OPERATOR INTERVENTION SYSTEM FOR REMOTE ACCELERATOR DIAGNOSTICS AND SUPPORT

A. Uchiyama[#], The Graduate University for Advanced Studies (SOKENDAI), Tsukuba, Japan
K. Furukawa, High Energy Accelerator Research Organization (KEK), Tsukuba, Japan
Y. Higurashi, RIKEN Nishina Center, Wako, Japan

Abstract

Large experimental physics projects, such as ITER and LHC, are typically managed by international collaboration. Similarly, the International Linear Collider (ILC), a next generation project, will be launched as a result of the collaborative efforts of multiple institutes from three regions. After its collaborative commencement, all collaborators apart from the host country will need to have methods for remote maintenance, control, and monitoring of its associated devices. For example, a method has to be provided for connecting to the control system network via wide area network (WAN) links from various collaborating institutions. However, from a practical application standpoint, the remote operation of an accelerator via WAN is beset by a number of issues. One such issue is that the accelerator has both experimental device and radiation generator characteristics. Additionally, any mistake operation of the remote control system could result in an immediate breakdown. For this reason, we propose the implementation of an operator intervening system for remote accelerator diagnostics and support that can obviate any differences between the local control room and remote locations.

INTRODUCTION

In an international collaborative project such as the International Linear Collider (ILC), remote operation is required in order for collaborators to utilize, monitor, and control the facility in the host country. Therefore, implementation of the global accelerator network (GAN) as a dedicated network for the ILC control system has been planned since March 2000 [1]; however, it remained unrealized until now. The idea underlying GAN is to construct remote accelerator control rooms that are virtually equivalent in terms of performance and features to the local control room in the ILC, for use by remote users of the facility. To realize the GAN project, it is necessary to implement a remote control system comprising an operator interface (OPI), a videoconference system, an electronic log system, and an online fault diagnosis system for accelerator devices. In addition, because communication between on-site operators and remote users is essential, all information about activities taking place in the local control room should be communicated to the remote operators.

A similar system to GAN, called the Global Accelerator Network Multipurpose Virtual Laboratory (GANMVL), was implemented in the EUROTeV project [2]. GANMVL facilitates remote operation using a client system that utilizes X11 windowing, virtual network computing (VNC), and JAVA VNC. However, these communication methods encounter issues such as low bandwidth and high network latency during remote operation over wide area links. Thus, with the limited network resources present in some areas, if these methods are used, it may prove difficult to stably operate and control the accelerator. Additionally, in GANMVL, the video/audio communication tools are invaluable in allowing experts to work together at the global level on accelerator operation problems. This is because they help to mitigate communication apprehension caused by differences in the native languages of the local staff and some of the global experts.

Their situation is similar to ours as regards the cooperation of experts and remote operation across WAN links. In situations such as accelerator troubles and change of beam conditions (beam emittance from ion sources, etc.), on-site accelerator operators need to seek direction from other engineers or scientists about accelerator components, for example, radio frequency (RF), vacuum, beam diagnostic, control system, and ion source, over the telephone. In such scenarios, the ability to give the exact directions required by accelerator operators is contingent on the amount of information needed for remote troubleshooting. To prevent operational mistakes, the accelerator conditions need to be understood as a whole. Even in cases where the native languages are not in conflict, it is difficult to correctly provide detailed information about accelerator conditions via telephone and voice communication because too little information is obtained by listening compared with seeing. Moreover, the GANMVL project reported that it was not necessary to consider a safety system in the monitoring of their system via remote access from outside. Note that a safety mechanism is indispensable when the remote operation needs not only to monitor the parameters but also to output control in order to prevent accelerator trouble caused by operational mistakes. To address safety issues and improve usability for remote operations, we developed an operator intervention system for WebSocket [3] access in the Experimental Physics and Industrial Control System (EPICS).

[#]a-uchi@riken.jp

WEBSOCKET-BASED OPI

WebSocket was originally designed to be implemented as part of HTML5 and was standardized as RFC6455 by the IETF in 2011 [3]. WebSocket realizes a reasonable interactive response using bidirectional communication and thereby overcome the disadvantage that could not be eliminated using traditional asynchronous JavaScript and XML (Ajax) web applications. Furthermore, since periodic polling is not necessary like Ajax, it becomes possible to reduce network traffic. Major web browsers such as Firefox, Chrome, Safari, and Internet Explorer can be used as cross-platform environments with the implementation of a WebSocket-based OPI (see Fig. 1). This allows the user to access the OPI from both a PC-based web browser and other devices such as Android and Apple smartphones and tablets. A prototype WebSocket-based OPI was constructed for the message and database oriented control architecture (MADOCA) developed at Spring-8 [4]. We also developed a WebSocket-based OPI for EPICS [5]. After satisfying the conditions for interactive access to EPICS, we implemented a WebSocket server, which connects to the EPICS IOC via Channel Access (CA), as a web-based OPI. The WebSocket server gets/puts the values as process variables (PVs) from the EPICS IOC by calling the CA API. Therefore, if security is not taken into consideration, it is technically possible to access and control the system using the WebSocket connections from outside the accelerator control network, such as from the Internet.

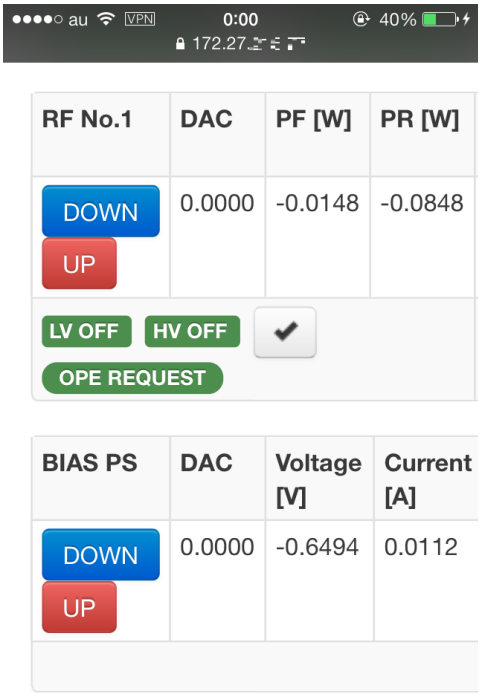

Figure. 1: Screen shot of WebSocket-based OPI on Apple iPhone4s

OPERATOR INTERVENTION SYSTEM

System Concept

The purpose of the operator intervention system is to ensure safe remote output control of EPICS via the WebSocket server. To simply monitor the status of the accelerator parameters using the WebSocket-based OPI, permission from the on-site operator is not necessary as long as authentication has been accomplished with an SSL connection. The WebSocket-based client system is designed so that output control via remote operation always requires the permission of an on-site accelerator operator who can intervene at any time. The main part of the operator intervention system consists of a PV gateway provided by the EPICS collaboration [6], a MySQL database, and Ajax web applications. Unlike in the OPI, real-time interactive response is not required for sending output control permission and to view access logs in the operator intervention system. Consequently, in consideration of the difficulty of system development, we utilized a LAMP (Linux, Apache, MySQL, PHP) environment for the operator intervention system without using WebSocket.

The on-site accelerator operator first gives permission to every output of the PVs corresponding to the hardware devices of EPICS. If the PVs have not been granted permission, then the operator intervention system always rejects the output command in the CA protocol layer. In addition, the on-site operator can decide on upper and lower limits for remote control operations before sending the permission command.

System Policy

The operator intervention system can control the availability of remote operations by sending system flag values to the MySQL database. The access control mechanism for the CA protocol is utilized by the access control security system of the PV gateway. Specifically, a daemon polls the database and updates the security access file (GATEWAY.pvlist) with information corresponding to the flag values dynamically. A flowchart illustrating the operation of the system for remote connections is depicted in Fig. 2. First, remote users send EPICS PVs requests to the operator intervention system for control of the outputs, such as caput command, via WebSocket (Flag 0). The on-site operator then ascertains whether the requested PVs are available for control (Flag 1). If control is possible, a command to accept is sent by the on-site operator (Flag 2); otherwise, a refuse command is sent (Flag 3). The on-site operator can terminate the remote operation at any time, for example, if problems with the accelerator arise (Flag 3). A process that manages the time duration of the remote operation sends a timeout command after a certain period of time has elapsed (Flag 4).

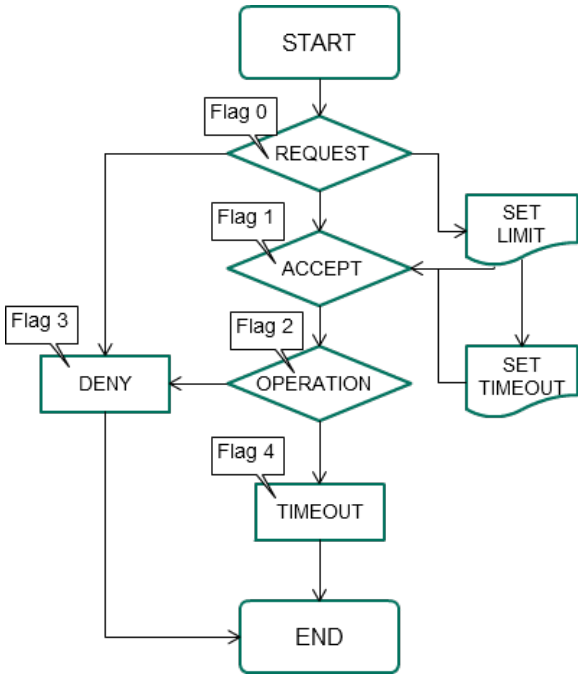

Figure 2: Flowchart illustrating the opration of the system for remote.

Required Services

The operator intervention system comprises important services running on several distributed hosts. A chart of the system is depicted in Fig. 3. The MySQL service is necessary to store the flag value via an internal network. The Apache web server and NFS run on an application server. NFS is used to share the log files among the WebSocket server, the Apache web server, and the PV gateway via the internal network, as well as the MySQL service. WebSocket server programs, developed using Node.js [7], run on another host that connects to the MySQL database and the EPICS IOCs via the PV gateway.

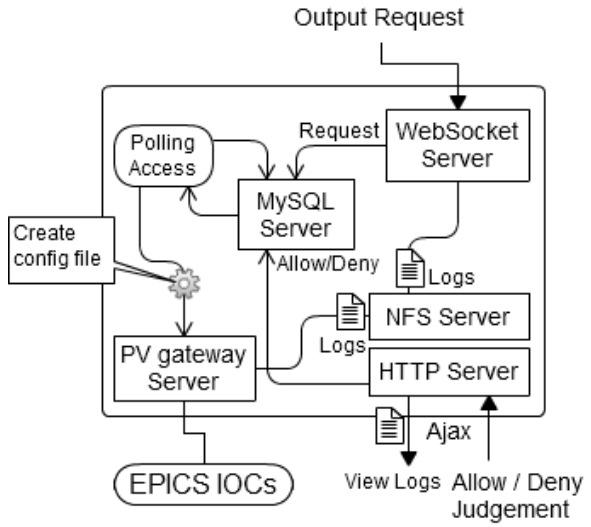

Figure 3: System chart showing the operator intervention system, EPICS IOCs, and the WebSocket server.

Virtualization Technology

The access control security system does not comprehensively cover access from the Internet because EPICS is not able to completely prevent impersonation. Generally, a defense-in-depth network system, which has a multi-layer network structure, is one of the most useful methods for improvement of network security. In our system, we implemented a multi-layer network structure consisting of servers running in a virtual environment on one physical server. In the system, network attacks and unlawful access are thwarted by using virtual machines to prevent access from the physical network (see Fig. 4). We implemented the virtual environment using VMware vSphere Hypervisor 5, which can be used free of cost. The specifications for the physical server are shown in Table 1. We used CentOS 5.9 as the operating system for the virtual machines.

Table 1: Specification for the physical server used in the virtualization environment.

CPU	Intel Core i7-3770 (4 cores, 8 threads)
Memory	16 GB
Storage	SATA
Ethernet	Dual network connections

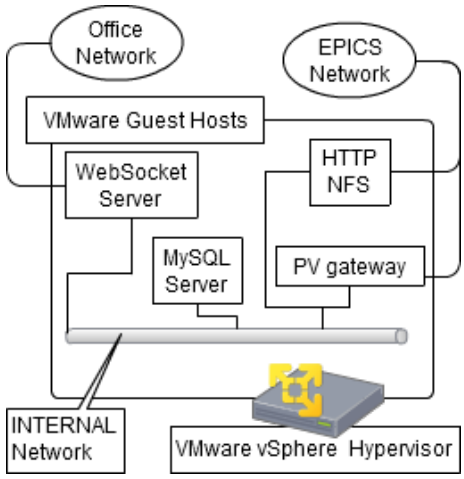

Figure 4: Network chart of the system in the VMware virtualized environment

Customized PV Gateway

In general, EPICS utilizes DRVH/DRVL fields to set the upper and lower limits of analog output (ao) records [8]. In this case, however, utilizing the DRVF/DRVL fields of the EPICS IOCs to control the system network is not wise because it may cause problems, such as lack of parameter resetting, in normal operation with remote users. As a result, we implemented the function by modifying the source code of the PV gateway. Consequently, our customized PV gateway has a GATEWAY.limit file to set the upper and lower limits as well as GATEWAY.pvlist and GATEWAY.access files for access control.

User Interface

We developed the interface of the operator intervention system as a web application using Ajax because it is not required to be as responsive as the WebSocket-based OPI. The user interface of the operator intervention system is shown in Fig. 5. On-site operators can check the requested EPICS PVs, completed PVs, and in-operation PVs in one view. Similarly, all the access logs and caput logs are available for checking by the on-site operator at any time.

Security for WebSocket-side

We ensure secure WebSocket access to the accelerator network from the WAN by using a virtual private network (VPN) and authentication with SSL. In addition, accelerator operators have to comprehensively verify a user (via login ID, etc.) seeking access to the networks and access route (full domain of Internet providers, etc.) before WebSocket control is allowed.

IMPLEMENTATION

At the RIKEN Radioactive Isotope Beam Factory (RIBF), we implemented an operator intervention system for the EPICS-based RIKEN 28 GHz superconfucting ECR ion source (28GHz SC-ECRIS) control system for an evaluation [9]. Using a WAN emulator producted by Apposite Technologies, Inc. [10], we emulated Internet access for a speed of 2.0 Mbps and a latency of 200 ms. Consequently, we were able to successfully operate part of the 28 GHz SC-ECRIS (gas valves, RF power, and electrode positions) remotely without any serious glitches. The on-site operators managed the digital and analog outputs for remote operation, and access was denied in the network protocol layer if certain criteria were not met.

CONCLUSION

In this paper, we proposed an operator intervention system for a WebSocket-based OPI in the Experimental Physics and Industrial Control System (EPICS). In order to prevent different kinds of troubles in far remote operation, a safety system is necessary. This system ensures secure remote operations, including for output devices, by allowing the intervention of an on-site operator. Following the implementation of the operator intervention system, it now facilitates the monitoring of a vacuum and a beam current as numerical values in the real-time web from remote locations. In addition, it makes it possible to perform output control without any lapse in operation safety.

REFERENCES

[1] "A Global Accelerator Network: ICFA Task Force Reports", Dec. 2001; http://www.fnal.gov/directorate/icfa/icfa_tforce_reports.html

[2] R. Pugliese, et al. Proceedings of ICALEPCS07, Knoxville, Tennessee, USA, P.418-P.420

[3] I. Fette and A. Melnikov, The WebSocket Protocol, IETF HyBi Working Group. 2011.

[4] Y. Furukawa, et al. Proceedings of ICALPECS 2011, Grenoble, France, 2011, WEMAU010.

[5] A. Uchiyama, et al. Proceedings of PCaPAC2012, Kolkata, India, 2012, WECC02

[6] K. Evans, et al. Proceedings of 10th ICALPECS, Geneva, 2005

[7] http://nodejs.org

[8] EPICS Application Developer's Guide, http://www.aps.anl.gov/epics/

[9] A. Uchiyama, et al. Rev. Sci. Instrum. (to be published) KEK Preprint 2013-38, http://www-lib.kek.jp/tiff/2013/1327/1327038.pdf

[10] http://www.apposite-tech.com/products/mini2.html

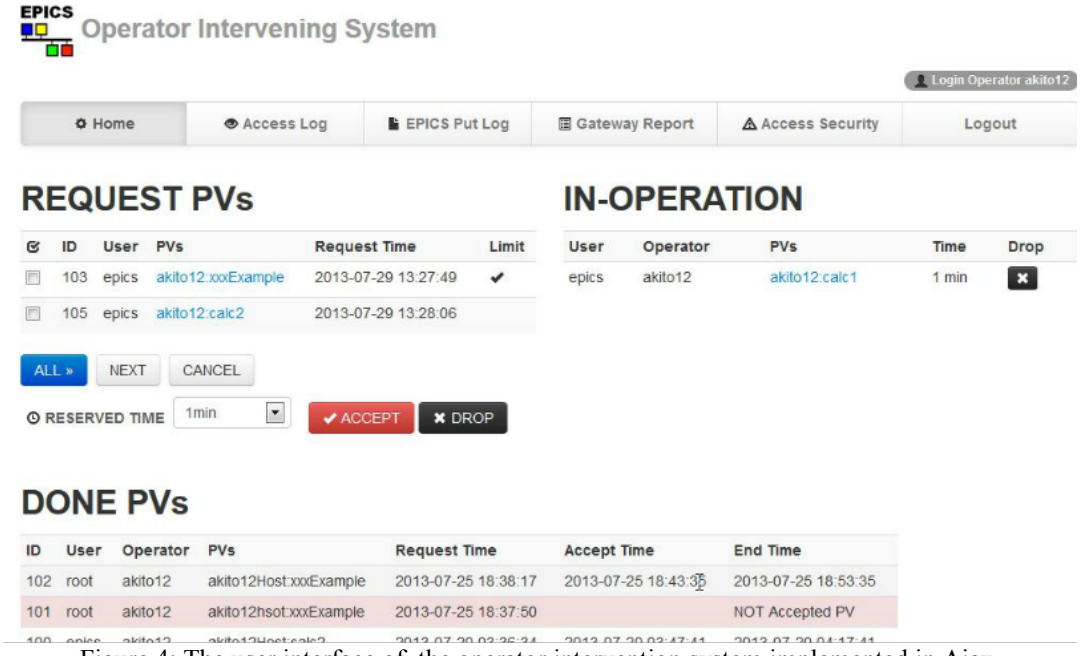

Figure 4: The user interface of the operator intervention system implemented in Ajax.