オペレータ介在による加速器機器遠隔制御システムの開発

DEVELOPMENT OF OPERATOR INTERVENING SYSTEM FOR REMOTE ACCELERATOR DIAGNOSTICS AND SUPPORT

内山暁仁[#, A), B)], 古川和朗[c)], 日暮祥英[B)], 中川孝秀[B)]
Akito Uchiyama [#, A), B)], Kazuro Furukawa[c)], Yoshihide Higurashi[B)], Takahide Nakagawa[B)]
[A)] The Graduate University for Advanced Studies (SOKENDAI)
[B)] RIKEN Nishina Center
[c)] High Energy Accelerator Research Organization (KEK)

Abstract

In a large experimental physics project such as LHC and ITER, the project is managed by an international collaboration. Similarly, ILC (International Linear Collider) as next generation project will be started by a collaboration of many institutes from three regions. After the collaborative construction, any collaborators except a host country will need to have some methods for remote maintenances by control and monitoring of devices. For example, the method can be provided by connecting to the control system network via Internet from own countries. On the other hand, the remote operation of an accelerator via Internet has some issues from a practical application standpoint. Failures in such remote operation may cause breakdown immediately. For this reason, we plan to implement the operator intervening system for remote accelerator diagnostics and support, and then it will solve the issues of difference between the local control room and other locations. In this paper, we report the system concept, the development status, and the future plan.

1. はじめに

次世代加速器である ILC (International Linear Collider) は国際協力で運用されようとしている。また、国際協力上ホスト国の制御室とは別に自国から装置の監視や制御を行う機構が必要になると考えられていた。そこで 2001 年に ILC 用に加速器専用の世界規模なネットワーク GAN (Global Accelerator Network) [1]が考案されたが、現在まで実現していない。GAN では、ホスト国にある制御室同等の物を他の地域にも構築し、遠隔制御を行う、という事である。その為には遠隔地における加速器の制御だけでなく、機器診断、現地スタッフとのコミュニケーション用ビデオ会議システム、電子ログシステムの導入が検討されていた[2]。

EUROTeV における GAN-like なシステムである GANMVL (Global Accelerator Network Multipurpose Virtual Laboratory)プロジェクト[3]では、遠隔機器制御用のクライアント端末に X11、VNC (Virtual Network Computing)、JAVA VNC の利用が検討されていた。しかし、これらの制御用クライアントの接続手法はネットワーク帯域の問題が考えられる。制御画面を遠隔地に飛ばす手法ではネットワークリソースが必要であると考えられるが、他の地域を経由した細い帯域では十分なパフォーマンスが得られない、と予想している。

また GANMVL では“外部エキスパートの協力”を実現する手段として、現地オペレータやコントロール室の雰囲気を伝えるカメラシステムが重要である、としている。これは現地スタッフとの母国語の違いによるコミュニケーション不足の問題が理由に挙げられている。一方で上記は遠隔地からの制御にも言える事である。加速器やビームの不具合時等に加速器オペレータが遠隔地の各コンポーネント(真空・RF・制御・イオン源等)の担当スタッフに指示を仰ぐ場合があるが、現地の加速器全体の現状を一番良く理解しているのは、現地オペレータである。よって、担当スタッフが的確な指示を出す為には現地オペレータと遠隔スタッフ間のコミュニケーションが重要になってくるが、母国語が異なっていなくても電話や音声で加速器の現状を詳細に伝える事は非常に難しい。なぜなら音声で伝える情報量と目で見て得られる情報量が明らかに異なっているからである。では制御 GUI (Graphical User Interface) 画面をスナップショットして画像で情報を提供すれば良いかというと、それではインタラクティブ性の問題がある。よってこの手法ではミスオペレーションが起こる可能性が高いと考えられる。

さらに GANMVL プロジェクトレポート[4]では、遠隔地からの機器モニタだけなら特に機器への安全性については考慮する必要がないが、外部からの遠隔制御には問題があり、何らかの安全システムが必要、としている。

以上を解決し、遠隔地より加速器を制御する為の手段として我々は WebSocket を用いた OPI (Operator Interface)の利用と WebSocket OPI におけるオペレータ介在システムの開発を行った。

a-uchi@riken.jp

2. WebSocket を用いた OPI

現在の社会一般において Web 及びそのネットワークは既にインフラの扱いであり、PC だけでなく様々な機器にブラウザが実装され Web を利用する事が可能である。しかし従来の Web ではサーバ、クライアント間の双方向通信が行えなかった為、一般的なソケット通信を用いた GUI のようなリアルタイムの応答性の確保が難しかった。

これを解決する手段として、2011 年 12 月 ITEF より Web で双方向通信を可能にさせるプロトコルである WebSocket の仕様が策定された[5]。一方 SPring-8 では仕様策定以前のドラフト版にて、MADOCA (Message And Database Oriented Control Architecture) 用 WebSocket OPI のプロトタイプが開発され、有用性が検証された[6]。また、我々は EPICS CA (Channel Access) に対応した WebSocket サーバと OPI 用クライアントの開発を行い、EPICS (Experimental Physics and Industrial Control System) 環境へのプロトタイプの実装に成功している[7]。以上のように WebSocket 通信、ブラウザを用いた OPI の開発、実装は進んでいる。よってセキュリティを考慮しなければ、インターネット等の加速器制御ネットワーク外部からのアクセス、制御は技術的には可能な状況にある。

3. EPICS におけるセキュリティ

3.1 アクセスセキュリティ

EPICS IOC と EPICS PV gateway にはアクセスセキュリティ機能が実装されている。これは CA クライアントに PV のパーミッション(書き込み・読み込みの可否) を持たせる機能であり、設定には OS のユーザ名とホスト名を利用する[8]。一方ユーザ名とホスト名は、そのホストの管理者でありさえすれば設定可能な為、いわゆる“なりすまし”の対策は行えない。よって、この機能だけではセキュリティとしては不十分であるが、制御システム専用のネットワークで運用している多くの場合では問題にならない。

3.2 EPICS CA における SSH 転送

一般的に通信プロトコルを暗号化する手段として SSH (Secure Shell) を利用する機会は多い。EPICS CA においても SSH ポート転送を利用する事が可能である。以下に設定例を示す。

```
% ssh -N -L 5064:localhost:5064 root@192.168.0.10
% export EPICS_CA_AUTO_ADDR_LIST=NO
% export EPICS_CA_ADDR_LIST=192.168.0.10
```

上記例は、標準で CA が利用する 5064 ポートの TCP のみを SSH ポート転送している。また、CA_SEARCH で利用される UDP ブロードキャストを行わないように環境変数に予め CA サーバ (EPICS IOC, PV gateway, CAS) の IP アドレスを設定する必要がある。一方 SLAC では CA の UDP ブロードキャストにおける SSH ポート転送にも対応したシステムの開発も行われている[9]。

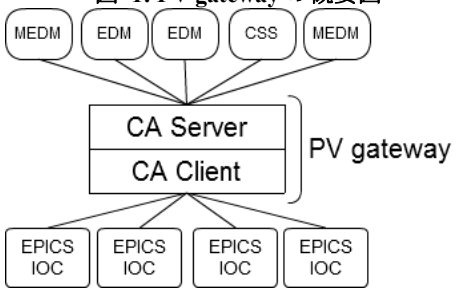
以上の様に制御用の通信を暗号化する手段として SSH は古典的ではあるが、有効な手段の一つである。

4. PV gateway

ここでオペレータ介在システムに利用している PV (Process Variable) gateway の仕組みについて説明する。

PV gateway は、多数の CA コネクションの代理をする事で EPICS IOC の負荷を減らす事が目的として開発された[10]。コネクションを中継する事で、CA クライアントからは CA サーバとして振る舞い、CA サーバからは CA クライアントとして振る舞う(図 1)。GATEWAY.access ファイルを設定する事で EPICS IOC と同様にアクセスセキュリティを実現している。また、GATEWAY.pvlist ファイルを設定、上記アクセスセキュリティと組み合わせる事で EPICS PV に対してルールに基づいたアクセス制御 (WRITE/TRAPWRITE/READ) をする事が可能である。また、GATEWAY.access, GATEWAY.pvlist の変更後の設定反映は、PV gateway 内部の PV である gateway:commandFlag をプロセスする事で動的に行う事が可能である。

図 1: PV gateway の概要図



5. オペレータ介在システム

5.1 システム概要

オペレータ介在システムの目的は、EPICS に基づいたシステムにおける真空度やビーム電流値といった値を Web から監視するだけでなく、デバイスに命令出力を伴う遠隔制御をオペレータ介在のもとで誤りなく、安全に実現させる事である。以上を実現する為に、機器出力における EPICS PV に対して厳格なアクセス制御をシステムに導入する事を提案する。このシステムの特徴は、遠隔制御者が現場にいる加速器オペレータに対して、出力制御点一つ一つに対して許可を求め、加速器オペレータが遠隔で制御されている EPICS PV を詳細に把握する事を可能にさせる仕組みである。全体のシステム図を図 2 に示す。

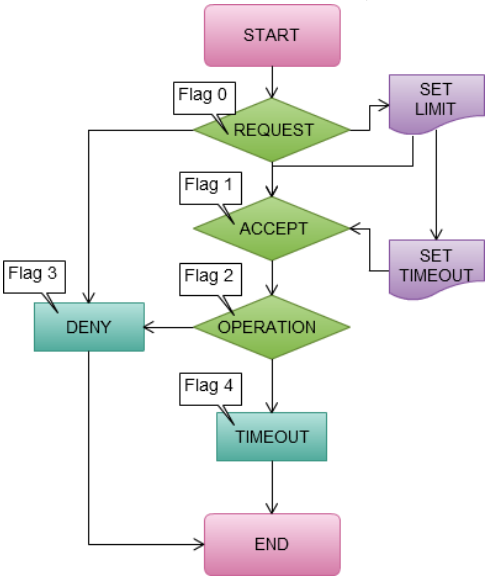
5.2 システムの振る舞い

EPICS PV の制御可否については PV gateway における GATEWAY.pvlist ファイルの作成と設定反映を

MySQL に格納されたフラグに応じて、動的に行う事で実現する。図 3 にフローチャートを示す。詳細な例を以下に述べる。

1. 遠隔制御者は PV 書き込みリクエストを MySQL に送る（フラグ０）。
2. リクエストの情報は現場オペレータに表示され、制御可否を決定する。その際、制御可能な時間 (タイムアウト) や値を変更しても良い範囲(上下限値)の設定も行う（フラグ１）。
3. 制御を許可すれば、Timeout プロセスが起動した後にフラグ２が設定され、拒否するのであればフラグ３が設定される。
4. 制御中の PV に対して現場オペレータが中止を判断した場合はフラグ３をセットする。
5. 設定時間を経過した場合 Timeout プロセスがフラグ４をセットする。

図 3： システムフローチャート



5.3 仮想マシンを利用する事による多層防御

3.1 で示した様に EPICS のアクセスセキュリティは“なりすまし”が行えてしまうので、インターネットアクセスにおけるセキュリティ対策としては不十分である。そこでセキュリティの観点から仮想マシンを多層にして構成している(多層防御)。つまり本システムでは MySQL にフラグを設定する事で PV gateway のアクセス制御(GATEWAY.pvlist の変更)を行っているが、物理的なネットワークからアクセス不可能な状況を仮想マシンで作り出す事でネットワーク攻撃や不正アクセスを防御しているのである(図２)。仮想環境を構築する為に我々は無償で利用できる VMware vSphere Hypervisor を利用した。

5.4 上下限値設定機能

EPICS を用いた制御システムでは DRVH フィールドと DRVL フィールドを設定する事で ao レコードの出力上限値または下限値を決める事が可能である。しかし制御ネットワークに実装されている EPICS IOC の DRVH ・DRVL の値を変えて遠隔制御からの出力上下限値を設定する事は遠隔制御以外のユーザに影響が出る可能性がある事を理由から行わなかった。結果として PV gateway のソースに手を加え、リミット機能を追加する事で上記機能を実現した。本システムにおける PV gateway は GATEWAY.access, GATEWAY.pvlist 同様 GATEWAY.limit ファイルを新たに読み込む機能を設け 5.2 に示されている上下限値の設定を行っている。読み込まれる GATEWAY.limit の書式例は以下の通りである。

akito12Host:xxxExample 10 30

上記の例は、指定した PV(*akito12Host:xxxExample*)に対して 10～30 の値は変更可能だが、それを以外の値は PV gatway が IOC に対して ca_put (若しくは ca_put_array)を拒否する、という設定になっている。

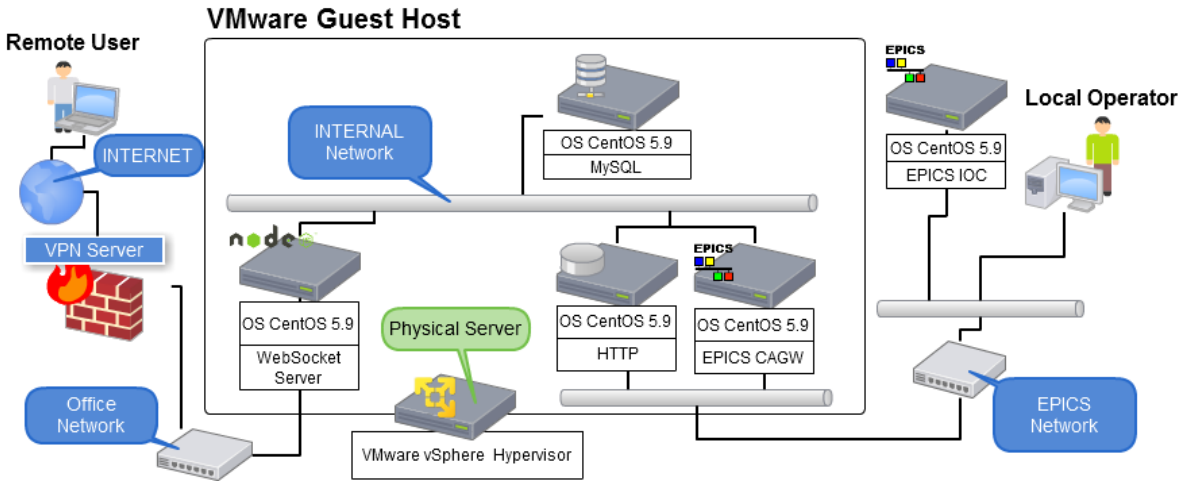


図 2 オペレータ介在システムの全体概要図

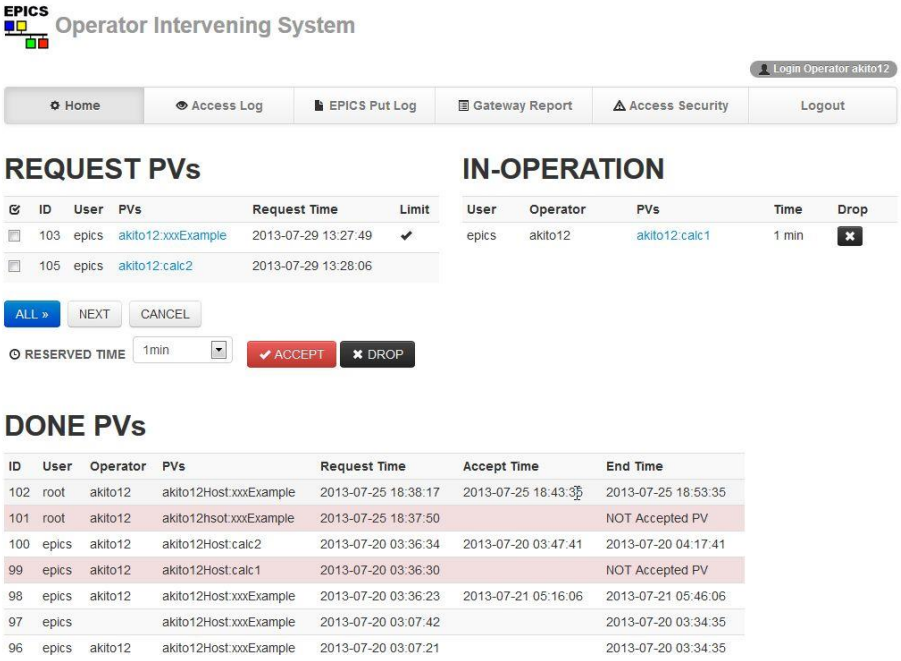


図 4 オペレータ介在システムのインターフェースのスクリーンショット

5.5 インターフェース

オペレータ介在システムのインターフェースは Web アプリケーションで開発した(図 4)。Ajax(Asynchronous JavaScript + XML)を用いてリアルタイムにリクエストやオペレーション中の情報が表示される。ここで WebSocket を利用せず Ajax を用いた理由は、オペレーションほどインタラクティブな更新が必要ない、かつ MySQL と PHP を利用したシステム開発手法 (LAMP)が容易であった点を重要視した。

5.6 WebSocket 側のセキュリティ

WebSocket OPI には認証機能が実装されている。また 3.2 同様に制御通信を暗号化する手段として、SSL/SSH 経由で WebSocket OPI にアクセスする。さらに一般的なオフィスのネットワーク環境では、別なローカルな社内ネットワークが実装されている事が多く、その場合 SSL/SSH 通信以前に VPN (Virtual Private Network) を経由する事になる。

6. まとめ

遠隔地から真空度やビーム電流値といった値を WebSocket で監視するだけでなく、EPICS に基づいたシステムにおける命令出力を伴う制御をオペレータ介在のもとで誤りなく、安全に実現させる為のシステムを開発した。本システムは RIBF (RI Beam Factory) における RIKEN 28GHz 超伝導 ECR イオン源の制御システムにて試験実装を開始し、有用性が検証された後、運用される予定である[11]。

参考文献

[1] “A Global Accelerator Network: ICFA Task Force Reports”, Dec. 2001 http://www.fnal.gov/directorate/icfa/icfa_tforce_reports.html
[2] S. Peggs, et al., Proceedings of PAC2003, Portland, Oregon, USA, P.278-P.282
[3] R. Pugliese, et al., Proceedings of ICALEPCS07, Knoxville, Tennessee, USA, P.418-P.420
[4] http://www.eurotev.org/work_packages/wp8_ganmvl/
[5] I. Fette and A. Melnikov, The WebSocket Protocol, IETF HyBi Working Group. 2011.
[6] Y. Furukawa, et al., Proceedings of ICALPECS 2011, Grenoble, France, 2011, WEMAU010.
[7] A. Uchiyama, et al., Proceedings of PCaPAC2012, Kolkata, India, WECC02
[8] EPICS Application Developer’s Guide, http://www.aps.anl.gov/epics/
[9] EPICS collaboration meetings, Apr, 2014 https://portal.slac.stanford.edu/sites/conf_public/epics_2012_04/presentations/Straumann_Friday_CA_Tunneling.pdf
[10] K. Evans, et al., Proceedings of 10th ICALPECS, Geneva, 2005
[11] A. Uchiyama, et al., Proceedings of ECRIS2012, Sydney, Australia, TUPP12 (to be published)