研究会発足提案書

FA用3Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

2021年7月21日(水)

FAオープン推進協議会

FA用３Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

（１）提案者名

電気通信大学　准教授　澤田 賢治

（２）目的

本研究会では，FAシステムにセキュリティ機能を適用したときの効果やコストリターンを検証するためのFA用３Dシミュレータのためのベンチマークモデルを目指す．セキュリティ機能を盛り込むべき状況や適切なシミュレータの整理を実施する．最終的に研究会で共有できるモデル，データセット，ドキュメントを構築する.

海外ではセキュリティ検証やAI検証のためにベンチマークモデルやデータセットが公開されているが，本研究会では最終的に日本の需要に適したベンチマークモデルを構築する事を目指して活動する.

FA用３Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

（3）背景

IoT化は制御システムの高効率化を促進するとともに，セキュリティインシデントの誘発も促進すると言われてきている．現状，システムのIoT化に伴うコスト投入では，高効率化とセキュア化はトレードオフにあり，FAシステムは特に高効率化にコスト投入される．これは，国内で報告されているインシデント事例が少なく，セキュア化にかけるコストに対するリターンを見積もりにくいのも要因である．現状打破のためには，

- 小規模なPoCから大規模なPoCへのシフト
- 効率化とセキュア化が両立するシチュエーションの明確化
- セキュリティインシデントを再現し，セキュリティ機能の防御範囲を明確化

が必要である．

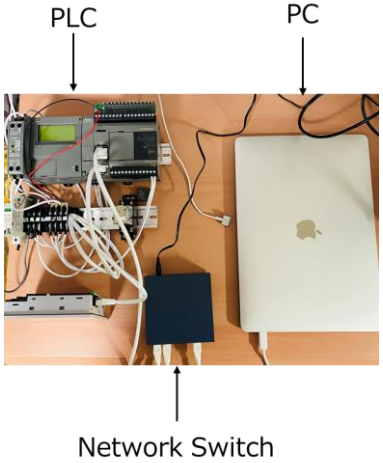
FA用３Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

（４）内容

本研究会では，背景の3項目を反映できるFAシステムの3Dシミュレーションモデルを構築する．本モデルでは，セキュリティ用であると同時に，データ収集量が性能を左右する機械学習系技術への転用も目指す．

- ベンチマークモデルを実現するのに適切な3Dシミュレータを選定する．ベンチマーク目的毎に3Dシミュレータの特性を整理することも含まれる．
- どういう状況をベンチマークするべきか検討する．どの種類のサイバー攻撃を再現するかの整理も含まれる．
- システムのセキュア化が，サイバーインシデント対処以外（ヒヤリハット対応やAI技術検証）にもシステムの効率化を促す状況を整理する．

FA用３Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

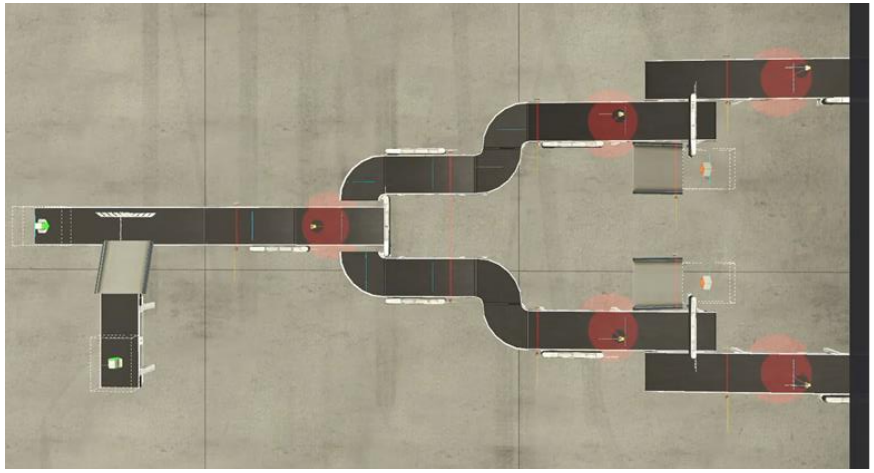


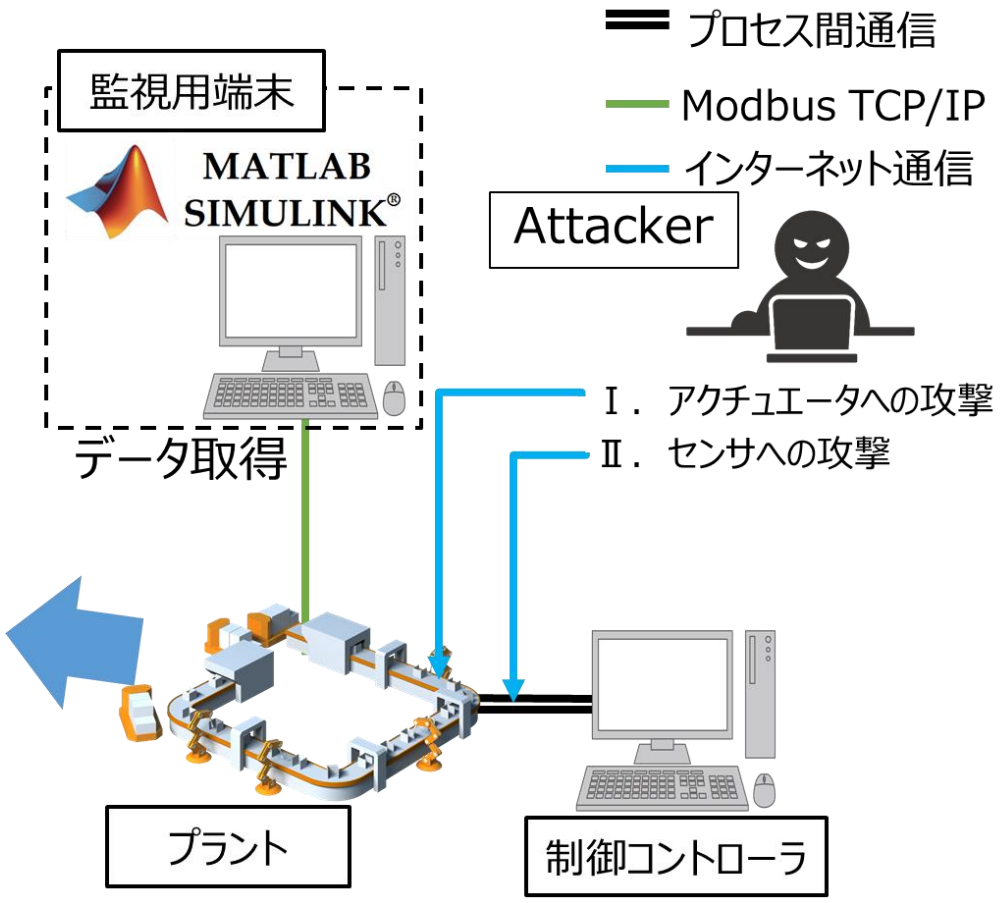
- サンプルシミュレータ：Factory IO
- Factory I/Oは工場の生産ラインをシミュレーションで再現できる
- Factory I/Oは外部のPLC(Simens S7)と使用可能
  ⇨PLC はModbus Sever or Clientとして機能
- Factory I/Oの制御プラットフォームにはコントローラに依存しない Control I/Oがある
- 実際のシステムでは検証しにくい状況を再現できる→次頁

FA用３Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

使用例：複数攻撃を想定した制御システムの異常検知
複数攻撃：センサとアクチュエータが従属関係であるプラントに対してアクチュエータの誤作動を発生させる攻撃

・速やかな異常検知とデータログによる異常特定を実施する.
・データログによる異常検知
→誤作動の原因を特定するため,
サイバー攻撃に加えてオペレータミスや機器故障の特定にも利用可能





FA用３Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

（５）成果物

既存のガイドラインや海外の取り組みなどを調査し，コミュニティで共有出来るドキュメントやモデルを構築する．参加者の意見を聞きつつ，最終的なアウトプットを決めていく予定である．

例1：セキュリティシナリオにはシステムレイアウトが良いか？
例2：実システムで採取しにくいデータとは？
例3：AIなどの新技術を検討するときに適したシナリオとは？
例4：セキュリティ技術がセキュリティ以外で効果を発する場面とは？

（６）スケジュール

研究会発足時は，PLCやPLCのエンジニアリングツールと連携できるFactory IOをシミュレータ例として，専門委員会発足後の活動項目（ドキュメント設計やモデル設計）を精査する．なお，シミュレータはこれに限るものではない．研究会発足の次年度は専門委員会の発足となる．

FA用３Dシミュレータによるセキュリティ検証用ベンチマークモデル開発

（7）募集対象者

FAシステムへのセキュリティ技術導入時にどこから取り組むべきかは誰もが悩む共通課題です．この共通課題の難易度を下げる事が出来れば，各社の強みを活かした生産技術やセキュリティ技術の開発に注力することができます．本研究会では，共通課題の難易度を下げたいと思っている方々，ベンチマークモデルに興味のある方々，以下のキーワードに関連する技術に興味の有る方々の参加をお待ちしております．

・リスクアセスメント
・アノマリー検知・特定・分類
・CAD連携
・シミュレーション技術（1Dシミュレーション，3Dシミュレーションなど）
・モデルベース開発
・生産計画
・制御システムセキュリティ