ISBN: 978-3-95450-200-4 doi:10.18429/JACoW-PCaPAC2018-THP04

REAL-TIME AND DETAILED PROVISION OF J-PARC ACCELERATOR OPERATION INFORMATION FROM THE ACCELERATOR CONTROL LAN TO THE OFFICE LAN

S. Yamada*, KEK / J-PARC Center, Tokai, Ibaraki 319-1195, Japan

Abstract

J-PARC Main Ring (MR) is a high-intensity proton synchrotron whose control system is developed based on EPICS. Its beam operation started in 2008, and since 2009 has been delivering beam to the T2K neutrino experiment and hadron experiments. Over the past decade, MR have become more sophisticated and more stable driving is required. Along with this, demands arose from users and experts of equipment such that acquiring detailed and real-time information on the apparatus from the office LAN. On the other hand, the accelerator control system is quarantined from the office LAN with firewall for security reasons. Therefore, despite being intentional or not, manipulating any equipment in the accelerator control LAN shall be prohibited from the office LAN. This article describes construction and prospects of such an one-way gateway system such that information is relayed via EPICS from accelerator control LAN to the office LAN while minimizing influence in the opposite direction.

INTRODUCTION

The office LAN in J-PARC is named “JLAN”.

J-PARC accelerator operation information has been provided to JLAN in a web page containing two items as following:

- “Latest Operation Status” which is manually typed by the accelerator shift leader as necessary.
- A image file showing summary of operation status, which is updated every one minutes.

Its example is shown in Fig. 1.

As MR become more sophisticated since it stated its operation in 2008, yet more stable operation is required. Accordingly, demands from equipment experts and users are increasing to acquire real-time and detailed status of the accelerators and equipment from their office. Those information such as

- detailed status of power supplies for magnets and RF,
- Present value of beam pipe vacuum as well as its history,
- Temperatures in power supply buildings and their history,

were only available in the control LAN but in JLAN.

EPICS AND CA GATEWAY

The control system of J-PARC Accelerator is based on EPICS [1]. Its protocol is called Channel Access (CA). CA is available within the same network under normal usage.

A front-end computer, which provides control points to access equipment under its control, is called I/O controllers (IOC). The operator interface (OPI), which act as a CA client, broadcasts UDP packet to search for a control point of interest. IOC will reply to the client when it is hosting the requested control point.

CA Gateway [2] is a standard EPICS utility to relay CA between two networks. It works as a CA client in one network and a as server in the other, so that accelerator operation status information in the control LAN will be available in JLAN in realtime.

MINIMIZATION OF INFLUENCE TO THE ACCELERATOR CONTROL LAN USING TWO-TIER GATEWAY

Accelerator control LAN is connected to JLAN via a firewall device. There is DMZ in the middle of those two networks, which is called “control-DMZ”. The policies in communications among those three networks are as following:

- No bridge connection is allowed other than the firewall device. Therefore any communication shall go through the firewall.
- Any direct communication between control LAN and JLAN is prohibited.
- Communication between control LAN and control-DMZ is allowed only if source IP address, destination IP address, and port number is listed in a whitelist.
- Communication between control-DMZ and JLAN is also limited by another whitelist.

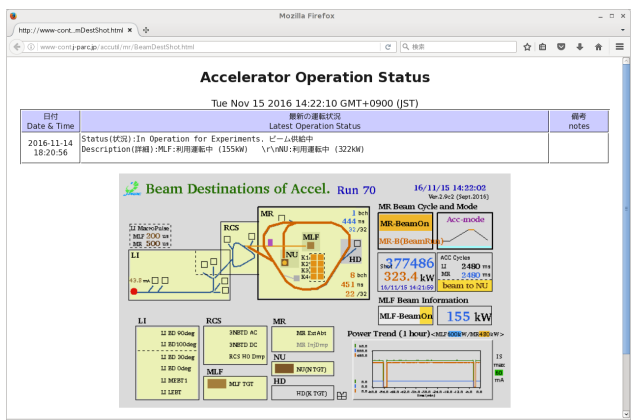
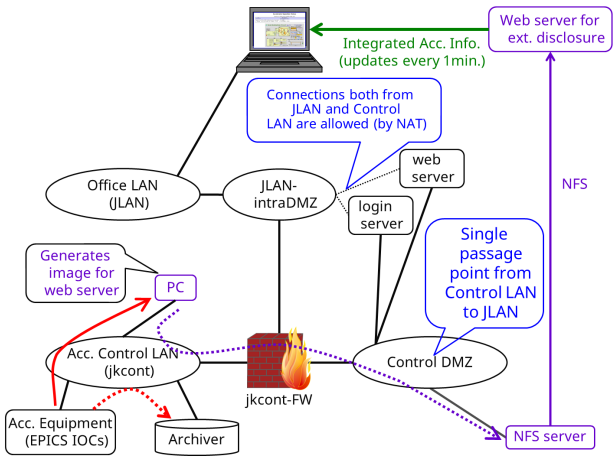


Figure 1: A web page which shows J-PARC accelerator status.

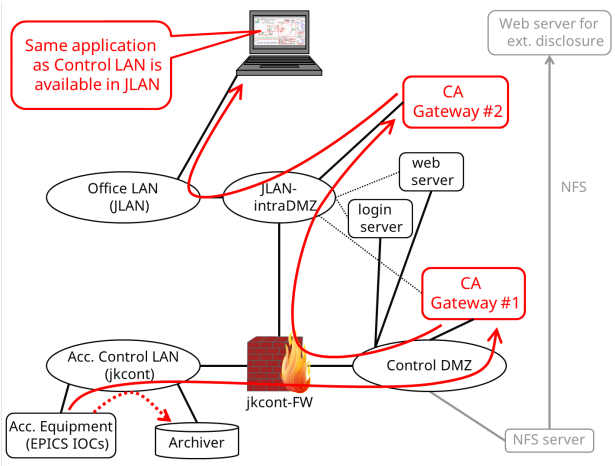
* shuei@post.kek.jp

ISBN: 978-3-95450-200-4 doi:10.18429/JACoW-PCaPAC2018-THP04

Figure 2a shows traditional path of accelerator operation status information from control LAN to JLAN. Every one minutes a PC connected to the control LAN generates an image file containing accelerator operation summary and saves to a file server in control-DMZ. Then a web server reads the image file and publishes to JLAN. There is no chance to operate any accelerator component from JLAN, because only an image file is provided from control LAN to control-DMZ and the web server has read-only access to the file server.



(a) Before introduction of the gateway system.



(b) After introduction of the gateway system.

Figure 2: Transmission path of information from the accelerator control LAN to JLAN.

As mentioned above, CA Gateway makes it possible to relay the CA protocol used by the control system to JLAN. Accelerator operation information is provided to JLAN in real time with the route shown in Fig. 2b.

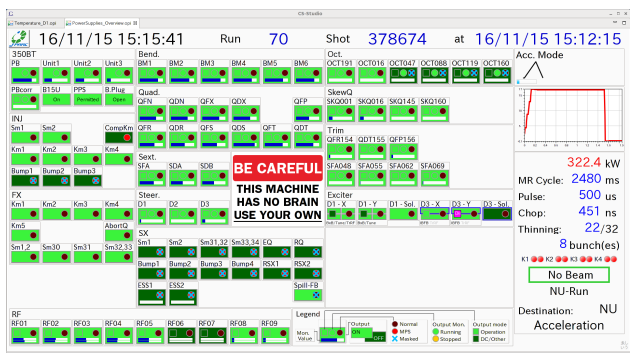
A two-tier, one-way gateway system is constructed, aiming only to read accelerator operation information from JLAN in realtime. It is not expected to manipulate any accelerator component from JLAN, regardless of whether being intentional or not. In order satisfy those requirements, each of those gateway is configured as following:

- CA Gateway #1 (located in control-DMZ):
  Provide accelerator operation information in read-only mode from the control LAN to CA Gateway # 2. An additional IP address is assigned for JLAN-intraDMZ using NAT function of the firewall. CA Gateway #1 is configured so that any I/O access to control-LAN is read-only. Connections between CA Gateway #1 and JLAN-intraDMZ is limited to CA Gateway #2, and only CA protocol is allowed. SSH access to CA Gateway #1 is limited only from the login-server.
- CA Gateway #2 (located in JLAN-intraDMZ):
  It provides read-only CA connections to clients in JLAN. CA Gateway #2 is also configured so that any I/O access to CA Gateway #1 is read-only. Connections between CA Gateway #2 and JLAN is limited to CA protocol. SSH access to CA Gateway #2 is limited only from the login-server.

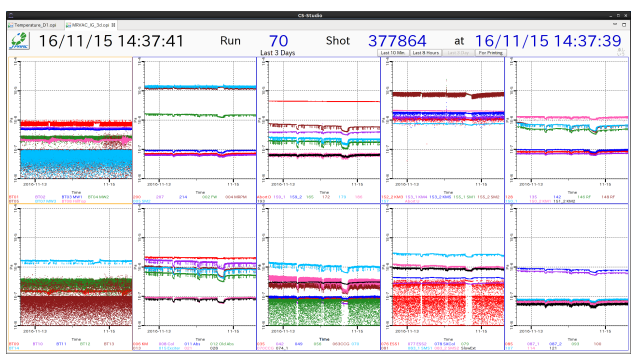
CA Gateway #2 is the sole server which is accessible for CA clients in JLAN. Therefore no CA client in JLAN is able to access equipment in control-LAN directly.

UTILIZING HIGHER LEVEL CONTROL APPLICATIONS IN JLAN

Historically, GUI applications in MR control system have been developed with EDM [3] and MEDM [4], which are GUI builders running on X Window System. There are more than 100 screen definition files used in MR operation, there-



(a) A screenshot of an OPI showing operation mode of MR and status of power supplies.



(b) A screenshot of an OPI showing time variation of pressure in MR beam pipe.

Figure 3: Example of OPIs actually used for MR operation.

ISBN: 978-3-95450-200-4 doi:10.18429/JACoW-PCaPAC2018-THP04

fore it was expected to be complicated for both developers and users to use EDM or MEDM in JLAN. Each user's PC in JLAN needs X Windows System installed on it to use those applications. In addition, screen definition files have to be distributed and installed on each user's PC.

In 2015 CS-Studio (CSS) [5] was introduced to MR for development of GUI application in its control system [6]. This solved those issues of distributing the latest of screen definition files to JLAN, installation to user's PC, and the prerequisite of X Window System.

CSS is a framework to build GUIs for EPICS-based large scale control system, available on Linux, macOS and Windows. Various kinds of modules are able to be cooperated in CSS, such as:

- BOY: GUI builder and runtime environment,
- Data Browser: real-time trend graph as well as historical data from archive system,
- Alarm system,
- Archive system.

CSS is configured appropriately for JLAN and distributed to JLAN in a zip-file. Screen definition files are automatically downloaded from the web server on the fly. Thus the latest version of screen definitions, identical to those used in operation of MR, are always available. Figure 3 shows examples of CSS display which are used in MR operation.

SUMMARY OF GATEWAY SYSTEM OPERATION AND FUTURE PROSPECTS

The gateway system started its service in April 2018. Two commercial tiny fanless servers, PiNON Sabataro ® Type-P, were deployed for the gateway system as shown in Fig. 4. Its specification is shown in Table 1.

Figure 4: Two server PCs running the gateway system.

Figure 5 shows operation status of Gateway #2, from the start of its service in April 2018 to the summer shutdown of the accelerator in July 2018. It will be summarized as following:

- There were constant access to the gateway from 10 – 20 clients, 8 out of them are archive system which records status of the gateway.

Table 1: Specifications of PiNON Sabataro® Type-P

Processor	Celeron J1900 (2–2.42 GHz), 4 cores
RAM	8 GB (1333 MHz DDR3L SO-DIMM × 1)
Storage	128 GB (mSATA SSD × 1)
Network	GbE × 2
Display I/F	HDMI
USB ports	USB 2.0 × 2
Dimension	W80.6 mm × D110.6 mm × H34.4 mm
TDP	max 15 W
Power Supply	DC 12 V (AC/DC Adapter)

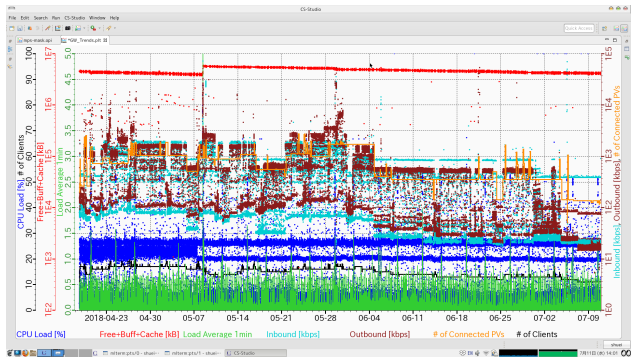


Figure 5: History of load of the gateway system for three months.

- 100 - 3000 control points have been accessed.
- Typical data rate of 1 – 10 Mbps went through the gateway.
- There are still plenty of root in CPU and memory; high CPU load of 25% was caused by anti-virus software scanning the gateway.

The gateway system have been operating stably so far. It is expected that gateway system is more utilized and the number of users of the gateway system will be increased.

REFERENCES

[1] EPICS - Experimental Physics and Industrial Control System, https://epics-controls.org

[2] Channel Access Gateway, http://epics.anl.gov/extensions/gateway

[3] EDM - Extensible Display Manager, http://ics-web.sns.ornl.gov/edm/edmUserManual/

[4] MEDM - Motif Editor and Display Manager, http://www.aps.anl.gov/epics/extensions/medm/index.php

[5] CSS – Control System Studio, http://controlsystemstudio.org/

[6] S. Yamada *et al.*, "Deployment of Control System Studio at J-PARC Main Ring", in *Proceedings of the 8th Annual Meeting of Particle Accelerator Society of Japan*, WEP103, pp. 543, 2011.