

NETWORK SECURITY SYSTEM AND METHOD FOR RIBF CONTROL SYSTEM



© A. Uchiyama^{A · B} M. Komiyama^B R. Koyama^{A · B} M. Fujimaki^B N. Fukunishi^B

A) SHI Accelerator Service Ltd. B) RIKEN Nishina Center

Outline of the ACC-LAN (Network system for RIBF control system)

Characteristics of ACC-LAN

Perfectly closed network system for ensuring security

Of course, No connection with other network. So

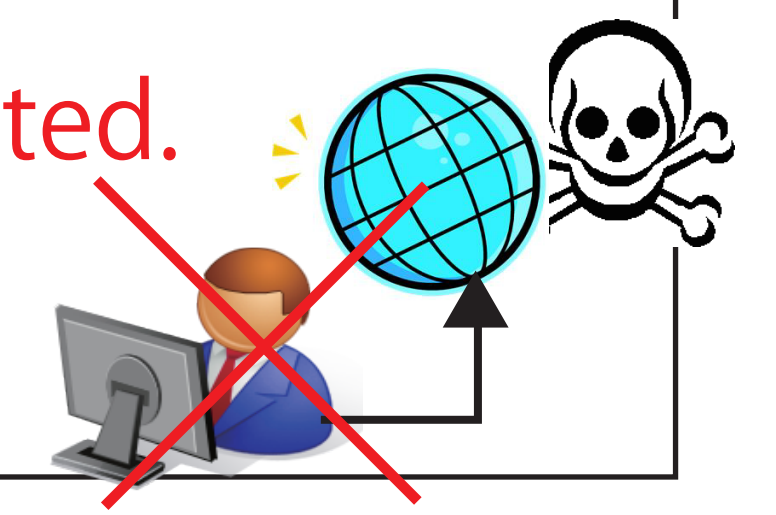
Problems

- Accelerator staff members can not monitor the Accelerator status from the office.
- RIBF beam users request wide variety of information for accelerators.
- When it is needed to fix security bugs, it is difficult to update software.
- It is not available to send E-mail alert automatically in serious trouble.



Next Best Policy

- Communications to the Internet or RIKEN-VLAN from client PCs are strictly prohibited.
- The information is provided by only web communication via reverse proxy server.
- The system opens only a minimum number of ports by the firewall.



OUR WORK

Reverse Proxy System for WEB Communication

ACC-LAN
(Accelerator Control)

Web Servers

Zope

Apache Tomcat

LabVIEW

Reverse Proxy
+ Authentication

(For Accelerator staff members)

HTTP

HTTP

Operator

Reverse Proxy

(For Beam users and visitors)

HTTP

RIKEN-VLAN
(Nishina Center)

Accelerator staff member

HTTP

Beam user and visitor

HTTP

Internet

Firewall

RIKEN-VLAN
(Other Lab)

Wi-Fi

- Web Communication is a suitable to provide information for a lot of people.
- Squid for reverse proxy server and IPtables for firewall.
- Two reverse proxy servers
 - For accelerator staff members with an authentication. (Single Sign-On)
 - For RIBF beam users with No authentication, but access only some specific website.

E-mail Alert in closed network

RIKEN-VLAN

POP3

SMTP

Receive

Send

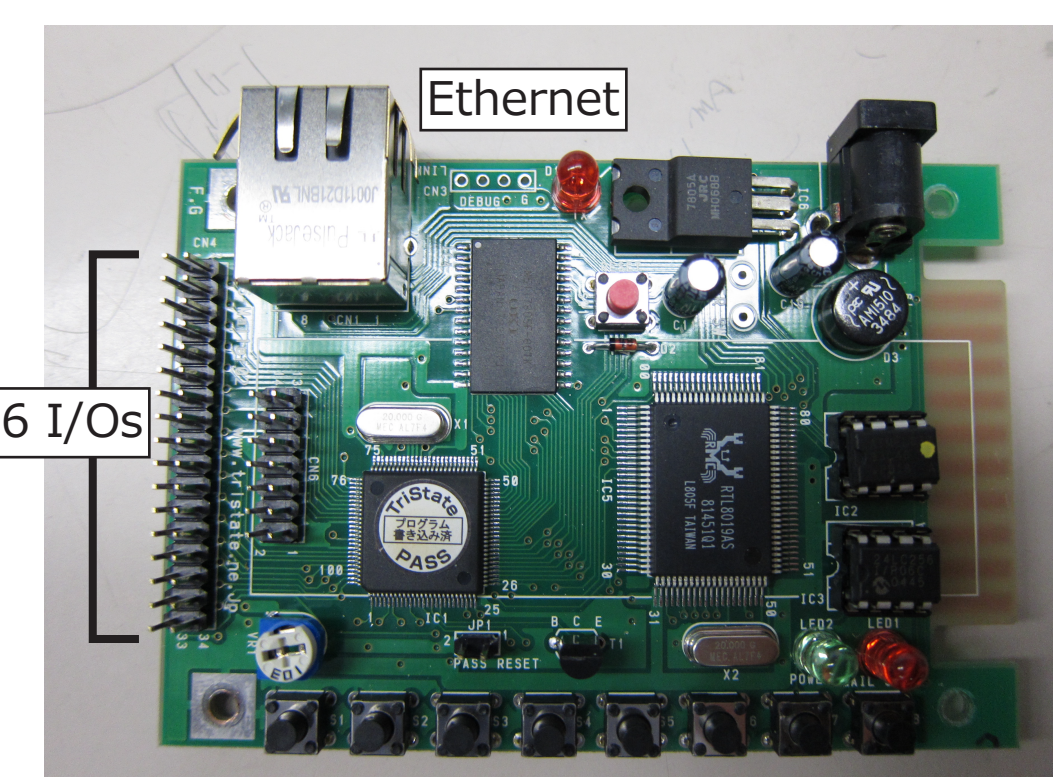
ACC-LAN

EPICS

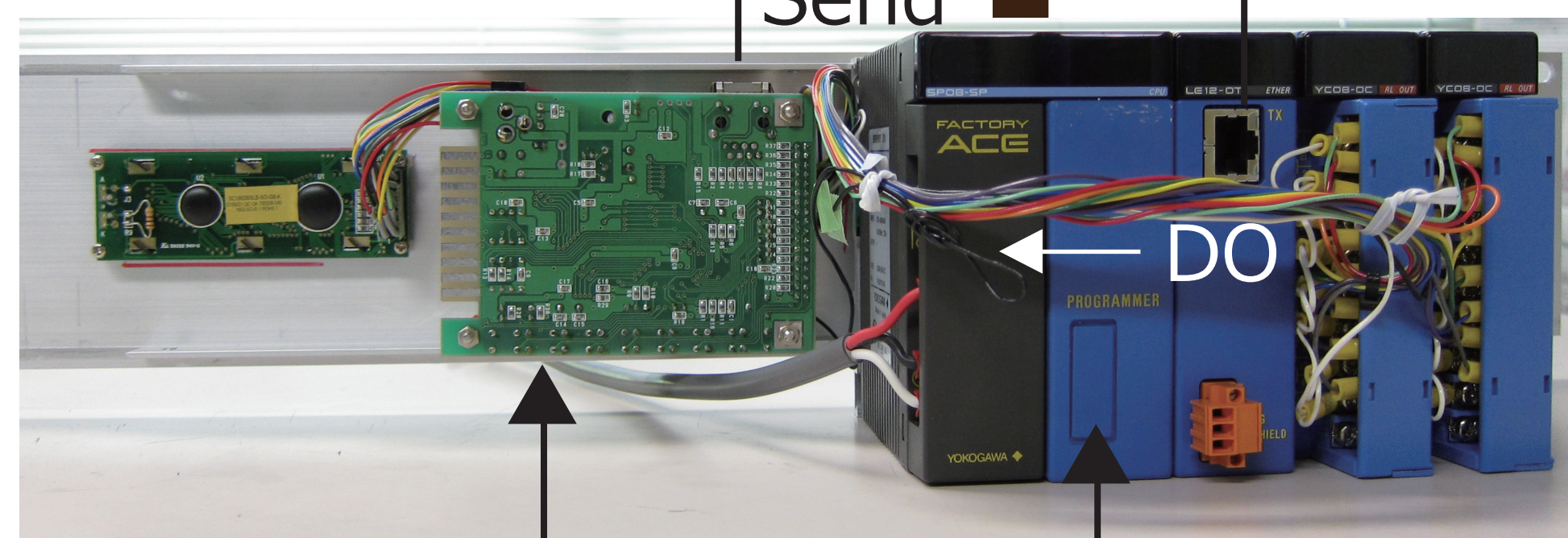
Linux IOC

DO

FA-M3



E-mail auto sender embedded board



Mailer Board

FA-M3



RIKEN-VLAN

Office

HTTP response

HTTP request

ACC-LAN

HTTP request

XML, HTML

MyDAQ2

ActiveX

Video Server

ActiveX

Network camera

HTML

BT MAP

LabVIEW (CA)

XML, JSON

EPICS

PHP-CA

- PVs are converted by the framework with XML and JSON.
 - We can develop EPICS clients running on the RIKEN-VLAN without channel access protocol.

- RIKEN-VLAN and ACC-LAN is separated completely.
- The system can send E-mails by using on-off control action of EPICS-based mechanical switches without a connection between the networks.