12th IAEA Technical Meeting
on Control, Data Acquisition and Remote Participation for Fusion Research
13-17 May 2019, Daejeon, Korea

RUSSIAN RPOTOTIPE OF ITER REMOTE RARTICIPATION CENTER

I. Semenov[1], L. Abadie[2], S. Kuzminov[1], A. Larionov[1], S. Lazareva[1], P. Makijarvi[2], E. Mironova[1], S. Simrock[2], S. Portone[1], D. Stepanov[2], O. Semenov[1]

1- “Project Center ITER”, Russia, Moscow, sq. Academic Kurchatov, 1 b.3

2- ITER Organization, St. Paul-les-Durance, France

Work done under contract H.4a.241.19.18.1027 with ROSATOM and Task Agreement C45TD15FR with ITER Organization.

Background and Objectives.

All Domestic Agency in ITER has a lot of plasma diagnostics and technological systems Procurement Arrangements for ITER project. In scope of this work in nearest future they will need some kind of Remote Participation Centre with Remote Participation Room for remote functions of these PA's for future monitoring from DA in scope of warranty coverage, maintenance support and ITER scientific collaboration.

Russian Domestic Agency work on Prototype of such RF DA Remote Participation Centre.

We do this work with ITER IO CODAC team and ITER IT Team.

THE MODEL OF Remote Participation Centre.

First step was to define model of a Remote Participation Center with the definition of basic parameters before deploying the prototype. What to define?

- Network and security issues;
- Communication issues. Audio and video links;
- Physical Cluster Infrastructure;
- Video wall and etc.;
- Remote Participation Centre users roles;
- Room model of RF DA RPC room according to RPC roles.

Network and security issues.

ITER infrastructure zoning is assumed in accordance with the requirements of information security and IEC 62645 standard. This standard defines three security degrees (S1, S2 and S3), to which graded security requirements. ITER defined these zones as follows:

S1 – Safety systems (POZ)
S2 – Conventional controls & interlocks (POZ)
S3 – External to POZ zone (XPOZ)

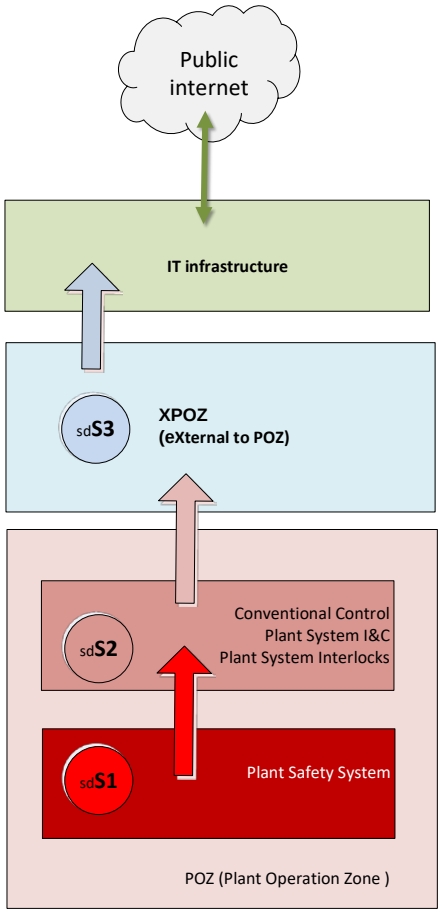
Anything outside S3 on ITER Site is IT zone.

Today, from RF DA for remote participation center we see 2 options:

Secure version: any remote participation center hardware infrastructure that have any kind of connection with XPOZ have to be in S3 security zone or in security zone that could be classified as S3.

Less secure version: move ITER XPOZ DMZ zone to IT zone. This will eliminate the need for classifying remote participation center hardware infrastructure to be in S3 security zone.

All this solution is not approved by ITER IO and it is still a big question about this approaches. This work is still in progress.



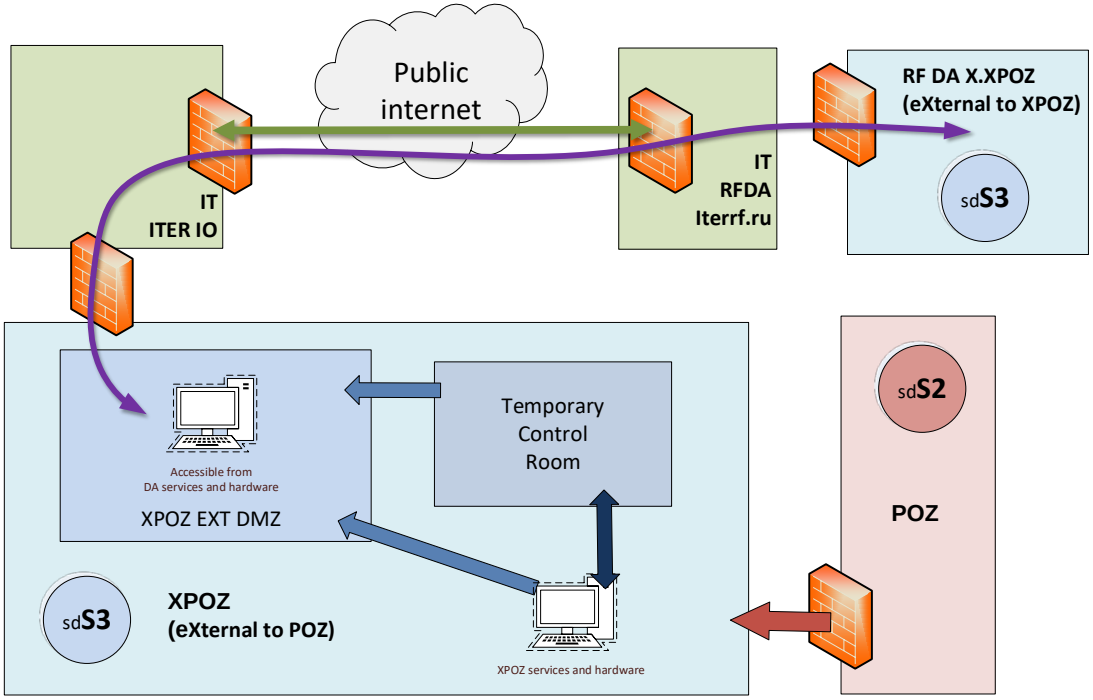
Network and security issues – current view - Secure version**.**

Current version from RF and IO - remote participation center hardware infrastructure that have any kind of connection with XPOZ have to be in S3 security zone or in security zone that could be classified as S3.

We name this zone as **external to XPOZ – X.XPOZ**.

X.XPOZ place in ITER network architecture (according to current construction stage) is shown left.

This variant is still under investigation and there is no final decisions.

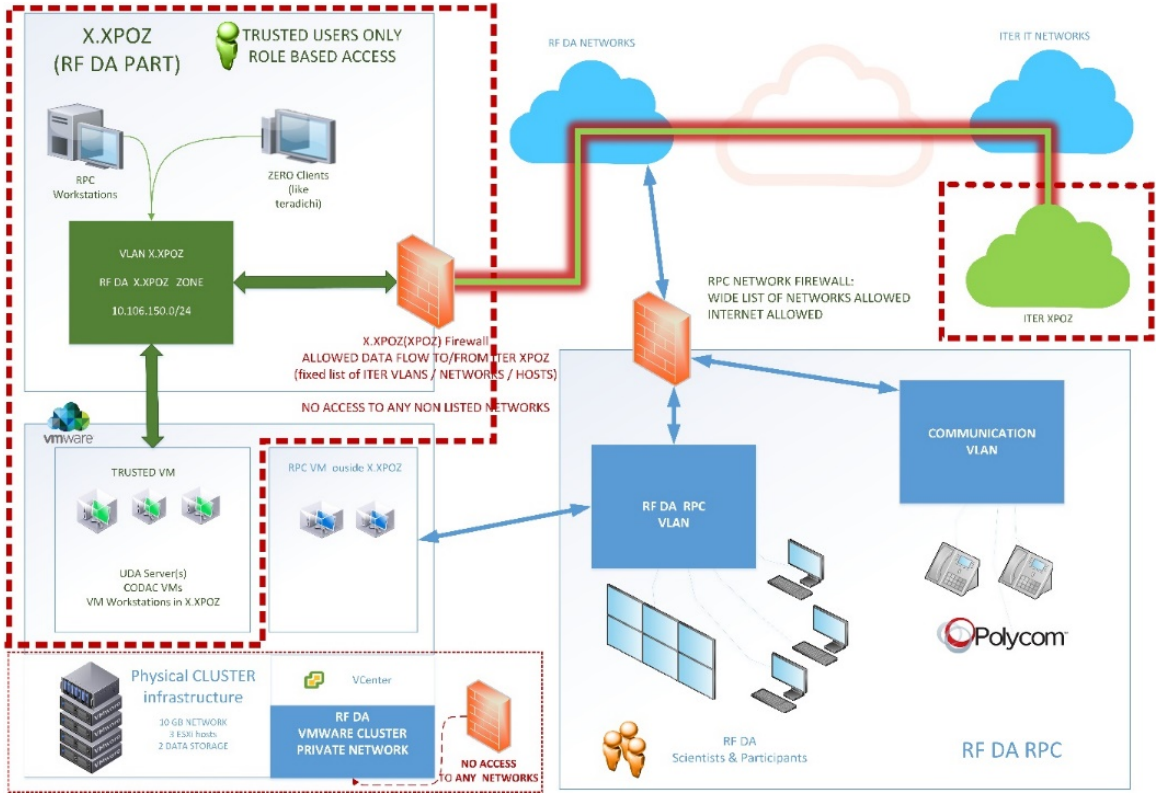


Network and security issues – current stage.

On the RPC side, a private dedicated subnet created. This subnet separated from any outside network and used exclusively for the RPC.

For communication purpose dedicated data link (IEEE 802.1Q) installed between ITER XPOZ and RPC private network. Any other outside communication is not allowed from this private dedicated subnet.

Only trusted hardware (and etc. are allowed in this subnet. Only role based access is possible to these machines and has to be controlled from ITER Organization.



Network and security issues –S3 Security degree conformity.

The minimum set of security requirements for S3-graded I&C CB&HPD systems:

- Access from non-I&C systems which could influence the I&C system functions shall be justified on a case-by-case basis and shall not compromise security and safety requirements associated to the system.
- Communications between S3-graded systems and non-I&C systems should be initiated from the S3 - graded systems. Exceptions shall be duly justified and the connection shall be monitored.
- Data transmission from a S3-graded system to a S2-graded system shall be strongly restricted and justified on a case-by-case basis.
- Software upgrade and configuration change of a S2-graded system shall not be possible from a S3-graded system.

In case of remote participation any possible access to I&C system, upgrade of software in s2 and etc. is already restricted in S3 XPOZ zone on plant side because RPC XXPOZ acts as a client to XPOZ data sources. In accordance with this, it can be stated that RPC network structure in the model complies with S3 requirement.

BUT… HERE STILL A BIG QUESTION.

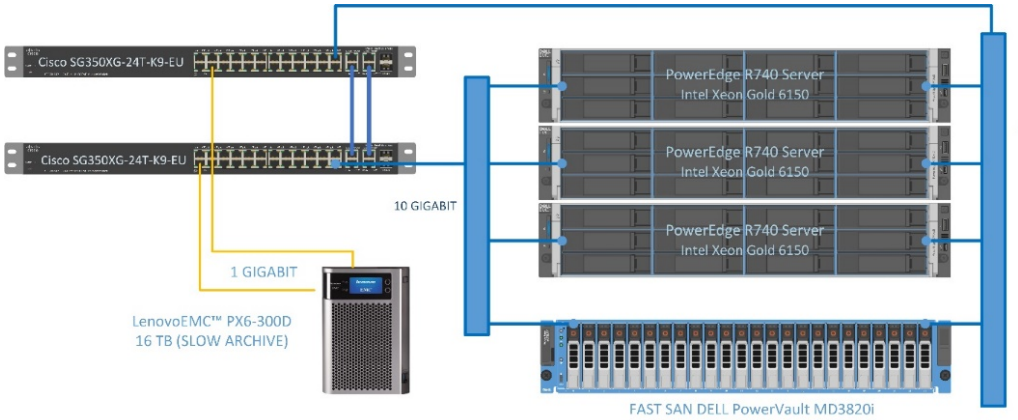
Audio and video links.

For communication purposes, solutions by POLYCOM and SKYPE FOR BUSINESS are used. In both cases, the remote participation center allows all participants to take part in a video conference or it is possible to use Skype for person to person communication. All this communication equipment is located outside X.XPOZ. Any data flow for communication purposes is not interact with S3 networks.

Cluster.

Considering scope of tasks, RPC cluster should meet the requirements of flexibility, scalability and should be easily adapted to any potential tasks.

To meet the requirements of flexibility and adaptability, we chose virtualization platform from VMware with VMware DRS cluster.



RPC Cluster hardware:

DELL PowerEdge R740 Server with dual Intel Xeon Gold 6150 (64 cores per host);

iSCSI SAN DELL PowerVault MD3820 with 10 Gigabit uplinks and 23 TB SSD Storage;

Cisco 10 Gigabit switches;

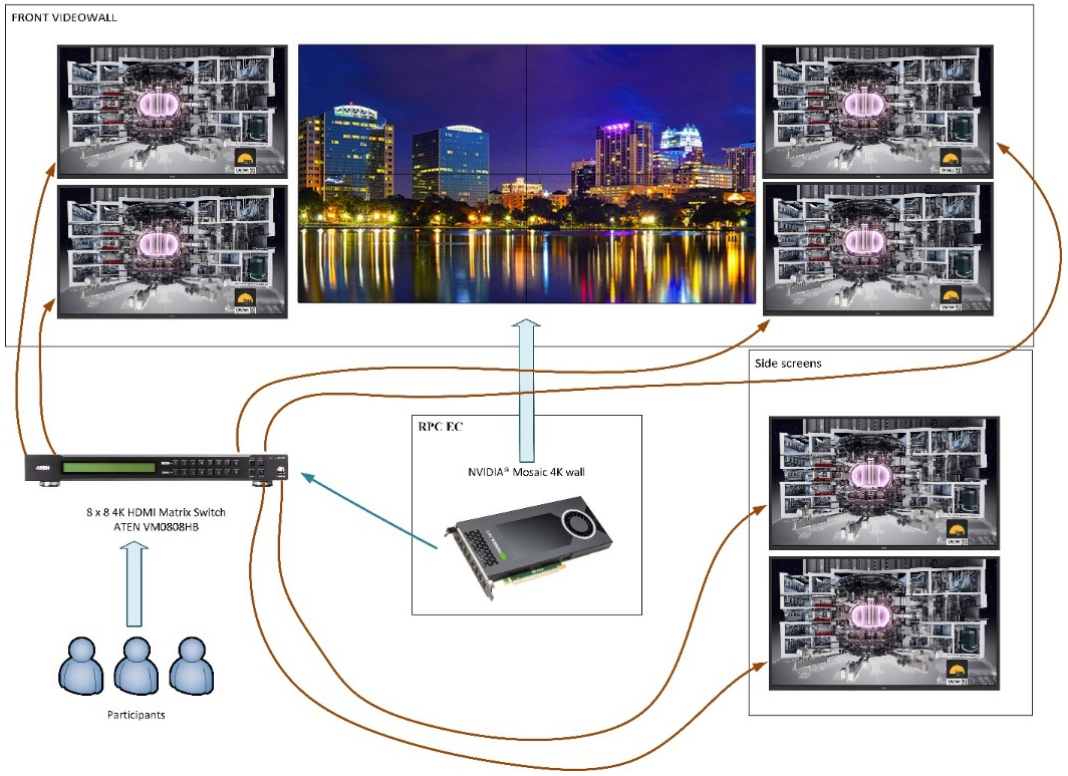
LenovoEMC PX6-300D 16 TB for slow data storage.

Video wall.

Video wall in a RPC is based on the principle of maximum flexibility for presenting information from different sources.

The central part of video wall is combined into a single screen by NVIDIA® Mosaic technology from dedicated Workstation in X.XPOZ. It is managed only by the RPC EC on the request from RPC RC.

For other purposes, we have foreseen the possibility of displaying any sources of information that are possible in the RPC on any other screens of the video wall in any time. All these displays are connected via the Matrix Switch. The selection of information sources is controlled by the RPC EC.



Remote Participation Centre Roles.

Remote Research Coordinator

Based on ITER Concept of Operations remote participants interact with the ITER Research Coordinator who gathers inputs and suggestions from both local and remote experts and ITER Research Coordinator interfaces with the ITER Session Leader. It is still a question, if some functions of Research Coordinator could be transferred outside ITER Main Control Room to remote participants but in any case the same concept to be applied for Remote Research Coordinator as in Concept of Operations for the role of Research Coordinator on site.

Engineer in Charge

Remote Participation Centre Engineer in Charge assists to Remote Research Coordinator in real time and adopting Remote Participation Centre infrastructure to current tasks. He is responsible for establishing any means of communication with Main Control Room and Remote Participation Centre video wall information structure.

Technician

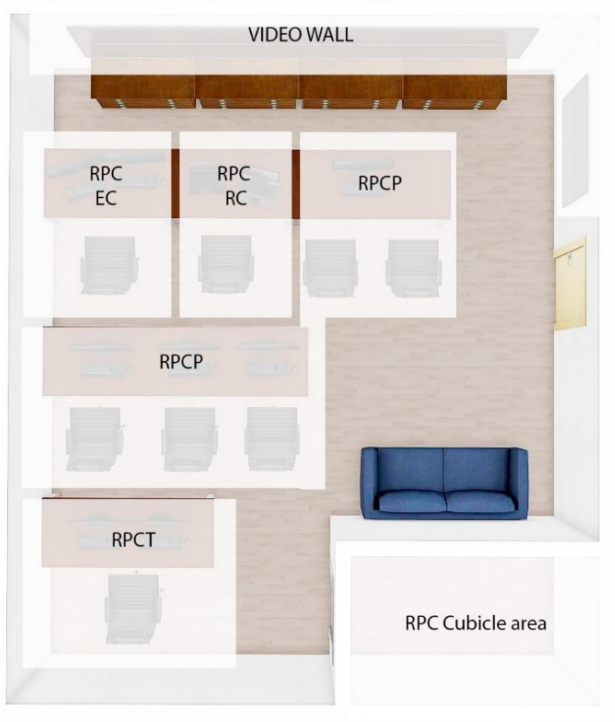
Responsible for all technical issues that are necessary for the functioning of the Remote Participation Center, commissioning, monitoring, configuration and operation of infrastructure.

Participants

Participants are part of scientific research team and engineers, which support Remote Research Coordinator in current session.

All remote participation staff is only allowed to be on Remote Participation Centre site by some prior approval procedure, that have to be defined in future by IO and DA.

Remote Participation Centre Room and working places.



RUSSIAN PROTOTIPE OF ITER REMOTE RARTICIPATION CENTER - TODAY

Remote Participation Centre tasks and progress.

Test of ITER remote participation interfaces (Unified Data Access server, Data Visualisation and Analysis tools, etc.). **Participation in ITER Temporary Main Control Room** activities (remote copy screens and HMI, data access, visual communication).

Network and security issues investigations. High-speed and low latency data transfer via existing public networks (reliability, speed accuracy, latency). Investigation of **Big data transfer** from ITER to DAs according to DA needs. Data collaboration and access to distributed storage resources, supporting wide range of use cases from personal data management to data-intensive scientific computations.

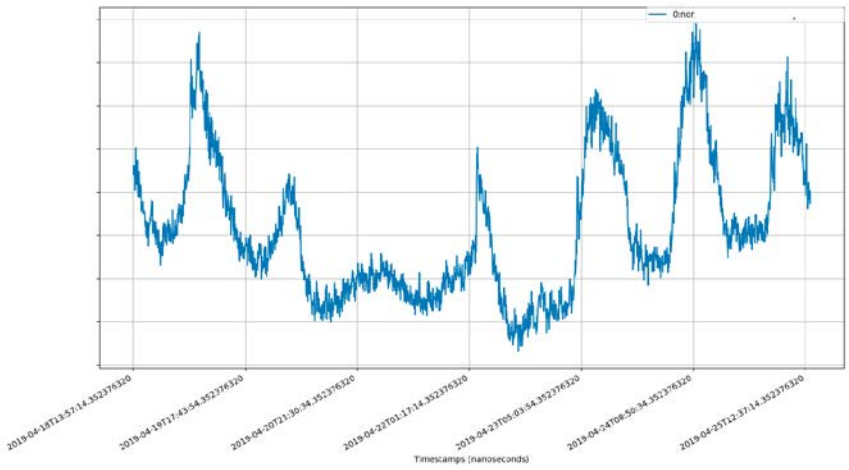
Local large-capacity data systems Investigations (archiving, storage, access).

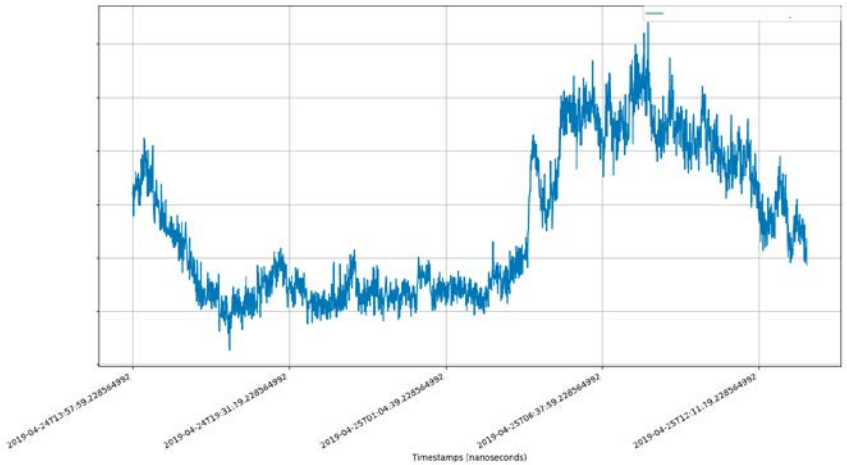
Test remote monitoring of plasma diagnostics and technical systems in scope of warranty coverage and maintenance support and ITER scientific collaboration.

Training of personal for ITER operation in future.

…. and a lot more….

Remote Participation Centre current **UDA access example** – Power consumption on ITER site - real time data.





THANK YOU