制御システムのための
モデルベースセキュリティ技術

電気通信大学
i-パワードエネルギー・システム研究センター
（iPERC）
澤田賢治

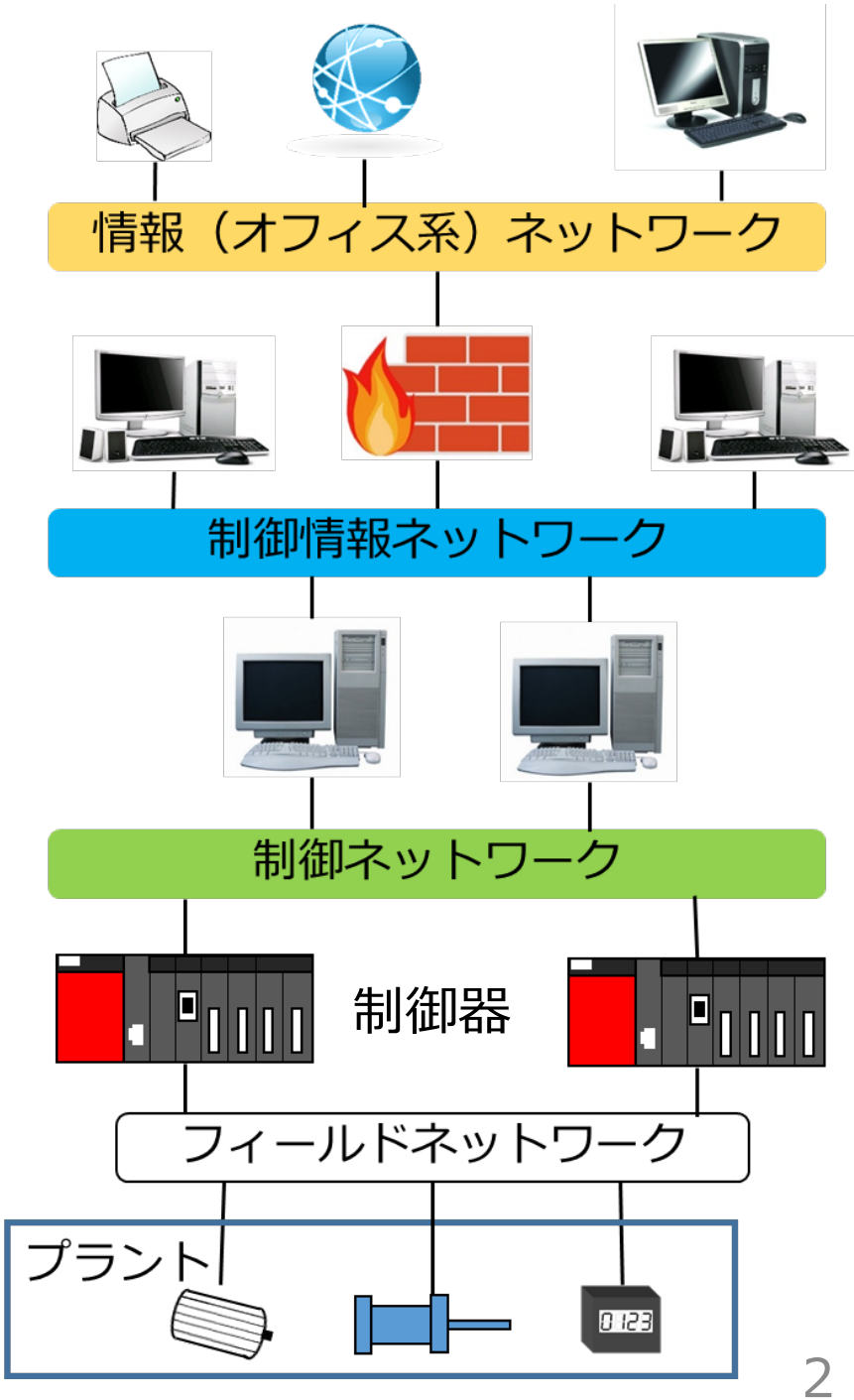
研究背景

制御システム

発電所，工場，化学プラントなど

重要インフラの制御系

- ネットワーク連携による高機能化・高性能化
- インターネットによる広域監視・制御
- 汎用OS・通信プロトコルの導入，オープン技術導入



研究背景

制御システム

発電所，工場，化学プラントなど

サイバー攻撃

物理的な影響

- 2010年

イランのウラン濃縮施設 ”Stuxnet”

- 2014年

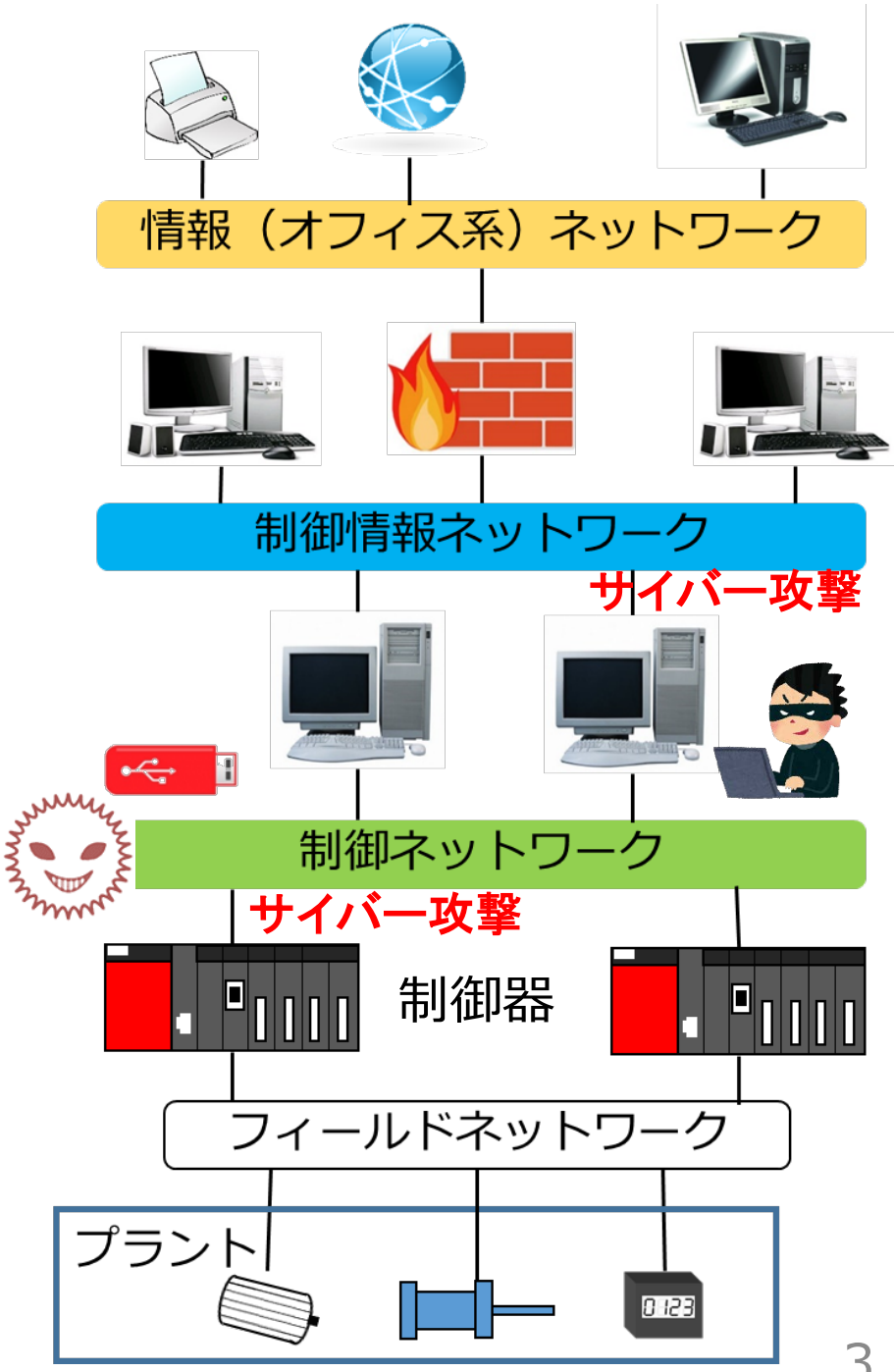
独国の製鉄工場へマルウェア侵入

溶鉱炉爆発→操業停止

- 2015年

ウクライナ電力会社へのサイバー攻撃

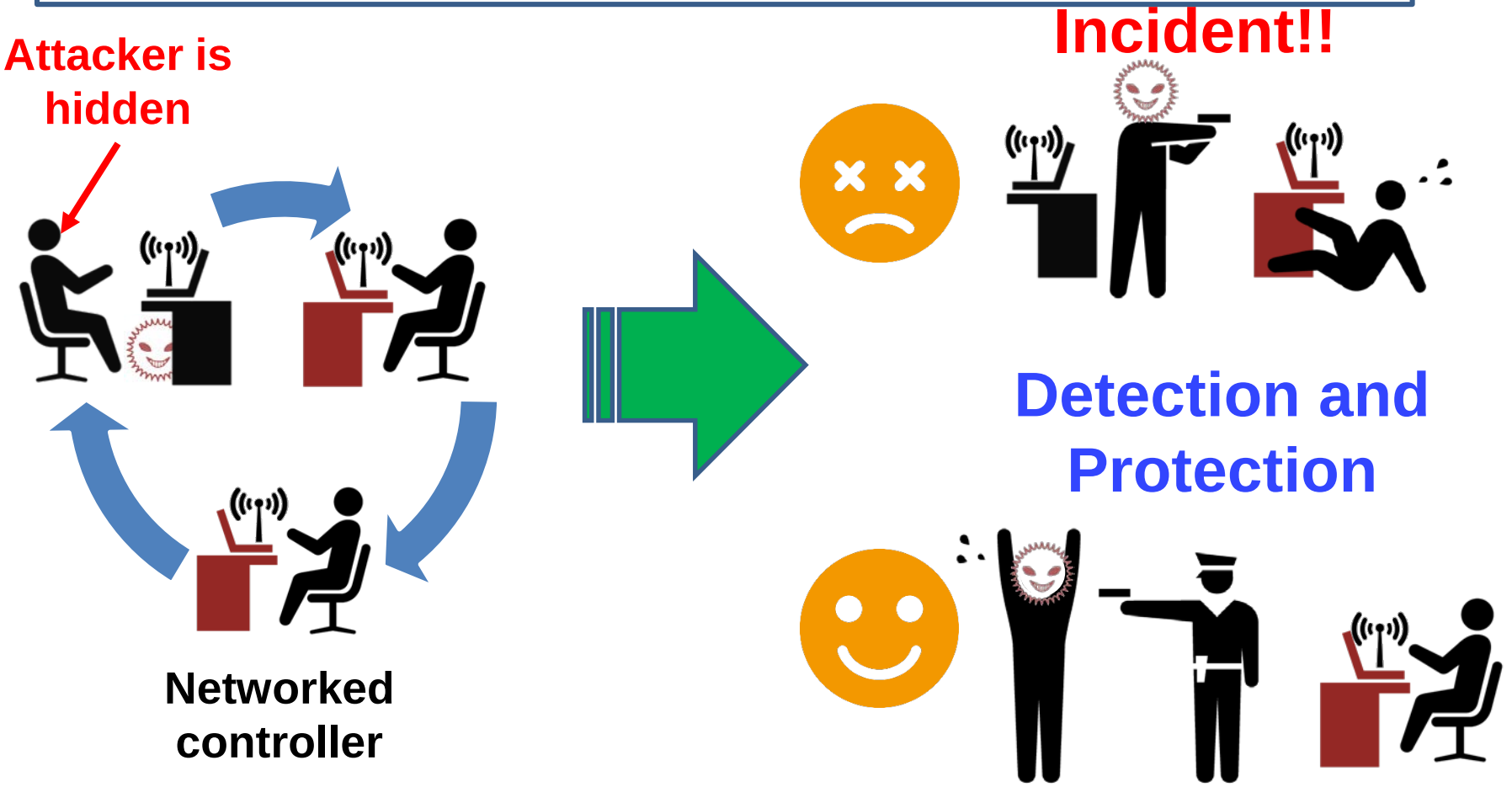
→停電



研究概要

事前対策技術

- ネットワーク振舞異常検知
- 制御システムに対するサイバー攻撃のリスク分析
- **ホワイトリスト**



ホワイトリスト

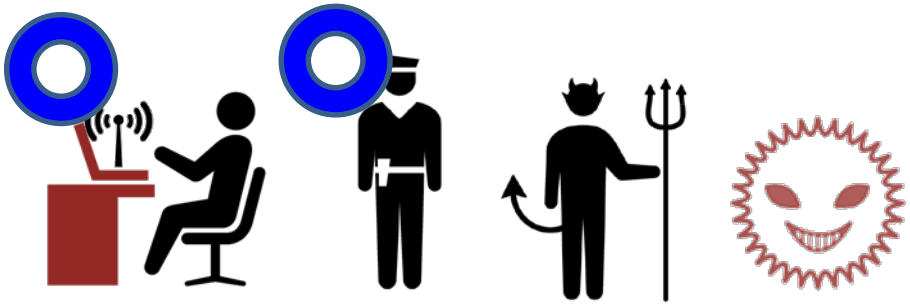
ブラックリスト型

実行不可の通信・プログラムのリスト化

- **常に最新の**パターンファイル更新が必須
- スキャン時のシステム負荷：**高**

ホワイトリスト型

実行可の通信・プログラムのリスト化



- **機能・構成変更時**にパターンファイル更新が必須
- スキャン時のシステム負荷：**低**

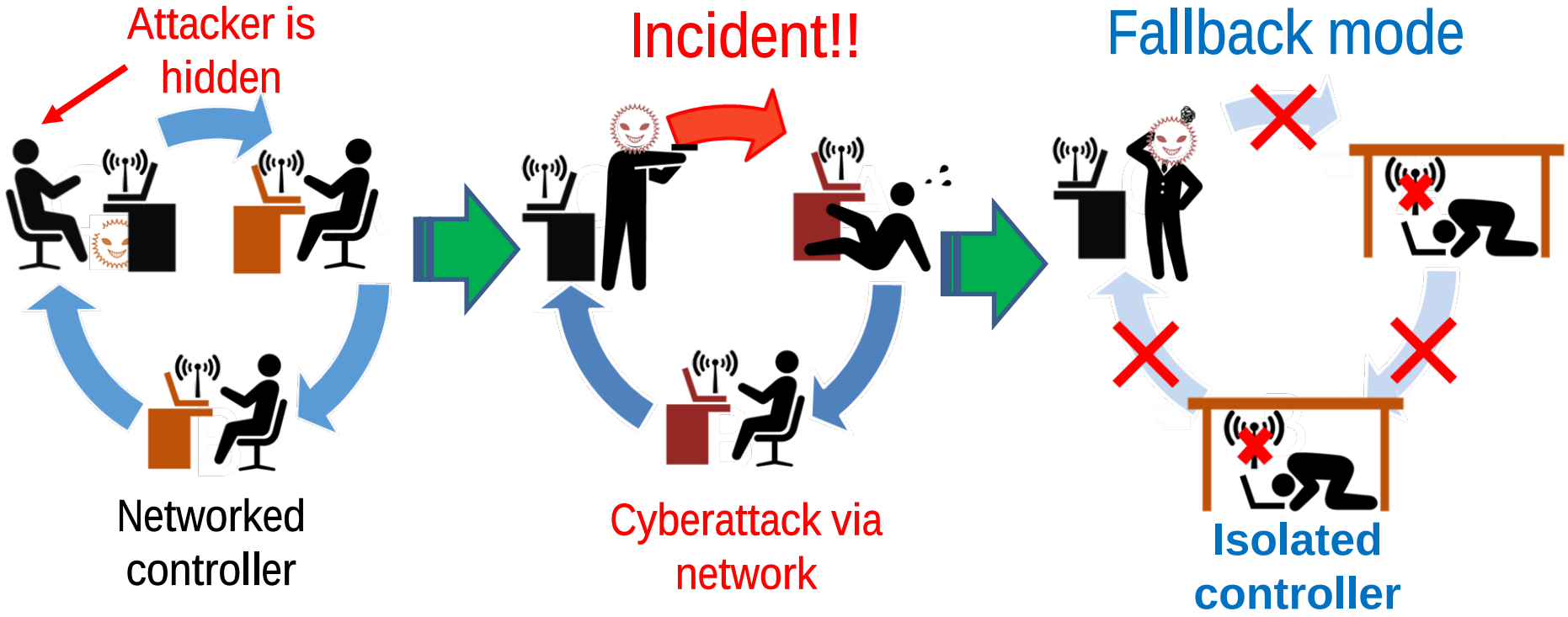
多くの制御システムは「ホワイトリスト」が有効

- レガシー問題（古いOS，最新プログラム動作保証外）
- 高負荷なウィルススキャンが不可能

研究概要

事後対応（ダメージコントロール）技術

縮退運転：防御のための機能限定稼働
サイバー攻撃後の安全側制御の実現



縮退運転システム

- ネットワーク切断・制限による二次感染・被害防止
- インシデント発生後の対応（インシデントレスポンス）

電気通信大学としての取組

- **事前対策**：コントローラ用のホワイトリスト（３）
  - フィールド機器（アクチュエータ・センサ）の正常動作プロセスをホワイトリスト化
- **事後対策**：縮退運転システム（１）
  - ネットワーク切断・制限による二次感染・被害防止
  - ネットワークを利用しない異常検知
- **事前・事後対策**：第三者監視システム（２）
  - ホワイトリスト機能
  - 縮退運転機能

上記を実現するためのモデルベース技術の開発

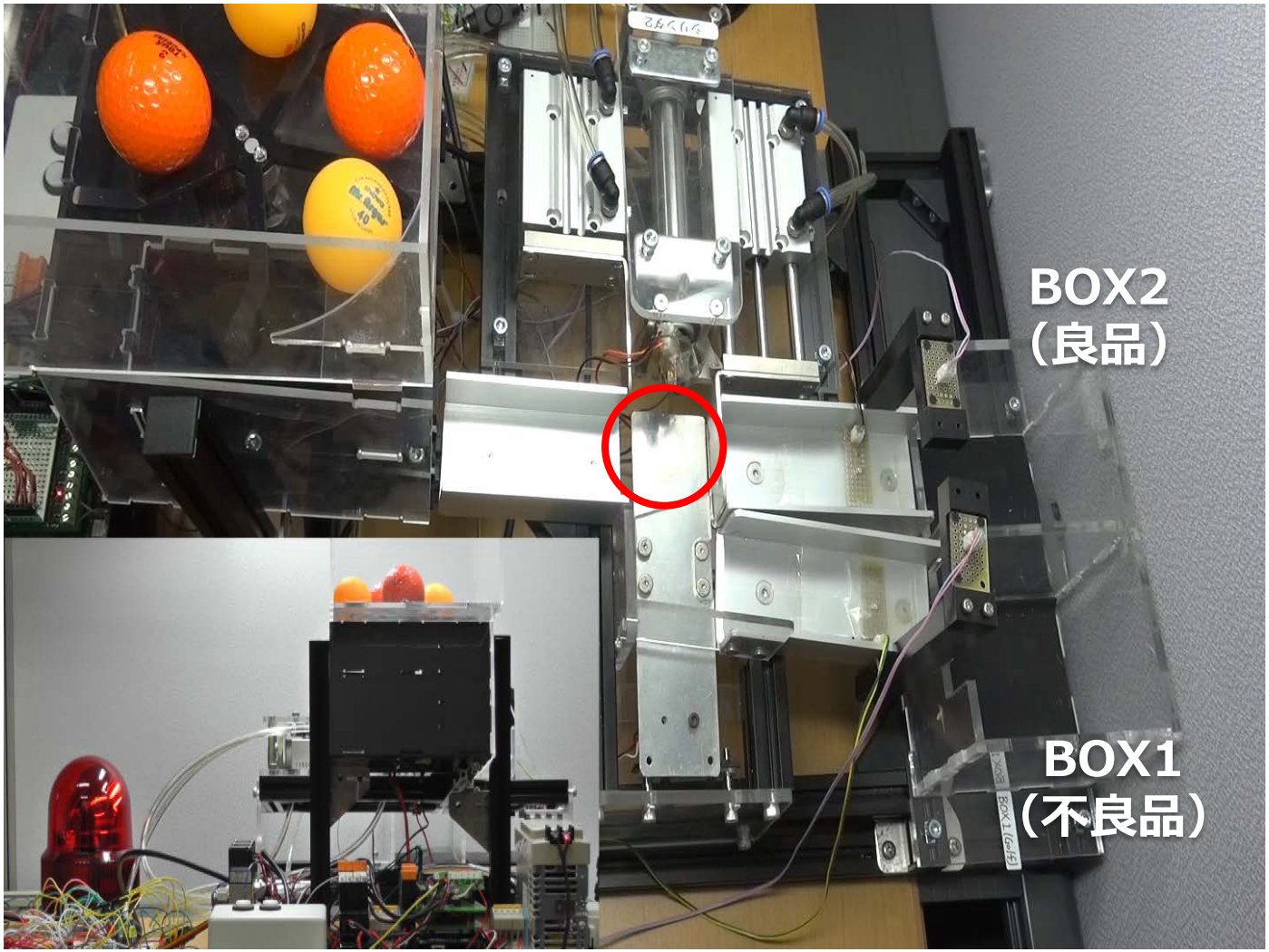
例：不良品判別器における縮退運転

卓球ボール・ゴルフボールを投入

Air cylinders

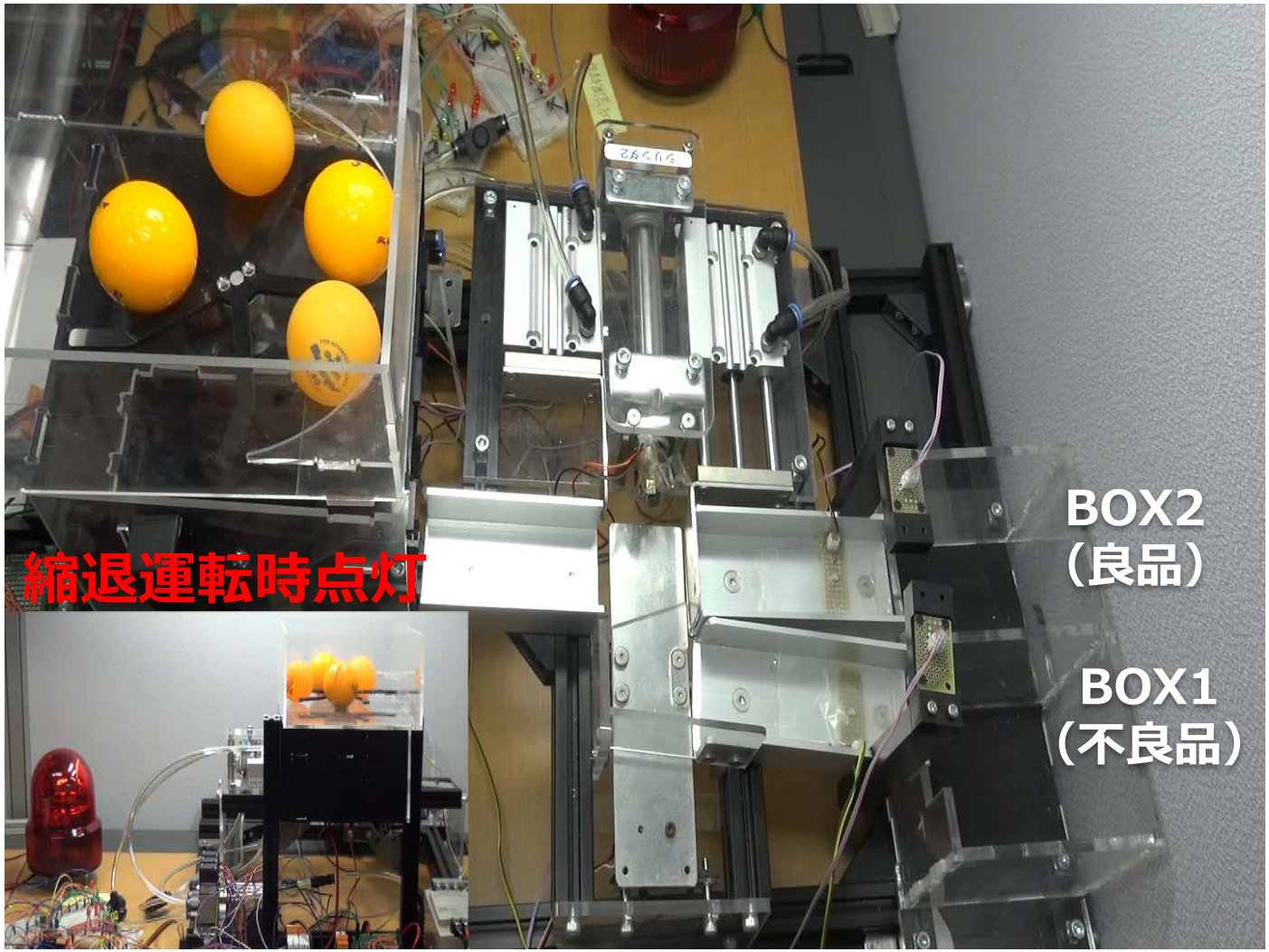
1　2　3

○: Sorting



例：不良品判別器における縮退運転

卓球ボール・ゴルフボールを投入



MITM異常発生

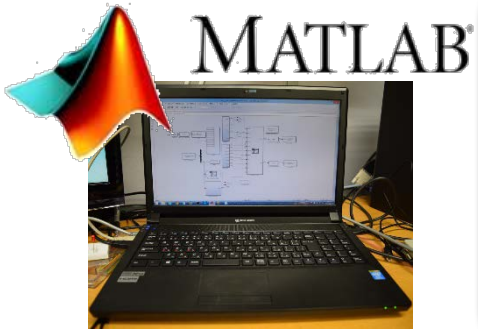
玉詰まり

縮退運転切り替え

玉詰まり解消

サイバー攻撃後の稼働継続を実現

実験環境



ネットワーク化
制御器

Modbus/TCP

L2スイッチ

Modbus/TCP

リモート入出力

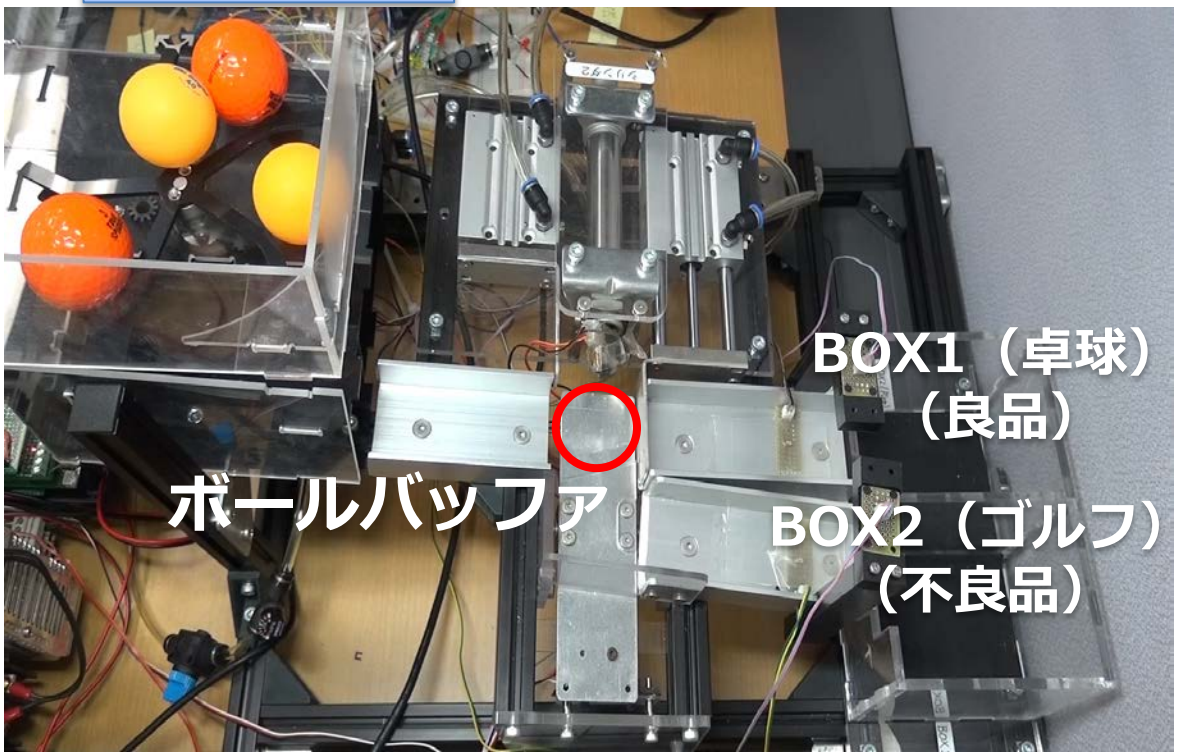
アナログ信号

模擬プラント

制御システム

- ネットワーク経由でリモート制御
  -産業用イーサネット規格（Modbus/TCP）
- 重量の異なるボールを仕分けるプラント
- 生産システムにおける不良品判別器を想定

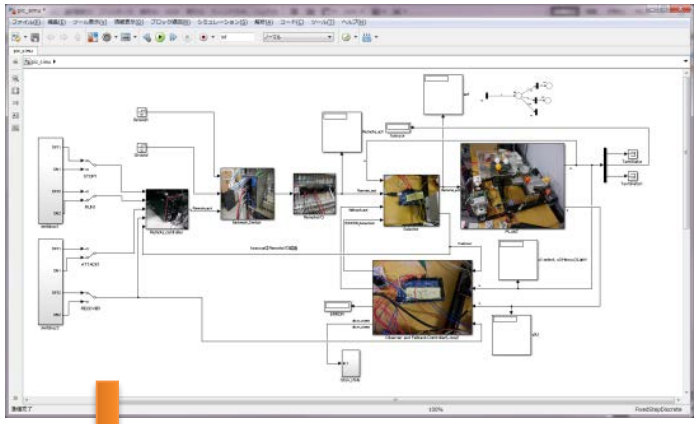
エアシリンダ　1　2　3　○：仕分け部



モデルベース開発

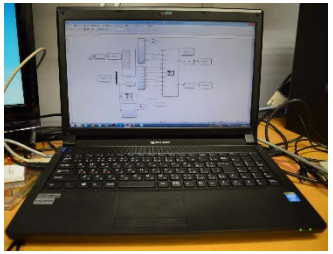
制御モデル

上位設計



制御システム

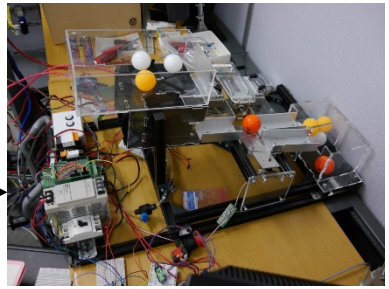
Auto coding



ネットワーク化
制御器

スイッチ

リモート入出力



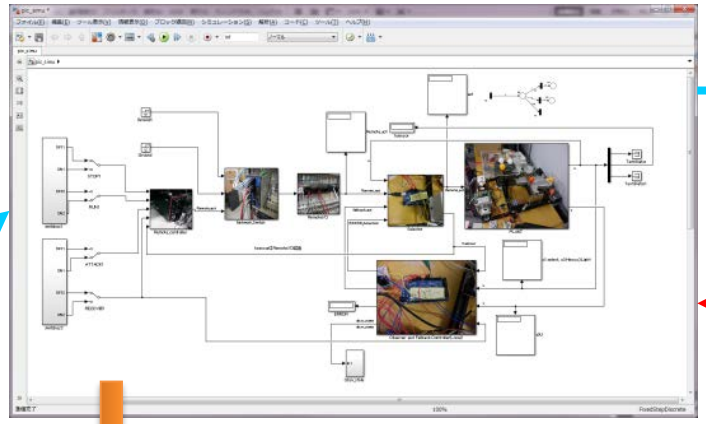
模擬プラント

モデルベースセキュリティ

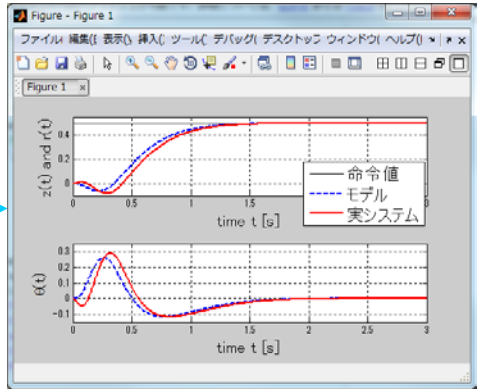
制御モデル

上位設計

MATLAB SIMULINK



動作比較
状態推定



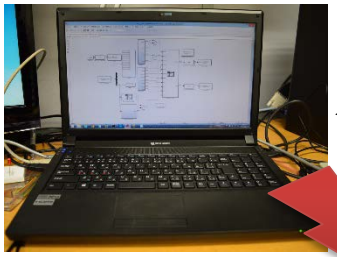
実振る舞い

010
101
011

命令値

制御システム

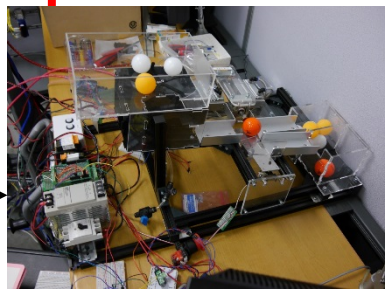
Auto coding



ネットワーク化
制御器

スイッチ

リモート入出力



模擬プラント

情報改ざん
通信妨害

モデルベース縮退運転適用フロー

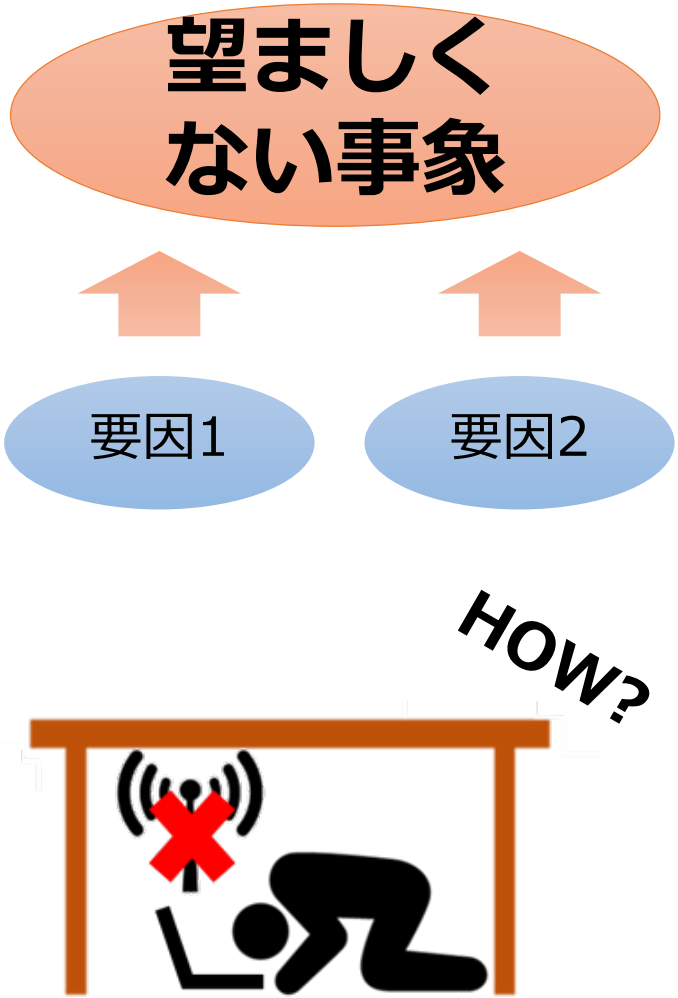
リスク分析

・望ましくない事象
・要因

縮退運転設計

・縮退運転制御ロジック
  ・どのように異常を検出するか？
  ・どこを縮退させるか？
・切り替えタイミング
  ・いつ縮退に切り替えるか？
・切替機構
  ・ネットワークをどのように切断するか？

実装および実機実験



リスク分析

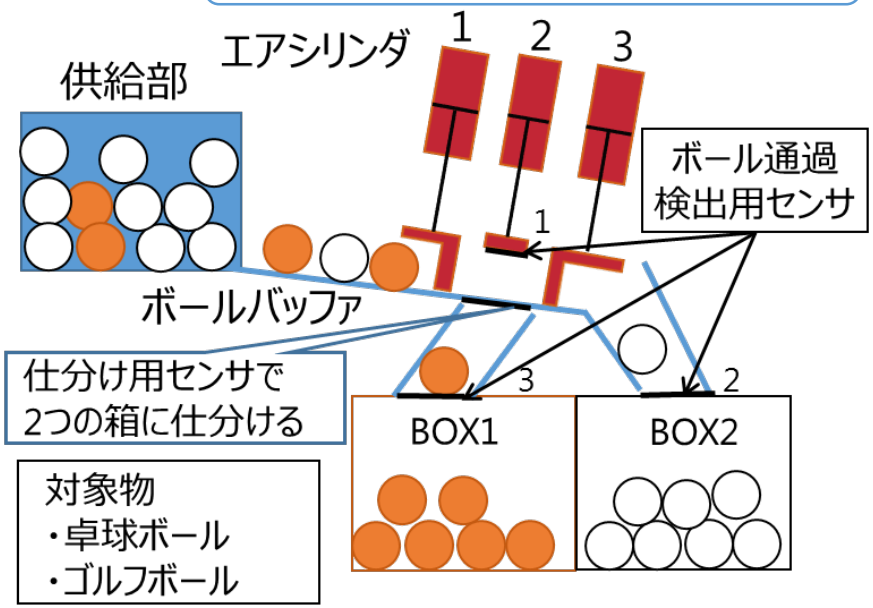
望ましくない事象

ボールバッファ許容量超過による非安全停止

要因

ボールバッファにおける玉詰まり

エアシリンダの異常



仕分け用センサの異常

センサ故障

サイバー攻撃

リスク分析

望ましくない事象

ボールバッファ許容量超過による
非安全停止

要因

ボールバッファにおける玉詰まり

エアシリンダの異常

仕分け用
センサの異常

センサ故障

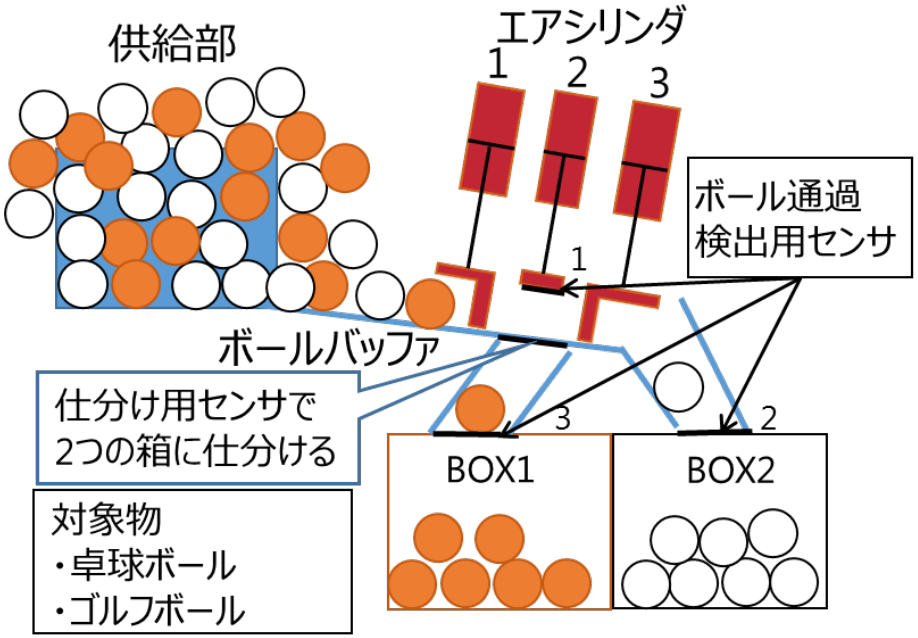
サイバー攻撃

想定するサイバー攻撃

MITM(Man In The Middle attack ：中間者攻撃)
通信に割り込み，情報の傍受・改竄を行う攻撃手法

攻撃側の狙い

仕分け用センサ情報改竄
→非安全停止



防御側の要求

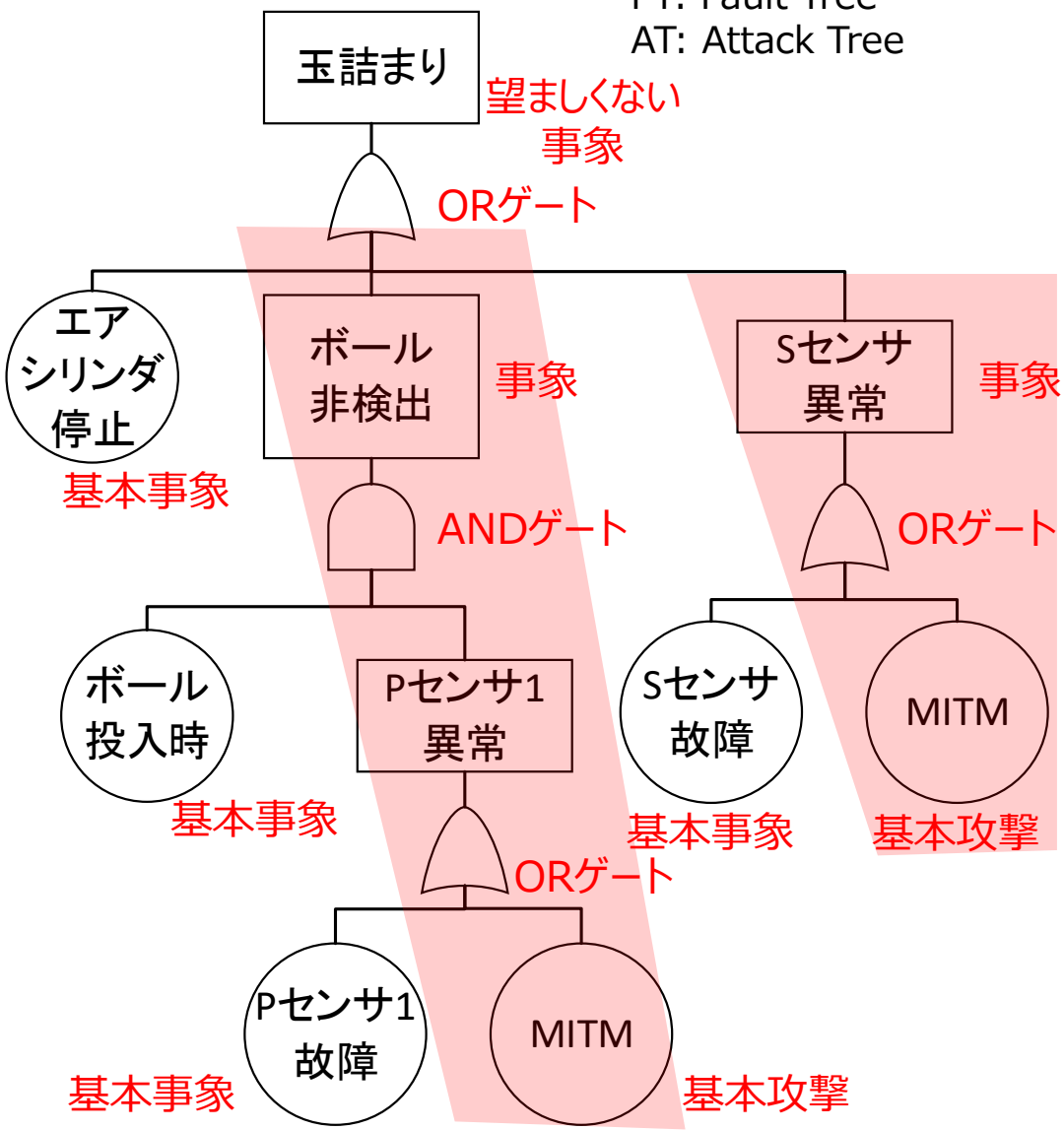
MITM後に
安全側へ制御
（仕分けは優先度低）

縮退運転システム

注目点：「ネットワーク情報を使わない」縮退運転システムをモデルベース技術により実現

参考：FT-AT図による脅威分析

FT: Fault Tree
AT: Attack Tree

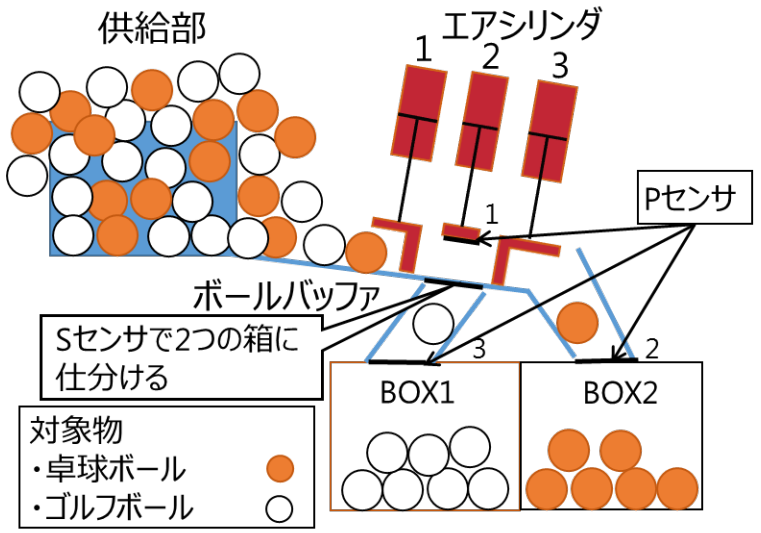


Pセンサ：ボール通過検出用センサ
Sセンサ：仕分け用センサ

防御側の要求

MITM後の安全側制御（仕分けは優先度低）

縮退運転システム



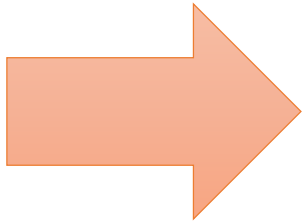
FT-AT:
https://www.gaio.co.jp/product/dev_tools/pdt_seculia.html

縮退運転設計

通常運転

サイバー攻撃発生!!

縮退運転

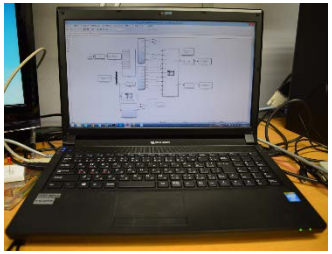


機能を限定してでも
稼働継続に専念
ネットワークから切断

要素技術

- MITM異常検出手法
- 縮退運転切り替え機構

MITM異常検知

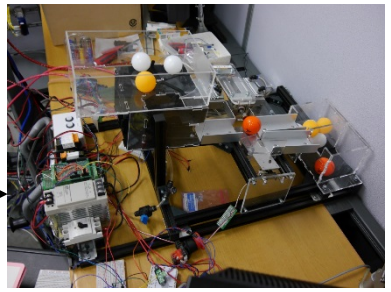


ネットワーク化
制御器

Modbus/TCP

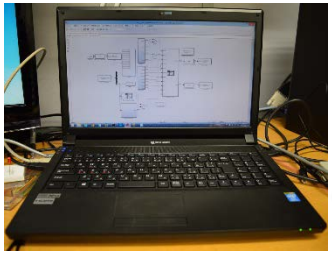
スイッチ

リモート入出力



模擬プラント

暗号化**無し**
認証システム**無し**



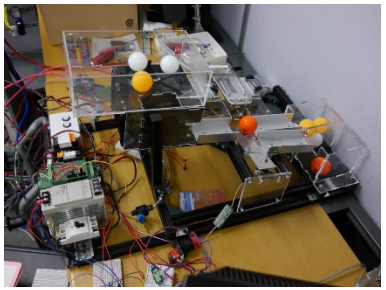
ネットワーク化
制御器

Modbus/TCP

スイッチ

リモート入出力

縮退運転システム

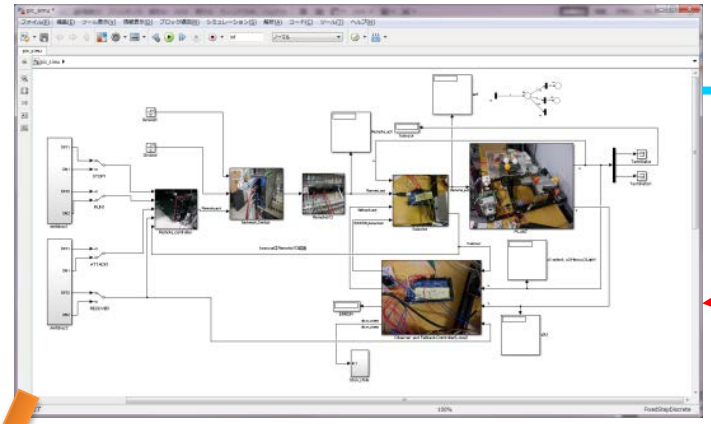


模擬プラント

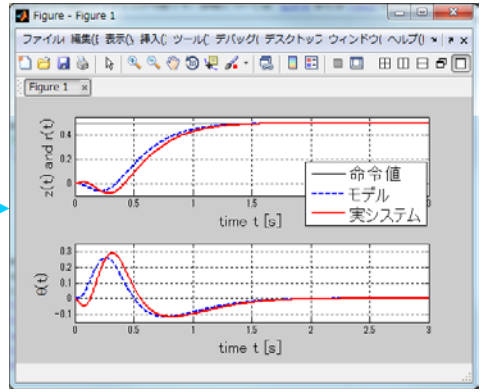
MITM

MITM異常検知

制御モデル

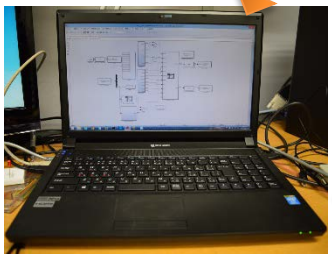


動作比較
状態推定



アナログ信号
（実振る舞い）

Auto coding（事前）



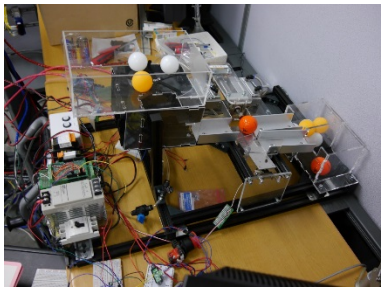
ネットワーク化
制御器

Modbus/TCP

スイッチ

リモート入出力

縮退運転システム

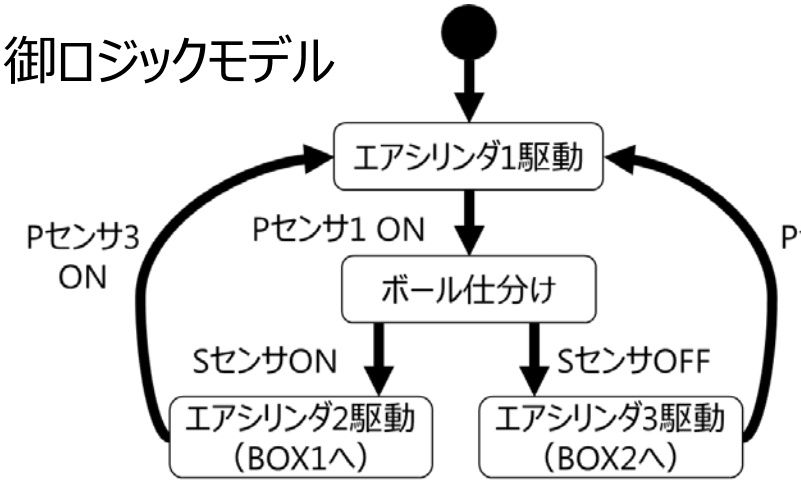


模擬プラント

MITM

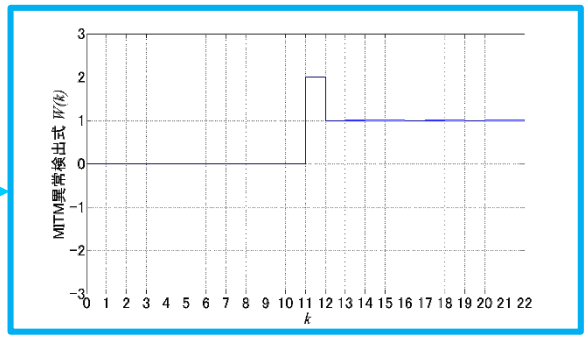
MITM異常検知（模擬プラント）

制御ロジックモデル



Pセンサ：ボール通過検出用センサ
Sセンサ：仕分け用センサ

＜MITM異常検出式＞

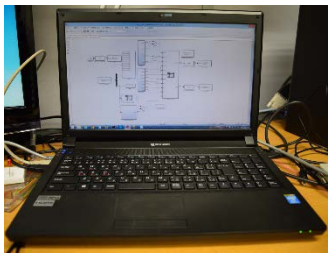


動作比較
状態推定

通常時 $W(k) \leq 0$

異常時 $W(k) > 0$

縮退運転システム



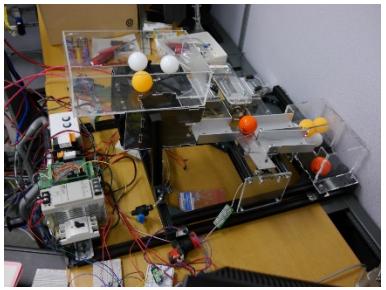
ネットワーク化制御器

Modbus/TCP

スイッチ

リモート入出力

MITM



模擬プラント

縮退運転切り替えアルゴリズム

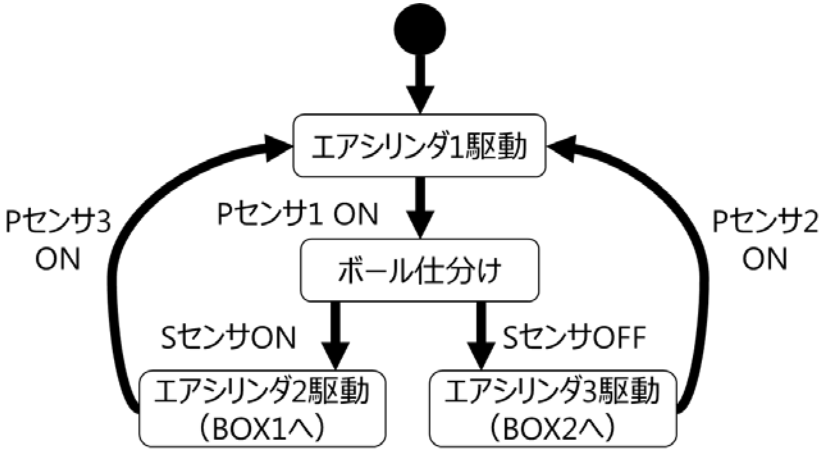
通常運転

ネットワーク化制御器

ボールの仕分け

縮退運転システム

MITM異常検出式計算



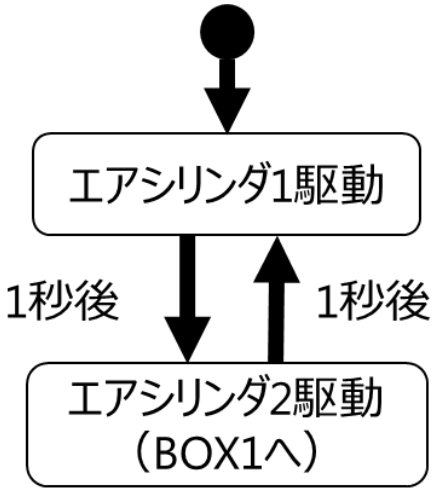
MITM異常検出

MITM異常検出後
即座に縮退運転へ切り替え

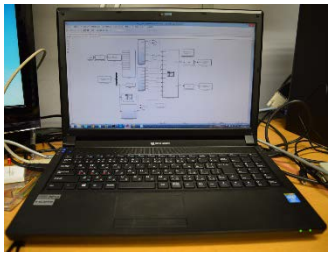
縮退運転

ボールの仕分けを行わない
→ボールを流すことに専念，**稼働継続**

防御側の要求に応えられる



縮退運転切り替え機構（通常運転時）



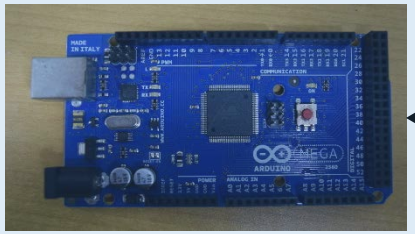
ネットワーク化
制御器

Modbus/TCP

L2スイッチ

Modbus/TCP

リモート入出力装置



縮退運転制御器
（Arduino）

アナログ信号

模擬プラント

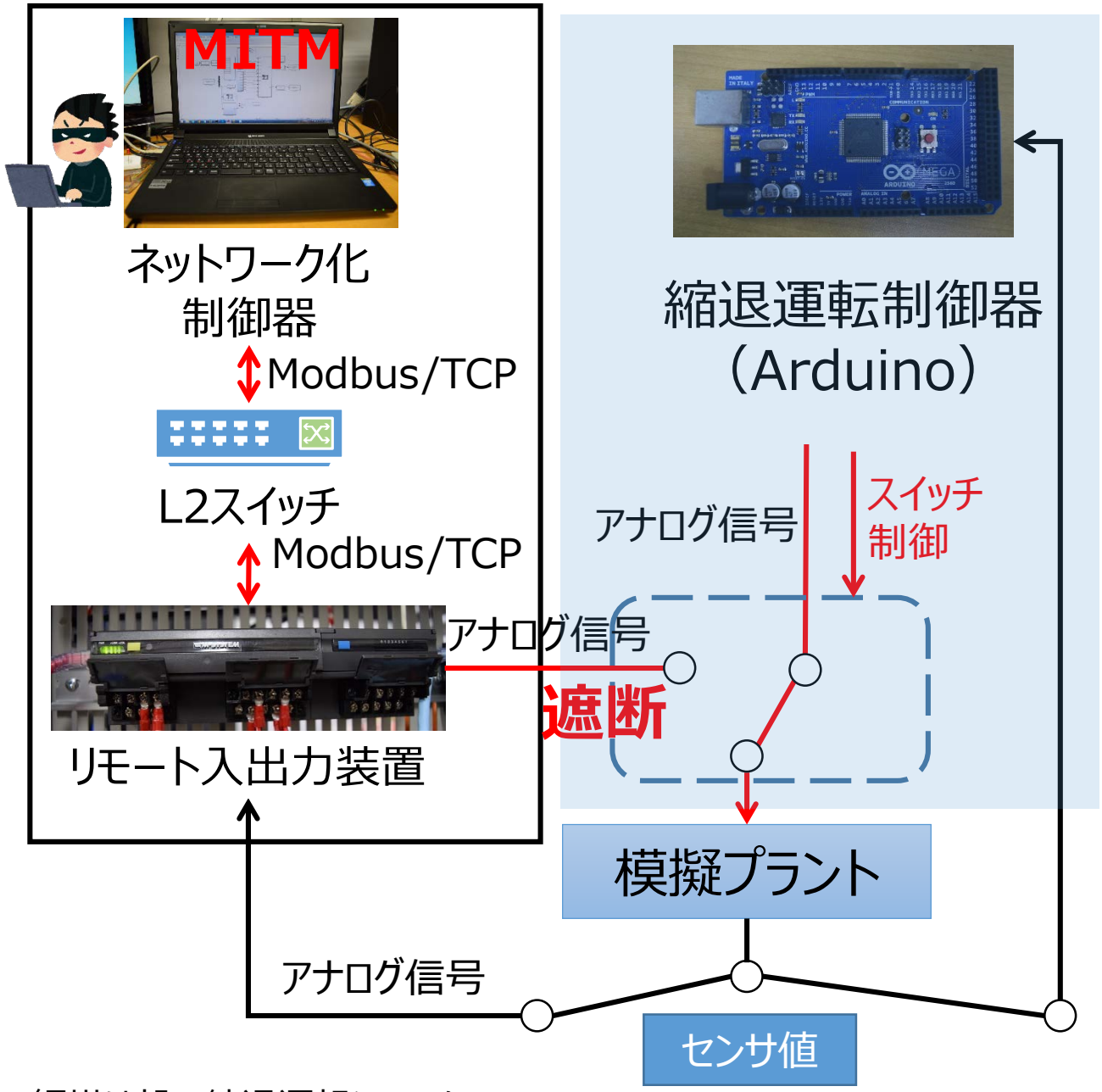
アナログ信号

センサ値

モデルと実システム
振る舞い比較

網掛け部：縮退運転システム

縮退運転切り替え機構（インシデント発生時）



インシデント検出

ネットワーク遮断

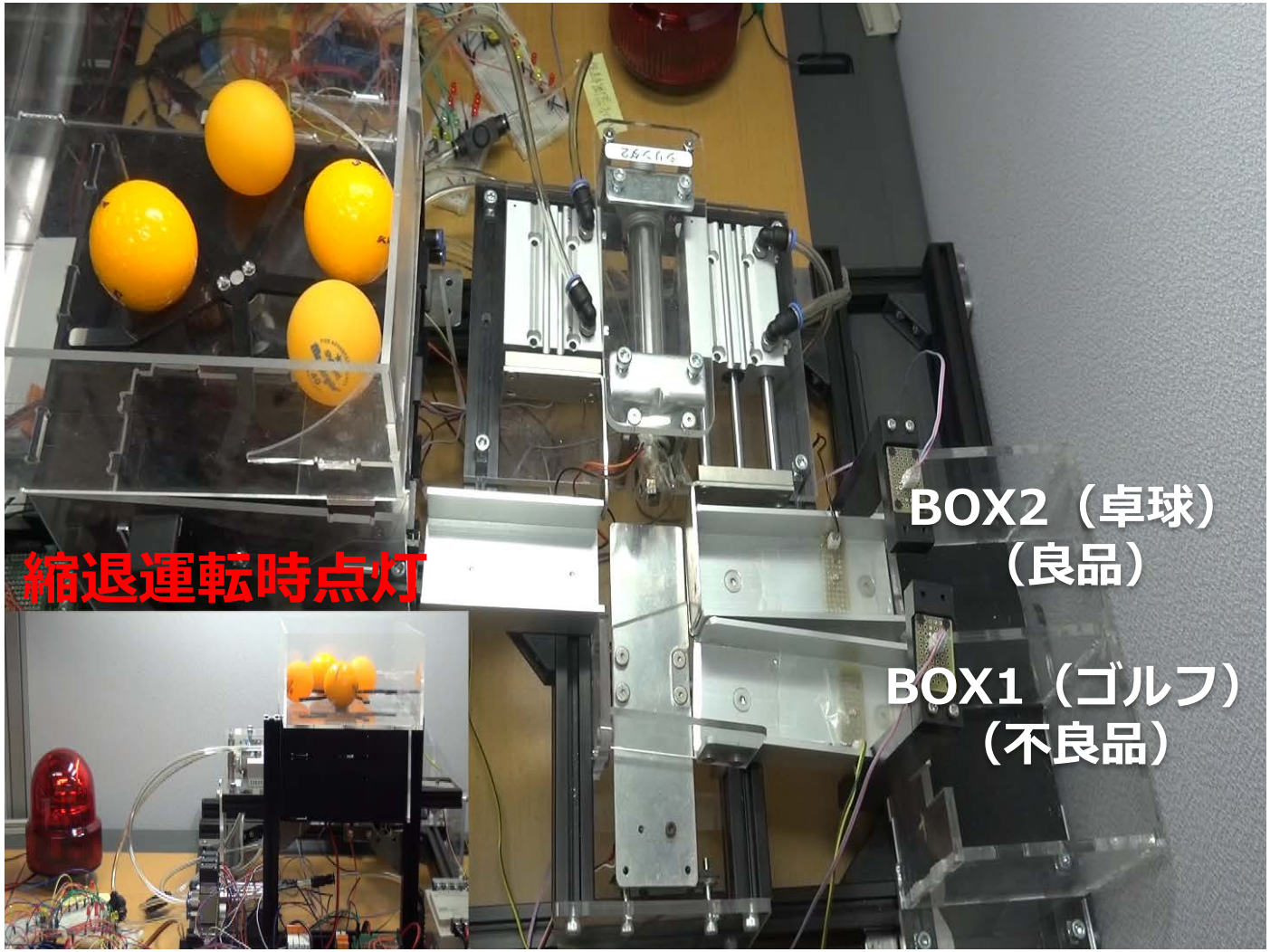
さらに

縮退運転制御器が
非イーサネット接続

サイバー攻撃から隔離

網掛け部：縮退運転システム

実機実験（MITM異常あり）



MITM異常
発生

玉詰まり

縮退運転
切り替え

玉詰まり解消

優先順位:安全側への制御＞ボールの仕分け

縮退運転:全ボール（全製品）をBOX1(不良品)へ

縮退運転における課題

実装面の課題

PLCによる縮退運転システムの実装

PLC: Programmable Logic Controller

運用面の課題

通常運転復帰前の試運転に実プラントを使用しない

縮退運転

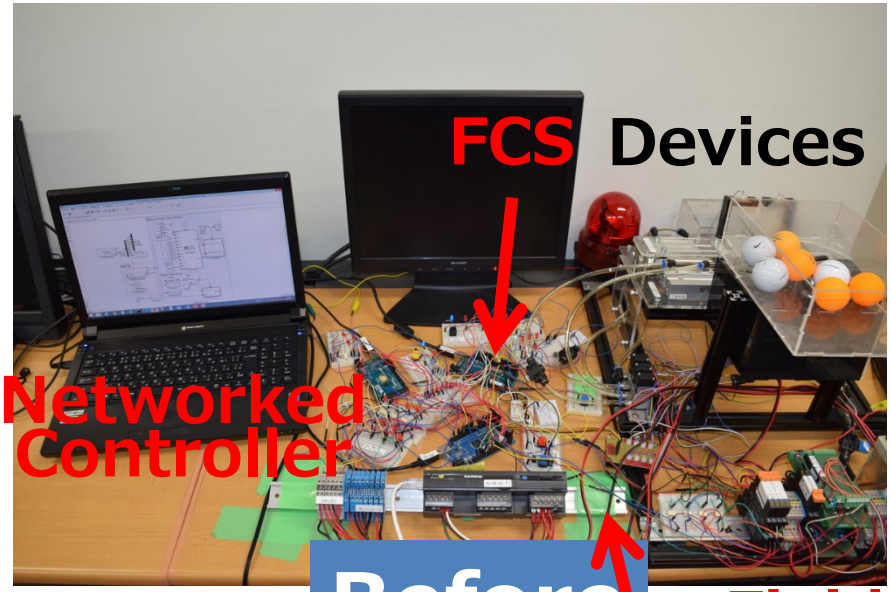
試運転

通常運転

PLCによる縮退運転システム

Proposal

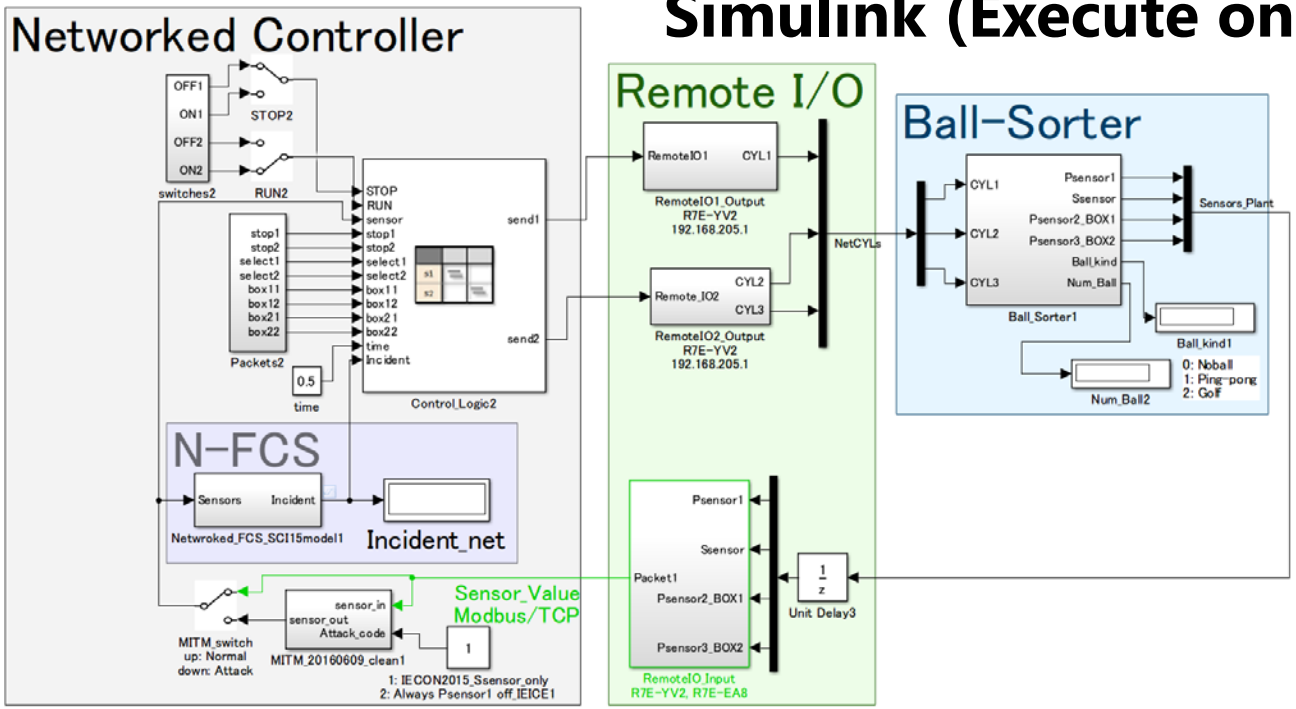
1. **ネットワーク型の縮退運転システム（N-FCS）**
2. **検知条件のモデルベース開発**



伝送系の変更がない.
物理系の変更がない.

検知条件のモデルベース開発

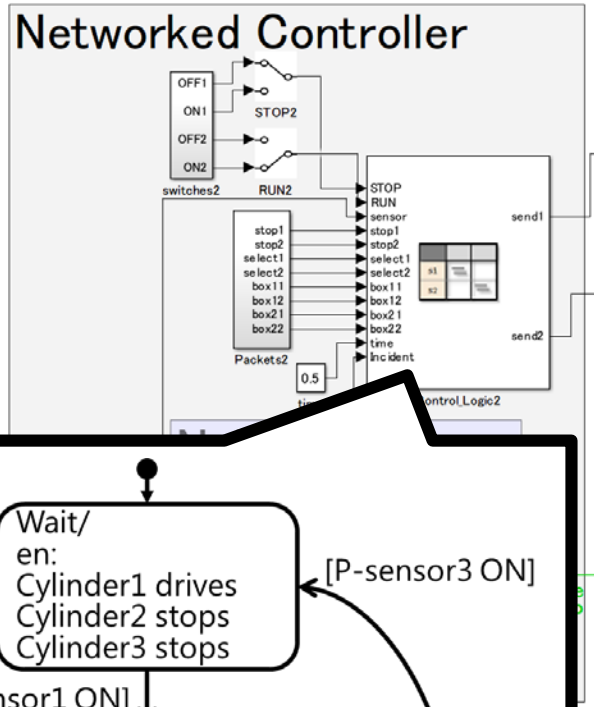
Simulink (Execute on Laptop)

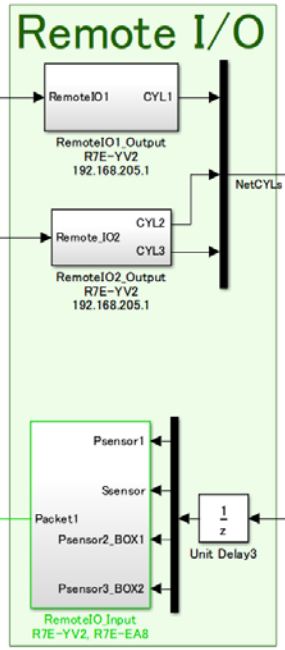


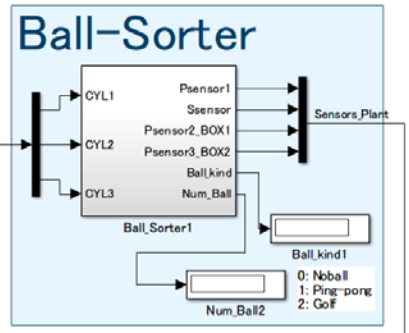
検知条件のモデルベース開発

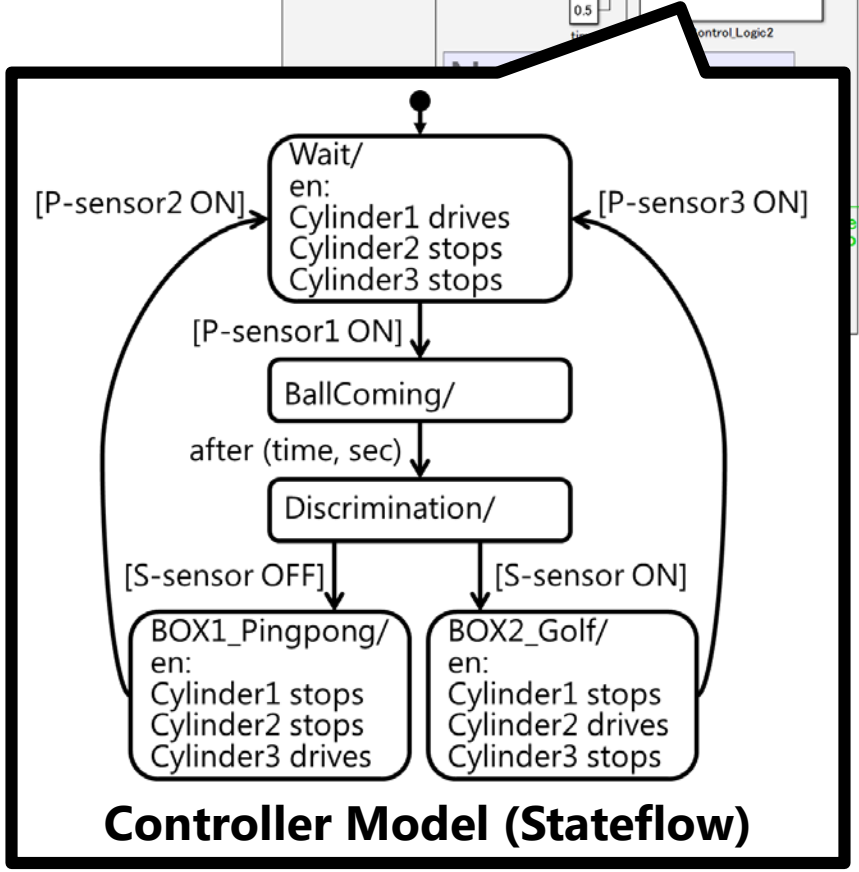
MATLAB SIMULINK

Simulink (Execute on Laptop)

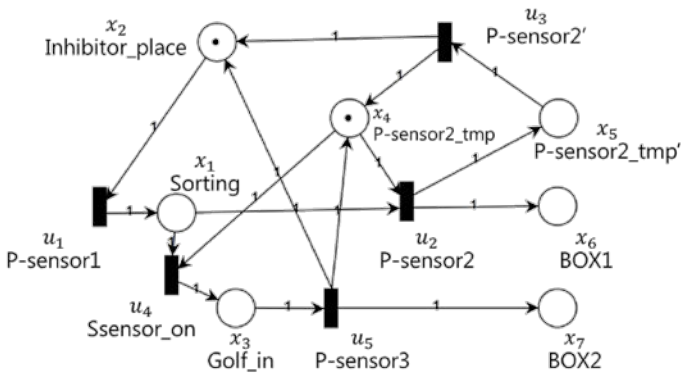








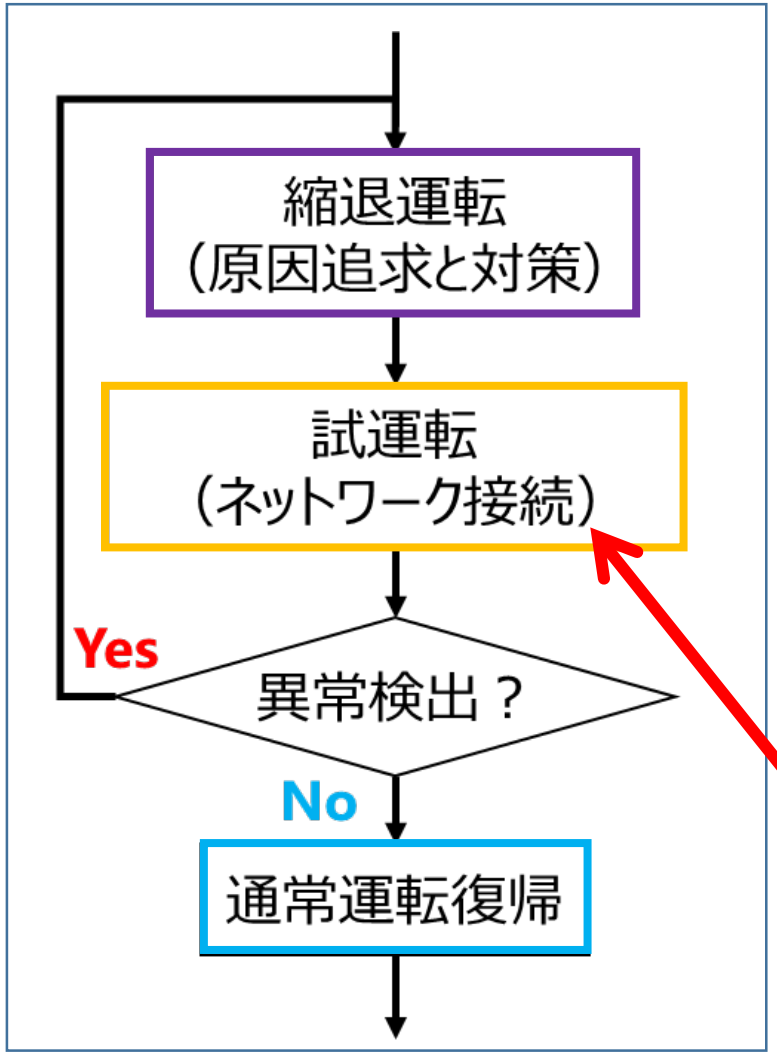
Controller Model (Stateflow)

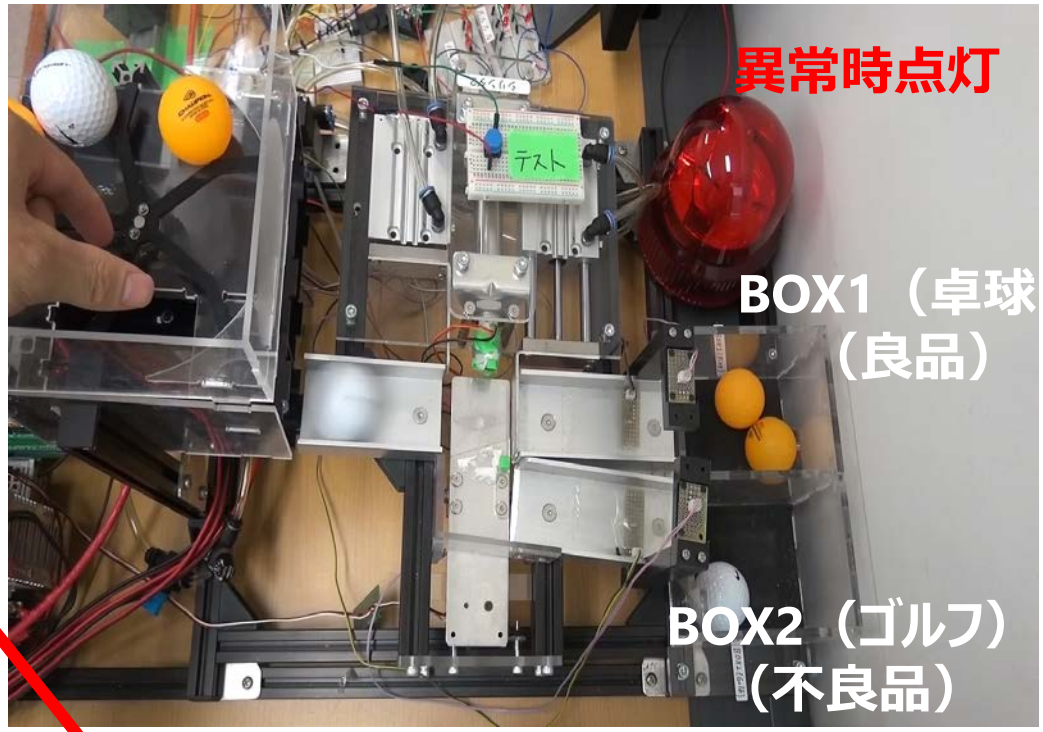


Petri net

PLC用の制御プログラム言語に
変換可能(MSCS2017)

現在の通常運転復帰（実機を用いた試運転）





実プラントをネットワークに
接続しなければならない

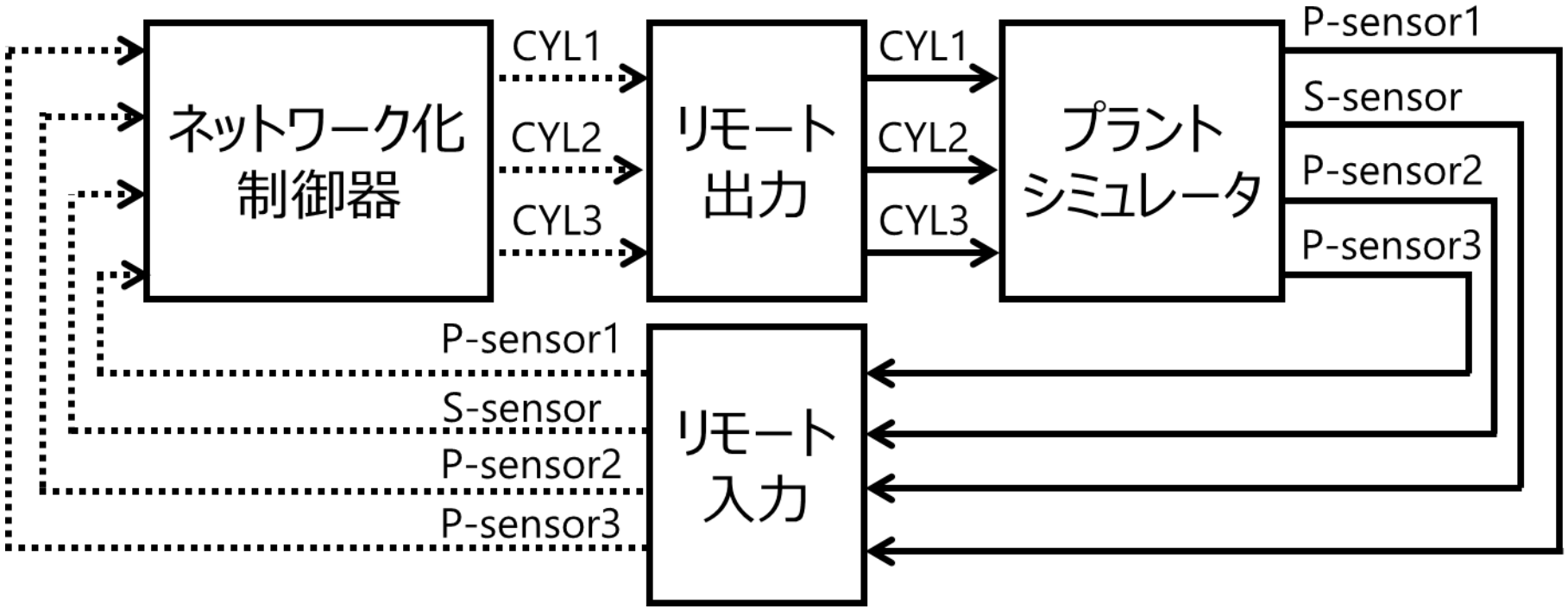
実プラントをネットワークに接続しない
新しい試運転方式がほしい

提案手法

新しい試運転方式
“仮想運転”

仮想運転？

- 実プラントの代わりにプラントシミュレータを使用する試運転

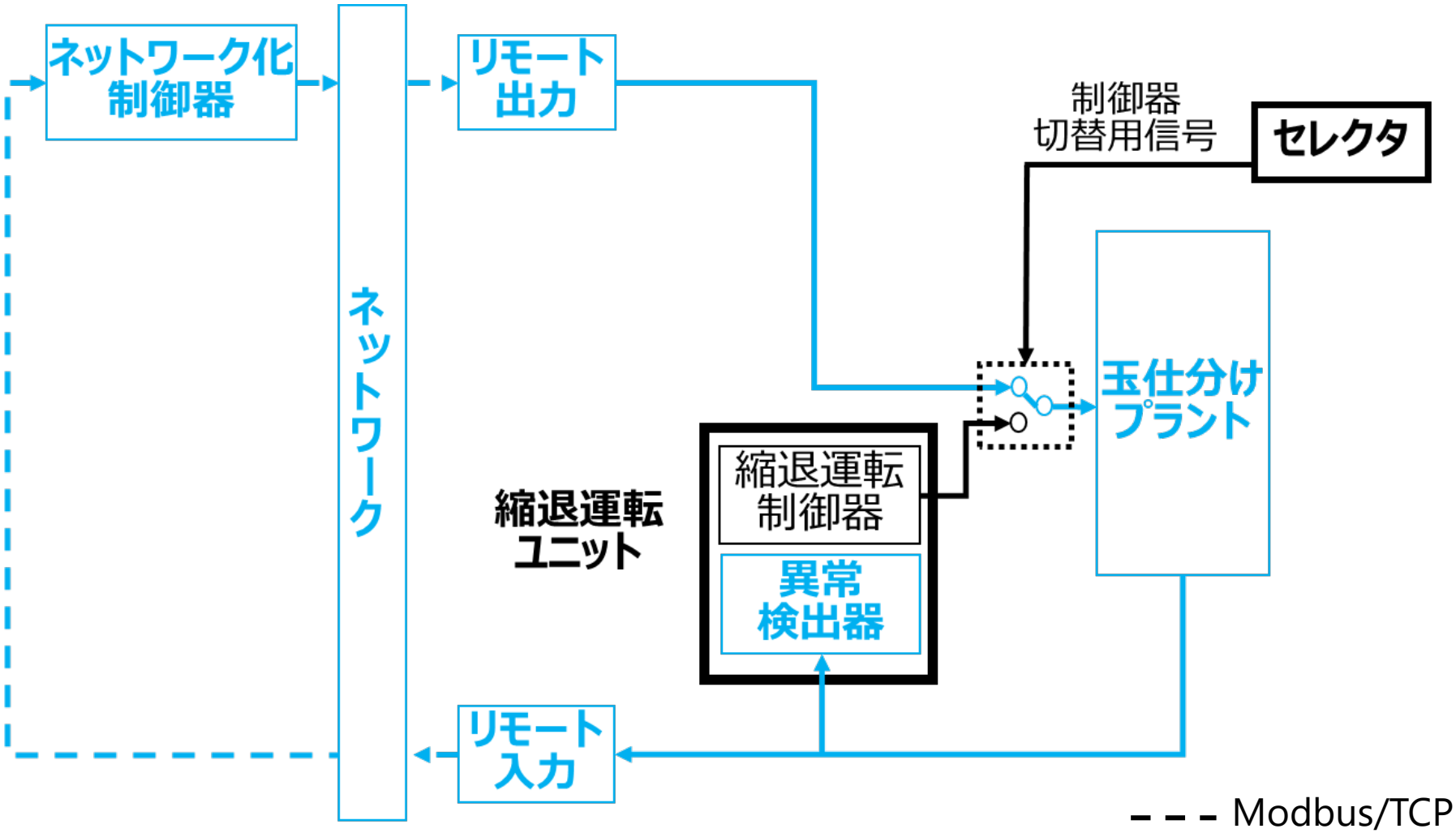


仮想運転による復帰機能付き縮退運転システムを実現する制御系構成とは？

Modbus/TCP

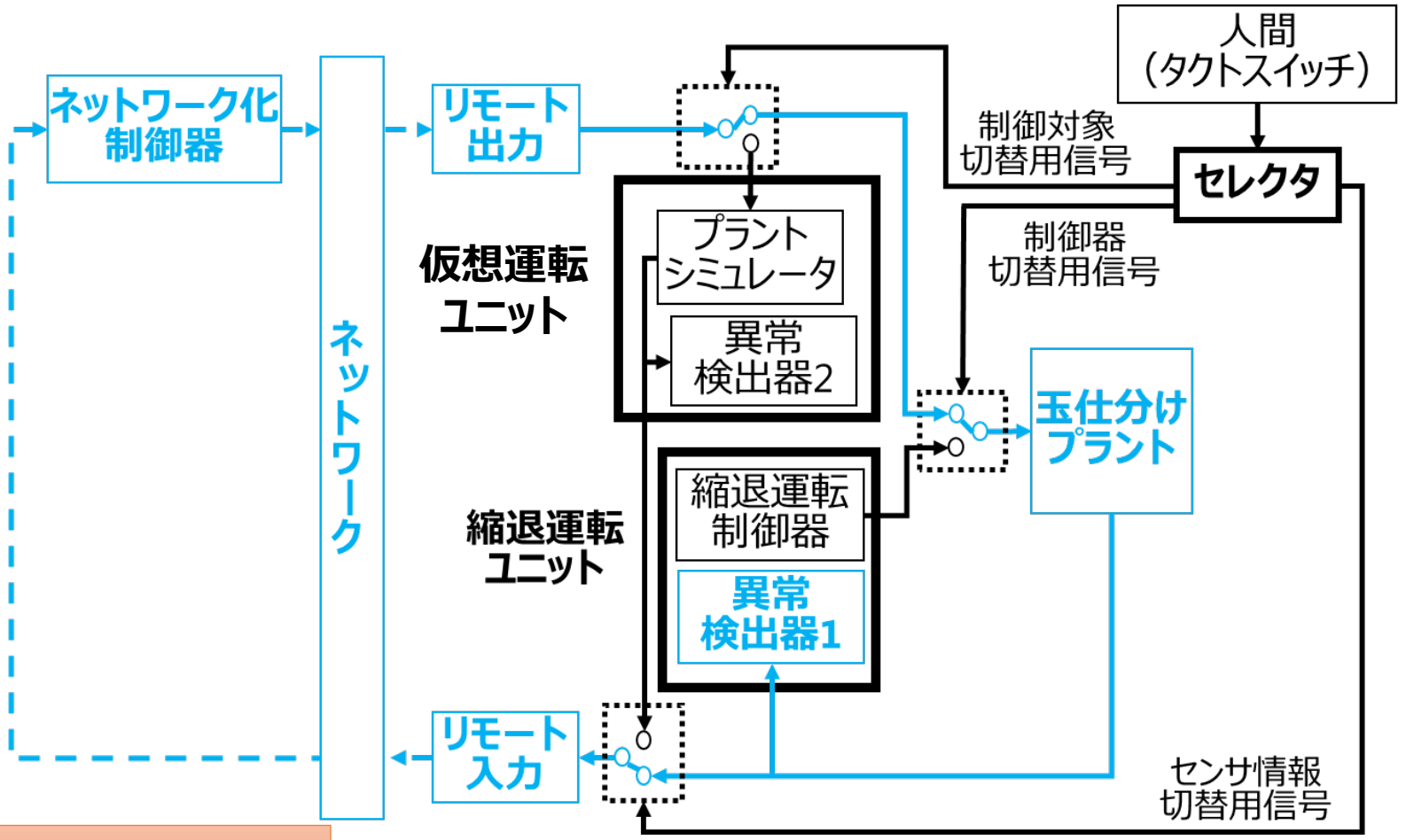
アナログ信号

これまでの制御系（通常運転）



水色：通常運転動作に関係

拡張後の制御系（通常運転）



追加されたもの

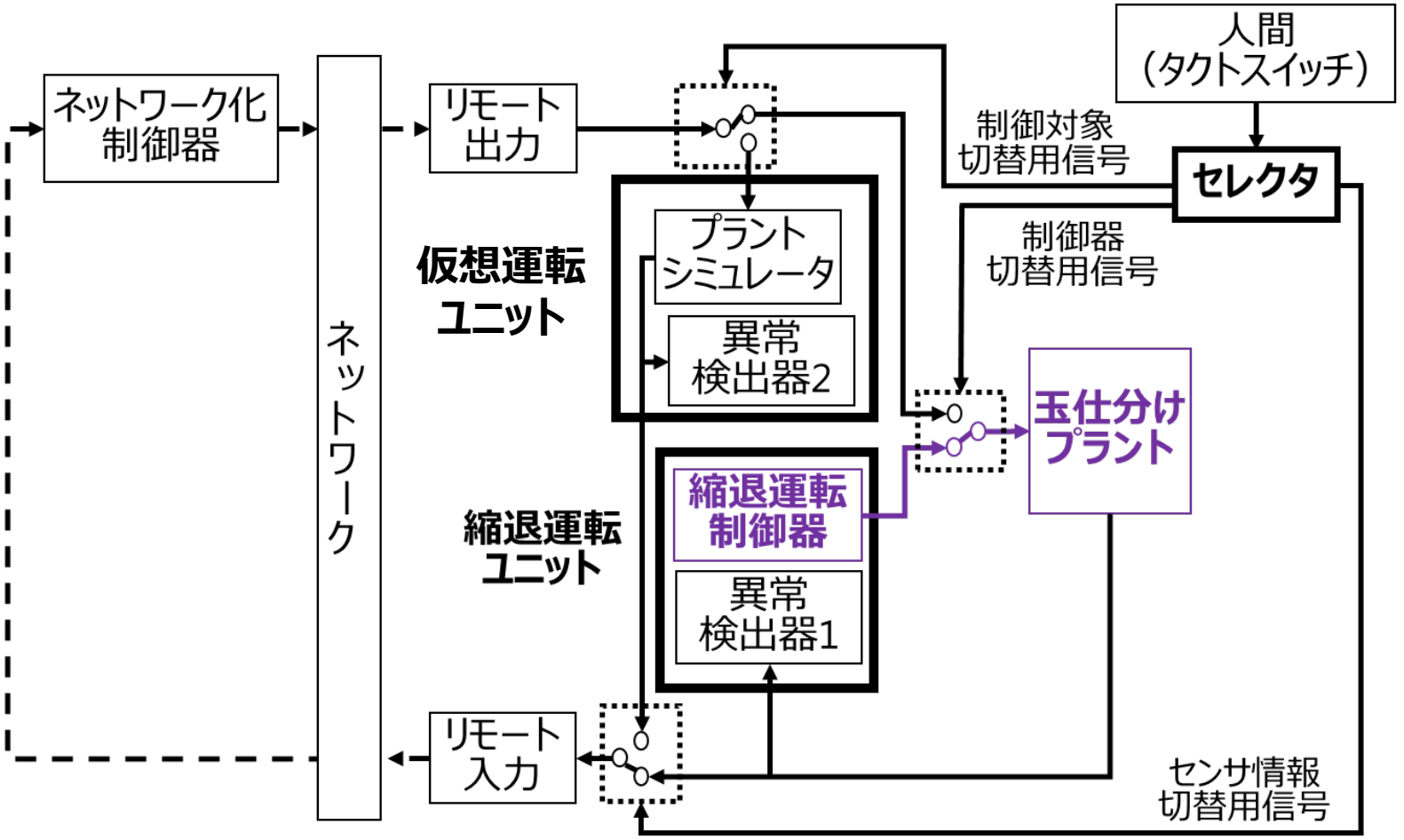
- **仮想運転ユニット**
  - **-プラントシミュレータ，異常検出器2**
- **信号切替用スイッチ×2，人間**

– – – Modbus/TCP

—— アナログ信号

水色：通常運転動作に関係

拡張後の制御系（縮退運転）



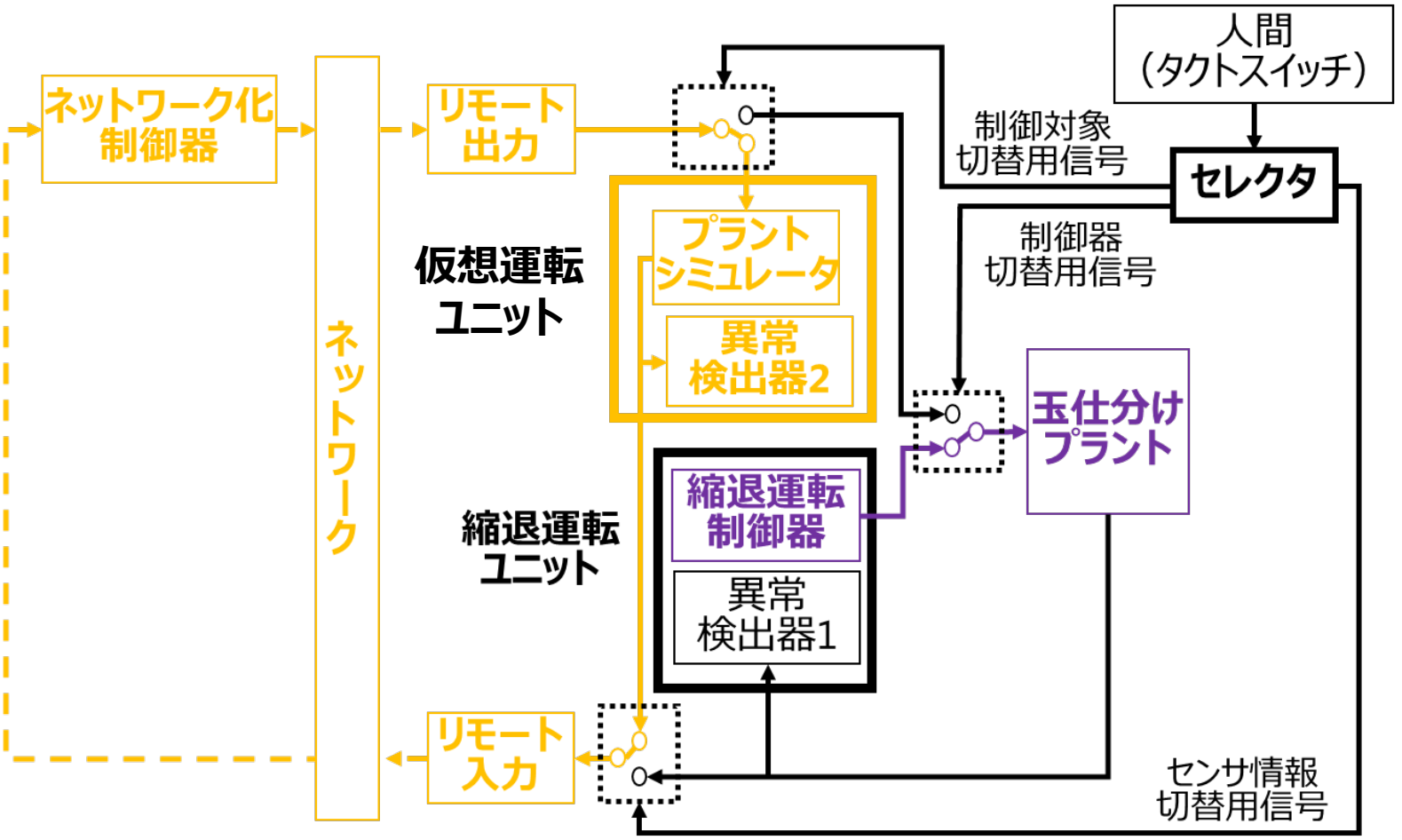
名前	役割
玉仕分けプラント	**縮退運転制御器の制御対象**
プラントシミュレータ	停止状態
異常検出器2	停止状態

- - - Modbus/TCP

—— アナログ信号

紫色：縮退運転動作に関係

拡張後の制御系（仮想運転）



名前	役割
玉仕分けプラント	縮退運転制御器の制御対象
プラントシミュレータ	ネットワーク化制御器の制御対象
異常検出器2	ネットワーク化制御器の健全性確認

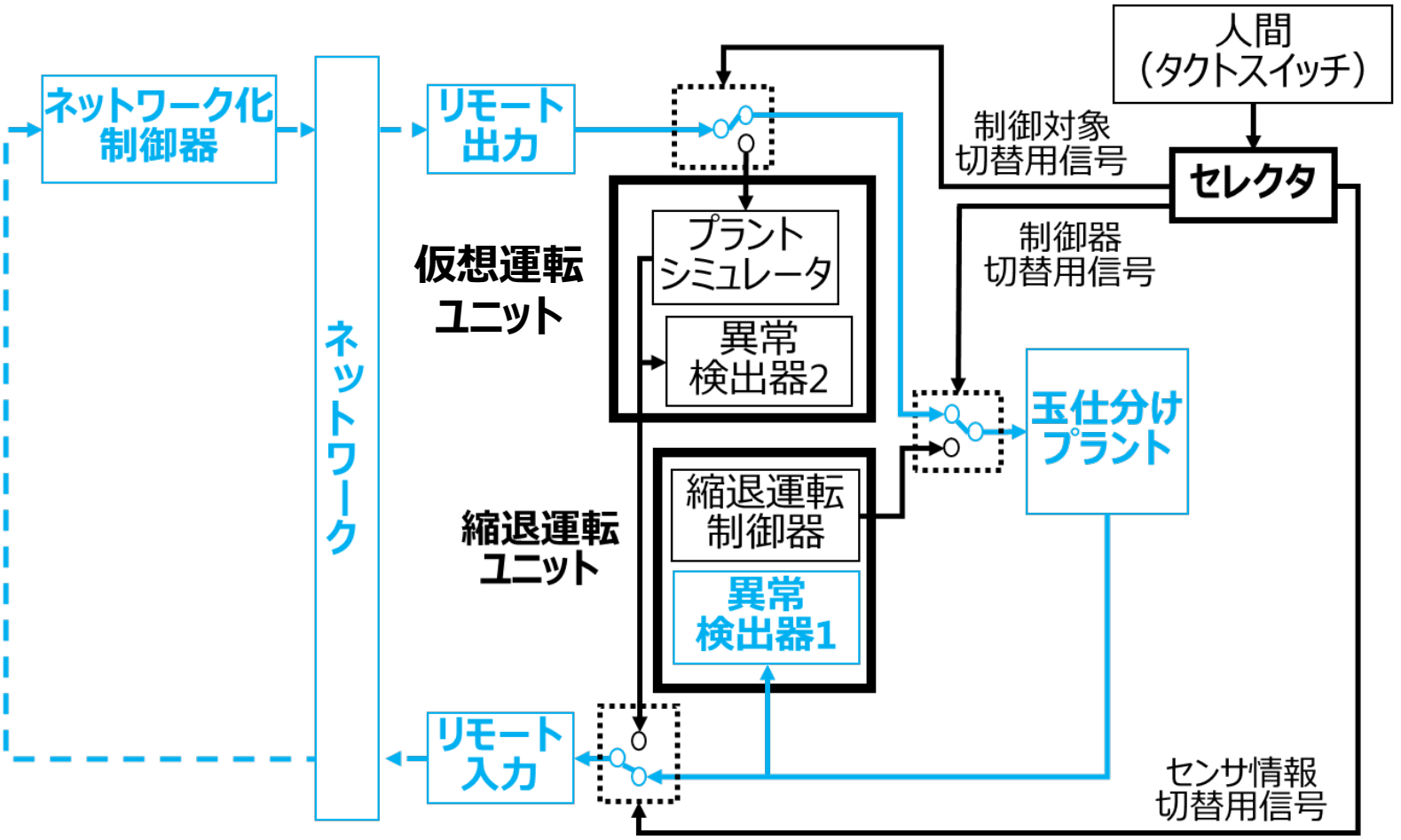
- - - Modbus/TCP

—— アナログ信号

黄色：仮想運転に関係

紫色：縮退運転動作に関係

拡張後の制御系（通常運転復帰）



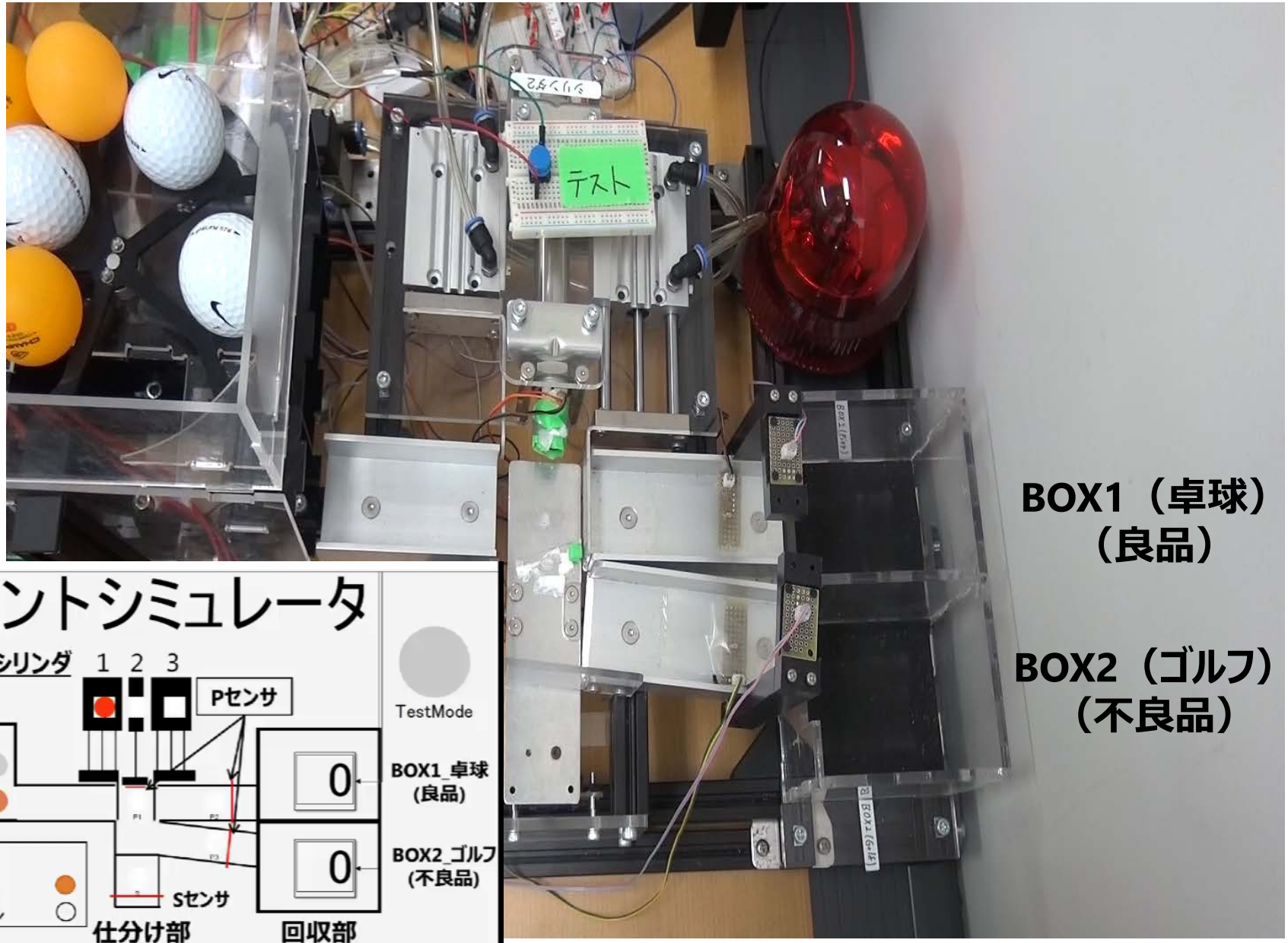
名前	役割
玉仕分けプラント	**ネットワーク化制御器の制御対象**
プラントシミュレータ	停止状態
異常検出器2	停止状態

– – – Modbus/TCP

—— アナログ信号

水色：通常運転動作に関係

実機実験（異常→縮退運転→仮想運転→復帰）



まとめと今後の展開

まとめ

- モデルベースMITM検出手法の提案と実機実装
- 通信制御系に対するモデルベース縮退運転を実現した

今後の展開

- 協調機能付き縮退運転ンシステム（MSCS2017）
- コントローラホワイトリスト（MSCS2017）

- **戦略的イノベーション創造プログラム**（SIP）「重要インフラ等におけるサイバーセキュリティの確保」：2020年オリパラのセキュリティ対策
  - コア技術開発チーム(a3)**「制御・通信機器およびシステムの防御技術」**に電気通信大学として参加
- 日本がコアとなるセキュリティ製品・技術の自給確保を達成し，2020年には国内の各事業者（電気・交通等）が運用できるように基盤を確立.