情報

試作品の状況

提供可

※提供の際は諸手続が必要となるため、問合せ先までご連絡願います。

文献・特許の情報

- 特願2020-001712『ネットワーク管理装置』 特願2020-001713『制御ネットワークにおける通信監視システム』 特開2018-073397『通信装置』 特許6598288『動的ゾーニングプラントシステム』

研究フェーズ



【お問合せ】

名古屋工業大学 産学官金連携機構

〒466-8555 名古屋市昭和区御器所町字木市29番

TEL:052-735-5627 FAX:052-735-5542

E-mail: nitfair@adm.nitech.ac.jp

URL: <https://technofair.web.nitech.ac.jp/>