〈特別研究課題〉　重要インフラに対するサイバー攻撃防御のための
制御ネットワークの開発
助 成 研 究 者　名古屋工業大学　　越島　一郎

重要インフラに対するサイバー攻撃防御のための制御ネットワークの開発

越島　一郎
（名古屋工業大学）

Secured Industrial Control System Network for Defensing Cyber-Attack against Critical Infrastructure

Ichiro Koshijima
(Nagoya Institute of Technology)

Abstract：

Recent serious accidents in Japanese chemical plants occurred in unsteady state operation. In startup and shutdown, the active controllers that need to be monitored are changed according to operation states. In this paper, not only spatial but also temporal zoning are discussed to reduce the possibility of accidents and to improve detection capability of cyber-attacks. Because availability of some parts of the plant might be spoiled in switching communication paths, the security of the switching system is very important. In order to realize dynamic zoning, design method of zoning of controller networks and control method of switching communication which is independent from plant control systems, are proposed. Moreover, an implementation of proposed dynamic zoning using an OpenFlow controller is illustrated.

1. はじめに

制御系システムのサイバーセキュリティの重要性は、2010年Stuxnet登場以来、意識されるようになり、制御システムセキュリティに関する世界標準であるIEC62443に基づく取り組みも進みつつある。また、世界に先駆け日本では産業用オートメーションと制御系(IACS)を対象にしたCyber Security Management System(CSMS)認証が2014年に始まっている[1]。しかしながら、ようやく制御系を対象としたホワイトリストや次世代ゲートウェイなどの対策ツールが提供されるように

なったものの、現状では普及するまでには至っていない。また、重要インフラの制御系システムでは、24時間365日稼働が要求されるため、リアルタイム処理への干渉は排除せざるを得ない。このため、一般的なITシステムに対するセキュリティ対策(煩瑣なアップデート、OSのバージョンアップ、アンチウイルスツールの適用等)は、適用されないのが一般的で、脆弱性を認識したまま運用されているシステムが少なくない。Stuxnetだけでなく、2014年に見つかったOPC(OLE for Process Control：制御システム向けに米国OPC Foundationが策定したアプリケーション間通信インターフェイス)サーバーを対象にしたHAVEXなどmalwareは、OS等が持つ未知の脆弱性を突いたものであり、既知の脆弱性に対して万全な状態であっても、安心できるわけではない。

重要インフラの制御系で最も重要なことは、重大事故を防止するための安全問題である。サイバー攻撃を不安全原因の一つと考えたとき、サイバー攻撃者の行為は「悪意の誤操作、悪意の誤作動(故障)」とみなすことができる。このためIEC62443-3[2]ではサイバー攻撃を局所化するため、フラットなネットワーク構成を避け、制御系ネットワークを複数のサブネットワークに分割するゾーン(制御系システムの機能における論理的、物理的な関係に基づいて、分割された制御システムの集合)とコンジット(共通のセキュリティ要件を保有する二つ以上のゾーン間における通信チャネルの論理的な集合)の考えに基づいたアプローチが提案されている。また、Eric Knapp[3]は実用的なゾーン設定手法として”Secure Enclaves”を提案し、制御系システムが持つ機能を8つのグループに分割して、それぞれの機能ごとに制御系ネットワークを深層防御の考えに基づいて分割することで、攻撃に対する露出を最小限にする手法を提案している。

筆者らも、先行研究においてサイバー攻撃による事故発生を回避するとともに、隠蔽工作下の攻撃も検出するための制御ネットワーク分割方法を提案している[4][5][6]。この分割方法では、制御ネットワークを空間的に分割し、サイバー攻撃の被害を一部分に抑制することで、たとえサイバー攻撃がコントローラやセンサーに到達したとしても重大事故を防ぐことを可能としている。

ただし、従来研究では運転期間の大半を占める定常運転でのサイバー攻撃を想定しているが、最近、日本の化学プラントで連発している重大事故は、スタートアップやシャットダウン等の非定常運転で発生している。また、非定常操作の制御は、バッチプラントや組み立て加工工程の制御にも通じ、より広範な産業システムにおける制御系のサイバーセキュリティ対策につながる研究としても期待できる。このため本論では、非定常運転でのサイバー攻撃にも有効な対策を検討する。

2. 重要インフラにおける非定常運転と制御のための通信ネットワーク

プラントには、大別すると以下の3種の制御システムが組まれている。

正常スタートアップ／シャットダウンのための制御：正常スタートアップ時やシャットダウン時では、予め定めた状態遷移に従って制御弁を開閉するシーケンス制御を組み込むことで、省力化を図っている。

定常運転のための制御：スタートアップ後の運転では、フィードフォワード／フィードバック制御機器のセットポイントを予め定めた値に設定・変更することで、定常運転の確立や運転モード変更の自動化を図っている。

緊急遮断のための制御：異常発生による緊急時にプラントを安全に自動停止するための制御系である。停電や計装空気喪失によって上記２つのプラント運転制御が機能しなくなる

ことも想定して、リレー回路によるハードワイヤ化等によって独立させて設置されることが多い。

スタートアップ時やシャットダウン時の同時多発で多様な操作を考えると、SCADAと接続して管理できると便利だが、そのようなシーケンスコントローラに対する弁の開閉指示などは、通信が必要とされるタイミングが限定的であり、定常運転中は通信を遮断した方が外部からの攻撃による事故を防ぐことができる。またセンサーにおいては、常時通信せずに変化が発生した時のみ通信しても、監視としては十分な場合もありうる。そのため、空間的な制御ネットワークの分割と時間的な通信の分割を組み合わせ、制御ネットワークを動的に切り替える(本論では“動的ゾーニング”と呼ぶ)ことによるセキュリティとセーフティの向上方法を検討する。

現場に設置されたコントローラは可用性が最重要視されるため24時間稼働が求められるものの、コントローラと上位監視系の通信[7]は必ずしも常時ネットワークによって接続されている必要はない。しかし、生産計画に合わせて運転モードを指示するためにはコントローラから運転状況の適時な通信は必要であり、異常の発生時にコントローラからの通信が無ければ異常に気づくことが出来ず安全性に問題が発生する。そのため、必要とされる通信に支障が生ずることは許されず、セキュリティ向上のために通信系に組み込んだ対策が新たな標的になり、必要な通信が阻害されて事故の原因となるのでは本末転倒である。また、せっかくゾーニングによってMalwareの感染範囲を限定したにも拘らず、制御ネットワークを動的に切り替えることで、別の場所も感染可能にするのでは、不安全領域を拡大することになってしまう。そのため、動的ゾーニングの設計には、定常状態における制御ネットワークのゾーニング以上に配慮すべき問題が存在する。

3. 解説に用いるテストベッド

3.1. テストベッド概要

動的ゾーニングは、様々なプラントの非定常運転に利用できるが、本論ではこれまでにもゾーン分割の例に用いていた研究室所有のテストベッドを利用して、スタートアップにおける制御ネットワークのゾーン設計手順と注意点並びに通信制御方法を要説する。

テストベッドの写真を図3-1に、構造図を図3-2に示す。このテストベッドは、下部のTank1で水を温水にして上部Tank2にポンプで揚水して循環させる運転を行う。実際の工業プラントで利用されている制御機器が使用されており、反応系や圧力容器は安全上搭載されていないが、実プラントの要素を多く含んだミニプラントである。

3.2. テストベッドにおけるスタートアップ手順

このテストベッドのスタートアップでは、水圧を検知することで水位を計測する差圧発信機LT1、LT2、圧力発信機PT1とマグネットポンプP1を使用可能とするため、計装配管P-1からP-2内のゴミをフラッシングすると共にLT1、LT2、PT1が正常に機能するために空気溜まりを取り除く必要がある。

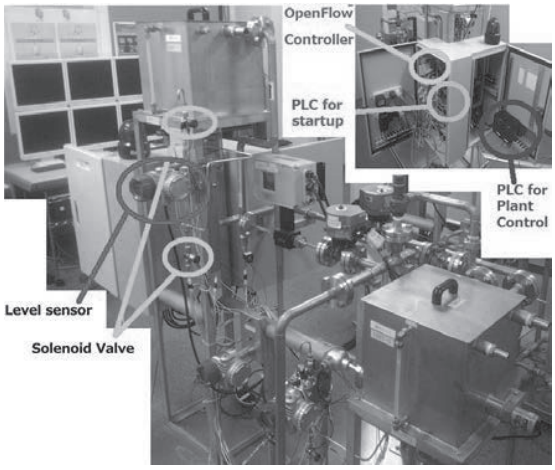

図3-1　テストベッドの写真

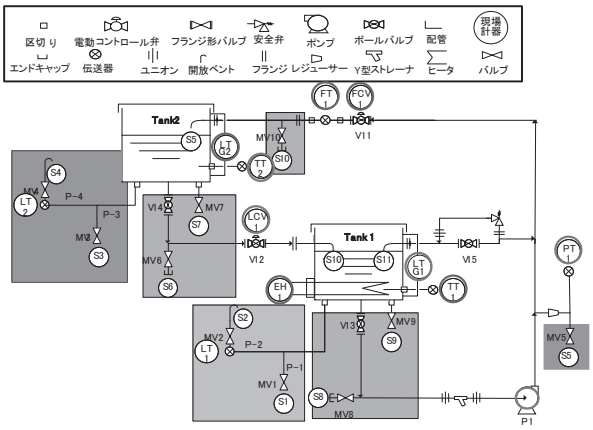

図3-2　テストベッドのPiping & Instrument図

スタート手順は、以下の通りである。

(1) 全ての調節バルブ、電磁弁を閉とし、タンク底の手動弁V13、V14を開く。

(2) Tank1に注水する。

(3) パイプP-1や差圧発信機LT1を使用できる状態にするため電磁弁MV1を開にし、水を流すことでパイプP-1の中にあるごみを取り除く。

(4) 水が流れていることを一定時間センサーS1

(5) で確認した後、MV1を閉とする。

(6) MV2を開にし、パイプP－2の中を水で満たすことで差圧発信機LT1を使用可能にする。

(7) 水が流れていることを一定時間センサーS2

(8) で確認した後、MV2を閉とする。

(9) 循環ラインの手動弁V15を少し開ける。

(10) オペレータがSCADAを通してポンプを起動する。

(11) Tank2へ水をくみ上げるために、SCADAから指示を送り、FCV1を開く。

(12) 手動弁V15を閉める。

(13) オペレータがTank2に水が溜まったと判断したときに、ポンプを一旦停止する。

(14) MV1、MV2と同様の手順でMV3とMV4を操作し、差圧発信機LT2を使用できるようにする。

(15) MV5を開にし、水が流れていることを一定時間センサーS5で確認した後、MV5を閉め、圧力発信機PT1を使用可能とする。

(16) オペレータがSCADAを通してポンプを再起動させる。

(17) SCADAからの指示でFCV1、LCV1のサービスを開始し、定常運転に移行する。

(18) 一般のプラントでは、スタートアップ用の原料の仕込みラインや、後工程に送れない間、運転を継続するための循環ラインが存在し、その仕込みや循環を制御するコントローラも存在する。

このテストベッドでは、スタートアップ時のセンサーの準備操作の電磁弁の動的ゾーニングを検討するため、スタートアップ用のラインの切り替え用の遮断弁やコントローラの操作を行うため、定常運転とは別のPLCを用意し、スタートアップが完了すると、そのPLCへの通信は遮断する構

成としている。これは、スタートアップ用のPLCを複数台用意して、コントローラへのアクセスを制限することで、スタートアップ時に発生する可能性のある重大事故を回避するようにゾーニングを行う構成問題に相当する。

3.3. スタートアップ用制御システム

図3-3に示されるSCADAにより、テストベッドのスタートアップは管理される。このプラントには、プラント運転用のPLCが2台存在し、異質(異なるメーカー、OS・ソフトウエアで構成されたの意)なゲートウェイで構成された異なるゾーンに含まれ、それぞれ図3-3に示される計器を管理している。

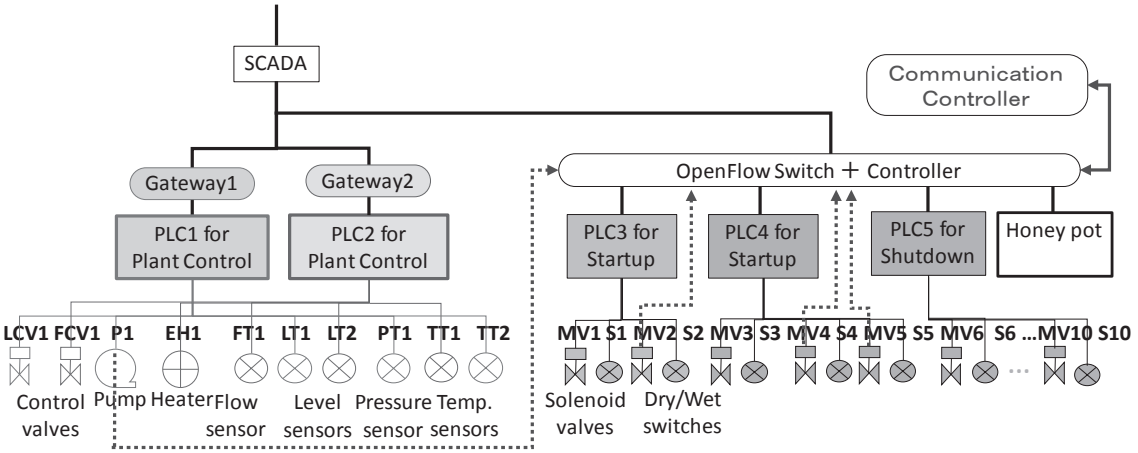

図3-3　自動スタートアップのための計装

プラント運転用のPLC以外に、スタートアップ時のセンサー準備操作用にPLCが2台、シャットダウン時の液抜き操作用にPLCが1台存在する。これらの非定常操作用のPLCは、OpenFlow Switchを介して、SCADAと接続される。このOpenFlow Switchには、Honeypotも接続され、PLCと切り替えて、SCADAと接続することができるようになっている。なお、OpenFlow Controllerは、DI/Oを有するRaspberry PIで実装され、Pumpや電磁弁MV2、MV4、MV5のON/OFF信号が取り入れられるようになっている。

スタートアップ時に必要なセンサー準備操作のシーケンスは、2台のPLCに登録されているが、そのシーケンスを起動する信号は、SCADAから送られ、シーケンスの完了信号がSCADAに送られる。

SCADAとPLCの通信が必要な状態であるかは、図3に示されているCommunication ControllerがOpenFlow Controllerと接続しているセンサーや電磁弁の信号を入手し、遷移中の状態を認識し、通信状態の切り替えが必要と判断すると、OpenFlow Switchの切り替えの指示がOpenFlow Controllerに送られる。また、SCADAとPLCの通信が必要でない場合は、PLCの代わり、Honey Potを接続し、攻撃者が現れると検知してアラームを発報できる構造としている。

本報ではOpenFlow ControllerとSwitchは、NEC社が開発したOpenFlowフレームワークであるTrema[8]を用いて、Raspberry Pi上に実装している。実装では、Tremaプロジェクトのサンプルである“スイッチングハブプログラム”に以下の機能を追加した。

- Communication Controllerからの情報を受け取るFile Server機能
- File Serverがファイルを受信するとその内容にRoute Fileを置き換える機能
- Route Fileの変更を検知し、Route Fileの内容に従ってOpenFlow Controllerに経路変更指示を送る機能
- OpenFlow Controllerが経路変更指示を受け取ると、その内容に従ってネットワーク構成を変更するための“Flow-mod message”をOpenFlow Switchに送信する機能

これらの機能を実現したことで、Communication Controllerから情報を受け取り、その情報をもとにゾーン構成に合わせたネットワーク構成に変更し、さらに通信が不必要な場合には通信経路を遮断することを可能としている。

4. 制御ネットワークのゾーン分割

4.1. セーフティを考慮したゾーン分割

制御システムにおける安全を確保するためのゾーン分割のアプローチとして、筆者らは重大事故をトップ事象としたフォールトツリーを作成し、AND条件にあるコントローラを特定したうえで、それらを別のゾーンに分離するという方法を提案している[4][5]。この手法を適用して先ずはプロセス安全を確保することが必要である。このため、異質なゲートウェイを通じてSCADAに接続したDCSあるいはPLCがゾーン内に存在し、重大事故を回避するという観点で、PLC、コントローラやセンサーのゾーンを選択する。

このテストベッドの場合、PLCが5台存在する。ヒータの過熱事故を重大事故と想定し、図3-3に示されるように、Tank1の液位制御(Gateway1)と温度制御(Gateway2)を別のゾーンに分割している。また、スタートアップとシャットダウンのときにのみ実行する操作用のPLC3台については、OpenFlow Switchを介してSCADAと接続しており、非定常操作の状態遷移に応じて、通信を切り替えることで、セキュリティとセーフティの向上を図る構成としている。

4.2 通信を考慮したゾーン分割

制御指示を伝える通信経路は、その指示が発生する以前に用意されていなければならない。したがって、通信が可能であるように、信号の送信が行われる以前にCommunication Controllerは、OpenFlowにその通信経路を開くように指示しなければならない。この観点から、スタートアップにおける通信タイミングを検討すると、以下の通りである。

LT1の準備操作：　Tank1に水が存在すれば開始できるのだが、Tank1に水があると知らせるべきセンサーであるLT1を利用可能にするための準備操作を始めるので、LT1のセンサーをLT1の準備操作のトリガーにはできない。そのため、この操作のトリガーは、状態の観測ではなく、外部(SCADA)からの開始指示となる。そのため、スタートアップのために、Communication Controllerを立ち上げた時点で、LT1をつなぐPLCとSCADA間の通信経路を開いておくことにする。したがって、LT1の準備操作の開始指示は、その開いている通信路を介して、SCADAからPLCに送られ、そのPLCに登録されているセンサーの準備操作が実行され、完了とともに、PLCからSCADAに完了信号が送られる。

LT2の準備操作：　LT2の準備操作も、Tank2に水が存在すれば開始できるのだが、Tank2に水が

あると知らせるべきセンサーであるLT2を利用可能にするための準備操作であるので、LT2のセンサー値を準備操作のトリガーにすることはできないのは、LT1の場合と同様である。前述のスタートアップ手順では、Tank1にまず水を充填し、その後、ポンプによりTank2に水が送られることになっている。そのため、Tank1の水位がある程度下がることで、Tank2の水があるはずと推測することもできるし、ポンプを稼働して時間がたてば、Tank2に水が送られているはずと考えることもできる。または、オペレータがTank2に水が溜まっていることを目視で確認して、SCADAからLT2の準備操作のトリガーを送ることも考えられる。このように、LT2の準備操作のトリガーをどのように定めるかは、一意に定まらないが、そのトリガーの信号は、SCADAからLT2が接続されているPLCに送られ、PLCに登録されたセンサーの準備操作が実行され、完了すると、PLCからSCADAに完了信号が送られる。

Pumpの準備操作：　準備操作の開始信号発生前の段階で、OpenFlow Controllerで観測できる情報を用いて通信経路準備の指示を発生すると、Tank2に水を送り出す操作に関する観測信号が候補になる。もちろん、LT1の準備操作の通信と同様に、スタートアップ操作開始前に行っても可能である。できるだけ、必要な時にだけで通信経路を開けておくという方針で考えると、Pumpの起動信号の観測が挙げられる。前述のスタートアップ手順では、ポンプは起動後、Tank2に水が入ったのち、一旦停止するため、ポンプがONのときという表現ではなく、トリガーはPumpがOFFからONに変わる瞬間に発信され、またOFFになったのちは、ONに変わっても発信しないことになる。

PT1の準備操作：　PT1は、ポンプが起動すると、PT1の導圧管の前に水が流れ、準備操作が可能になる。前述のスタートアップ手順では、ポンプは一旦停止、その後再起動されることになっている。PT1の準備操作のトリガーとして、何を選択するかで、通信経路の準備のトリガーの選択が左右される。前述のスタートアップ手順では、Tank2に水が溜まった時点で、ポンプを停止し、その後、PT1の準備操作を行っている。そのため、LT1と同様にポンプが停止したことをPT1の準備操作のトリガーにすることが考えられる。そして、その時点以前に、PT1が接続されるPLCとの通信経路を開いておけばよい。

LT1の準備操作は最初にTank1に水が充填されるとともに可能になるが、PT1とLT2の準備操作は、いずれもTank1から水を抜き出さないと開始できない。そのため、２つのPLCに分離して登録する場合、通信が必要な時間の共通性が高いPT1とLT2は同じPLC、LT1は別のPLCに登録するようにゾーン分けすることにする。

今回は、シャットダウン時における動的ゾーニングは検討せず、シャットダウンのみに利用される電磁弁は、残りの一つのPLCにまとめる。さらに、そのPLCに関係する弁が、サイバー攻撃で、あるいは誤操作で開いてしまうと、漏洩事故が発生するので、シャットダウン操作時以外には、そのPLCとSCADAの通信は遮断しておくものとする。

5. 通信の切り替えと制御シーケンス

5.1. スタートアップでの通信タイミング

表5-1に、スタートアップ時のオペレータの手動操作、SCADAでの操作、PLCでのセンサー準備操作と開始指示や完了報告に必要な通信の期間を示している。表中の矢印は、イベントの前後関係を示していて、通信のトリガーの列には、各センサーの準備操作のための通信のトリガーとして適切なタイミングに○、○よりは適時性は劣るが利用可能ではあるタイミングには△をつけた。起動時○は、外部からのトリガーではなく、Commination ControllerがOpenFlow Switchを起動するときにまず、その通信経路を開くことを示している。

表5-1には、二通りのスタートアップの仕方を示した。どちらもセンサーの準備操作を行い、定常状態に到達できる手順である。スタートアップ手順(A)は前述のスタートアップ手順を示し、スタートアップ手順(B)はポンプの停止、再起動を行わないより簡略した手順である。このようなスタートアップ手順の変更がオペレータによりなされたとしても、センサー準備操作用のPLCや通信を管理するCommunication Controllerは何も変更する必要なく実行することが望まれる。そのために必要なPLCでのシーケンスアルゴリズムと通信の制御アルゴリズムの設計について考える。

表5-1　スタートアップ時の状態遷移と通信の必要性

スタートアップ手順（A）

オペレータ		センサ準備操作用コントローラ			通信制御トリガ候補		通信経路の必要性		
（手動）	（SCADA）	PLC（LT1）	PLC(LT2)	PLC(PT1)	開始トリガ	終了トリガ	(LT1)	(LT2)	(PT1)
Tank1水充填					起動時○				
	開始指示				△ △				
循環弁V18開		LT1開始							
	ポンプ起動	LT1完了			△ △	○			
	FCV1を開く				△ △				
循環弁V18閉									
Tank2液位目視確認									
	ポンプ停止				○ ○				
			LT2開始	PT1開始					
			LT2完了	PT1完了					
	LC1,FC1起動					○ ○			

スタートアップ手順（B）

オペレータ		センサ準備操作用コントローラ			通信制御トリガ候補		通信経路の必要性		
（手動）	（SCADA）	PLC（LT1）	PLC(LT2)	PLC(PT1)	開始トリガ	終了トリガ	(LT1)	(LT2)	(PT1)
Tank1水充填					起動時○				
	開始指示				△				
		LT1開始							
	FC1起動	LT1完了			○	○			
	ポンプ起動				○ △				
	LT1減少確認			PT1開始					
			LT2開始	PT1完了		○			
	LC1起動		LT2完了			○			

5.2. 通信切り替え条件の設定と制御シーケンス

通信が必要な時に、通信経路が遮断されてしまっては、プラントの可用性、安全性を損なうことになりかねない。SCADAとPLCとの通信はOpenFlow Controllerを用いてCommunication Controllerが切り替えるが、OpenFlow Controllerのサイバー攻撃に対する防御が、SCADAやPLCと同様なものであるのならば、安全性が向上するのではなく、可用性が失われる確率を高めることになってしまう。少なくとも、SCADAやPLCのネットワークからは完全独立なものである必要がある。

そのため、SCADAとPLCの通信の必要性を、外部からの通信ではなく、独自の入力により識別

することを考えた。OpenFlowは、DI/OとA/D変換器をもつシングルボードPC(Raspberry Pi)に実装した。(図5-1参照)そのため、スタートアップ用のPLCに接続されている電磁弁の開閉信号、水センサーの信号も、電圧信号としてDIポートから取り入れることができる。この電圧信号は、サイバー攻撃があったとしても実際のプラントの状態を示すものであり、改竄や隠蔽を受けることはない。これらの信号を用いて、SCADAとPLC間の通信を制御するため、スタートアップ中のPLCが実現すべき電磁弁と水センサーの状態と通信の必要性を表5-2のように整理した。

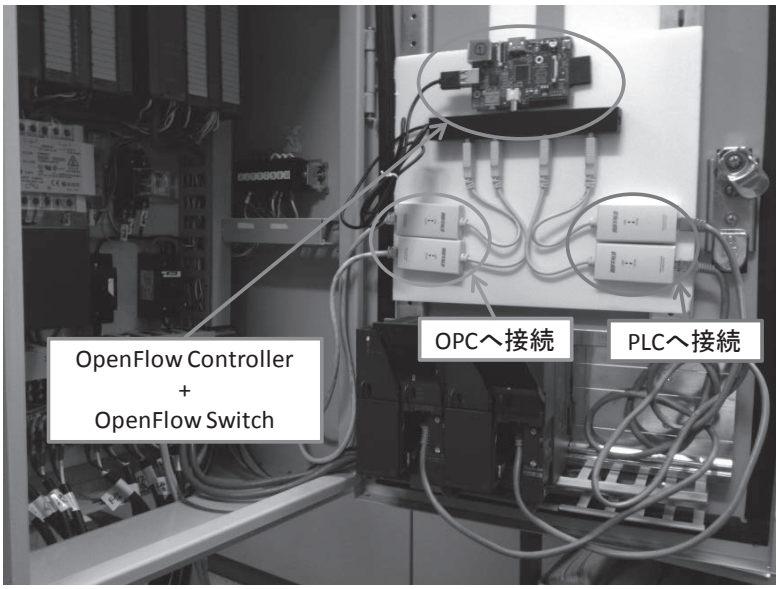

図5-1　OpenFlow Controller

表5-2　センサー準備操作のシーケンス

センサ準備操作手順	SCADAとの通信の必要性	LT1			
		MV1	S1	MV2	S2
LT1準備指示	○	×	×	×	×
水導入開始	×	○	×	×	×
水排出	×	○	○	×	×
水排出完了	×	×	○	×	×
気泡抜き開始	×	×	○	○	×
気泡抜き	×	×	○	○	○
気泡抜き完了	×	×	○	×	○
完了報告	○	×	○	×	○

センサ準備操作手順	SCADAとの通信の必要性	LT2			
		MV3	S3	MV4	S4
LT2準備指示	○	×	×	×	×
水導入開始	×	○	×	×	×
水排出	×	○	○	×	×
水排出完了	×	×	○	×	×
気泡抜き開始	×	×	○	○	×
気泡抜き	×	×	○	○	○
気泡抜き完了	×	×	○	×	○
完了報告	○	×	○	×	○

センサ準備操作手順	SCADAとの通信の必要性	PT1	
		MV10	S10
PT1準備指示	○	×	×
水導入開始	×	○	×
水排出	×	○	○
水排出完了	×	×	○
完了報告	○	×	○

各PLCは、センサー準備操作の開始指示の信号をSCADAから受けることができれば、以降は通信の必要はなく、完了した時に、完了をSCADAに伝えられればよい。通信を許す期間をできるだけ短くするためには、開始信号を受け取れば、まず通信を遮断して、完了信号を送りたくなったら、通信経路を開けて、完了信号を送ると、また閉じるという通信制御も考えられる。ただし、通信経路は通信が必要となる前に開けておく必要がある。そのため、ここでは、開始指示を受ける前に、通信経路を開き、完了報告の後に遮断するというアルゴリズムを検討することにした。

表5-1から、どちらのスタートアップ手順でも共通に利用できる開始トリガーを探すと、LT1の制御を行うPLC3に対する通信経路は、状態によるトリガーではなく、スタートアップ開始前にOpenFlow Controllerを起動するときに、初期設定として通信経路を開いておくということになる。LT2とPT1の二つを制御するPLC4については、スタートアップ手順(B)ではポンプを停止しないので、PLC4への通信経路を開くのは、ポンプを起動したときということになる。

通信の遮断については、LT1用のPLC3の通信は、センサー準備操作の最後の操作であるMV2が開から閉になる瞬間をトリガーとしてPLCからSCADAへの信号の送出が完了するのに十分な時間を待って、遮断されるものとする。LT2とPT1の二つを管理するPLC4は、２つのセンサー準備操作の最後の操作であるMV4とMV5が共に開から閉になったのを確認してさらに、PLCからSCADAへの信号の送出が完了するのに十分な時間を待って、OpenFlow Controllerに通信の遮断を指示する。

前述のように、SCADAとの通信を開始信号を受け取って、一旦遮断し、完了前に、再開することも考えられるが、そのためには、PLC内でのシーケンスを詳細に理解し、通信を制御することが必要になり、SCADAやPLCと独立に管理すべきCommunication Controllerのアルゴリズムが PLCでのシーケンスの実行と同等の多くの信号を要した複雑なものになってしまう。そのため、通信のコントローラの保全等の管理を考えると得策とは考えにくい。

OpenFlowは切り替える機器のIPアドレスが同一でも支障はないという特徴をもっているため、テストベッドでは、PLCとの通信が必要がないときには、ハニーポット[9]と切り替えて、PLCを偽装し、もし侵入してくる攻撃が検知されれば、そのアクセスしてきているアドレスを特定し、Cyber-Incident Response Team(CIRT)に報告するとともに、相手の手口を探るという罠を仕掛けている。

6. 動的ゾーニングの設計手順

以上、事例を通して説明してきた動的ゾーニングの設計の手順を整理すると、以下のように表せる。

(1) 非定常操作における状態遷移をコントローラの状態とその実現に必要な通信という形で、表1のように整理する。

(2) 遷移する各状態に対して、すでに提案している手法を適用して[4]、[6]、安全を考慮したコントローラのゾーン分割を設計する。

(3) 各状態遷移に対するゾーン分割結果に対して共通性を検討し、できるだけPLCとコントローラの組み合わせが固定となる組を選択する。

(4) 各状態遷移により、PLCへの配置を変更した方が安全性向上に有効なコントローラについ

ては、動的にPLCとコントローラの組み合わせの変更が可能なメカニズムの導入を検討する。

(5) PLCとコントローラの組み合わせを動的に切り替える場合、その通信を切り替えるトリガーとできるセンサーや電磁弁のデジタル信号を選択し、そのコントローラの切り替えアルゴリズムを設計する。

(6) 各PLCで、表2に示すように、SCADAから開始信号を受けると、できるだけSCADAとの通信を必要とせずに操作を実施でき、操作が完了すると報告信号を送信して終了するというシーケンス設計する。

(7) PLCとSCADAの通信を切り替えるためのトリガーになる信号を、表1を基に決定し、その信号の観測を基にしたCommunication Controller用の通信切り替えアルゴリズムを設計する。

動的ゾーニングには、様々な課題がある。SCADAからの限られた指示によって、複数のPLCが独立なシーケンスを実行することで、スタートアップが実現できるように、スタートアップ手順を分解する必要がある。さらに、そのSCADAからの通信が確実に行えるための通信経路開通タイミングを、OpenFlow controllerのDI/Oの情報だけから、適切に決定するための、DI/Oに接続するセンサーやアクチュエータの選択と、そのトリガー信号の決定を行わなければならない。

空間的なゾーン分割については、設計用のCAD[6]を開発している。しかし、対象が大規模になると、動的ゾーニングを支援するCADが必要になる。プラントが大規模になれば、スタートアップ手順のバリエーションの数も多くなる。手順の異なるスタートアップにも、可用性が損なわれないことが保証できるように、PLCのシーケンスと通信制御のアルゴリズムを開発するのは、容易ではない。しかし、表5-1や表5-2の整理を大規模プラントに対しても行えば、利用するスタートアップ手順のバリエーションを限定することで、動的ゾーニングが可能になると期待できる。

7. おわりに

従来の手法では、固定的な状況における、空間上(物理的、論理的)でのゾーン設定が行われてきた。これに対し本報では、新たに動的ゾーニング手法を提案し、動的ゾーニングによる通信管制システムのプロトタイプに実装した。この手法では、時間軸上でのゾーニングが可能になる。人間が直接制御するのではなく、機械が制御している制御システムだからこそ、状況が変化していくことを把握しやすいため、時間軸上でのゾーニングは非常に有効であると考える。

さらに、時間軸上で制御系システムが変化していくことで、攻撃者にとっては状況を把握することが困難になり、さらに、ハニーポットという罠に切り替えることで、検知能力も向上し、サイバー攻撃による重大事故発生のリスクを低減させることが可能になると考える。このようにして、出来る限り攻撃者が意のままに行動できるフリータイムを無駄に使わせることで、防御者側に時間的な余裕が生まれ、筆者らが開発している制御システムセキュリティ演習プログラム[10]も効力を発揮すると考える。

8. 謝辞

積極的に協力かつ共同で本研究を推進して頂いた名古屋工業大学制御システムセキュリティグループの橋本芳宏教授、渡辺研司教授並びに両研究室の所属員に感謝の意を表します。

9. 参考文献

[1] cyber security management systems (CSMS)
http://www.meti.go.jp/press/2014/04/20140425003/20140425003.html

[2] International Society of Automation, ISA-62443-4-2, D4E6, 2013.

[3] E. Knapp, Industrial Network Security, Syngress, 2011.

[4] Y. Hashimoto, et al. Safety securing approach against cyber-attacks for process control system, International Journal of Computers and Chemical Engineering, Vol. 57, pp. 181-186, 2013.

[5] T. Morita, et al., Detection of Cyber-Attacks with Zone Dividing and PCA, Proceedings of Procedia Computer Science, Vol. 22, pp. 727-736, 2013.

[6] H. Moritani, et al., Development of CAD for Zone Dividing of Process Control Networks to Improve Cyber Security, Proceedings of 14th International Conference on Control, Automation and Systems, 2014.

[7] M. Matta, et al., Industrial Control System Monitoring based on Communication Profile, Journal of Chemical Engineering of Japan, vol.48, No.8, pp.609-618, 2016.

[8] 高宮 安仁, 鈴木 一哉, クラウド時代のネットワーク技術OpenFlow 実践入門, 技術評論社, 2013.

[9] H. Naruoka, et al., ICS Honeypot System (CamouflageNet) Based on Attacker's Human Factors, Procedia Manufacturing, pp. 1074-1081, 2015.

[10] T. Aoyama, et al., Studying Resilient Cyber Incident Management from Large-scale Cyber Security Training, Proc. of The 10th Asian Control Conference 2015, pp.2890-2893, 2015.