Development of remote participation tools for LIPAc operation

J. Franco Campos[3], T. Nakayama[1,3], M. Kojima[3], S. Tokunaga[3], A. Jokinen[2], F. Sartori[2], Y. Carin[1,2], A. S. Duarte[4],

[1]IFMIF/EVEDA Project Team, Rokkasho, Japan, [2]F4E, Garching, Germany, [3]QST, Rokkasho, Japan, [4]IPFN, Lisbon, Portugal

Presented at WAO2023, Tsukuba, Japan – PO37

Introduction

Accelerator-based high energy neutron sources are studied to characterize future fusion reactors material. The Linear IFMIF Prototype Accelerator (LIPAc) is a full-scale prototype aiming at validating the production of a deuteron beam of 125 mA at 9 MeV in continuous wave in an international collaboration between Japan and the European Union.

The accelerator is located in Rokkasho, Japan, and many experts all around Japan and Europe are participating to LIPAc operations. For this reason, we have developed a web-based remote participation system, which can be used by experts to monitor the status of the operation in real-time from anywhere in the world. Our solution provides to each user a virtual desktop with the same environment and tools as the control room in Rokkasho, and a real-time, read-only copy of the accelerator data.

We will explain the technical and organizational challenges met during the development, and the solution adopted to ensure the security and safety of the operation, balanced against the ease of use for our experts.

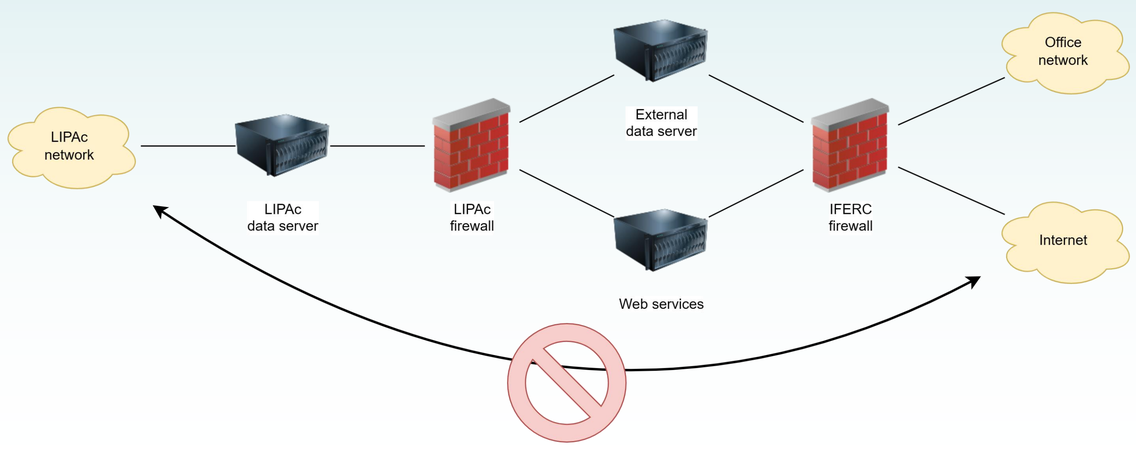
1. Background and requirements

- LIPAc uses EPICS as its control system framework, CSS for the operator interfaces, and CSS' Archive Engine over PostgreSQL with TimescaleDB to record and retrieve historical PV data. Our system should provide access to both the operator interfaces with live PV data, and to data plotting tools with historical PV data.
- Data transfer must be unidirectional, only from LIPAc to the outside world. We don't want external users to be able to operate the machine remotely.
- To prevent data leaks, access by external users must be encrypted and authenticated.
- The system should be as user friendly as possible.

2. Network topology

For security reasons, the LIPAc network is isolated from the Internet. To transfer data in a secure way, we created the following topology:

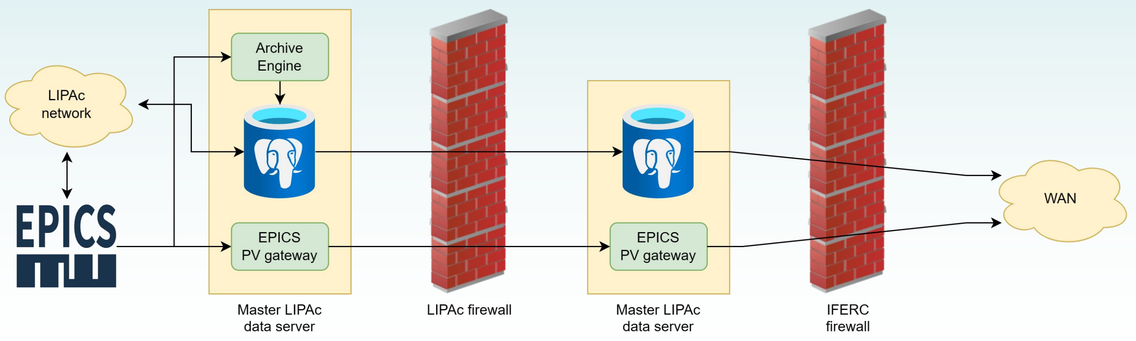
- The original data is stored in the master LIPAc data server, located in the accelerator building and connected directly to the LIPAc network.
- A replica server in a dedicated server subnet in the supercomputer building in Rokkasho. This subnet also hosts the other web services that we provide.
- The master data server has two network interfaces, one for the LIPAc network and one for data transfer. The replica server also has two interfaces, one for LIPAc and one for the outside world.
- Both connections are protected by independent firewalls. This way, we ensure that a direct connection between the LIPAc network and the outside world is impossible.



3. Unidirectional data transfer

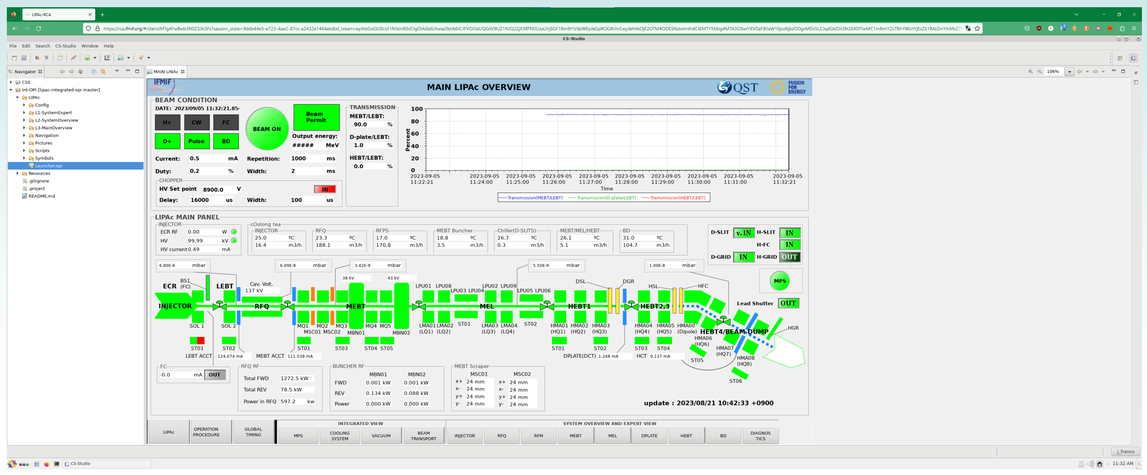
We want to provide access to both the live EPICS data, and the archived historical data:

- For the archived data, there is a primary PostgreSQL server running inside the LIPAc network, and a replica server in the server network. Data transfer is accomplished through PostgreSQL's streaming replication, which is read-only by design.
- For the live PV data, we have decided to use EPICS PV gateway. There is one gateway running in the server network, pulling data from another gateway running inside LIPAc. Both gateways are configured as read-only.



4. RDA (remote data access) and RCA (remote control access)

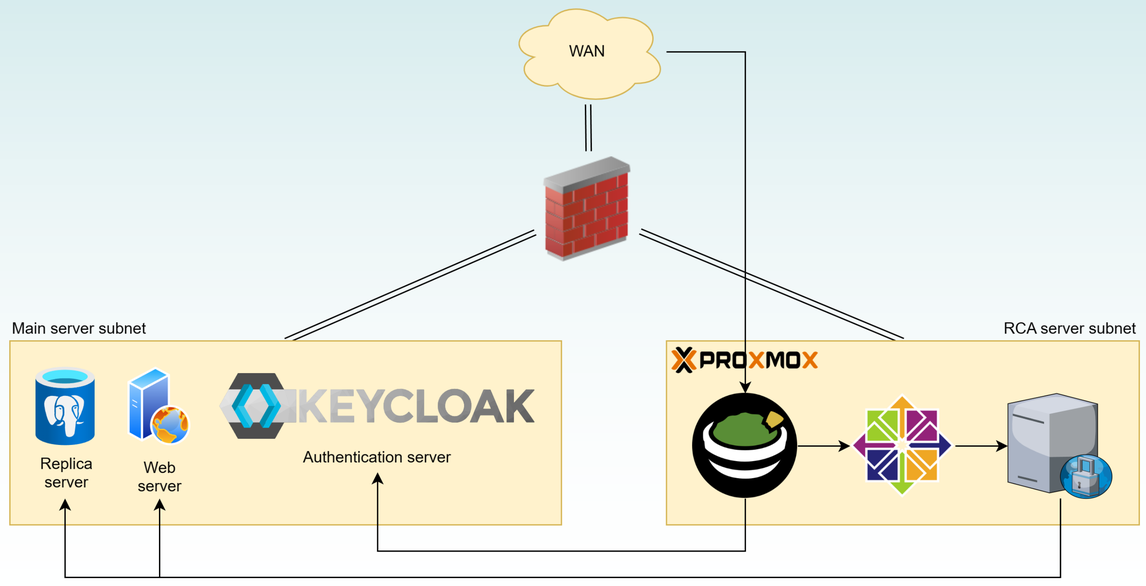
- For OPI developers that require raw data access, we provide the option of connecting directly to the PostgreSQL database and to the EPICS PV gateway.
- For normal users, we provide a virtual desktop solution (VDI) accessible through the web browser. The virtual environment runs on CentOS 7 and provides the same environment as the LIPAc control room:



5. Technical details

The RCA environment runs on a ProxMox server with 3 virtual machines. For security reasons, this server runs on separate subnet from the main web servers:

- One VM for the virtual desktop itself, running on CentOS 7 with xorgxrdp as it display server. We use RDP instead of the more traditional VNC because RDP provides better desktop resizing and handles dynamic user sessions more easily. To prevent unauthorized actions, the commands "su" and "sudo" are disabled.
- One VM running Apache Guacamole to provide web access to the virtual environment, integrated with our single sign-on system based on Keycloak.
- One VM to provide access from the VDI to the EPICS data and the other web services.



6. References

CSS	https://controlsystemstudio.org
PostgreSQL	https://www.postgresql.org
TimescaleDB	https://timescale.com
EPICS PV Gateway	https://github.com/epics-extensions/ca-gateway
Keycloak	https://www.keycloak.org
Apache Guacamole	https://guacamole.apache.org
Xorgxrdp	https://github.com/neutrinolabs/xorgxrdp
ProxMox	https://www.proxmox.com/

Conclusions and future work

The remote participation system was a long-standing request of the LIPAc project. The system that we have built is proving to be very useful for the on-going beam campaign of summer 2023. User satisfaction is high, with the external collaborators commending the ease of use and the performance of the system.

However, we feel that there are still one field where we could make the system more efficient. Due to the long distance between Japan and Europe, the network latency is very high, a minimum of 200 ms. We are working on building a second RCA environment in Europe, with a dedicated IPSec VPN to the primary Rokkasho datacentre for secure data transfer. This way, users in Europe would be able to access the European system and get much faster response times.

This work was undertaken under the Broader Approach Agreement between the European Atomic Energy Community and the Government of Japan. The views and opinions expressed herein do not necessarily state or reflect those of the Parties to this Agreement.