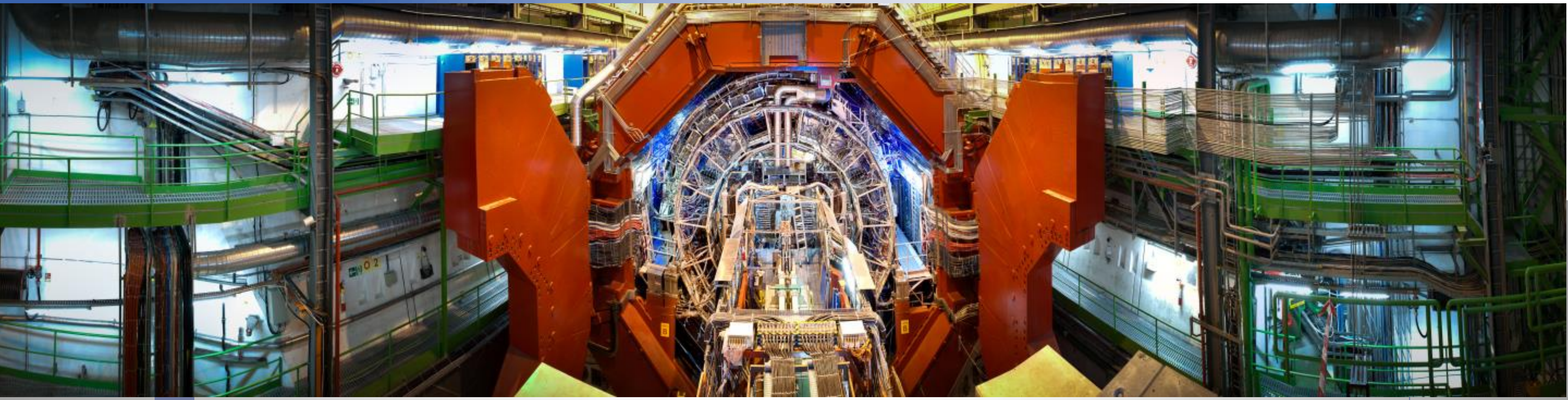
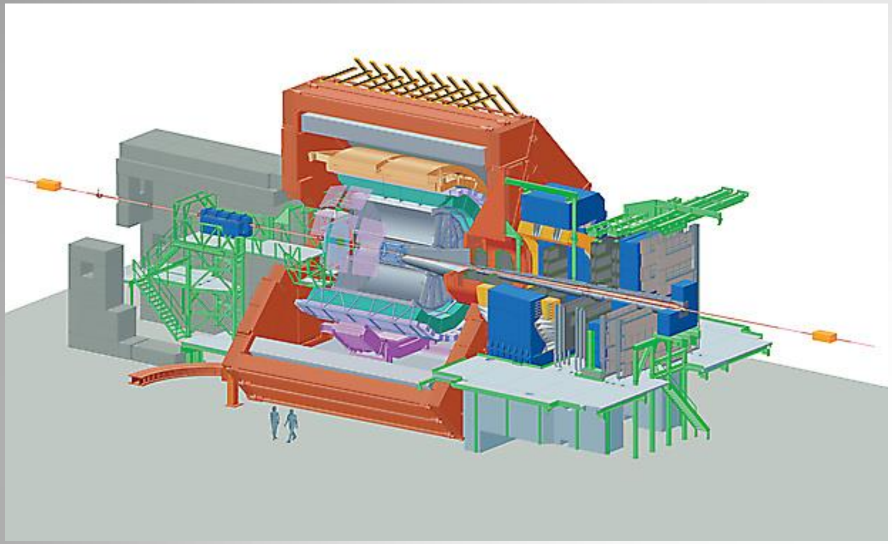


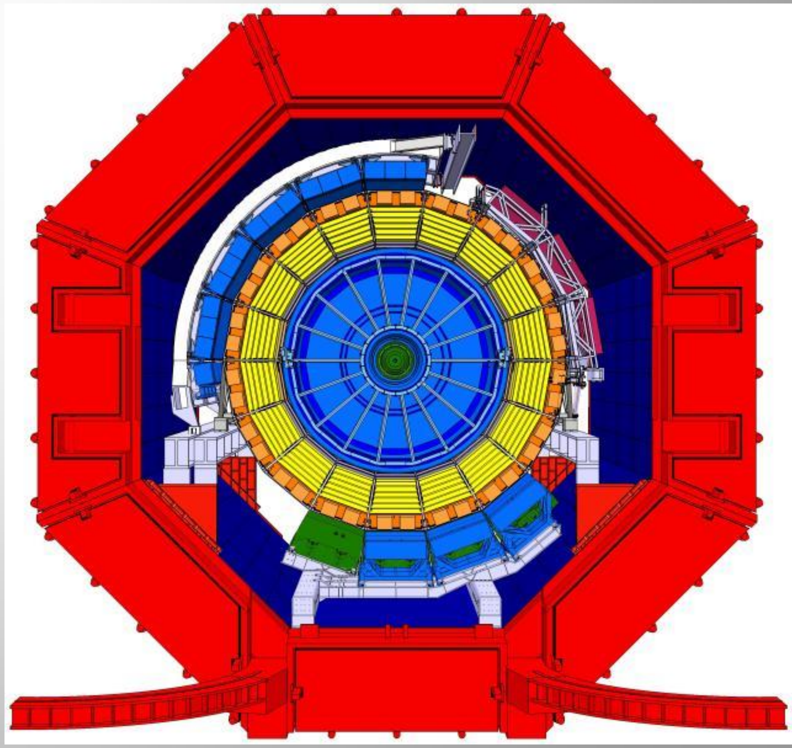
Remote access to ALICE control system

Peter Chochula
CERN – Alice

ALICE – Heavy ion experiment at LHC

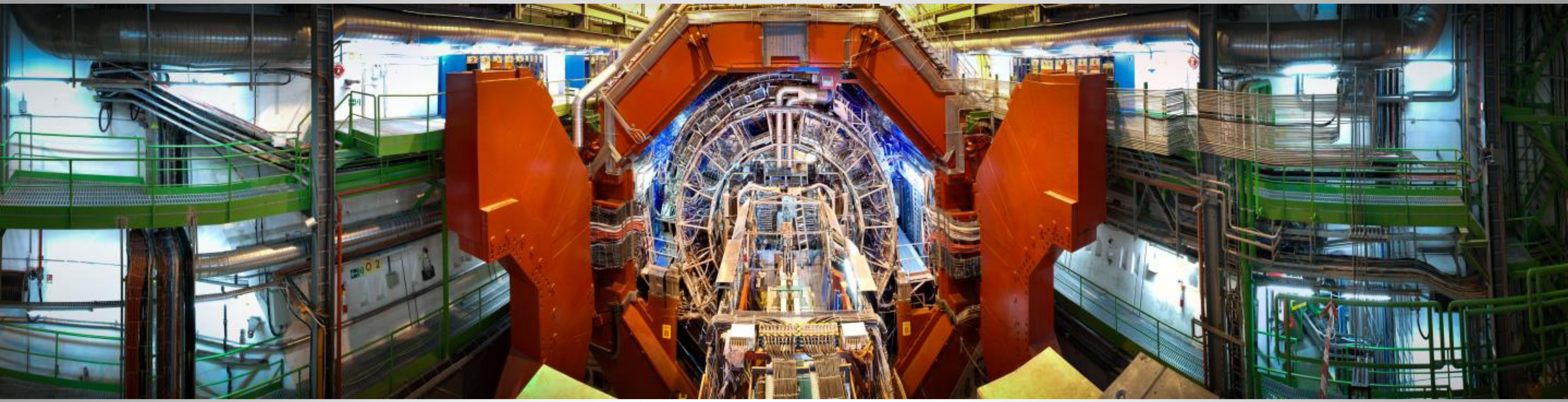


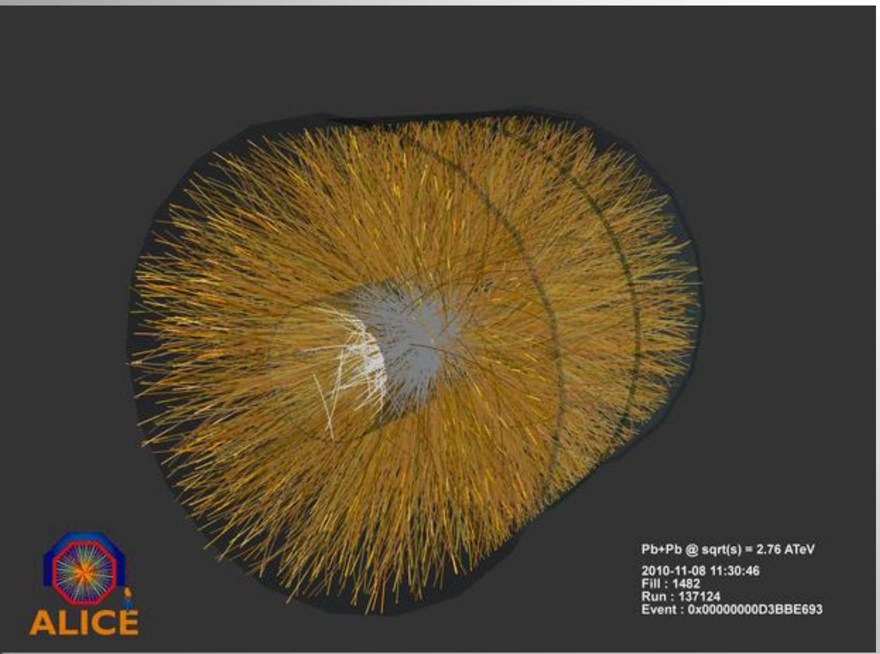
Detector:
Size: 16 x 26 m (some components installed >100m from interaction point)
Mass: 10,000 tons
Sub-detectors: 18
Magnets: 2

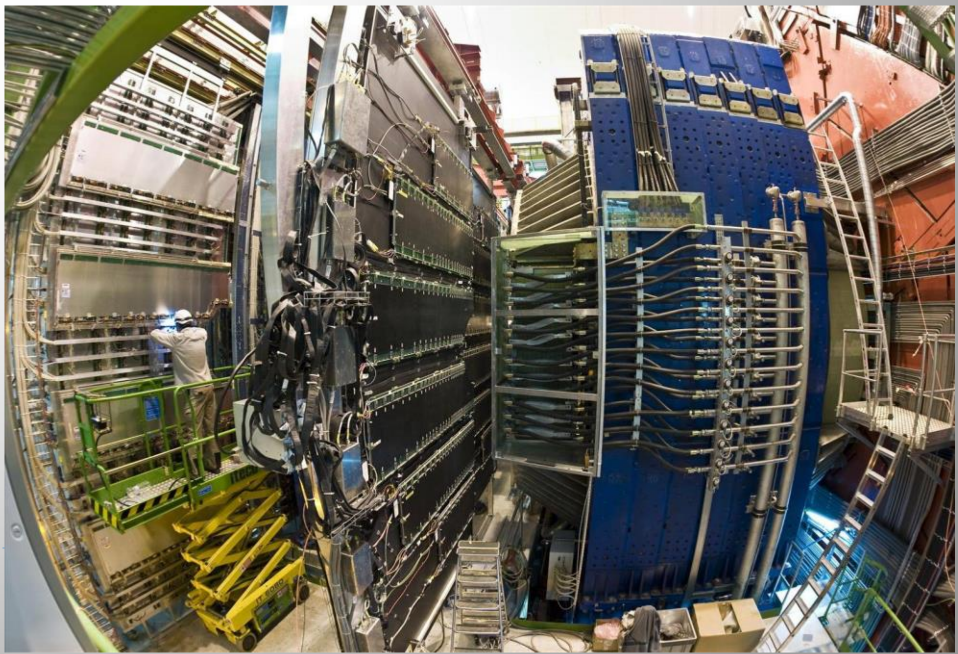


Collaboration
Members: 1500
Institutes: 140
Countries: 37

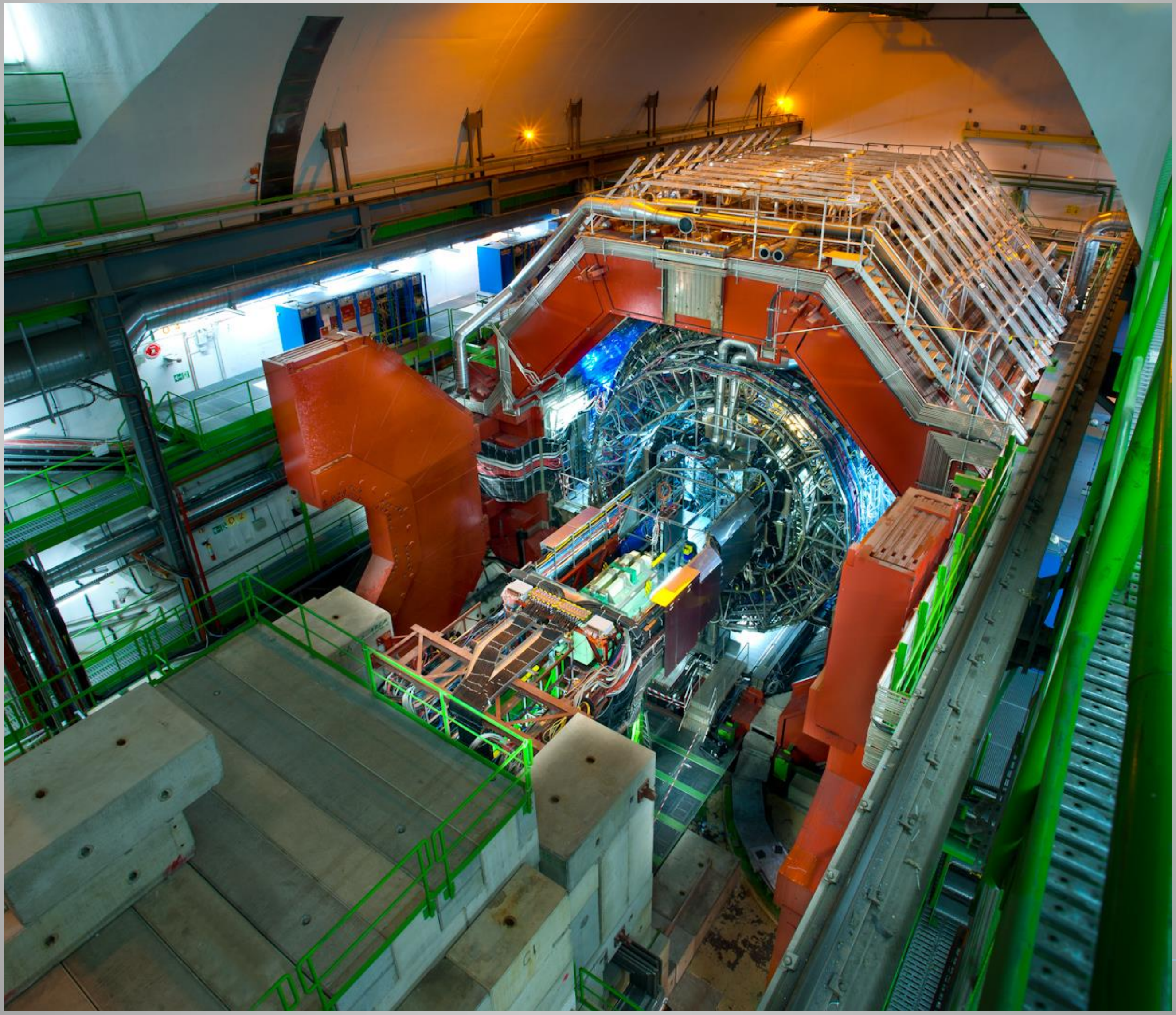
ALICE – Heavy ion experiment at LHC

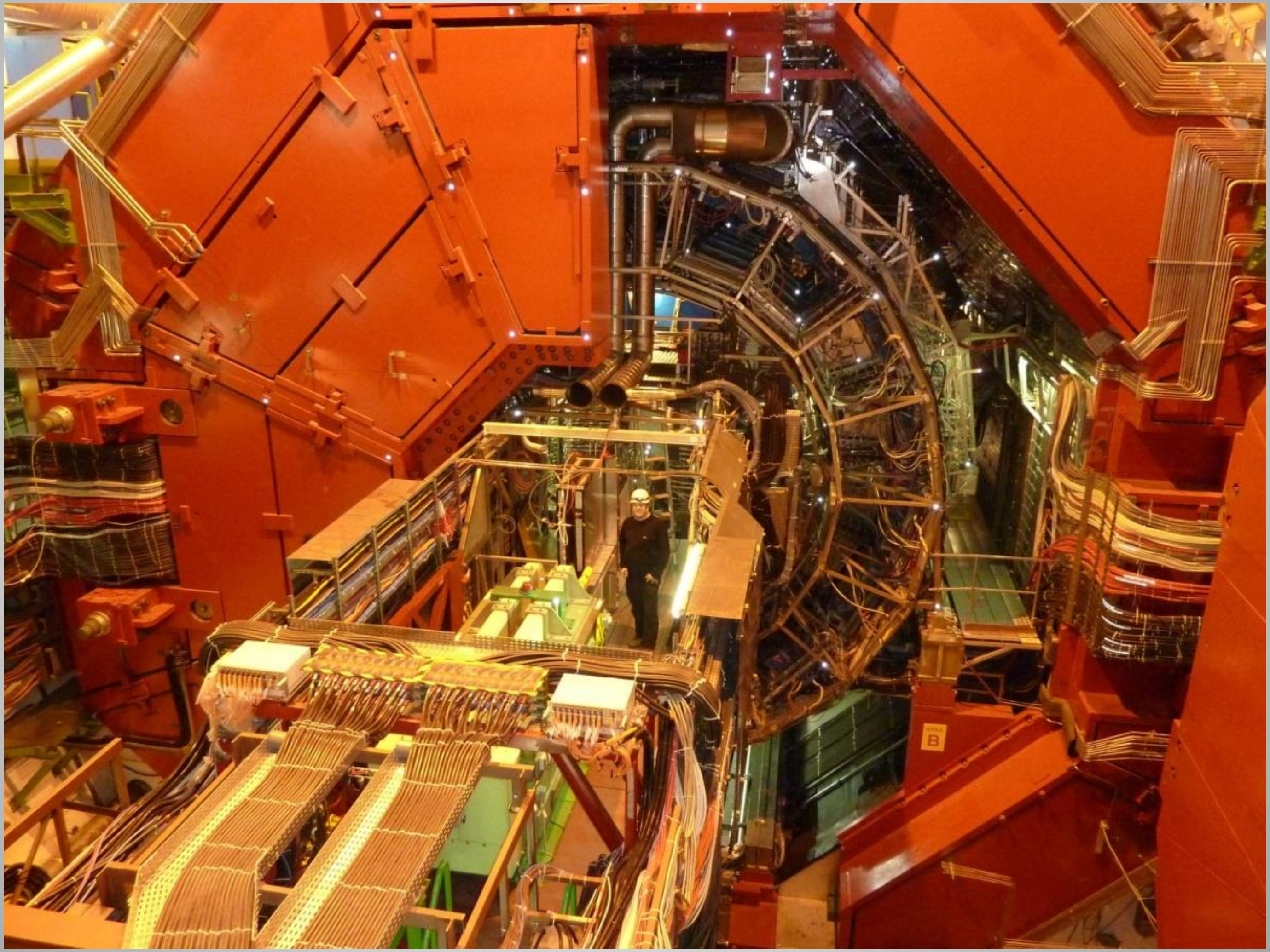






ALICE – Heavy ion experiment at LHC





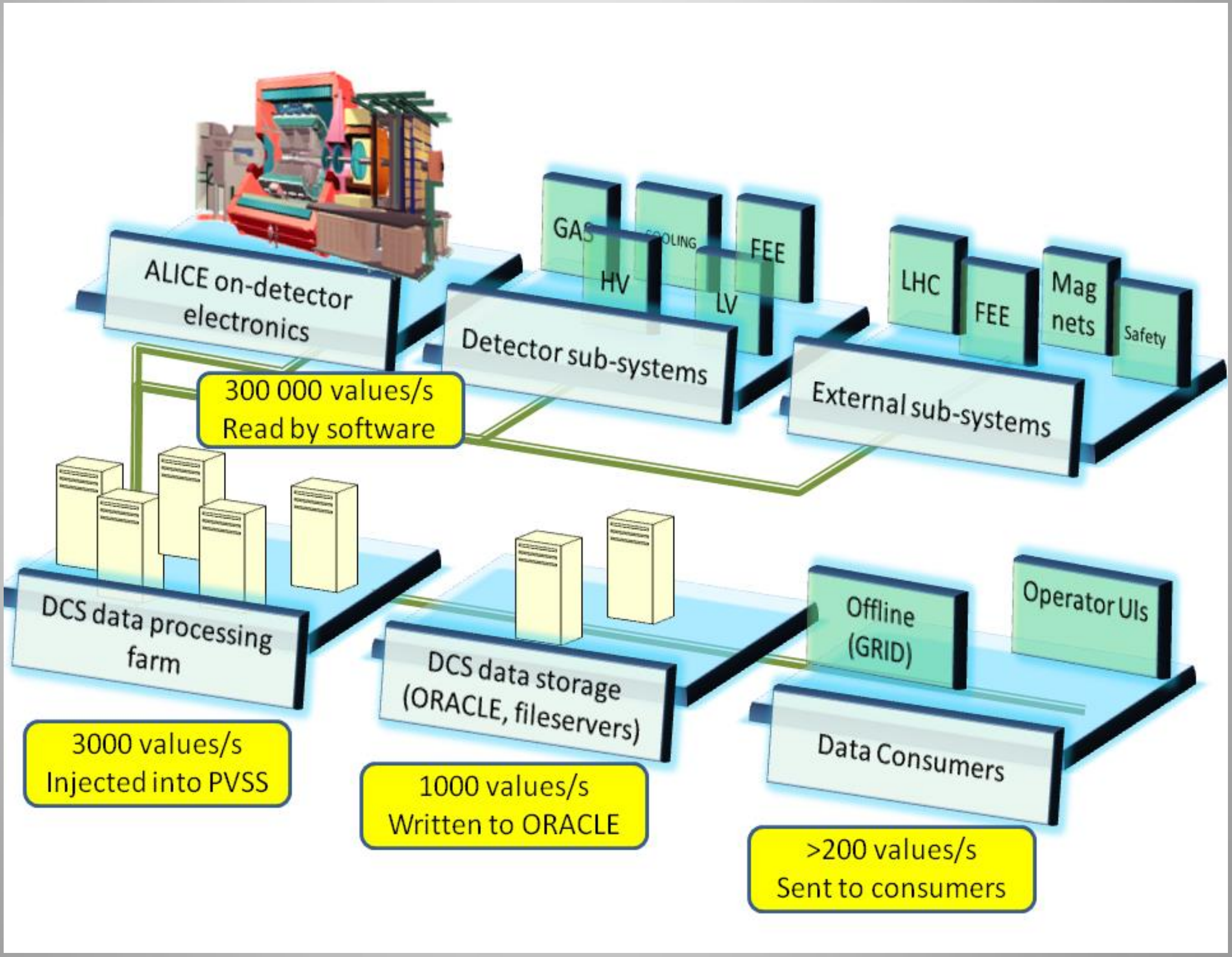
The Detector Control System

- Responsible for safe and reliable operation of the experiment
  - Designed to operate autonomously
  - Wherever possible, based on industrial standards and components
  - Built in collaboration with ALICE institutes and CERN JCOP
  - Operated by a single operator

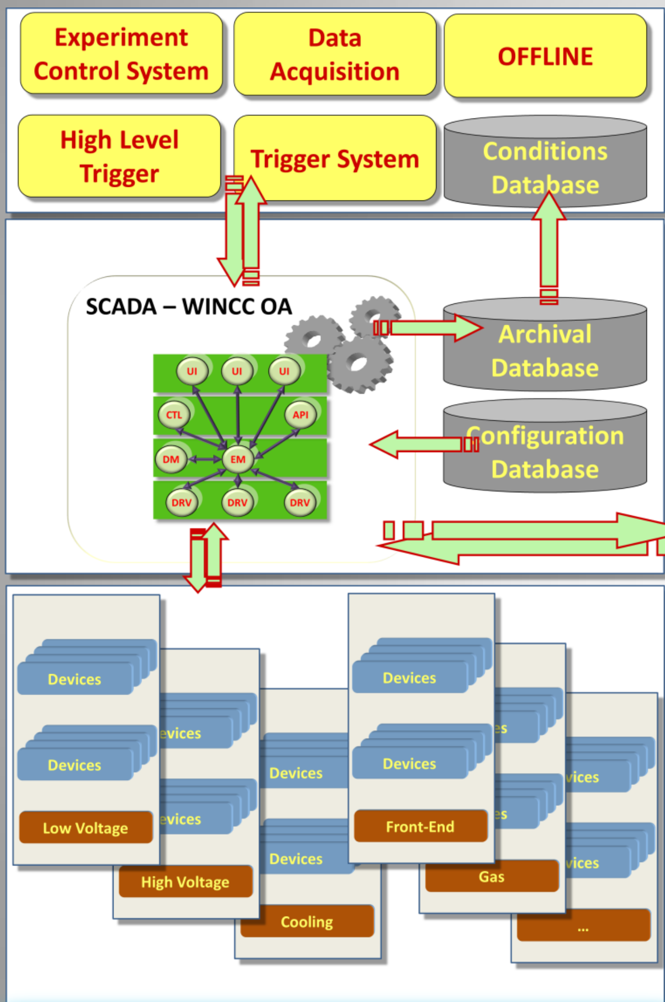
THE ALICE DCS AUTONOMY

- DCS autonomy guarantees safe operation in the absence of external services
- In the worst case scenario the DCS shuts down critical components

The DCS data flow



The DCS context and scale



Devices with similar functionality are grouped into subsystems. About 100 different subsystems are implemented in ALICE. .

18 autonomous detector systems

1200 network attached devices

100 WINCC OA systems

>700 embedded computers

>100 subsystems

170 control computers

270 crates

200 000 OPC items

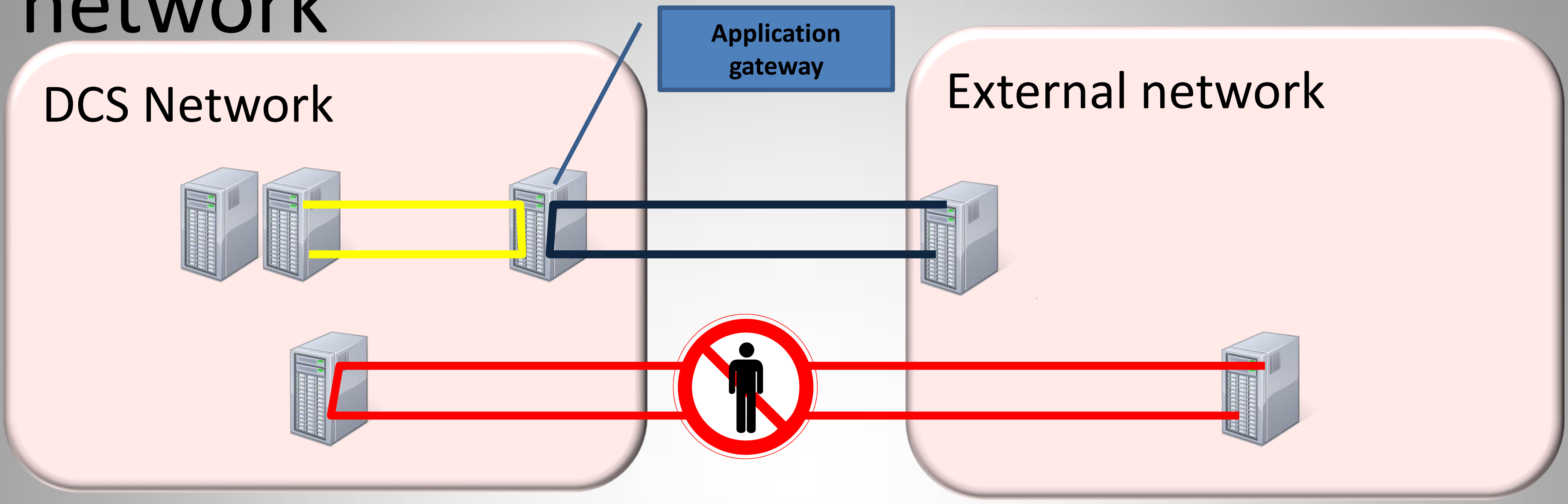
1 000 000 supervised parameters

100 000 frontend services

Are we really autonomous?

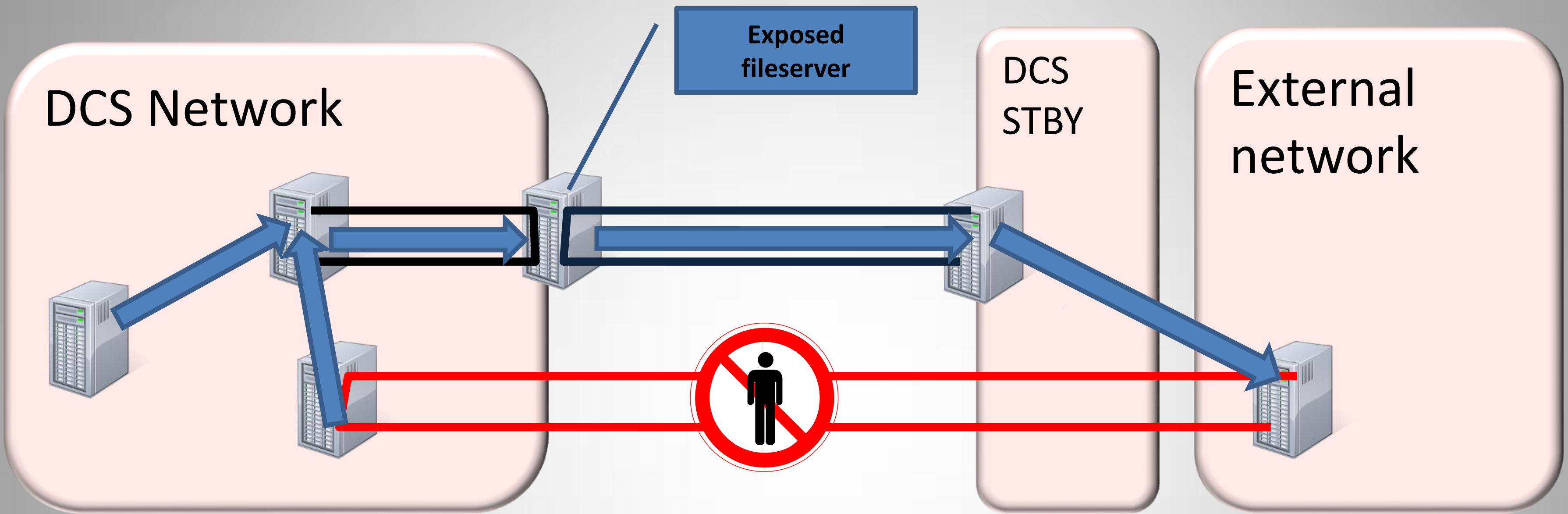
- Absence of external services could trigger immediate shutdown
  - Pixel detectors might melt in absence of cooling
  - Photon spectrometer might freeze if frontend electronics turns off while cooling is present
- ALICE operation is impossible without DCS feedback
- We are almost autonomous……

Remote interactive access to the DCS network



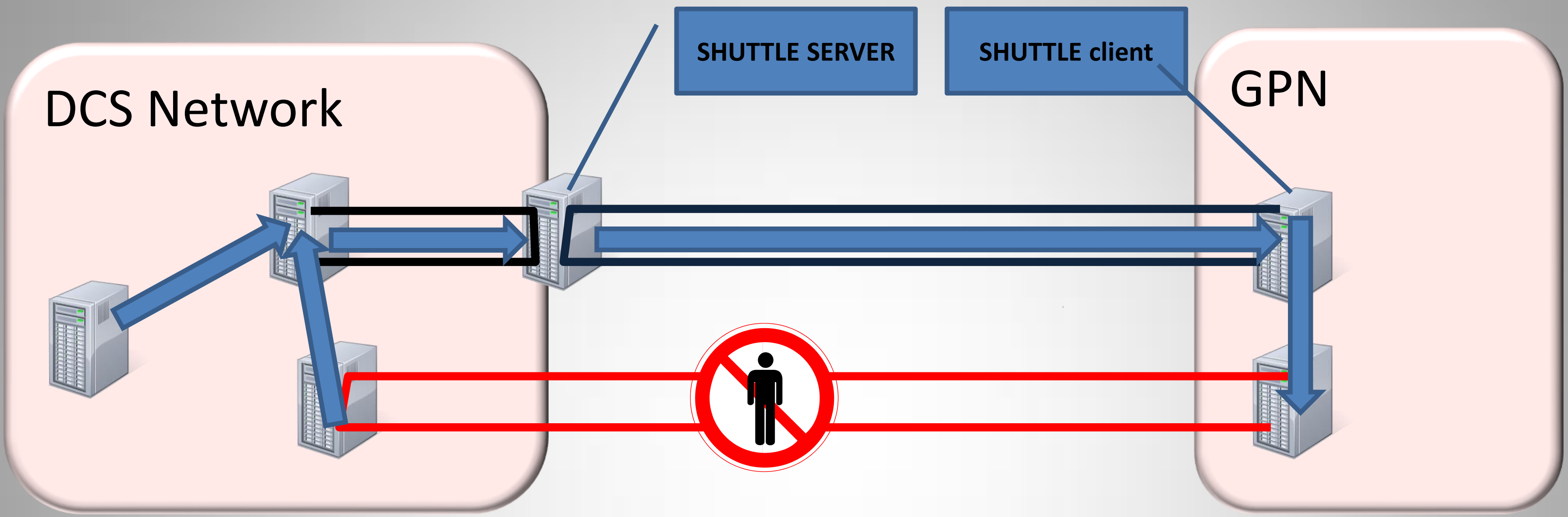
- No direct user access to the ALICE network
- Remote access to ALICE network Is possible via the application gateways
  - User makes RDP connection to the gateway
  - From the gateway further connection is granted to the network

Exposing files to external networks – DCS TELEPORT



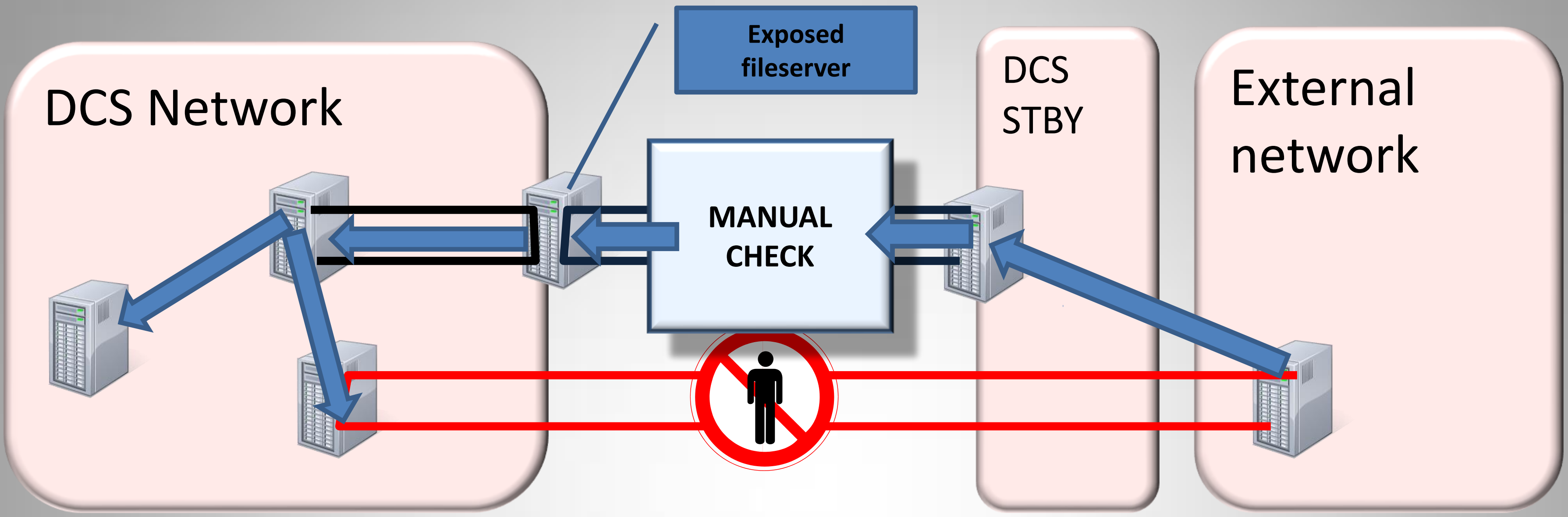
- No direct user access to DCS fileservers
- Files copied to dedicated area are automatically transferred to READ ONLY DCS STBY fileserver (on campus network)
- Read/only access granted to STBY fileserver
  - Access rights apply

Exposing files to OFFLINE – DCS SHUTTLE



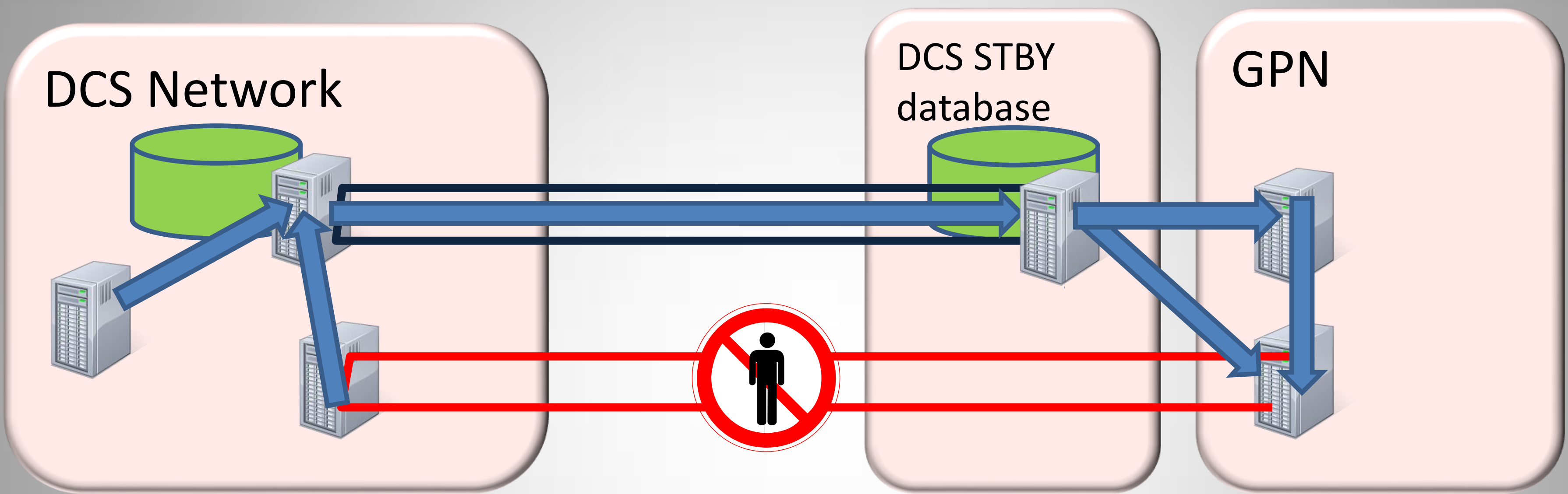
- As we do not know which files will be required by OFFLINE, a SHUTTLE service has been created
  - Trusted OFFLINE client searches the bookkeeping DCS database for available files and creates a request
  - DCS client delivers the files

Uploading files to DCS network



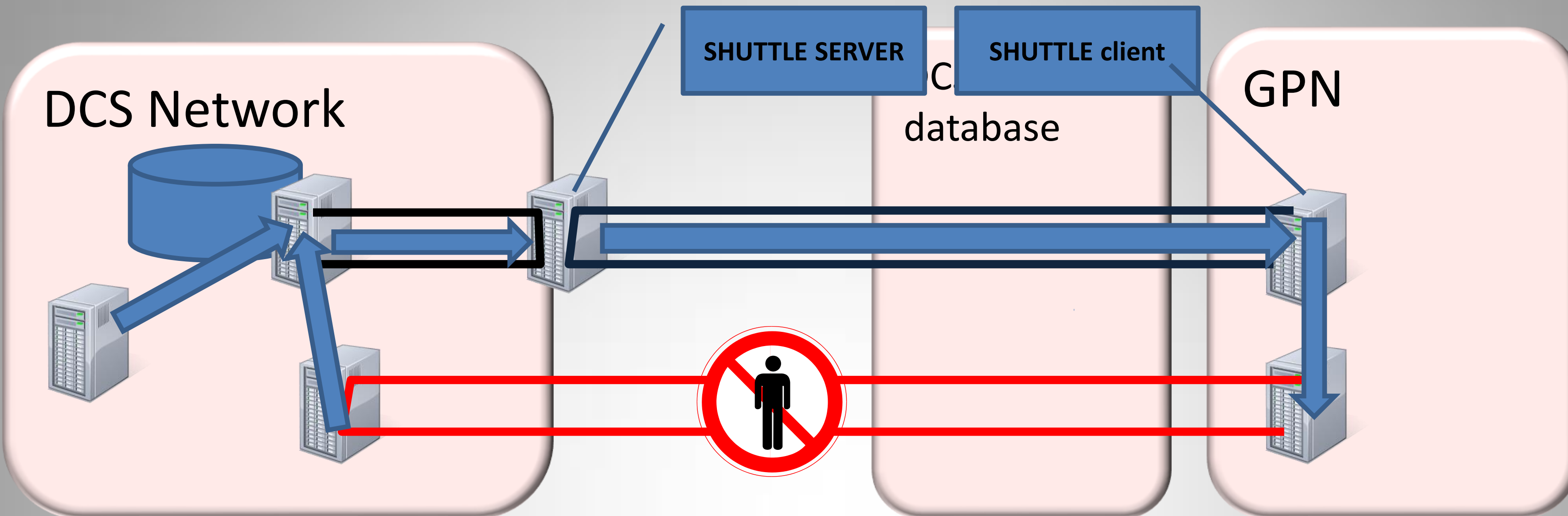
- No direct user access to DCS fileservers
- Files are uploaded on request
- No teleport

Exposing DCS database to external networks



- DCS archive database is mission critical
  - No direct access from outside
- All DCS data is replicated to standby read only instance available to clients

Exposing DCS database to OFFLINE



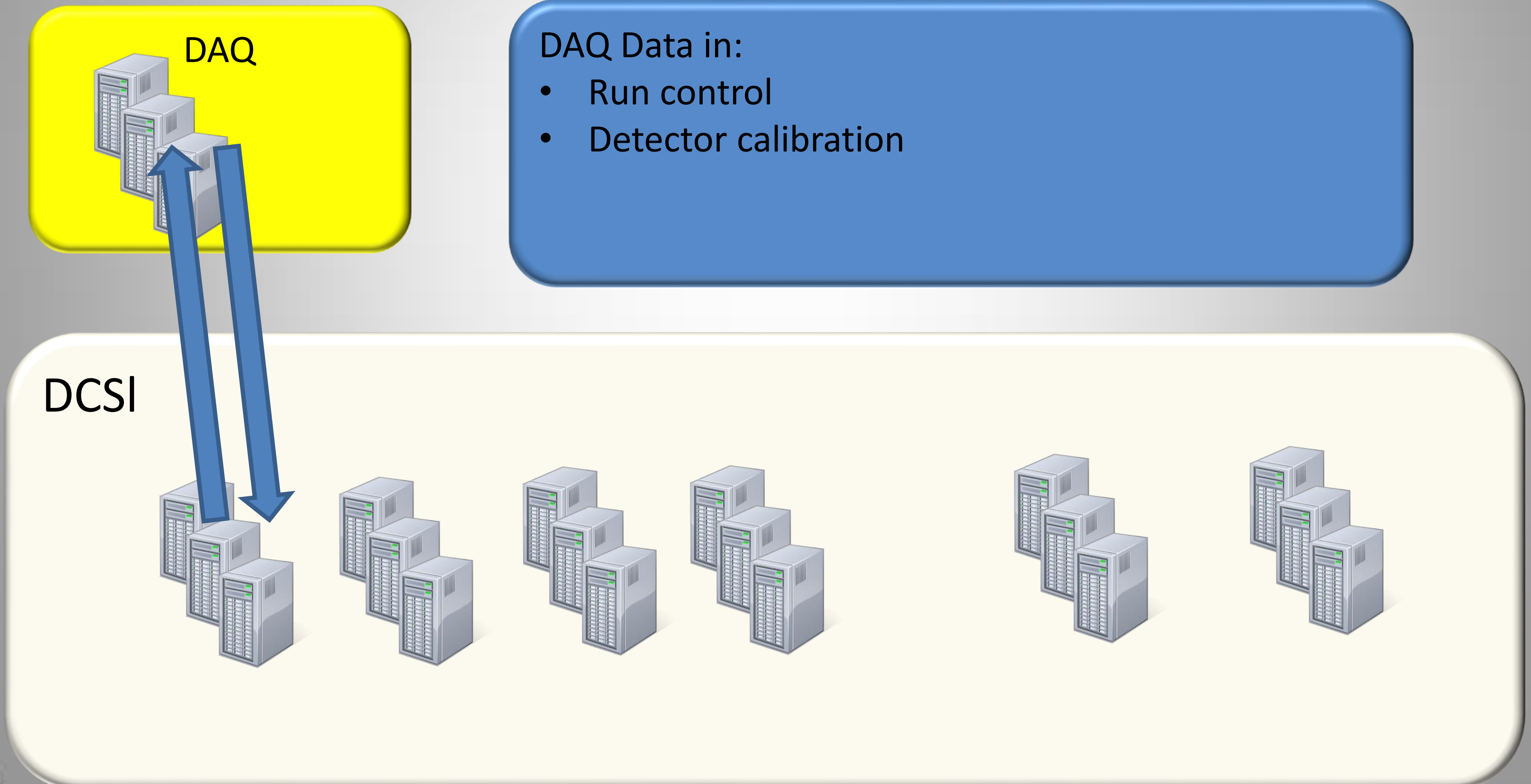
- Database replication latency would delay processing
  - Trusted OFFLINE client requests data
  - SHUTTLE server retrieves data from database and sends it to OFFLINE
    - Protection against excessive requests

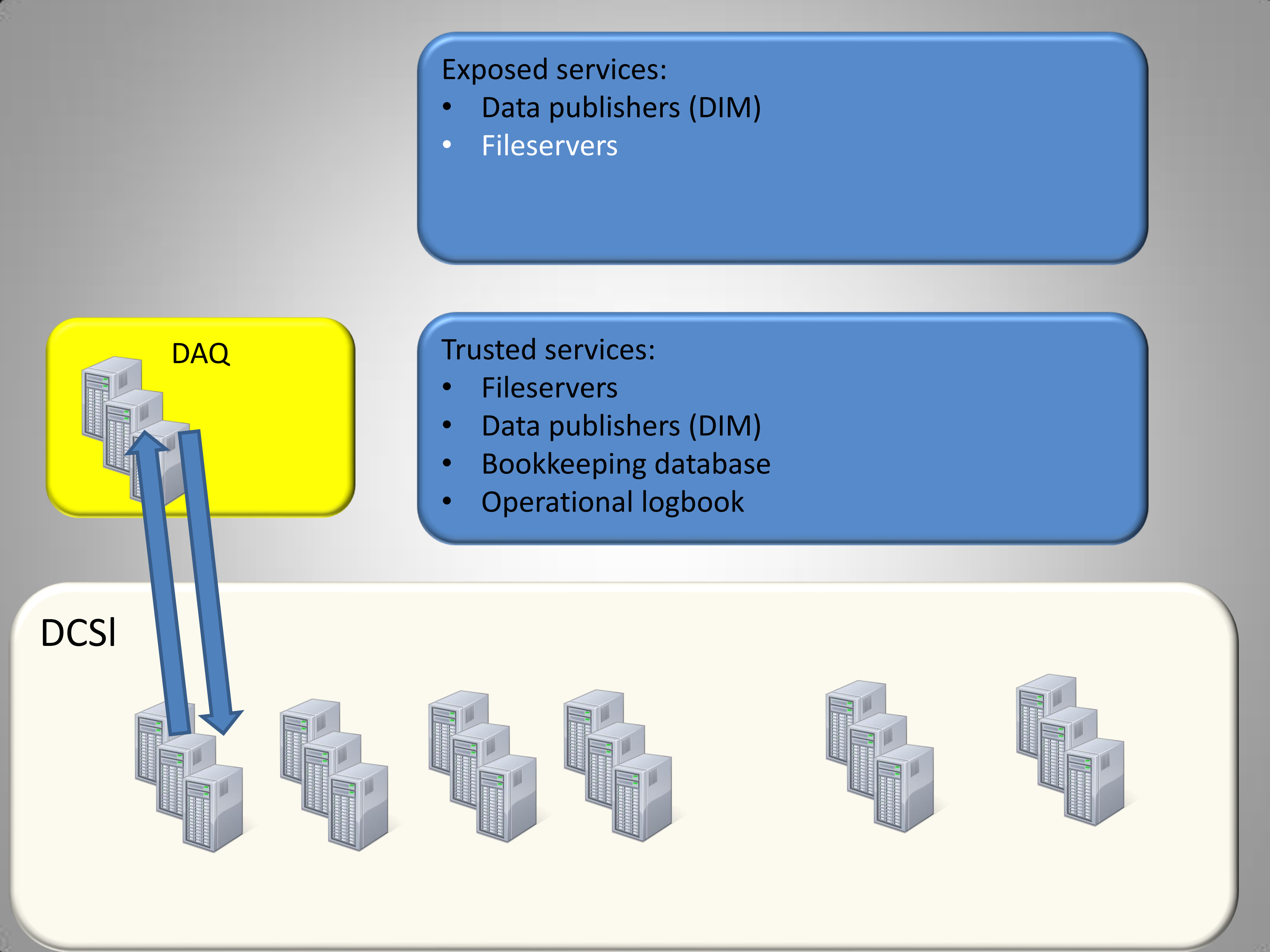
DCS Data out:

- Run conditions
- Environmental parameter conditions
- LHC conditions
- Detector calibration data

DAQ Data in:

- Run control
- Detector calibration




Exposed services:
• Data publishers (DIM)
• Fileservers
DAQ
Trusted services:
• Fileservers
• Data publishers (DIM)
• Bookkeeping database
• Operational logbook
DCSI

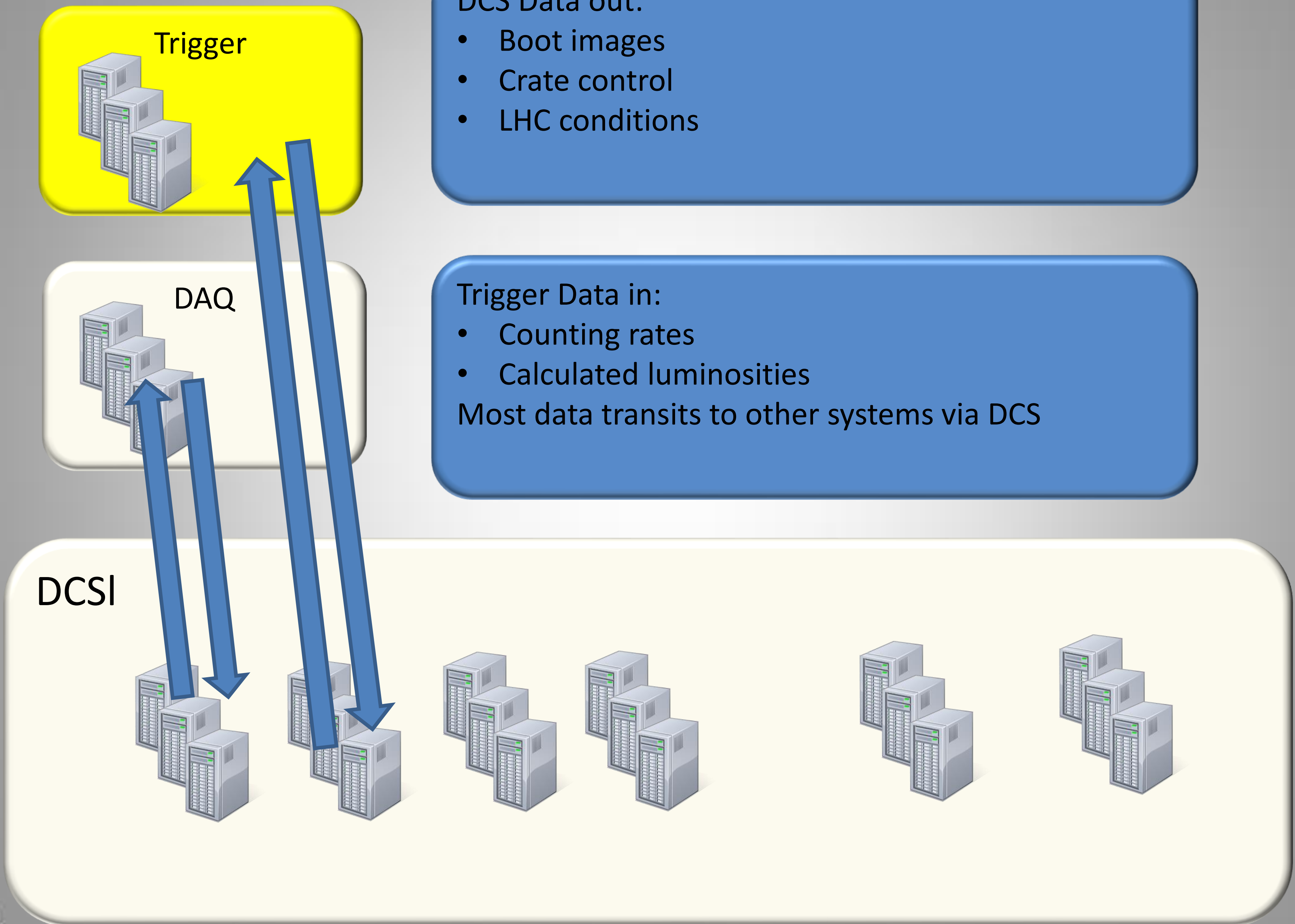
DCS Data out:

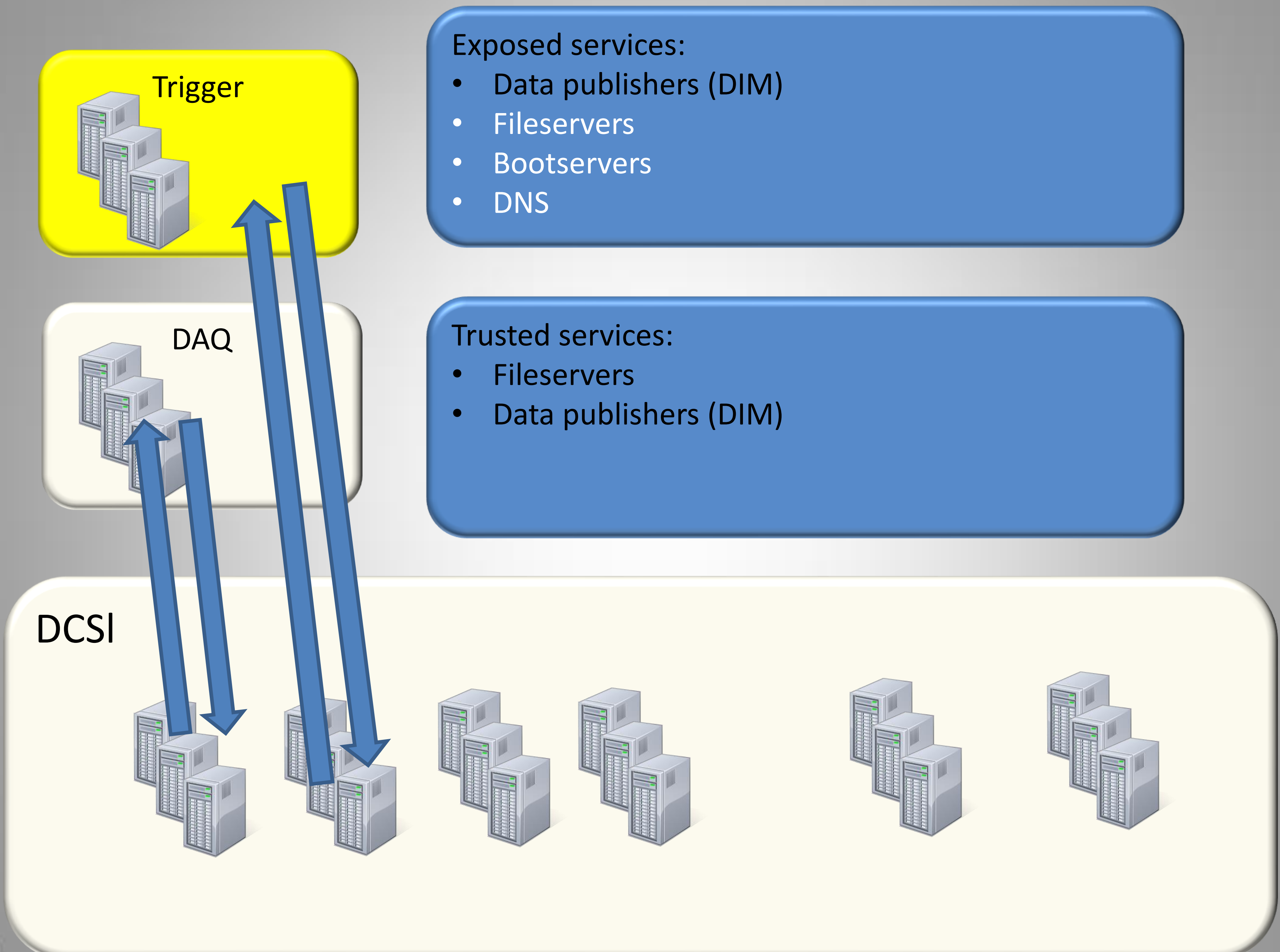
- Boot images
- Crate control
- LHC conditions

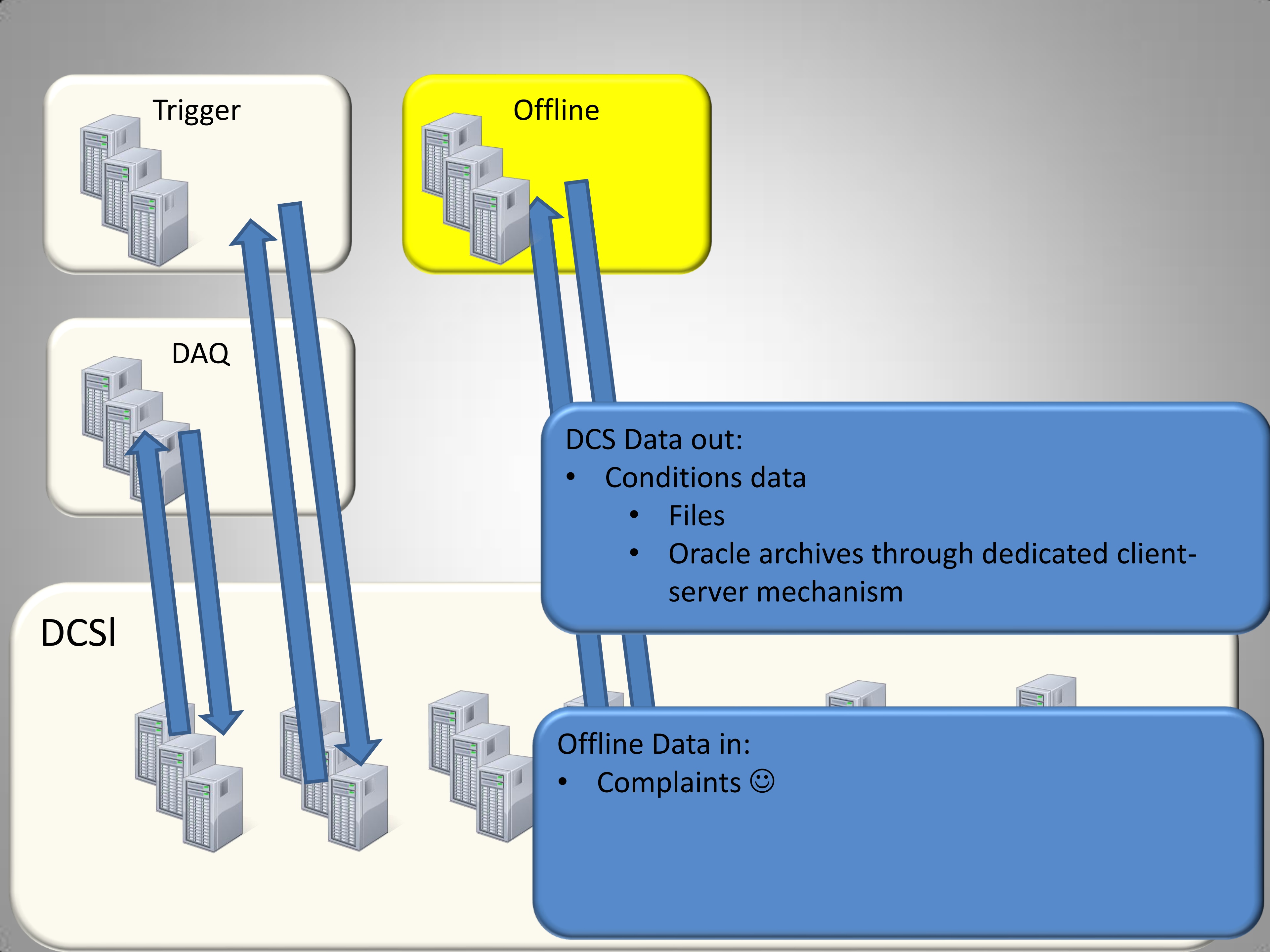
Trigger Data in:

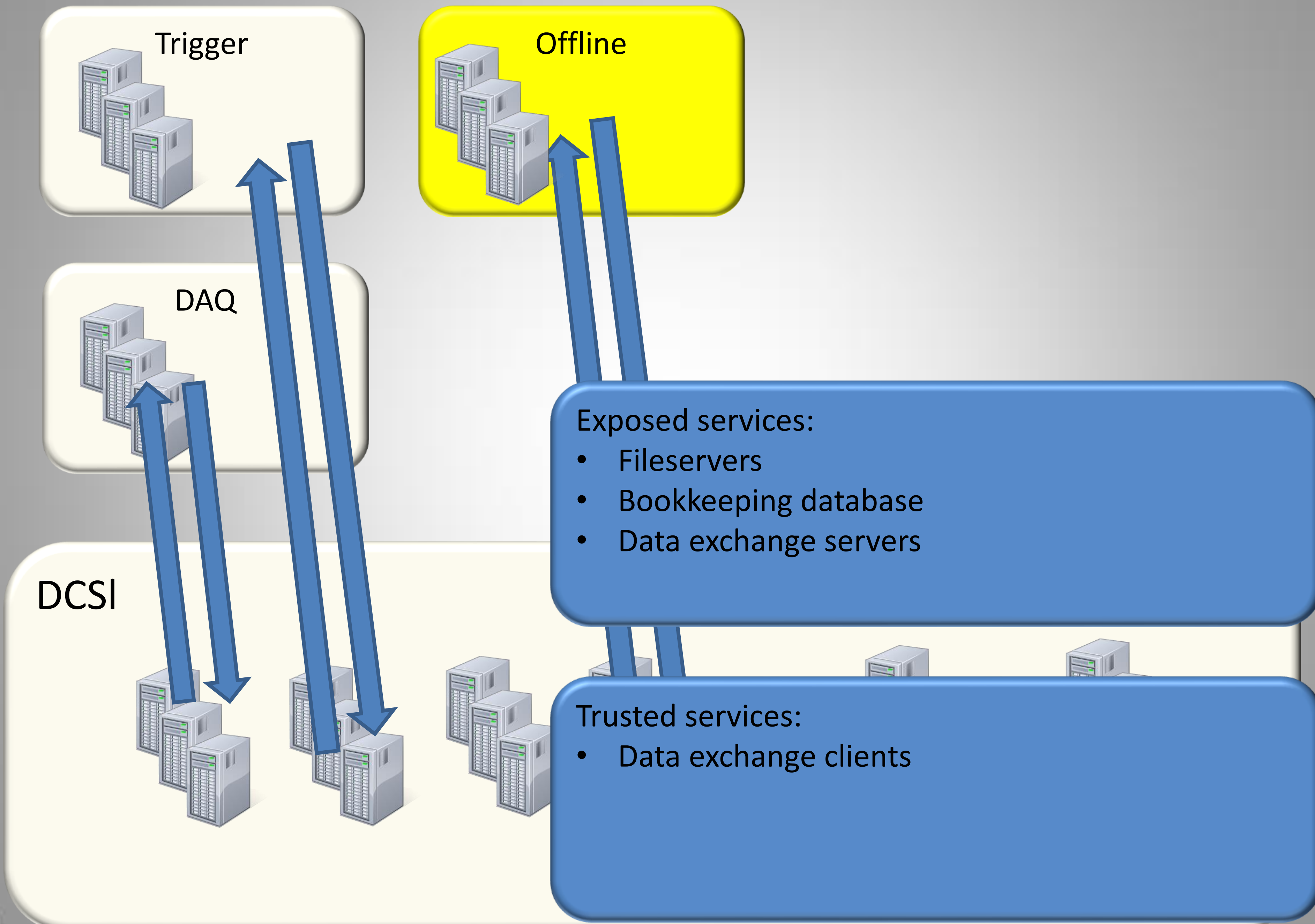
- Counting rates
- Calculated luminosities

Most data transits to other systems via DCS

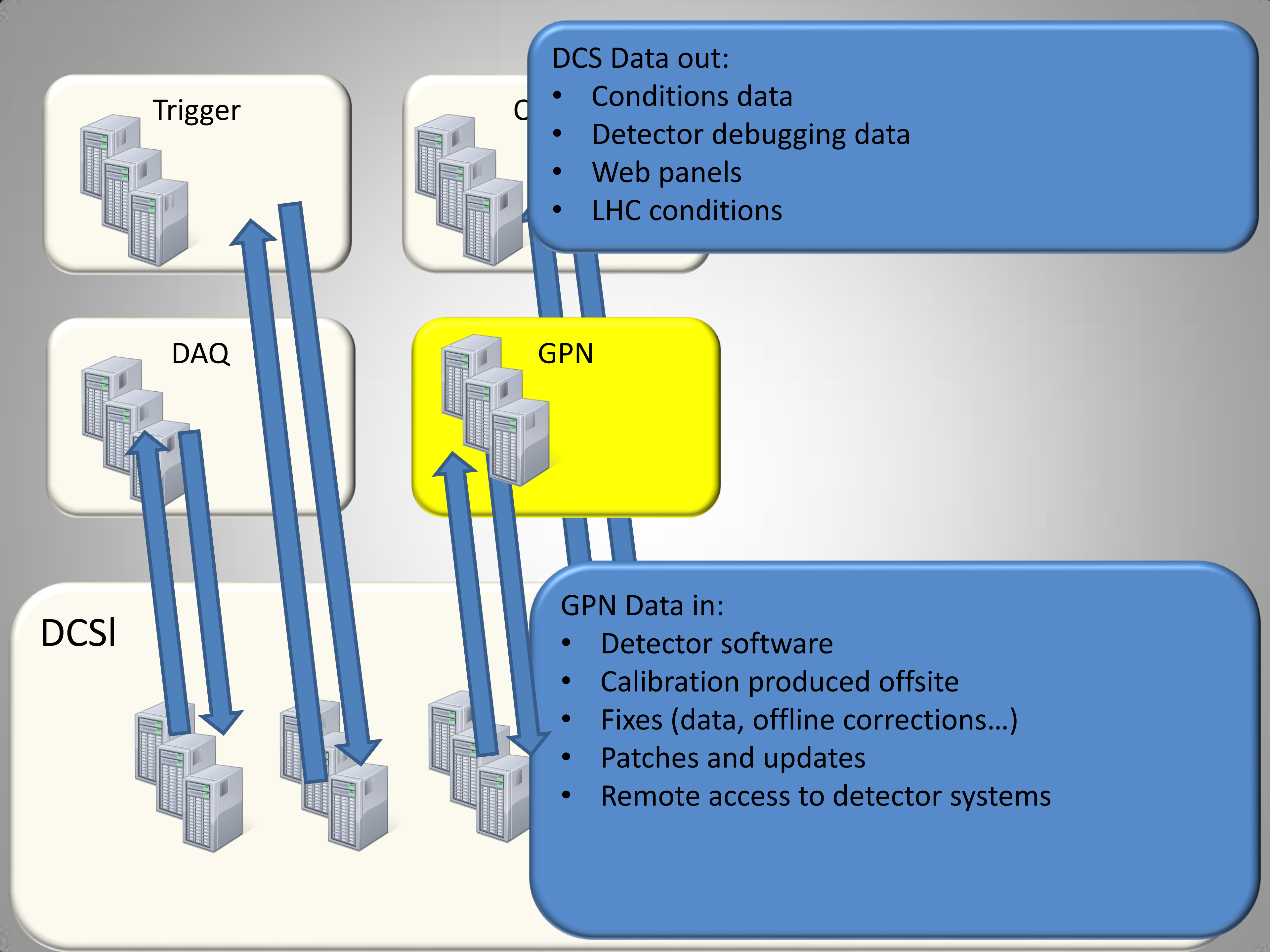


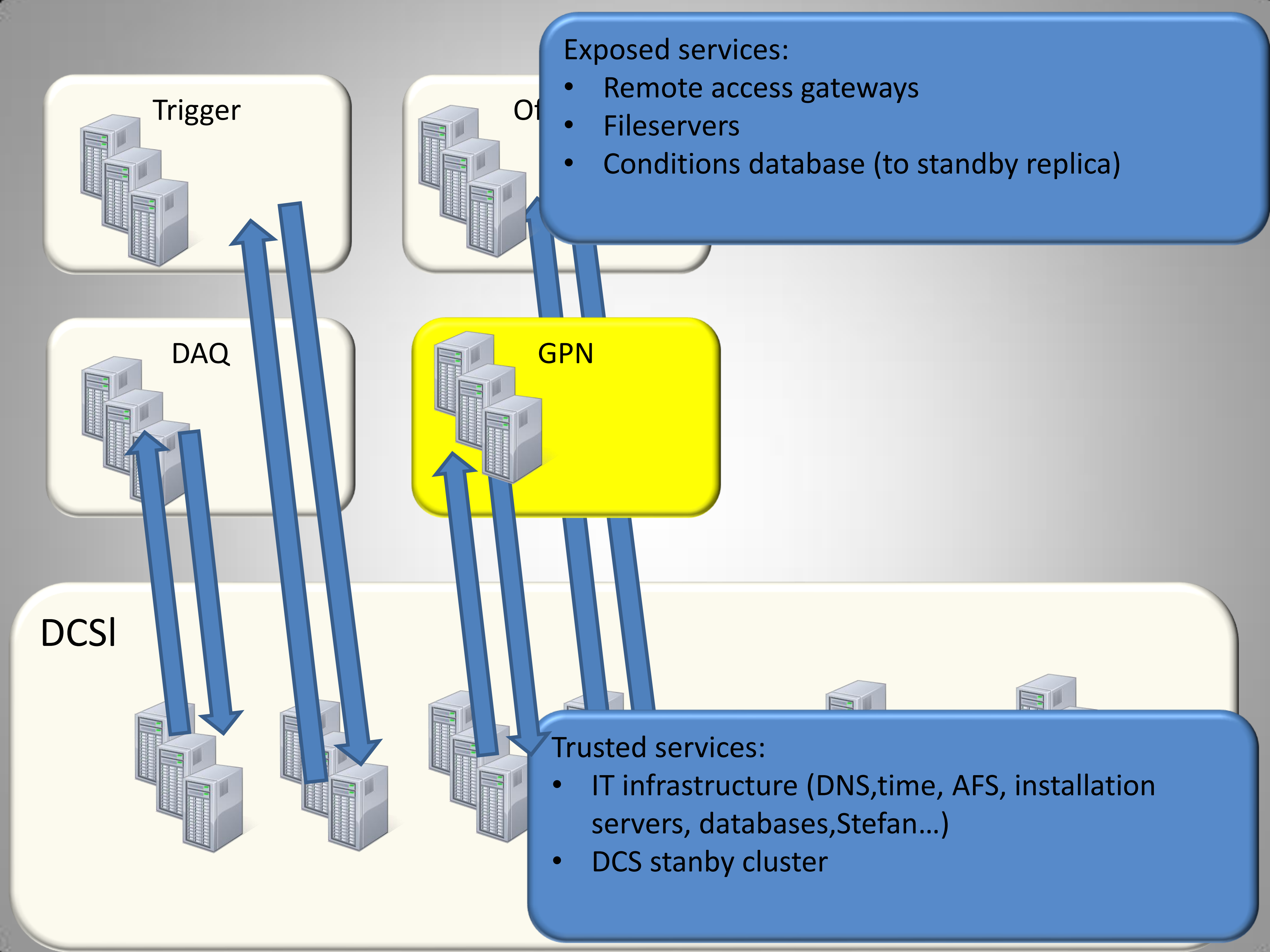

Trigger
Exposed services:
• Data publishers (DIM)
• Fileservers
• Bootservers
• DNS
DAQ
Trusted services:
• Fileservers
• Data publishers (DIM)
DCSI

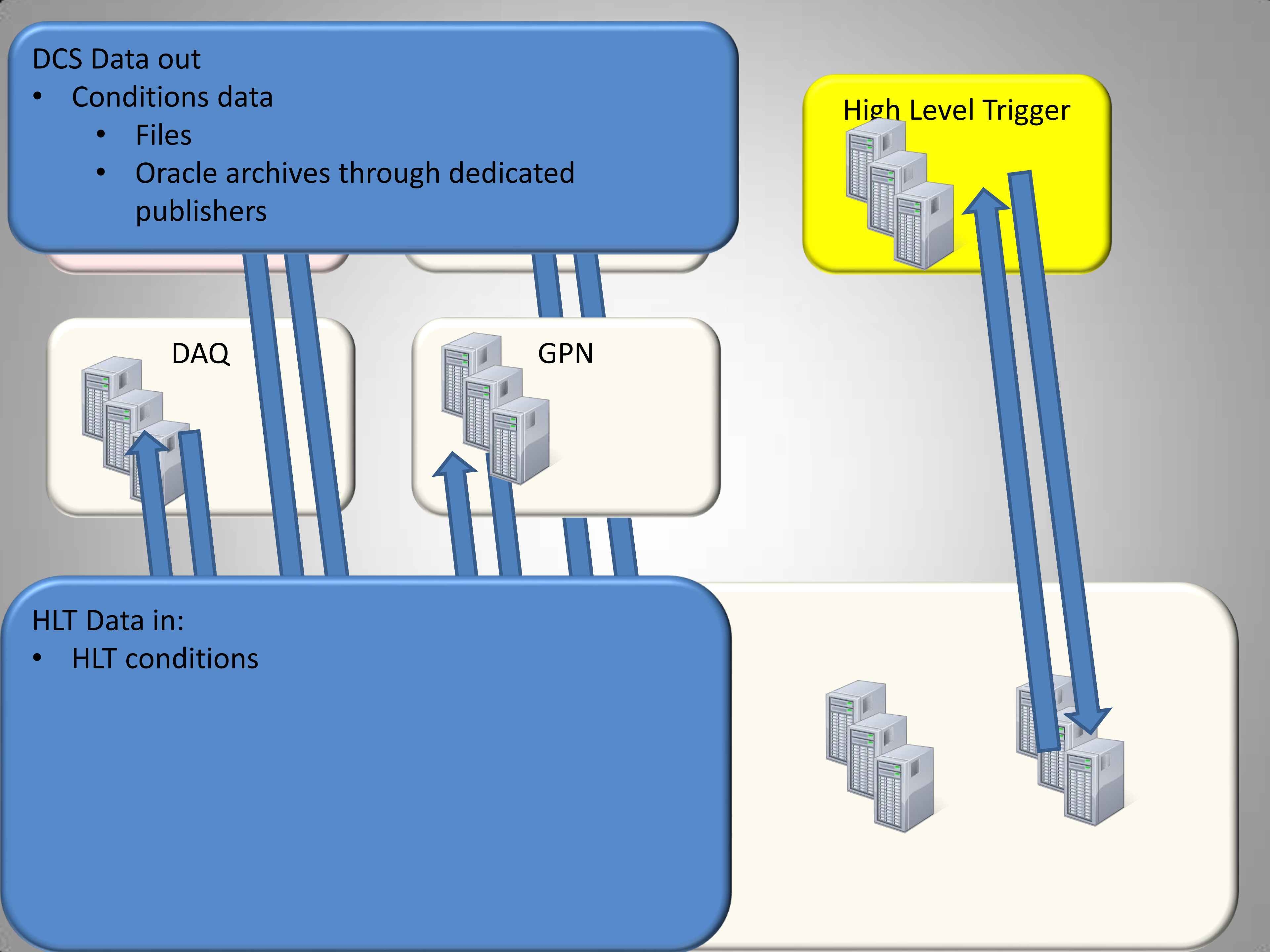

Trigger
Offline
DAQ
DCSI
DCS Data out:
• Conditions data
• Files
• Oracle archives through dedicated client-server mechanism
Offline Data in:
• Complaints ☺



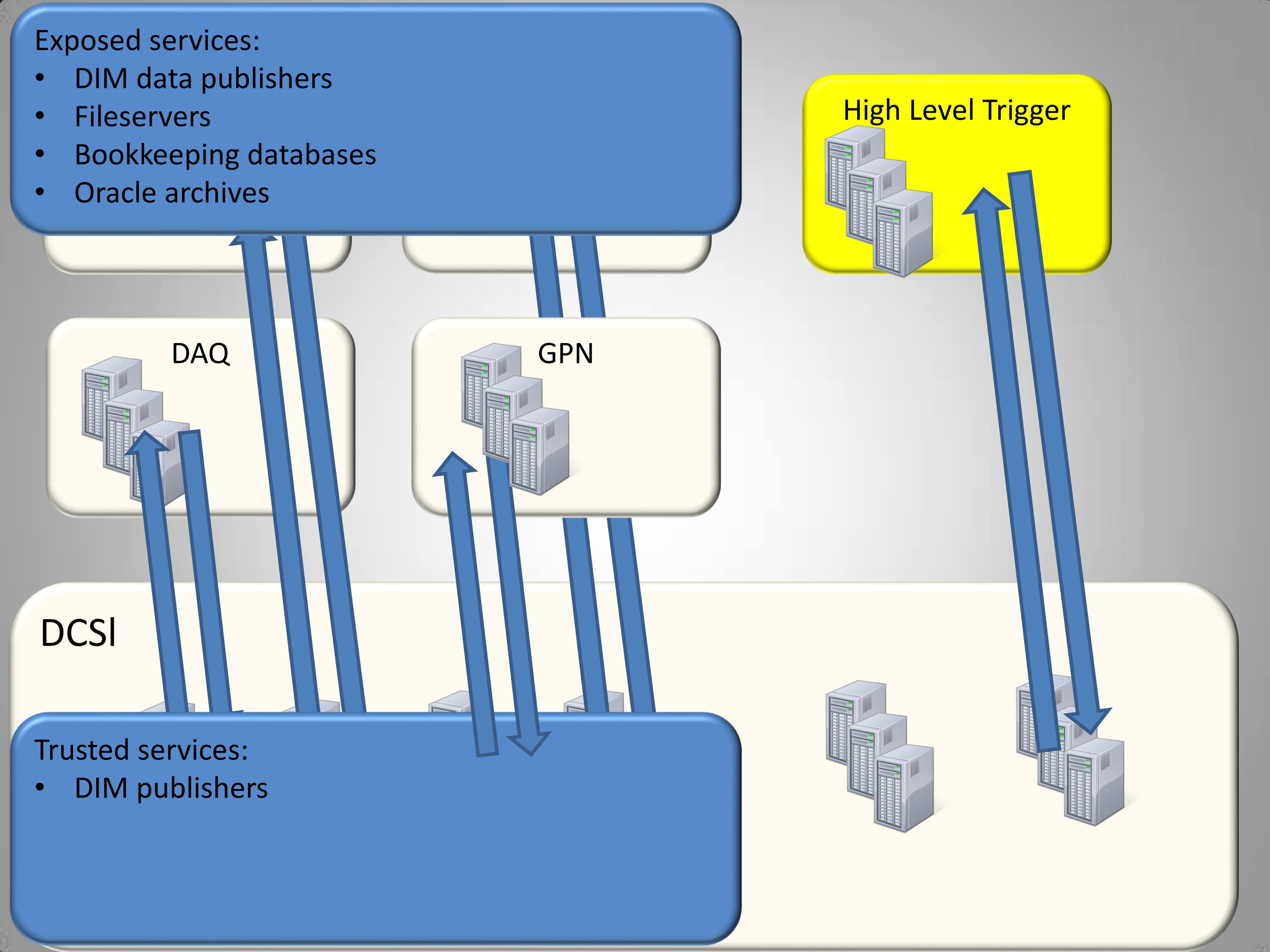
Trigger
Offline
DAQ
DCSI
Exposed services:
• Fileservers
• Bookkeeping database
• Data exchange servers
Trusted services:
• Data exchange clients

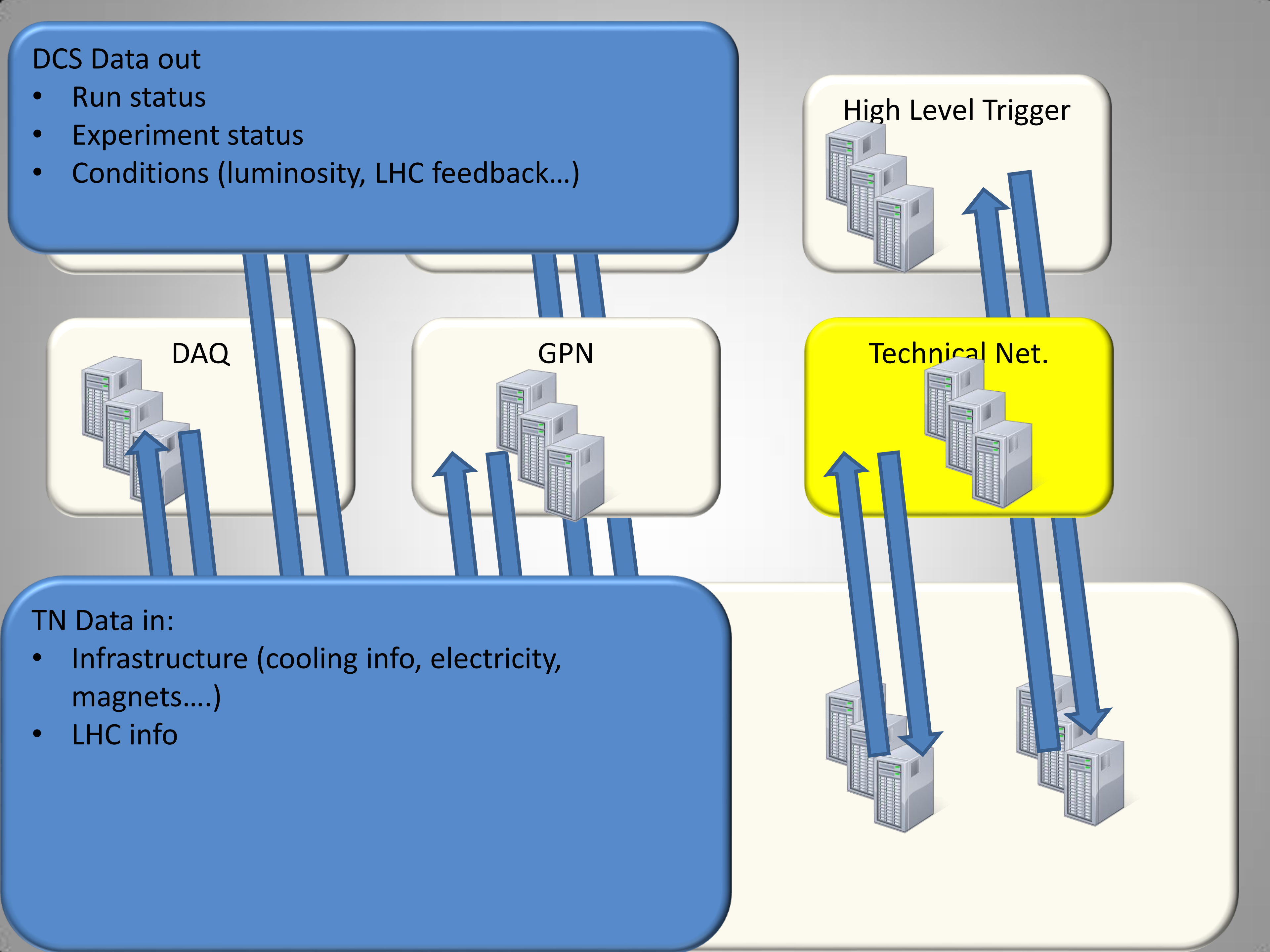

DCS Data out:
• Conditions data
• Detector debugging data
• Web panels
• LHC conditions
Trigger
DAQ
GPN
DCSl
GPN Data in:
• Detector software
• Calibration produced offsite
• Fixes (data, offline corrections…)
• Patches and updates
• Remote access to detector systems

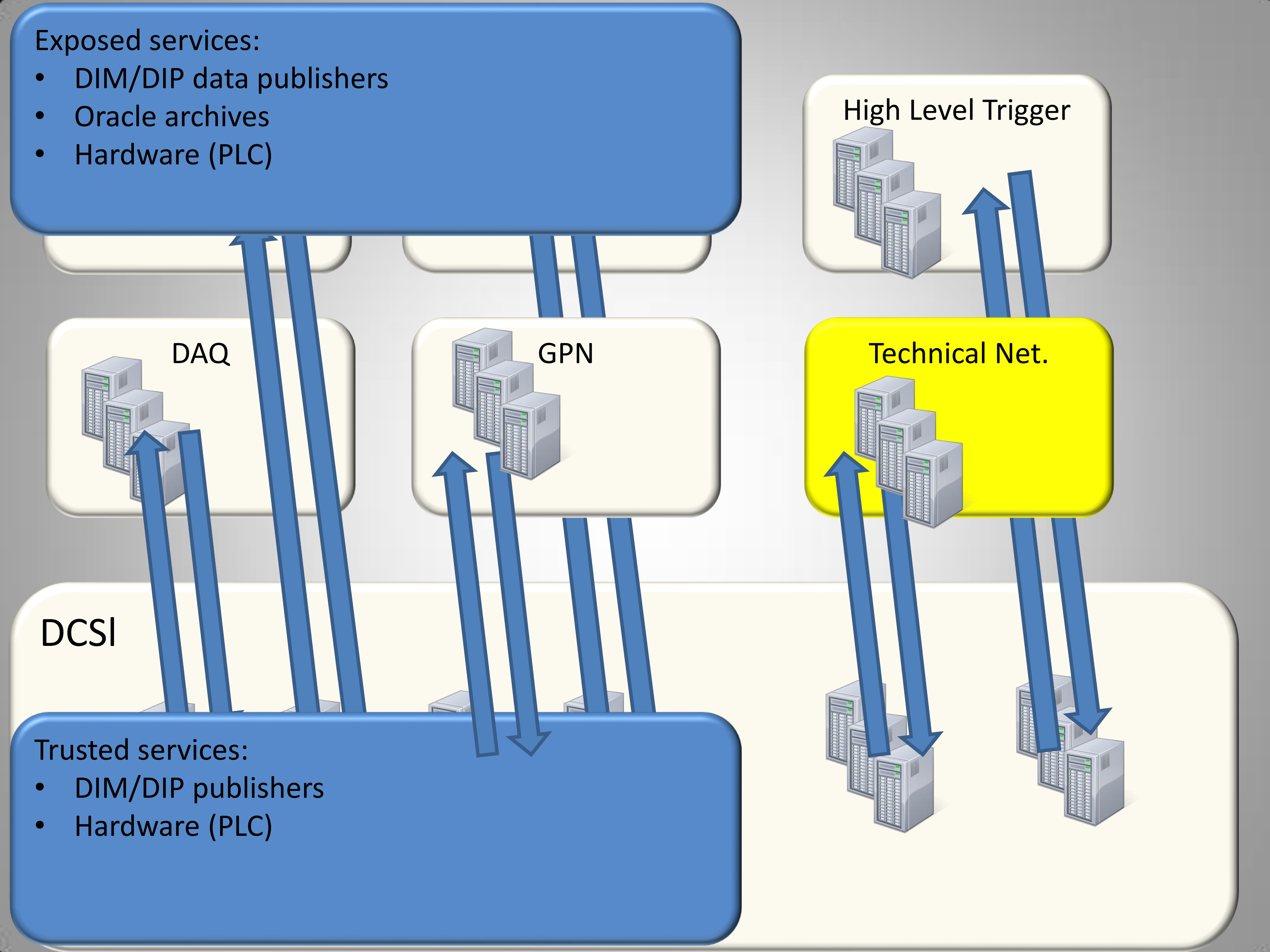

Exposed services:
• Remote access gateways
• Fileservers
• Conditions database (to standby replica)
Trigger
Of
DAQ
GPN
DCSI
Trusted services:
• IT infrastructure (DNS,time, AFS, installation servers, databases,Stefan…)
• DCS stanby cluster

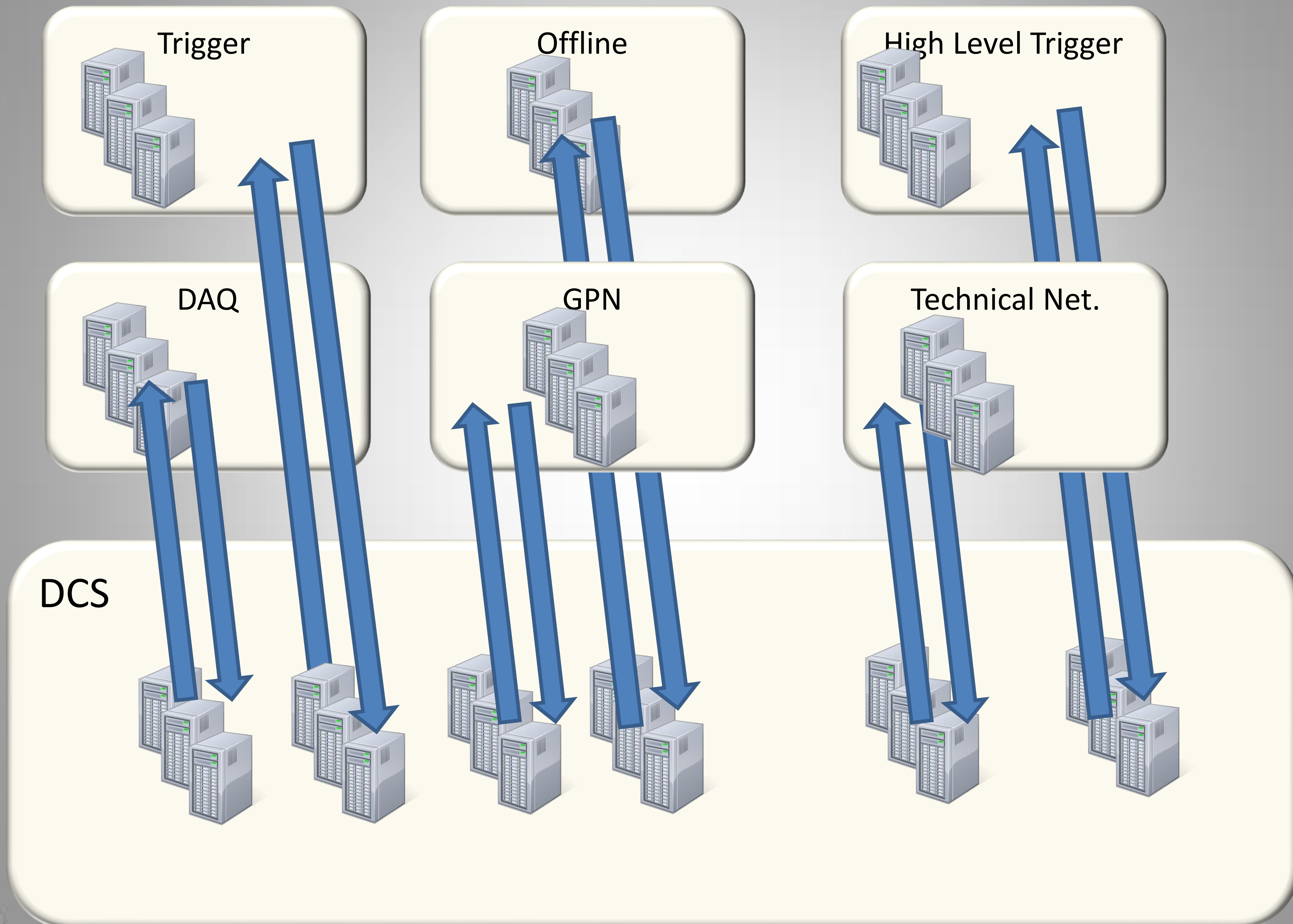


DCS Data out
• Conditions data
• Files
• Oracle archives through dedicated publishers
High Level Trigger
DAQ
GPN
HLT Data in:
• HLT conditions

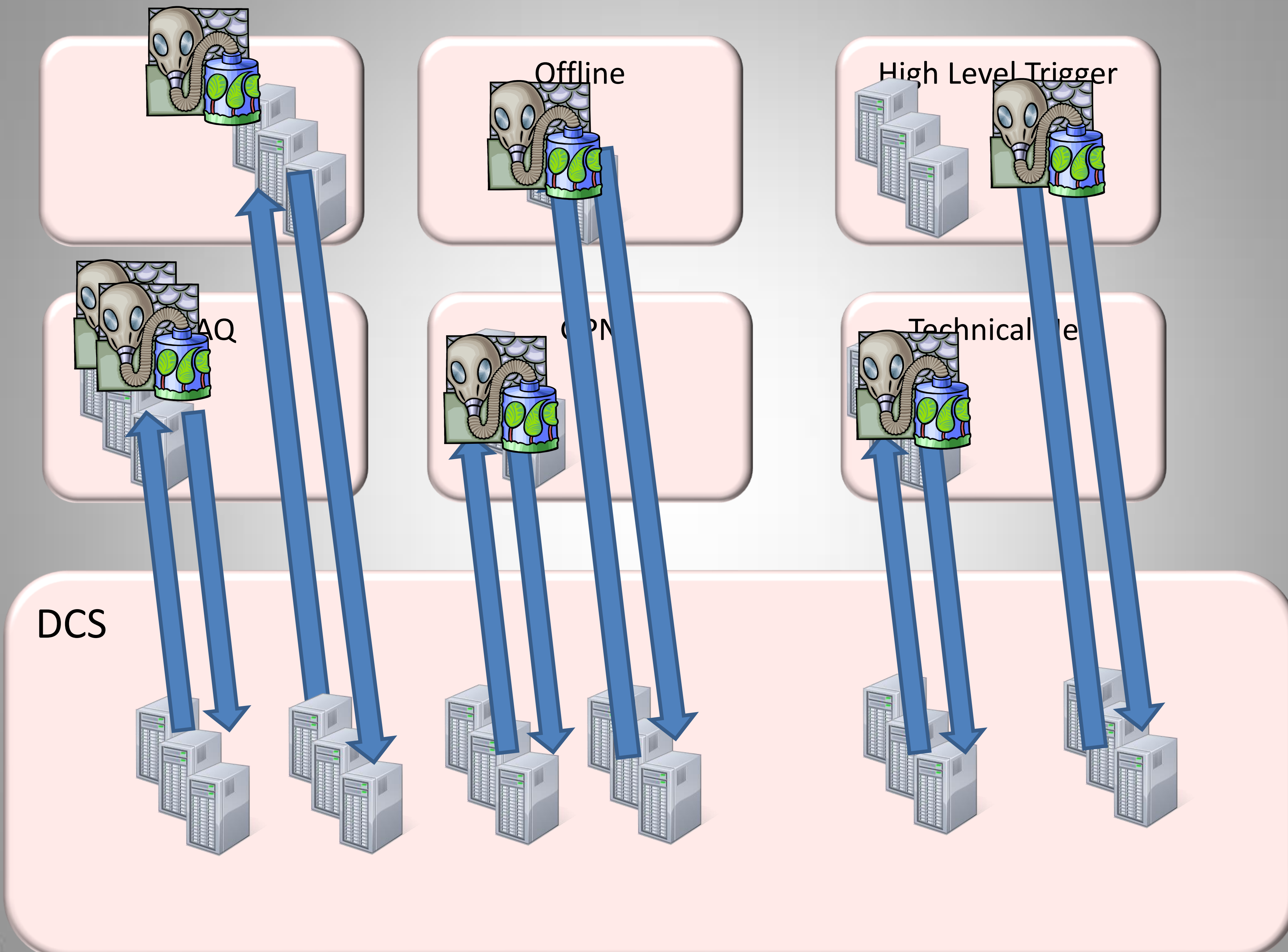

Exposed services:
• DIM data publishers
• Fileservers
• Bookkeeping databases
• Oracle archives
High Level Trigger
DAQ
GPN
DCSI
Trusted services:
• DIM publishers


DCS Data out
• Run status
• Experiment status
• Conditions (luminosity, LHC feedback…)
High Level Trigger
DAQ
GPN
Technical Net.
TN Data in:
• Infrastructure (cooling info, electricity, magnets….)
• LHC info


Exposed services:
• DIM/DIP data publishers
• Oracle archives
• Hardware (PLC)
High Level Trigger
DAQ
GPN
Technical Net.
DCSI
Trusted services:
• DIM/DIP publishers
• Hardware (PLC)

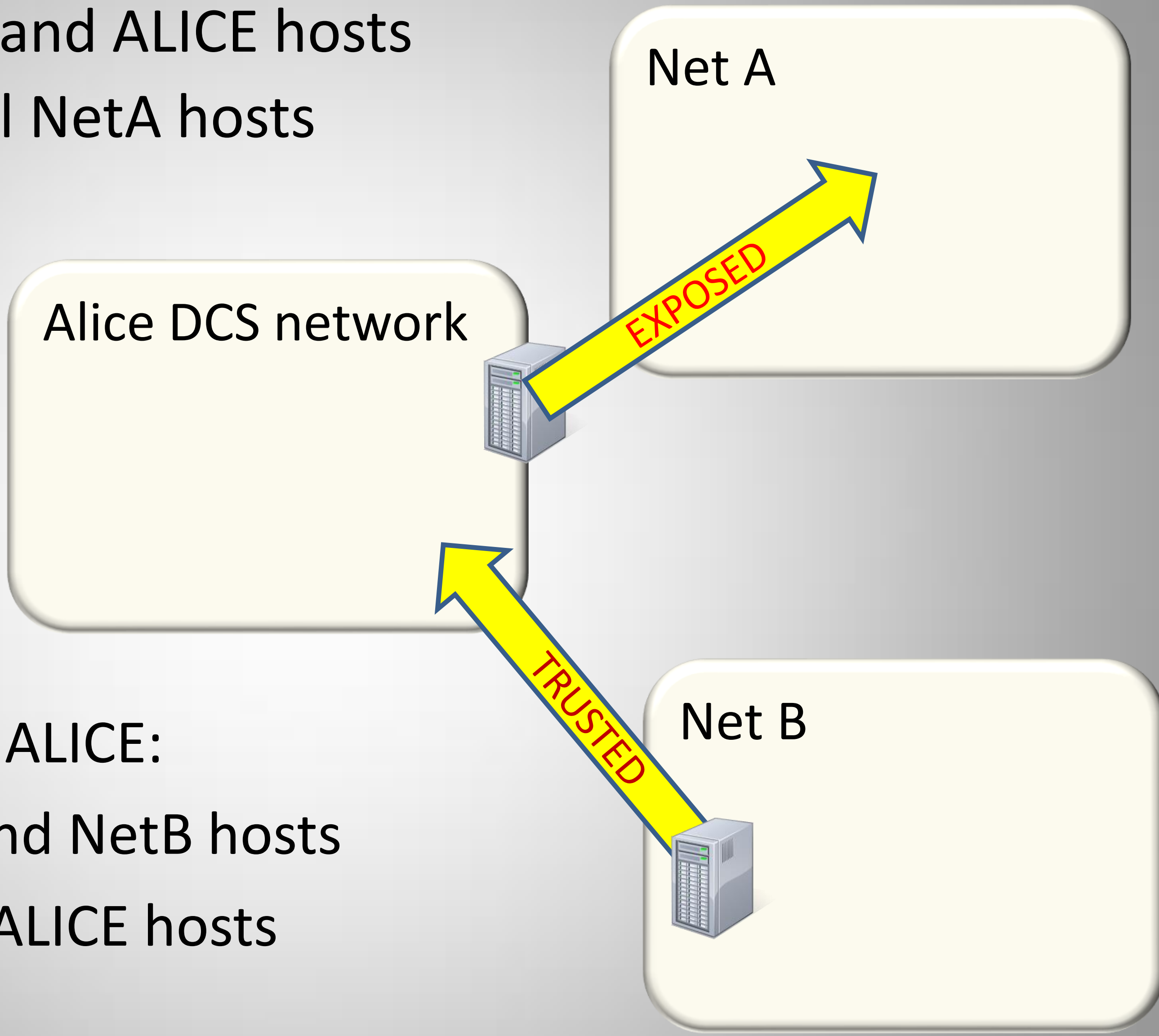


Trigger
Offline
High Level Trigger
DAQ
GPN
Technical Net.
DCS


Offline
High Level Trigger
Technical
DCS

ALICE host exposed to Net A

- Can see all Net A and ALICE hosts
- Can be seen by all NetA hosts

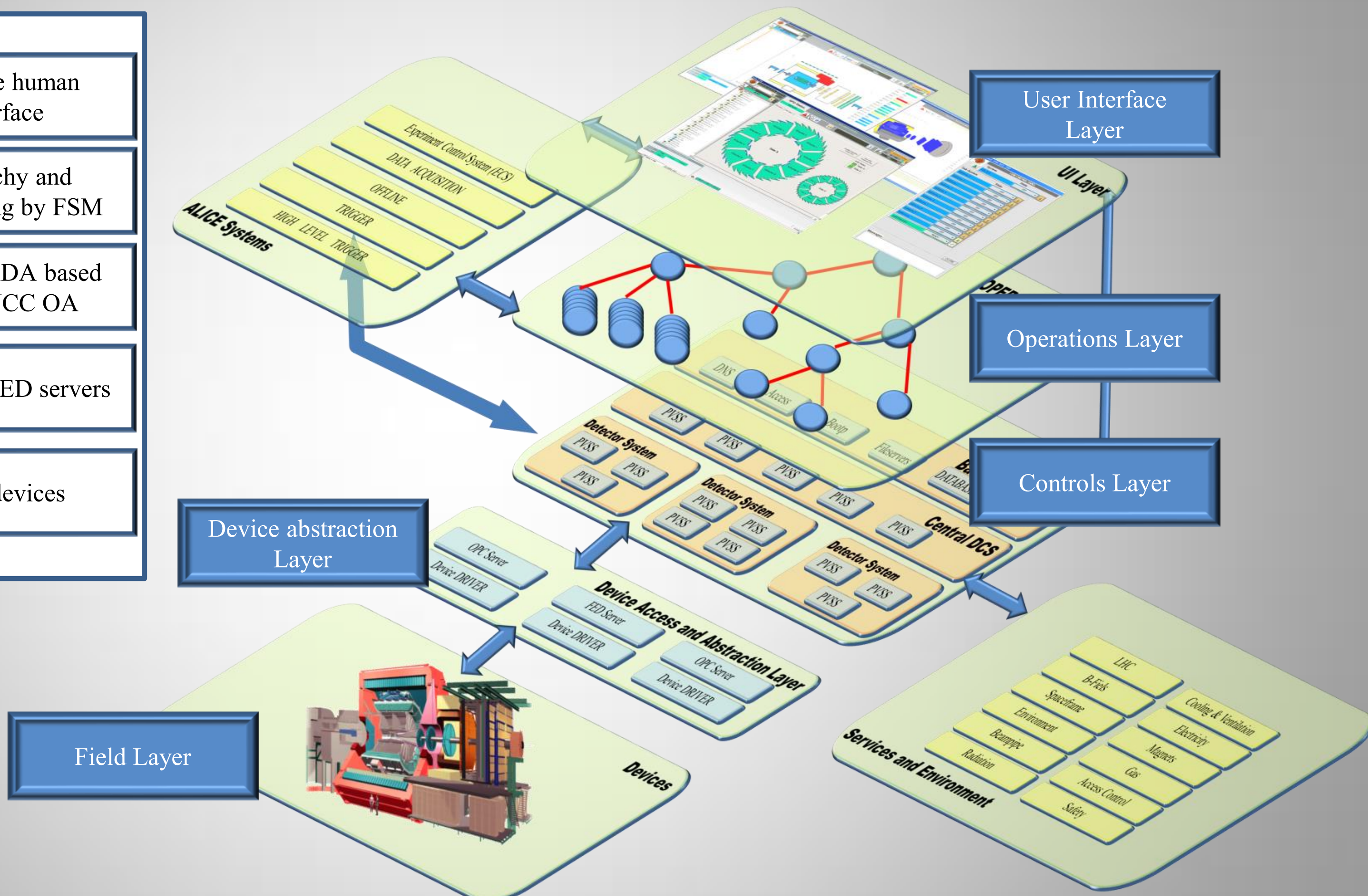


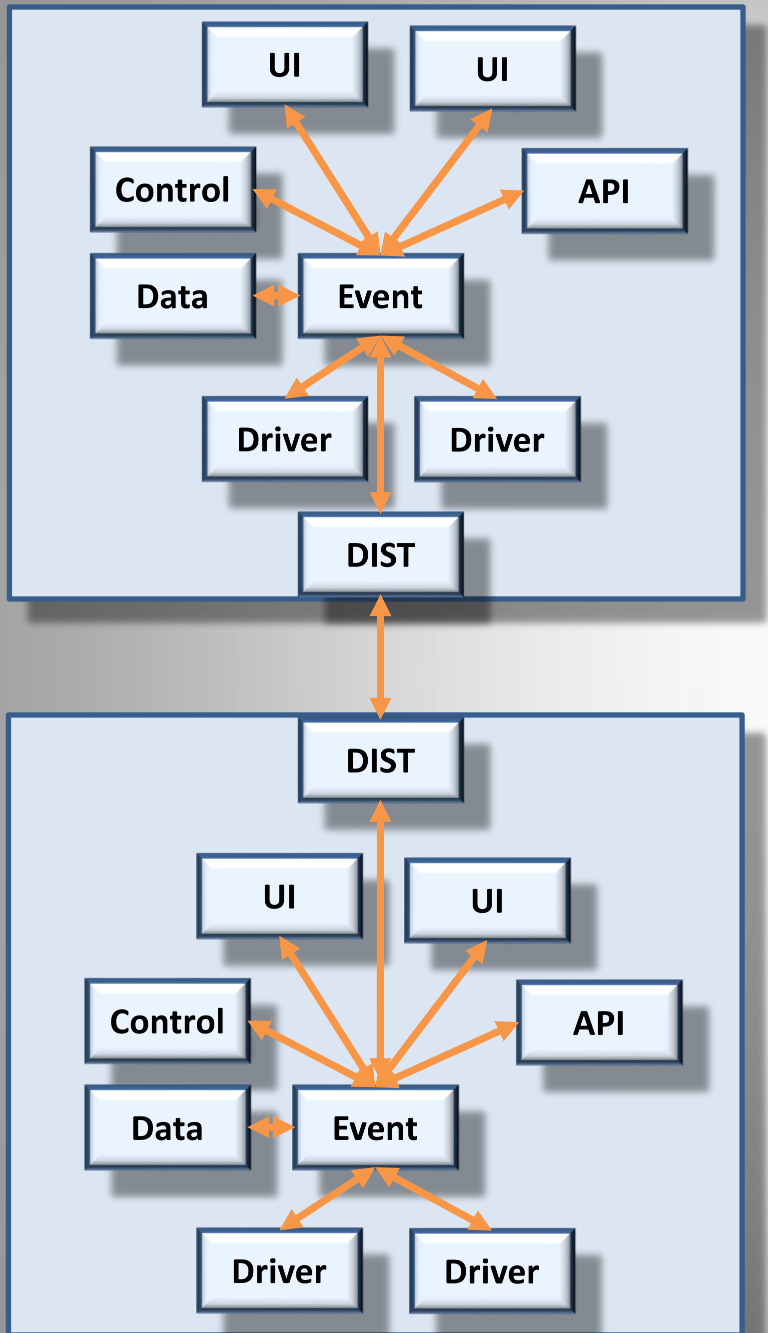
Net B host trusted by ALICE:

- Can see all ALICE and NetB hosts
- Can be seen by all ALICE hosts

DCS Architecture

User Interface Layer	Intuitive human interface
Operations Layer	Hierarchy and partitioning by FSM
Controls Layer	Core SCADA based on WINCC OA
Device abstraction Layer	OPC and FED servers
Field Layer	DCS devices

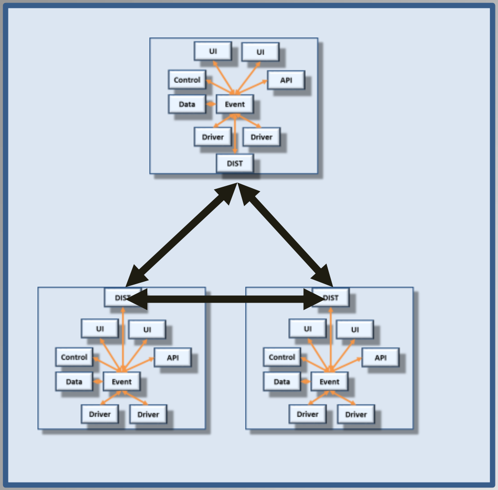


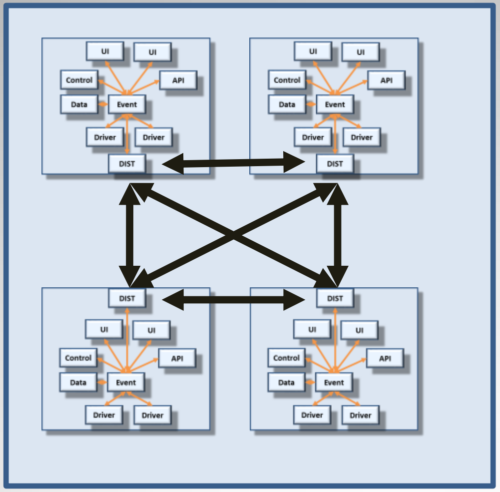


- Core of the Control Layer runs on WINCC OA SCADA system
- Single WINCC OA system is composed of managers
- Several WINCC OA systems can be connected into one distributed system

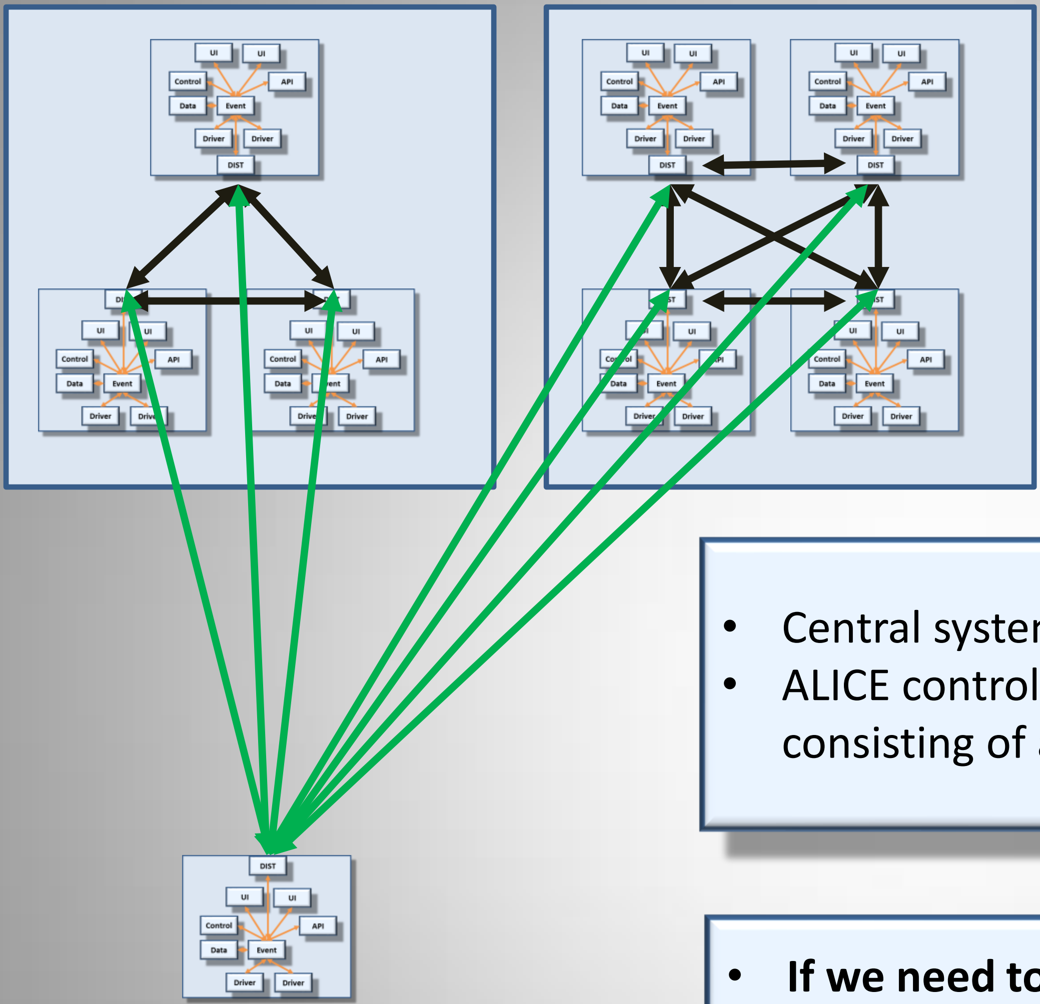
100 WINCC OA systems

2700 managers





- **An autonomous distributed system is created for each detector**



- Central systems connect to all detector systems
- ALICE controls layer is built as a distributed system consisting of autonomous distributed systems

- **If we need to exchange information between DCS and external systems, there is always one data collector, involved in the transfer**
  - **We never expose data providers**

Are we there?

- The simple security cookbook recipe seems to be:
  - Use the described network isolation
  - Implement secure remote access
  - Add firewalls and antivirus
  - Restrict the number of remote users to absolute minimum
  - Control the installed software and keep the systems up to date
- Are we there?
  - No, this is the point, where the story starts to be interesting

- ALICE is a heavy ion experiment
  - there is a **small** room for system tuning during the proton run
  - External experts require access
    - For debugging and development
    - 24/7 for troubleshooting
- Bidirectional data flow

Central shift organization

- DCS operator is fully responsible for the experiment
  - 24/7 shift coverage during ALICE operation periods
  - Detector babysitting if devices are ON

- In the period 2011-2013:
  - 1800 shifts manned shifts
    - 80 different shifters in 2011
    - 100 different shifters in 2012
  - Shifter training and non-stop on call service provided by central team

WHAT ARE THE IMPLICATIONS?

- Remote access required 24/7
- Remote experts require easy access to critical data and notifications in case of problems

DCS Organization

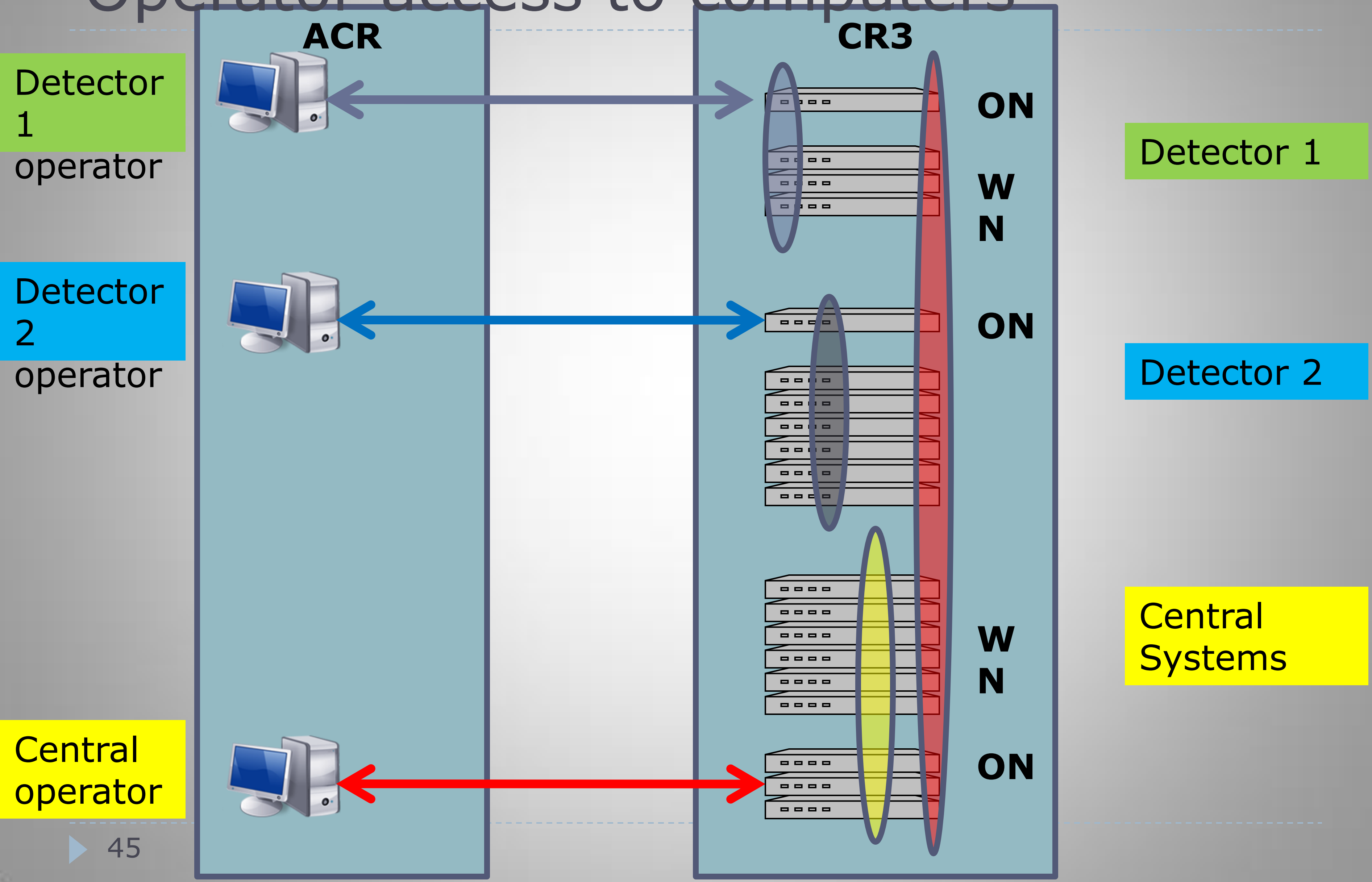
- Detector systems are developed in collaborating institutes
  - **Experts** can modify their systems
  - **Operators** can use their systems
- Original expectations evolved with time:
  - ~30 expected experts → 167 experts
  - ~100 detector operators → 610 operators
- Small central team (7 people) based at CERN
  - Provides infrastructure
  - Guidelines and tools
  - Consultancy
  - Integration

- How do we manage the users?

Authorization and authentication

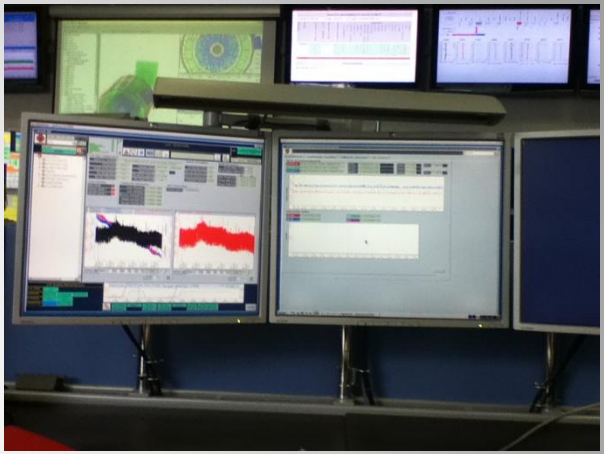
- User authentication is based on CERN domain credentials
  - No local DCS accounts
  - All users must have CERN account (no external accounts allowed)
- Authorization is managed via groups
  - **Operators** have rights to logon to operator nodes and use WINCC OA
  - **Experts** have access to all computers belonging to their detectors
  - **Super experts** have access everywhere
- Fine granularity of user privileges can be managed by detectors at the WINCC OA level
  - Only certain people are for example allowed to manipulate very high voltage system etc.

Operator access to computers



- Could there be an issue?

Authentication trap



- During the operation, the detector operator uses many windows, displaying several parts of the controlled system
  - Sometimes many ssh sessions to electronic modules are opened and devices are operated interactively
- At shift switchover old operator is supposed to logoff and new operator to logon
  - In certain cases the re-opening of all screens and navigating to components to be controlled can take 10-20 minutes, during this time the systems would run unattended
    - During beam injections, detector tests, etc. the running procedures may not be interrupted
- Shall we use shared accounts instead?
  - Can we keep the credentials protected?

Information leaks

- Sensitive information, including credentials, can leak
  - Due to lack of protection
  - Due to negligence/ignorance

....in scripts

```
echo " ----- make the network connections -----"
rem --- net use z: \\alidcsfs002\DCS_Common XXXXXX
/USER:CERN\dcsoper
rem --- net use y: \\alidcscom031\PVSS_Projects XXXXXX
/USER:CERN\dcsoper
echo " ------ done ---------"
rem ---ping 1.1.1.1 -n 1 -w 2000 >NUL
```

```
START C:\Programs\PVSS\bin\PVSS00ui.exe -proj lhc_ui -user
operator:XXXXXX
-p
lhcACRMonitor/lhcACRDeskTopDisplay.pnl,$panels:BackGround:lhcBackgr
ound/
lhcBackgroundMain.pnl;Luminosity_Leveling:lhcLuminosity/
lhcLuminosityLumiLevelling.pnl;Collisions_Schedule:BPTX/
lhc_bptxMonitor.pnl;V0_Control:lhcV00Control/lhcV00ControlMain.
```

These examples are real, original passwords in clear text are replaced by XXXXXX in this presentation

```
# Startup Batch Program for the LHC Interface Desktop
#
# Auth : deleted v1.0 4/8/2011
# - rdesktop -z -f -a 16 -k en-us -d CERN -u dcsoper -p XXXXXX
-s “D:
\PVSS_Profiles\ACRLHCDesk.bat” alidcscom054
rdesktop -z -g2560x1020 -a 16 -k en-us -d CERN -u
```

…. In documentation

Entries like this :

The relevant parameters are
• Window dimension : 1920x1050;
• RDP credentials : host = alidcscom054, user = dcsoper, password = XXXXXX;
• shell command to start : D:\PVSS_Profiles\ACRLHCBigScreen.bat
• panel to reference : lhcACRMonitor/lhcACRMain.pnl

Can be found in

Thesis

Reports

Web pages

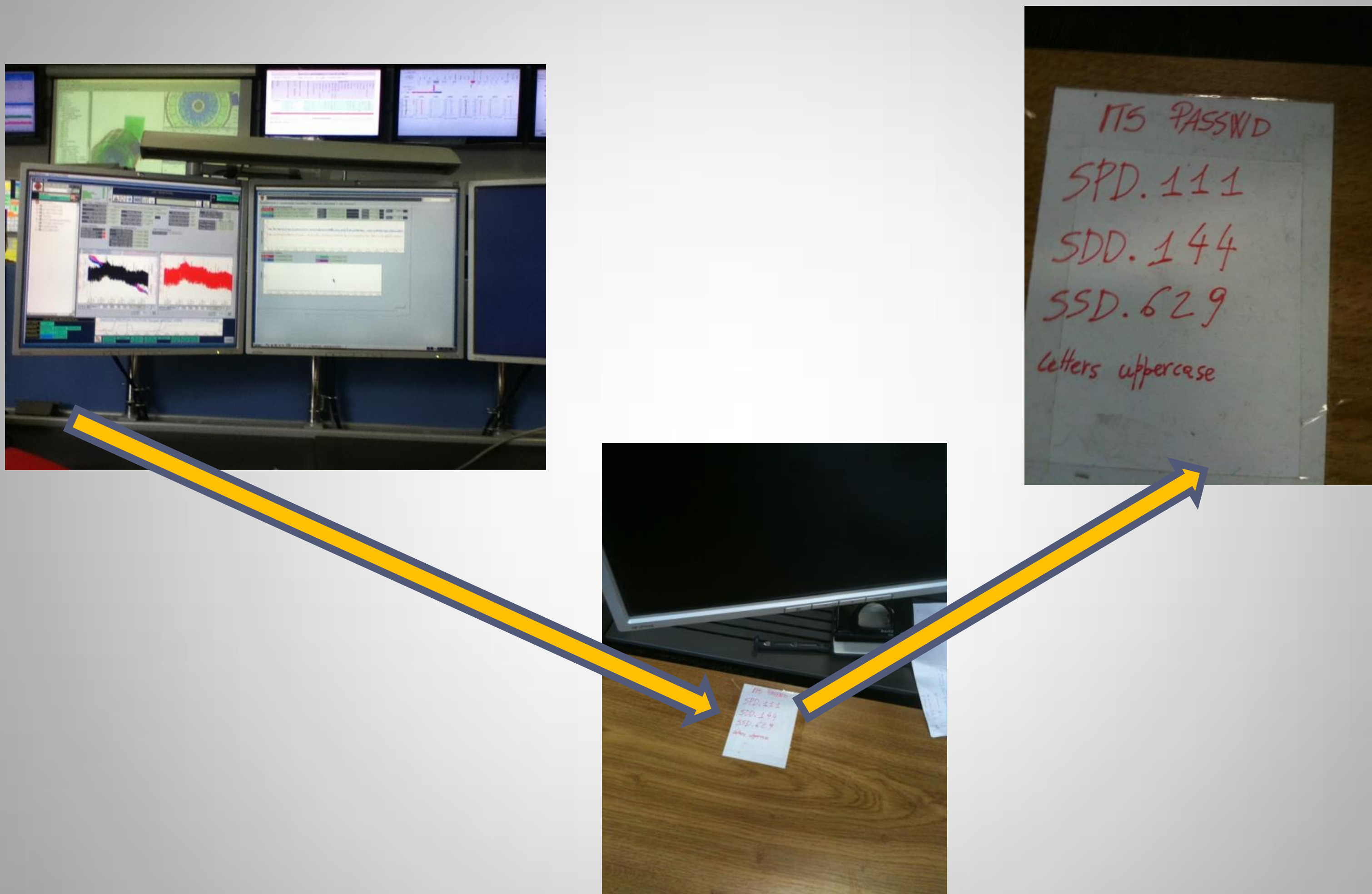
…..

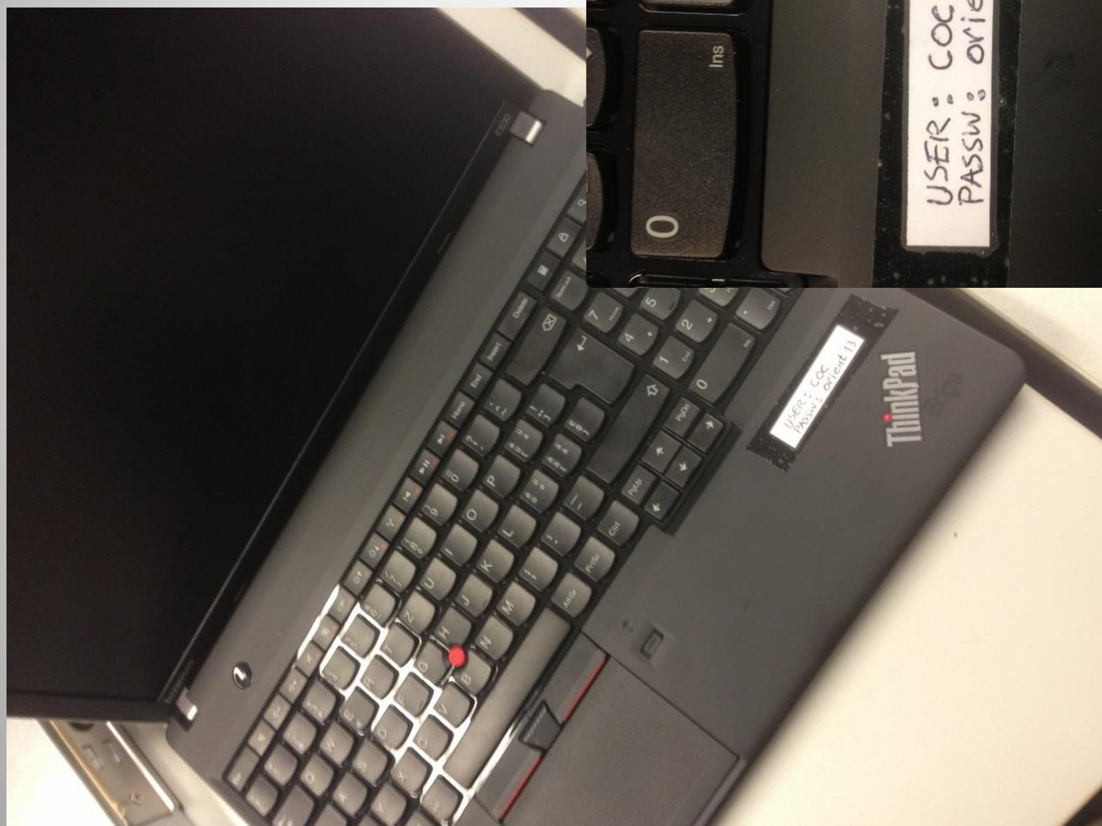
Twikies

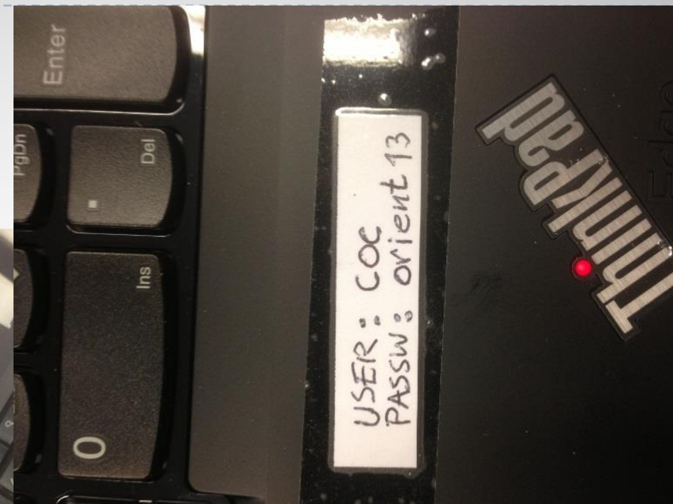
Printed manuals

We protect our reports and guides, but institutes republish them very often on their unprotected servers

… or even worse!

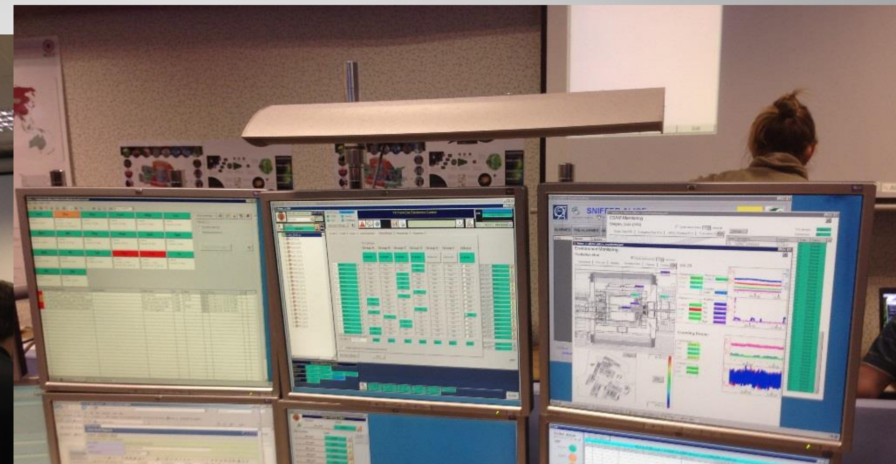


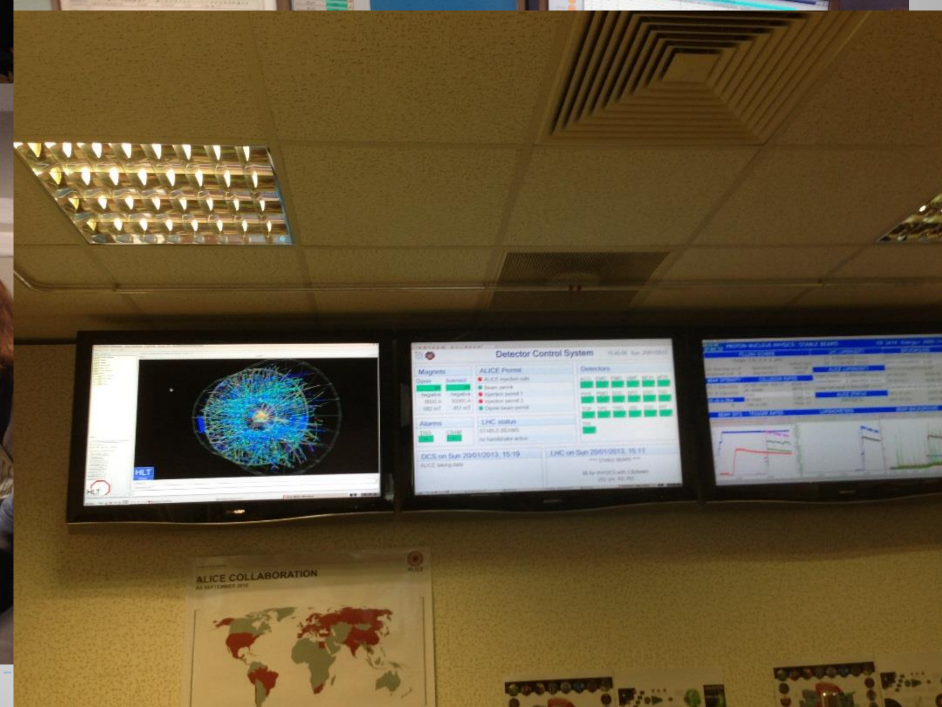

ThinkPad


Enter
Del
Ins
USER : COC
PASSW: orient 13
ThinkPad

- But OK,this is all in control rooms, so what….


ALICE Control Room




Detector Control System
HLT
ALICE COLLABORATION





User: Admin
Password:
j c

Using shared accounts

- In general, the use of shared accounts is undesired
- However, if we do not allow for it, users start to share their personal credentials

- Solution – use of shared accounts (detector operator, etc.) only in the control room
  - Restricted access to the computers
  - Autologon without the need to enter credentials
  - Logon to remote hosts via scripts using encrypted credentials (like RDP file)
  - Password known only to admins and communicated to experts only in emergency (sealed envelope)
- Remote access to DCS network allows only for physical user credentials

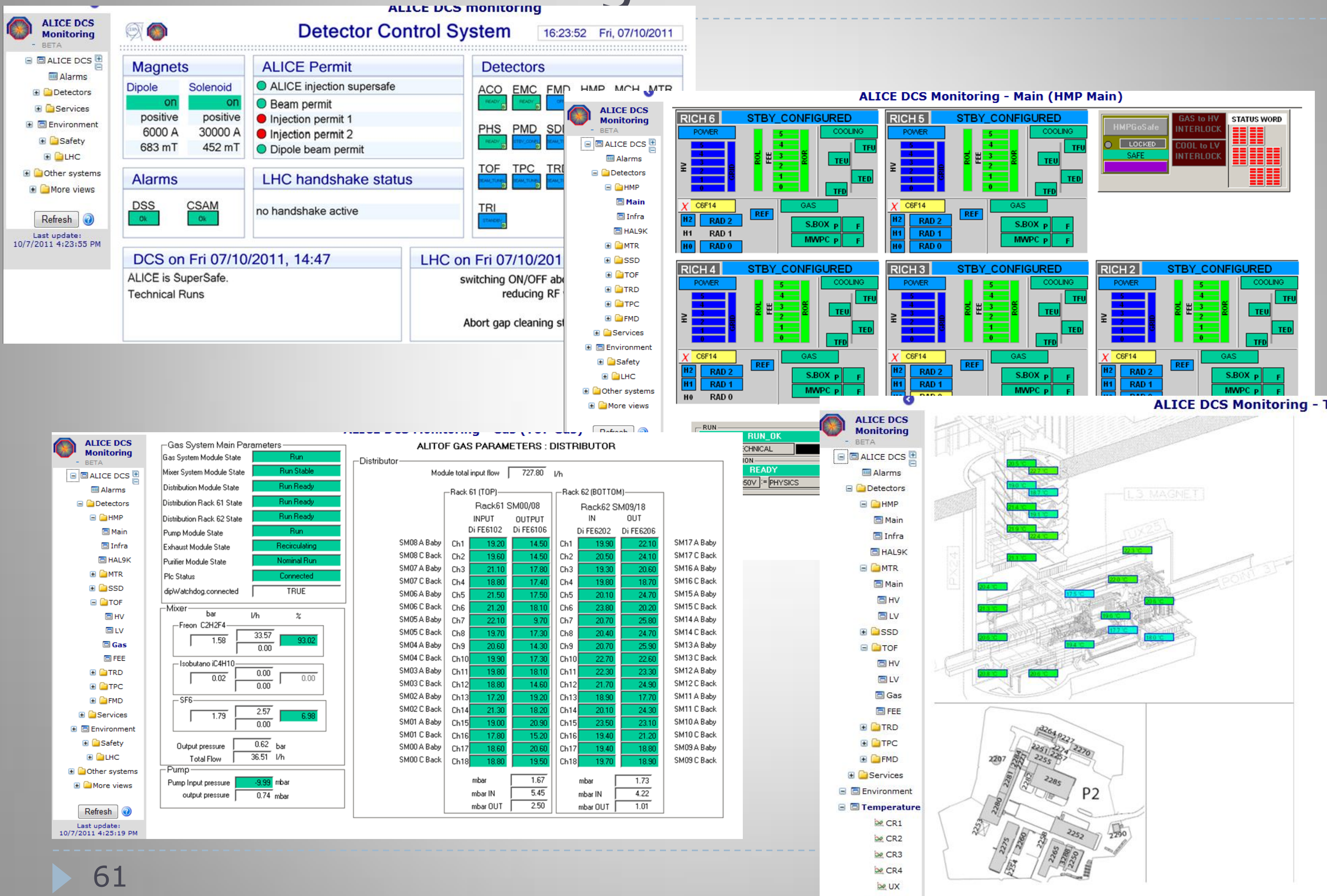
- OK, so we let people to work from the control room and remotely.
- Is this all?

DCS WWW monitoring

- WWW is probably the most attractive target for intruders
- WWW is the most requested service by institutes

- ALICE model:
  - Users are allowed to prepare a limited number of PVSS panels, displaying any information requested by them
  - Dedicated servers opens these panels periodically and creates snaphosts
  - The images are automatically transferred to central Web servers
- Advantage:
  - There is no direct link via the WWW and ALICE DCS, but the web still contains updated information
- Disadvantage/challenges:
  - Many

WWW monitoring



USING WEB SYNDICATION FOR FLEXIBLE REMOTE MONITORING

Ombretta Pinazza [(1) (2)], André Augustinus[(1)], Peter M. Bond[(1)], Peter Chochula [(1)],
Alexander N. Kurepin [(1) (3)], Mateusz Lechman [(1)], Peter Rosinský [(1)],
ICALEPCS 2013, San Francisco

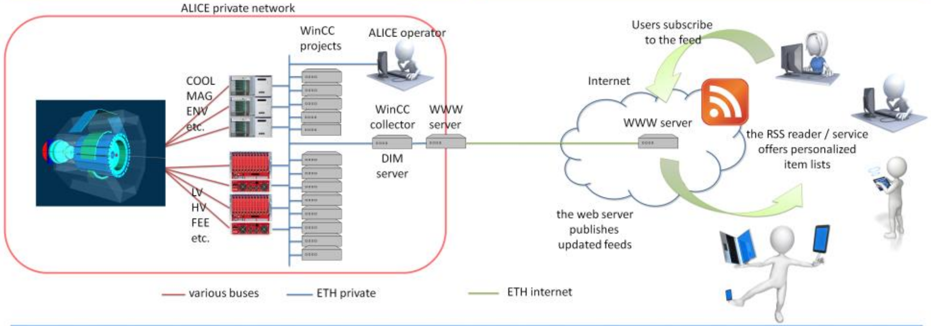
ALICE
A JOURNEY OF DISCOVERY

ALICE DCS is developing a flexible, web based software structure to provide its users a further way to stay updated on their experiment.

Exploiting standardized web syndication and RSS it is possible to distribute up-to-date web content from one web site to thousands of other web sites around the world.
Subscribed readers can access the content in their most convenient manner, profiting from their preferred device, which could be a web browser running on a smartphone or a computer, a dedicated app for their iPhone or Android tablet, etc.

Remote systems wishing to provide data and screenshots to the collector run a specific process (a WinCC CTRL manager) based on the AliceRSS library written by the ALICE DCS group for WinCC. The library reworks data to build the RSS array and send it to the collector using the DIM client-server software.

The collector is running a web and a DIM server and generates the XML item list, as well as the HTML file containing the extended description. Every time a new post is received, a new XML file containing all items is assembled and published on the official web site, reachable from the Internet.



The information to be published comes from several sources connected to different private networks: sensors installed in the experimental site, sub-detectors online projects, alert systems and operation logbook. Data in numerical format are plotted or organized in tables; screenshots are displayed as images, periodic reports are filled to summarize the operations performed and the status of the experiment. Information tagging allows readers to subscribe to the web content according to their interests.

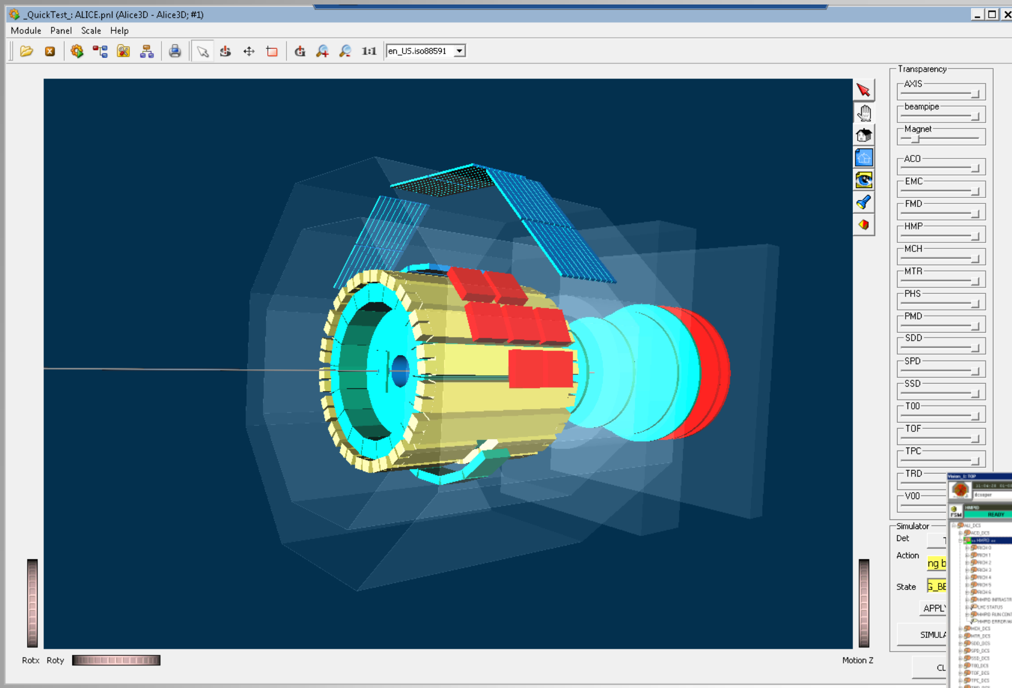
Nowadays several free web aggregators and services are available on smartphones, tablets and computers.
This publication technique is offered as a complement to more traditional ways of accessing the control system, like logging into gateways and accessing the SCADA systems directly. It's a lightweight and secure way to deliver customizable information and facilitates a personal experience to interested users.

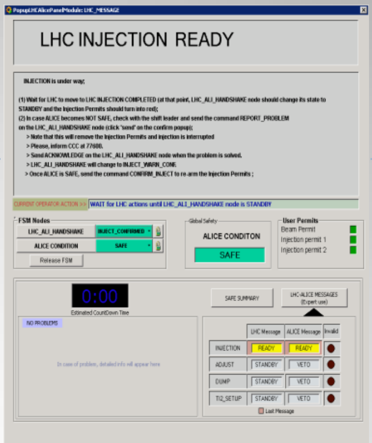
Figure 1: resulting page, read with a web based plugin from Chrome

Figure 2: an excerpt from the AliDcs.rss feeds list

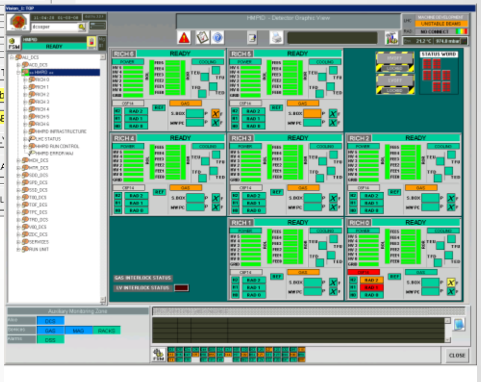
Figure 3: the RSS Feedly app, running on an Android smartphone

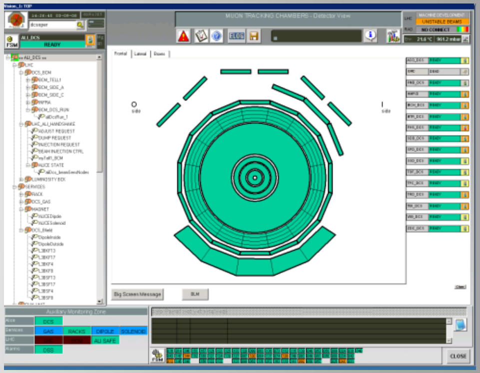
(1) CERN – European Organization for Nuclear Research, Geneva, Switzerland, (2) INFN – Sezione di Bologna, Bologna, Italy,
(3) INR RAS - Institute for Nuclear Research of the Russian Academy of Sciences, Moscow, Russia

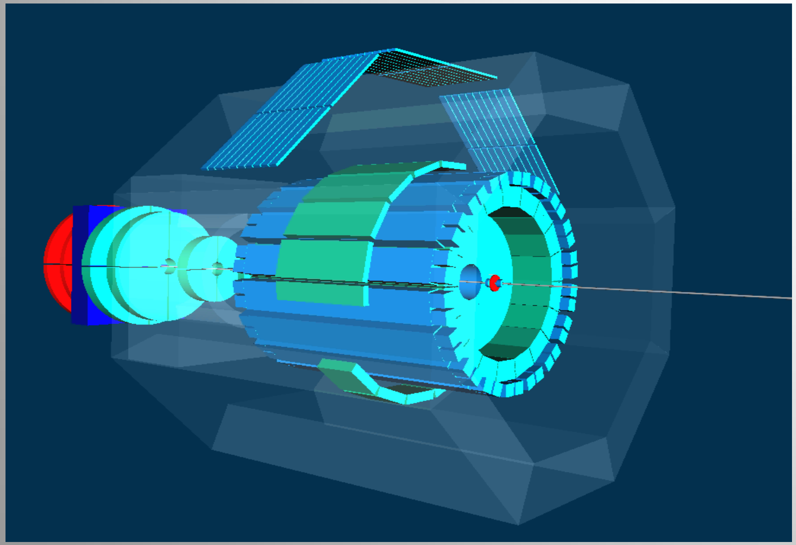

QuickTest: ALICE.pnl (Alice3D - Alice3D; #1)
Module Panel Scale Help
Transparency
AXIS
beampipe
Magnet
ACO
EMC
FMD
HMP
MCH
MTR
PHS
PMD
SDD
SPD
SSD
T00
TOF
TPC
TRD
V00
Simulator
Det
Action
State
Rotx Roty
Motion Z

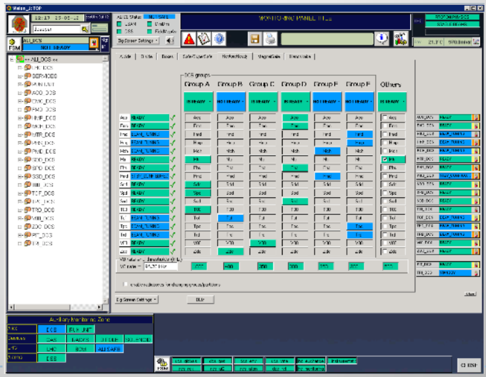

LHC INJECTION READY
ALICE CONDITION
SAFE
0:00

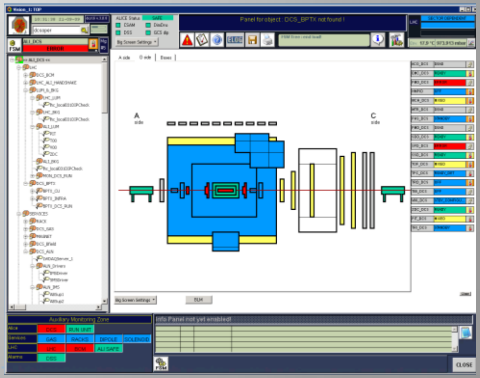

LHC INJECTION WARNING
ALICE CONDITION
NOT SAFE
6:22



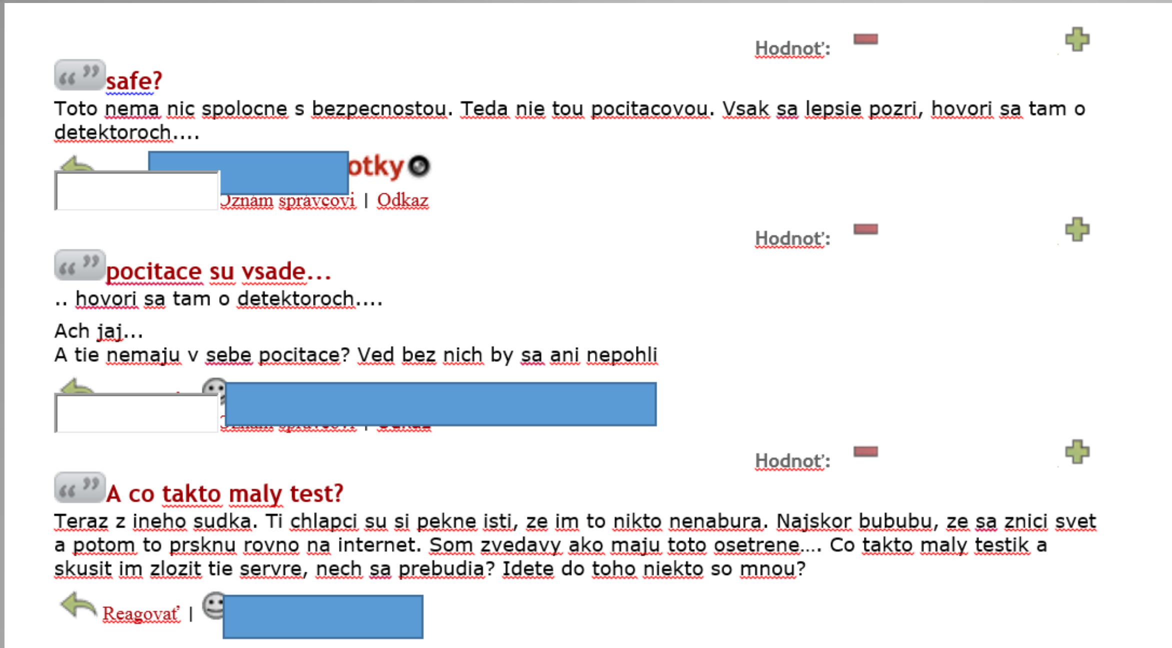








WEB hurts



Hodnoť:

safe?

Toto nema nic spolocne s bezpecnostou. Teda nie tou pocitacovou. Vsak sa lepsie pozri, hovori sa tam o detektoroch....

otky

Oznam spravcovi | Odkaz

Hodnoť:

pocitace su vsade...

.. hovori sa tam o detektoroch....

Ach jaj...
A tie nemaju v sebe pocitace? Ved bez nich by sa ani nepohli

Hodnoť:

A co takto maly test?

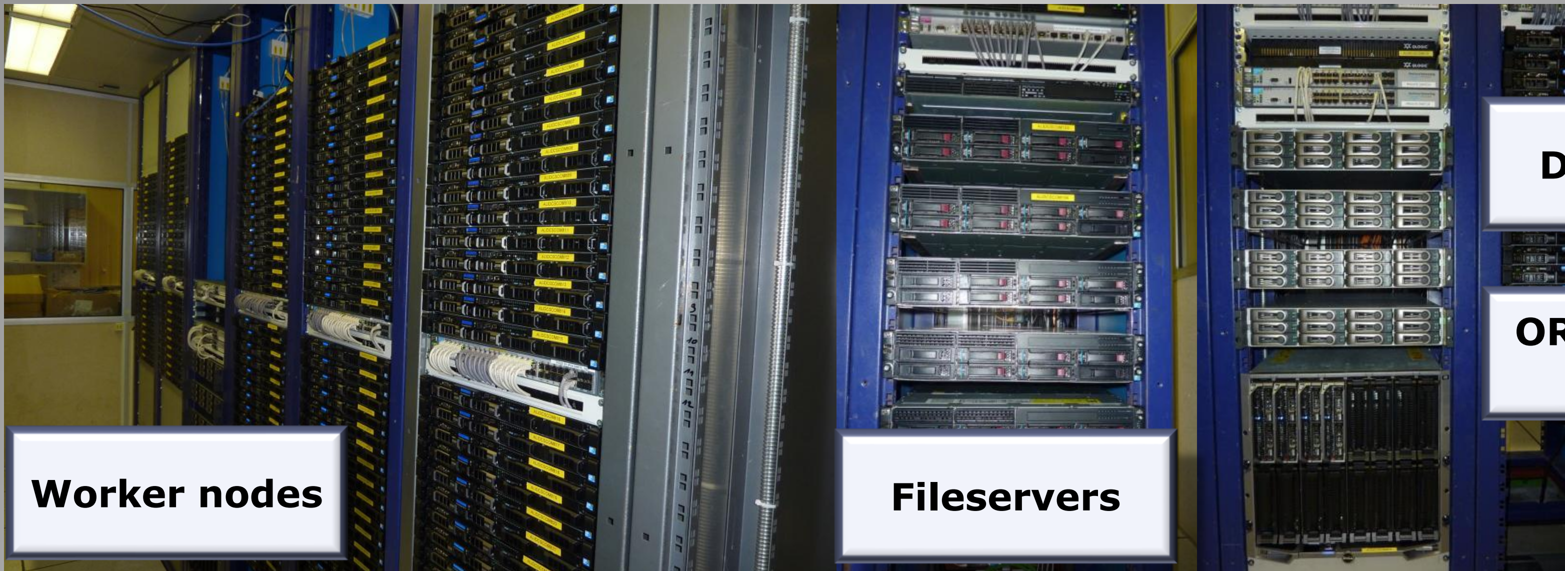
Teraz z ineho sudka. Ti chlapci su si pekne isti, ze im to nikto nenabura. Najskor bububu, ze sa znici svet a potom to prsknu rovno na internet. Som zvedavy ako maju toto osetrene.... Co takto maly testik a skusit im zlozit tie servre, nech sa prebudia? Idete do toho niekto so mnou?

Reagovať |

- Example of a real discussion triggered by innocent article about ALICE
  - One guy got a brilliant idea to check if the web server is really secure and is looking for supporters….

Firewalls

- In the described complex environment firewalls are a must
  - Can be the firewalls easily deployed on controls computers?

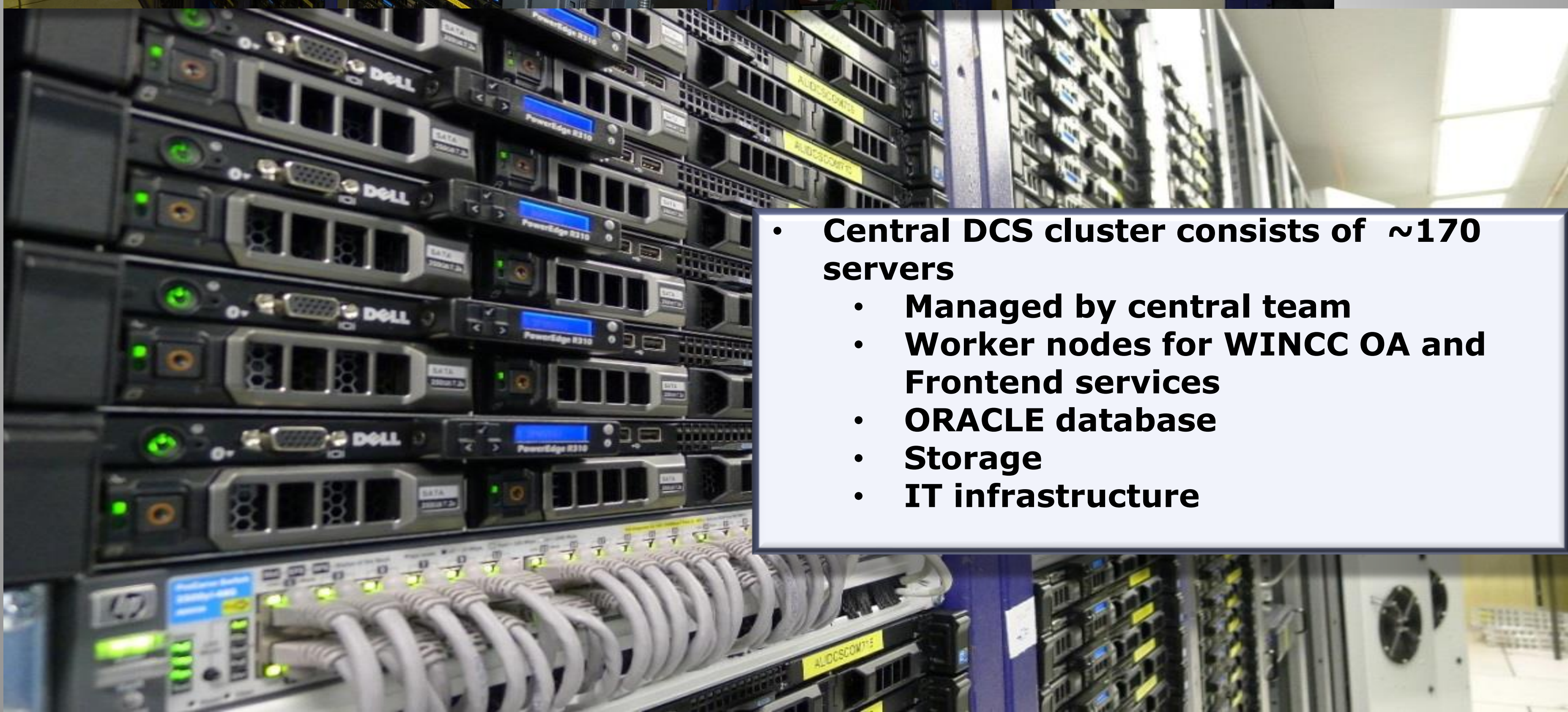


Worker nodes

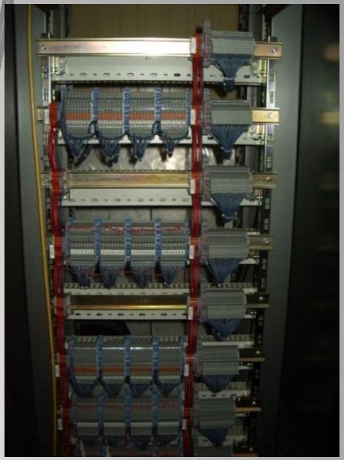
Fileservers

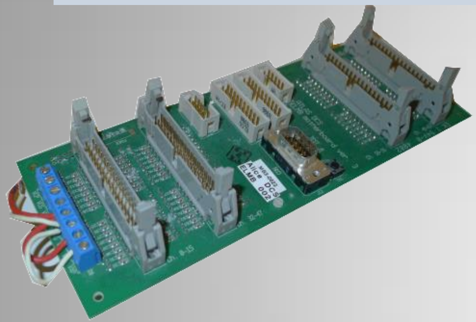
DB servers

ORACLE size: 5.4 TB



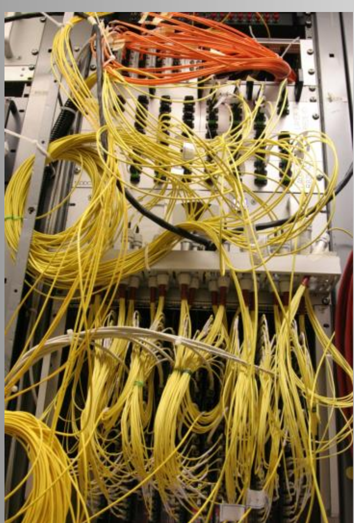
- Central DCS cluster consists of ~170 servers
    - Managed by central team
    - Worker nodes for WINCC OA and Frontend services
    - ORACLE database
    - Storage
    - IT infrastructure

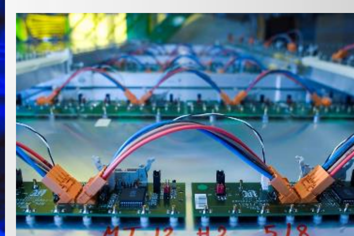


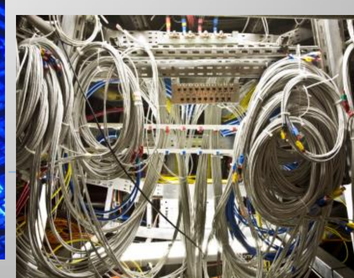


- **Wherever possible, standardized components are used**
  - **Commercial products**
  - **CERN-made devices**

- Frontend electronics
  - Unique for each detector
  - Large diversity, multiple buses and communication channels
    - Several technologies used within the same detector







CAN

ETHERNET

EASYNET

VME

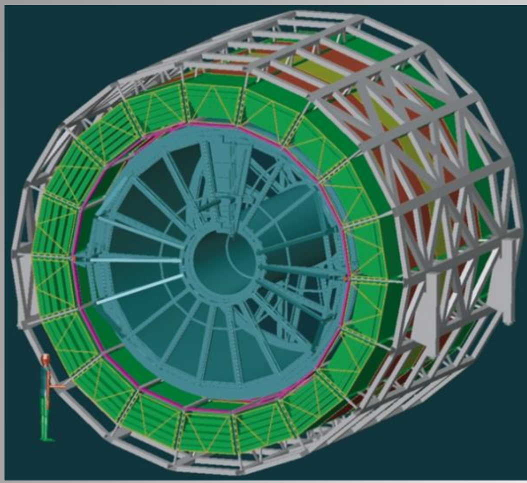
JTAG

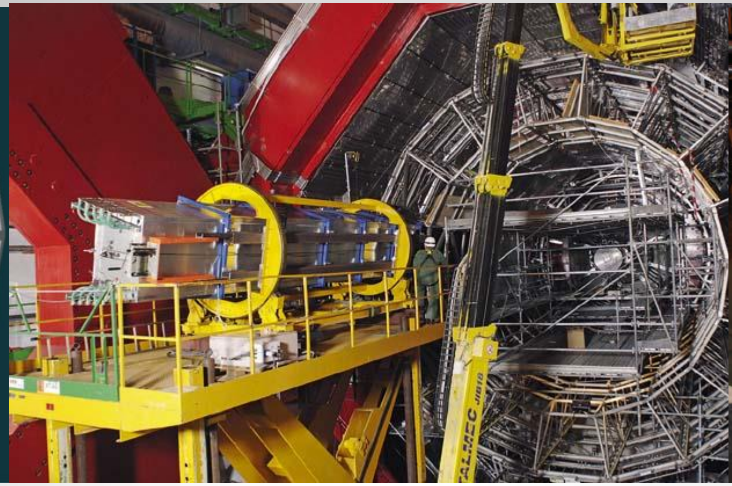
RS 232

PROFIBUS

Custom links…

One example for all
ALICE Transition Radiation Detector (TRD)

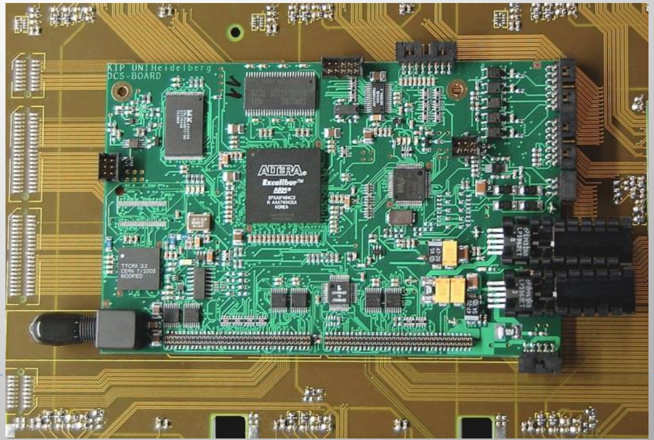


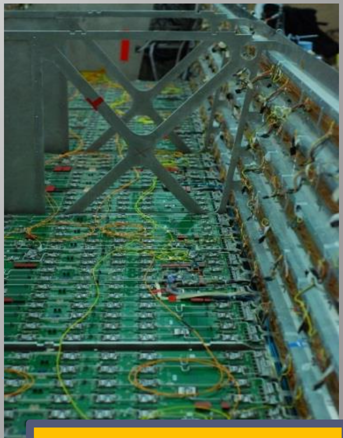


1 of 65000 MCMs

- > 500 drift chambers, 760 m^2
- 28 m^3 Xe based gas mixture
- 1.2M electronics channels
  - 65000 MCM
  - **250 000 tracklet processors**
  - **17TB/s raw data**
- 89 LV Power supplies
  - ~65 kW heat

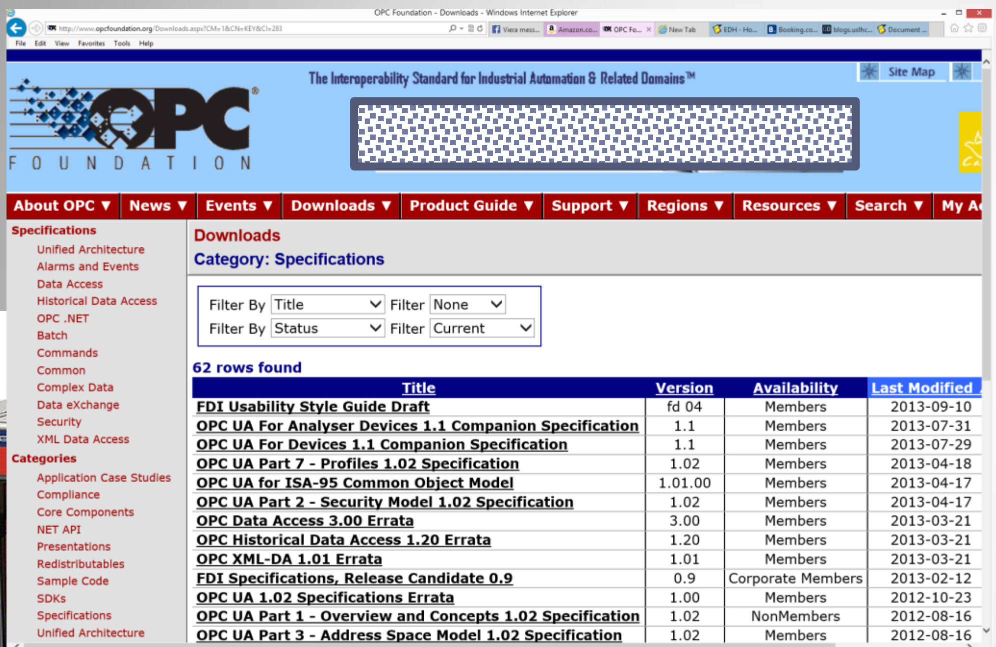
DCS control board (~750 used in ALICE)





Readout boards

- **OPC used as a communication standard wherever possible**
  - **Native client embedded in WINCC OA**



The Interoperability Standard for Industrial Automation & Related Domains™

Site Map

OPC FOUNDATION

About OPC ▼ | News ▼ | Events ▼ | Downloads ▼ | Product Guide ▼ | Support ▼ | Regions ▼ | Resources ▼ | Search ▼ | My A

Specifications
- Unified Architecture
- Alarms and Events
- Data Access
- Historical Data Access
- OPC .NET
- Batch
- Commands
- Common
- Complex Data
- Data eXchange
- Security
- XML Data Access

Categories
- Application Case Studies
- Compliance
- Core Components
- NET API
- Presentations
- Redistributables
- Sample Code
- SDKs
- Specifications
- Unified Architecture

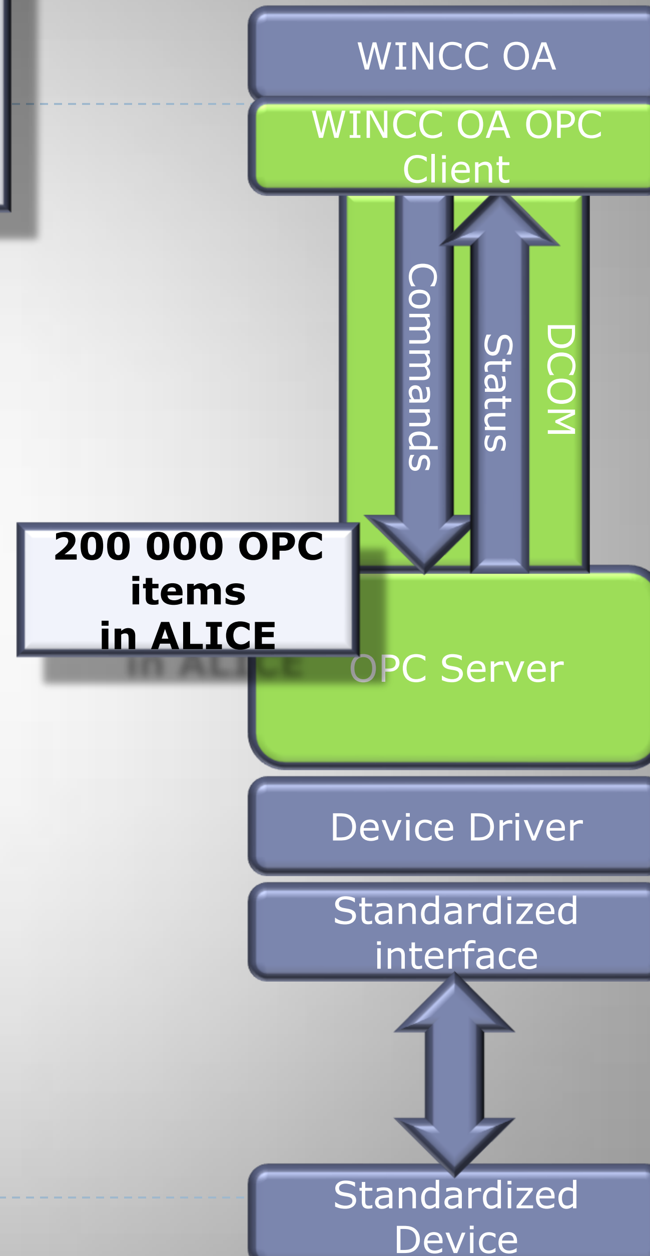
Downloads

Category: Specifications

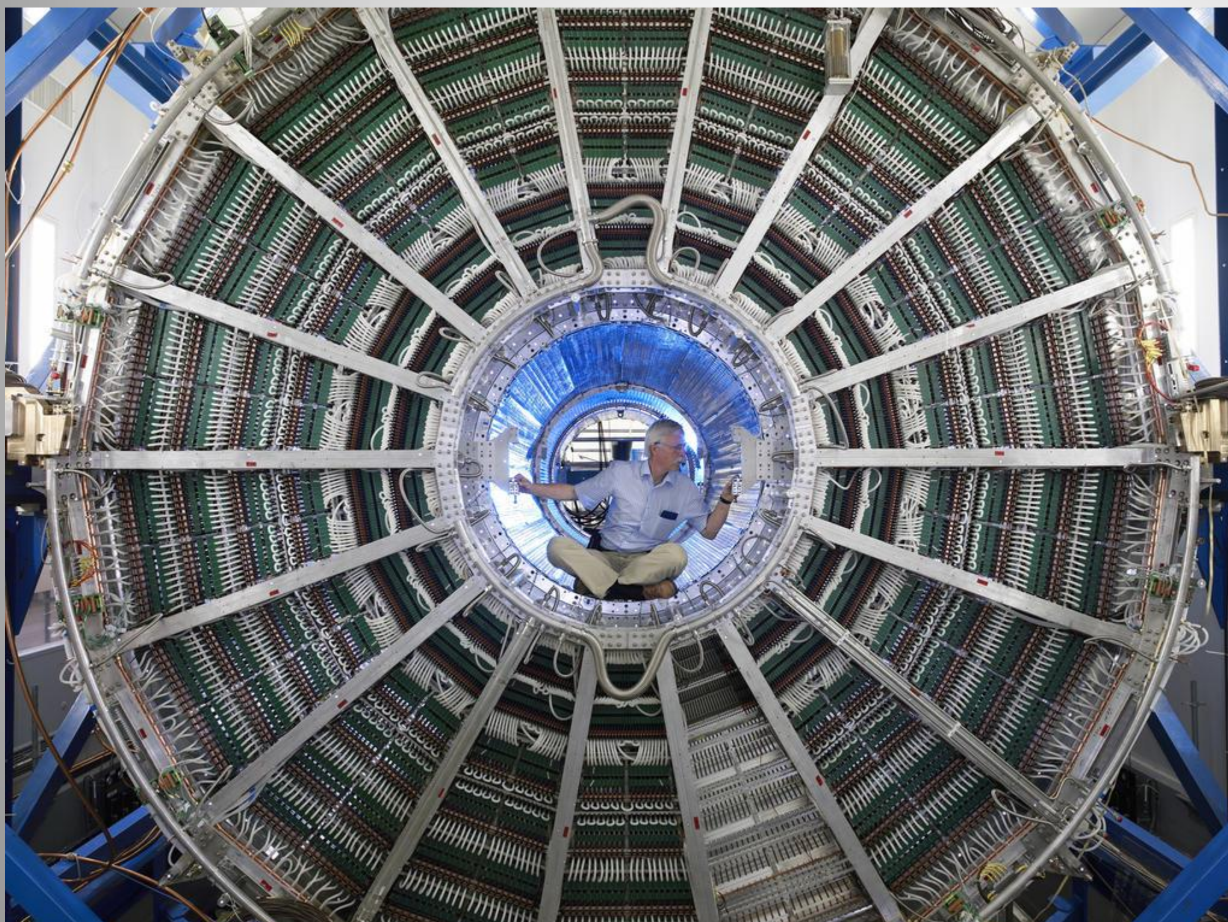
Filter By Title | Filter None
Filter By Status | Filter Current

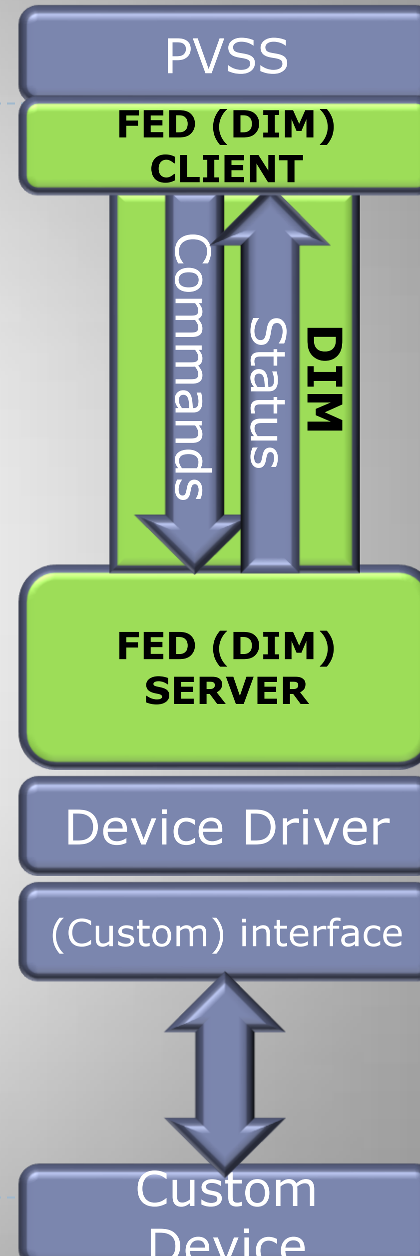
62 rows found

Title	Version	Availability	Last Modified
FDI Usability Style Guide Draft	fd 04	Members	2013-09-10
OPC UA For Analyser Devices 1.1 Companion Specification	1.1	Members	2013-07-31
OPC UA For Devices 1.1 Companion Specification	1.1	Members	2013-07-29
OPC UA Part 7 - Profiles 1.02 Specification	1.02	Members	2013-04-18
OPC UA for ISA-95 Common Object Model	1.01.00	Members	2013-04-17
OPC UA Part 2 - Security Model 1.02 Specification	1.02	Members	2013-04-17
OPC Data Access 3.00 Errata	3.00	Members	2013-03-21
OPC Historical Data Access 1.20 Errata	1.20	Members	2013-03-21
OPC XML-DA 1.01 Errata	1.01	Members	2013-03-21
FDI Specifications, Release Candidate 0.9	0.9	Corporate Members	2013-02-12
OPC UA 1.02 Specifications Errata	1.00	Members	2012-10-23
OPC UA Part 1 - Overview and Concepts 1.02 Specification	1.02	NonMembers	2012-08-16
OPC UA Part 3 - Address Space Model 1.02 Specification	1.02	Members	2012-08-16

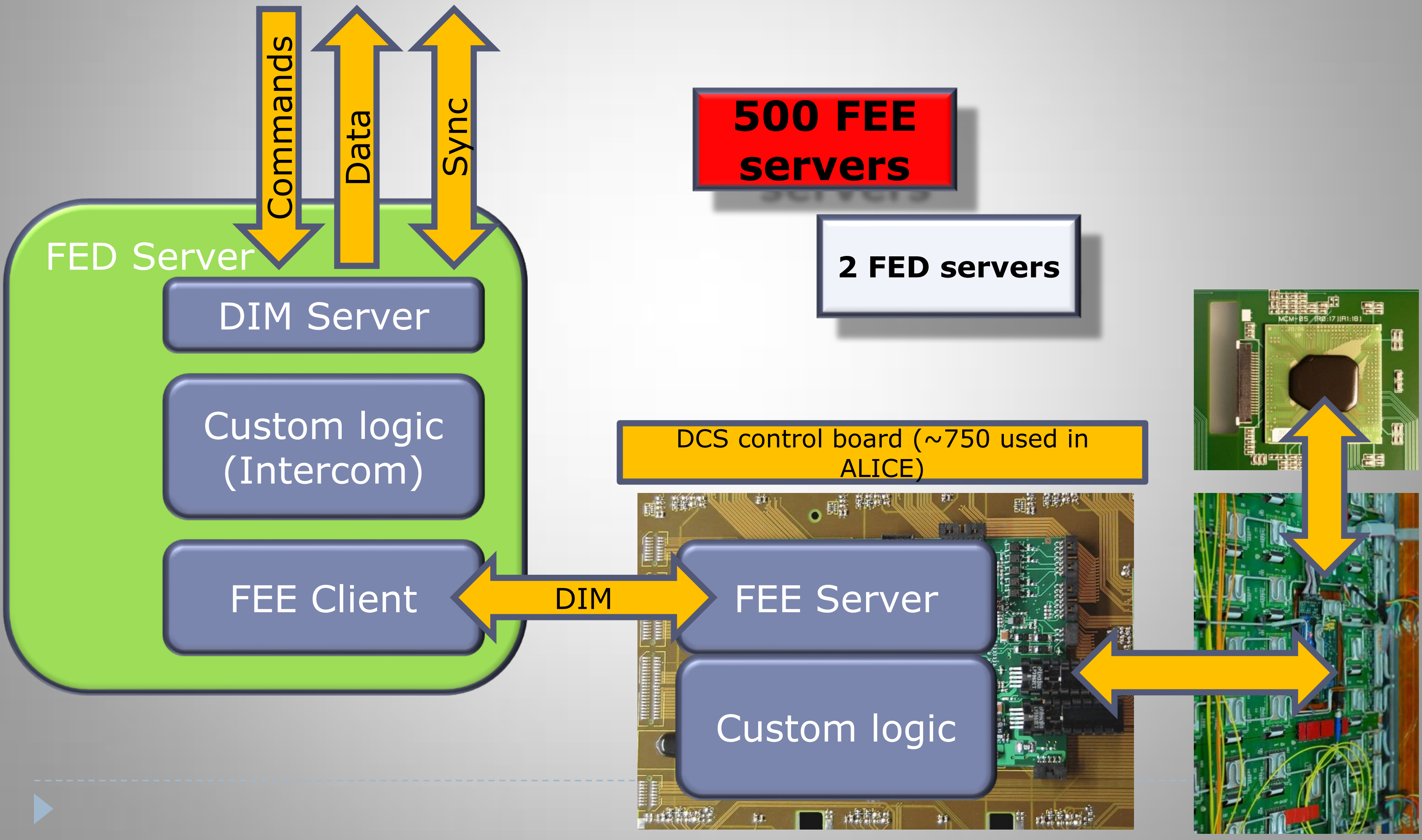


- **Missing standard for custom devices**
  - **OPC to heavy to be developed and maintained by institutes**
  - **Frontend drivers often scattered across hundreds of embedded computers (Arm Linux)**





TRD FED Implementation



Firewalls

- The firewalls cannot be installed on all devices
  - Majority of controls devices run embedded operating systems
    - PLC, front-end boards, oscilloscopes,...
  - The firewalls are MISSING or IMPOSSIBLE to install on them

Firewalls

- Are (simple) firewalls (simply) manageable on controls computers?

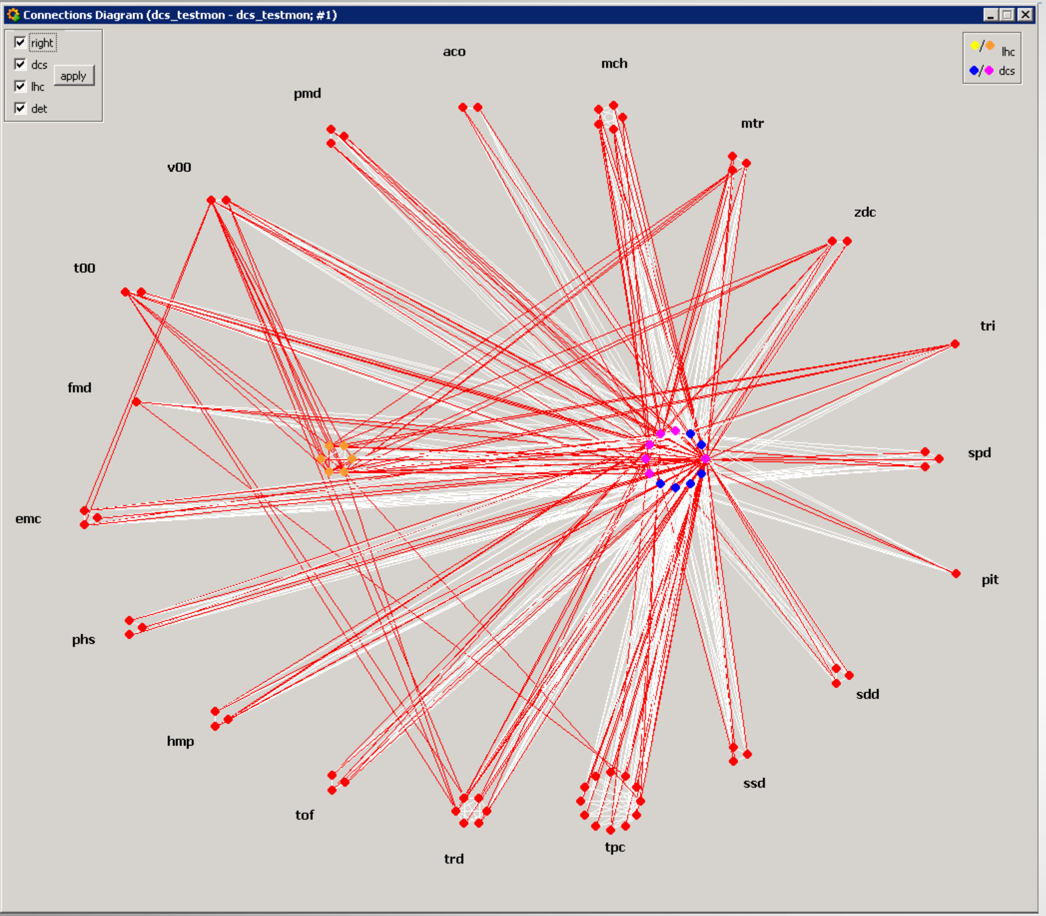
Firewalls

- There is no common firewall rule to be used
- The DCS communication involves many services, components and protocols
  - DNS, DHCP, WWW, NFS, DFS,
  - DIM, DIP, OPC, MODBUS, SSH,
  - ORACLE clients, MySQL clients
  - PVSS internal communication
- Efficient firewalls must be tuned per system
- Each DCS computer and device has a unique setup!

Firewalls

- The DCS configuration is not static
  - Evolution
  - Tuning (involves moving boards and devices across detectors)
  - Replacement of faulty components
- Each modification requires a setup of firewall rules by expert
  - Interventions can happen only during LHC access slots, with limited time for the actions
    - Can the few central admins be available 24/7?

System Complexity



Example of the cross-system connectivity as seen by monitoring tools

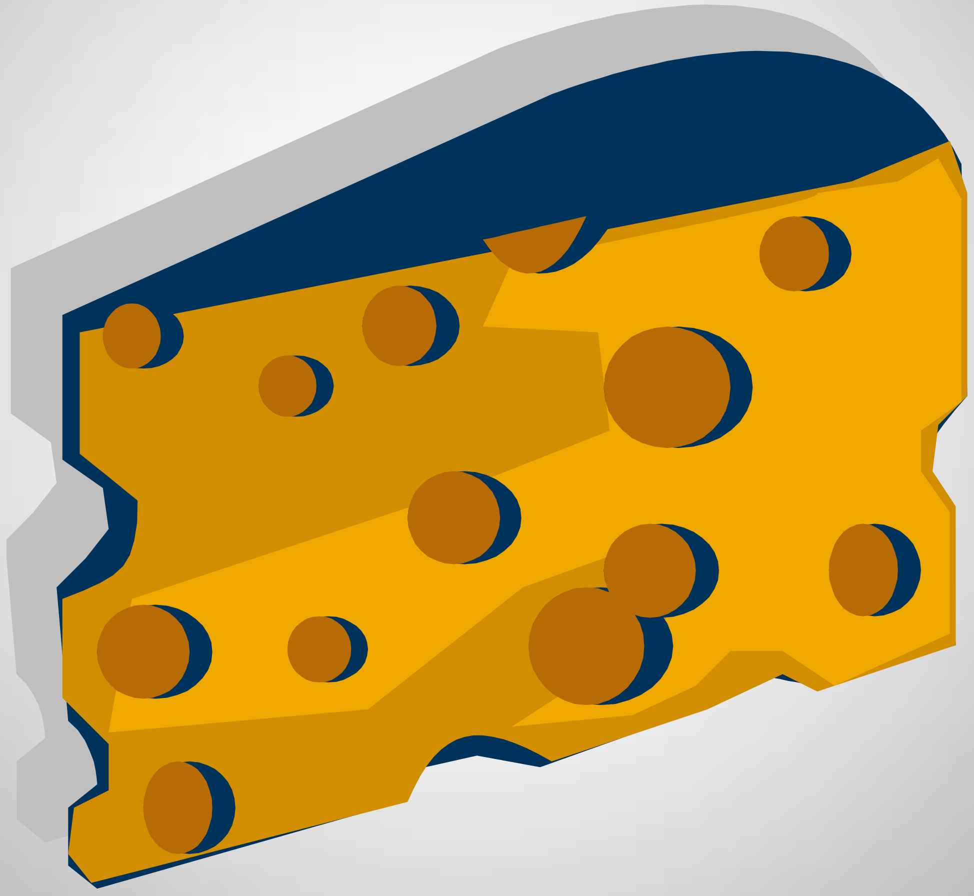
- Red dots represent PVSS systems

Firewalls

- Firewalls must protect the system but should not prevent its functionality
  - Correct configuration of firewalls on all computers (which can run firewalls) is an administrative challenge
  - Simple firewalls are not manageable and sometimes dangerous
    - for example Windows firewall turns on full protection in case of domain connectivity loss
      - Nice feature for laptops
        - **Killing factor for controls system which is running in emergency mode due to restricted connectivity**
- And yes, most violent viruses attack the ports, which are vital for the DCS and cannot be closed...

Typical controls firewall configuration

Typical controls firewall configuration



Antivirus

- Antivirus is a must in such complex system
- But can they harm? Do we have resources for them?

Antivirus

- Controls systems were designed 10-15 years ago
  - Large portion of the electronics is obsolete (PCI cards, etc.) and requires obsolete (=slow) computers
- Commercial software is sometimes written inefficiently and takes a lot of resources without taking advantage of modern processors
  - Lack of multithreading forces the system to run on fast cores (i.e. Limited number of cores per CPU)

Antivirus

- Operational experience shows that fully operational antivirus will start interacting with the system preferably in critical periods like the End of Run
  - When systems produce conditions data (create large files)
  - When detectors change the conditions (communicate a lot)
    - adopt voltages as a reaction to beam mode change
    - Recovery from trips causing the ERROR and aborting run...

Antivirus and firewall finetuning

- Even a tuned antivirus typically shows on top 5 resource hungry processes

- CPU core affinity settings require huge effort
  - There are more than 2700 PVSS managers in ALICE DCS, 800 DIM servers, etc.

- The solutions are:
  - Run firewall and antivirus with very limited functionality
  - Run good firewalls and antivirus on the gates to the system

Btw…

- How much does it cost?
- Local firewall can reduce the amount of data flowing between WINCC OA systems by 10%
- Active antivirus can reduce the throughput by additional 20-30%

Software versions and updates

- It is a must to run the latest software with current updates and fixes
  - Is this possible?

Software versions and updates

- ALICE operates in 24/7 mode without interruption
- Short technical stops (4 days each 6 weeks) are not enough for large updates
  - DCS supervises the detector also without beams
  - DCS is needed for tests
- Large interventions are possible only during the long technical stops - around Christmas
- Deployment of updates requires testing, which can be done only on the real system
- Front-end boards run older OS versions and cannot be easily updated
- ALICE deploys critical patches when operational conditions allow for it
  - Whole system is carefully patched during the long stops

Conclusions

- The cybersecurity importance is well understood in ALICE and is given high priorities
- Even under the described conditions, the DCS if responsible for safe and stable operation of the experiment