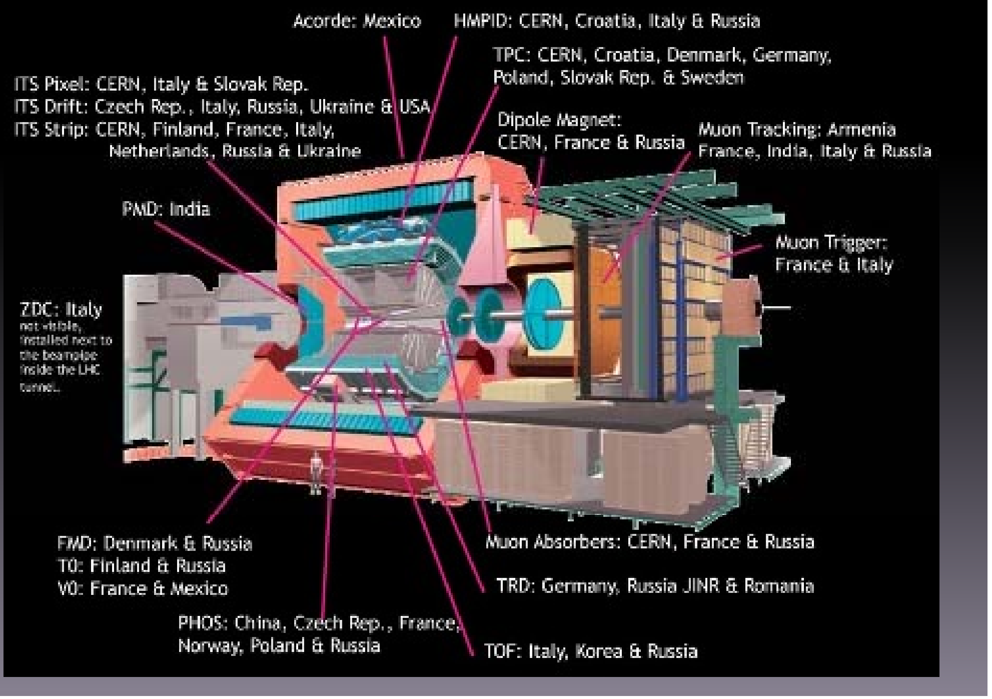
CYBERSECURITY IN ALICE DETECTOR CONTROL SYSTEM

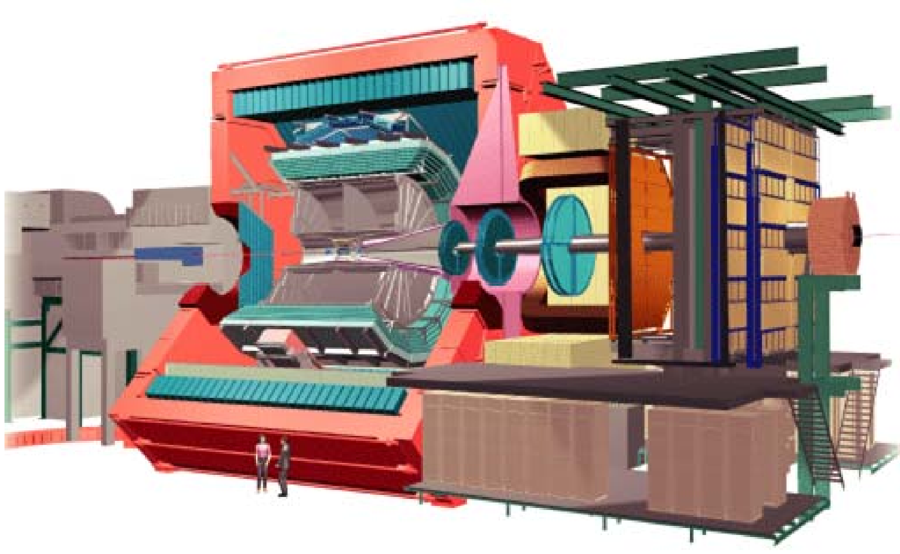
Peter Chochula
for ALICE DCS team
CERN, Geneva Switzerland

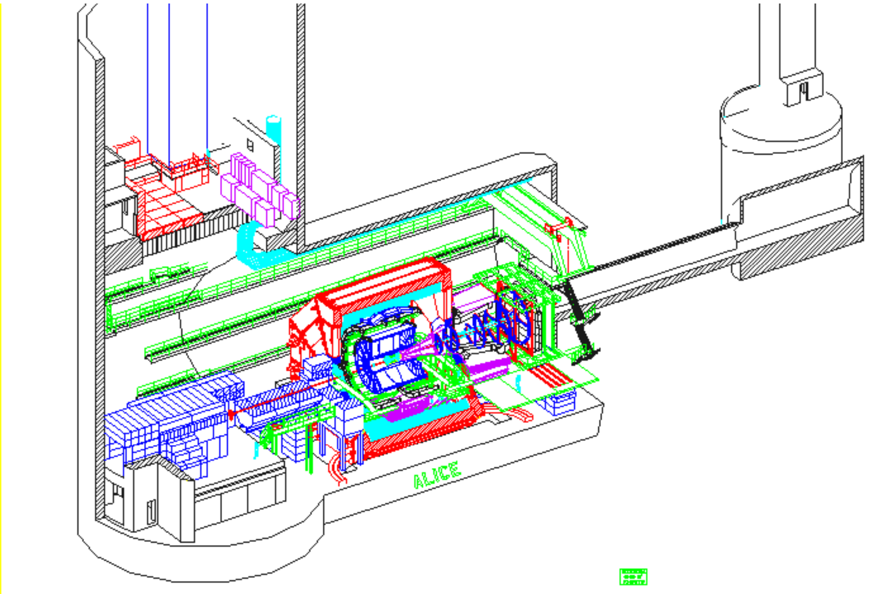
ALICE Experiment at CERN

- Dedicated to study of ultrarelativistic heavy ions collisions at LHC
- Built as joint effort of more than 1000 physicists from more than 100 institutes in 30 countries


Acorde: Mexico
HMPID: CERN, Croatia, Italy & Russia
TPC: CERN, Croatia, Denmark, Germany, Poland, Slovak Rep. & Sweden
ITS Pixel: CERN, Italy & Slovak Rep.
ITS Drift: Czech Rep., Italy, Russia, Ukraine & USA
ITS Strip: CERN, Finland, France, Italy, Netherlands, Russia & Ukraine
Dipole Magnet: CERN, France & Russia
Muon Tracking: Armenia France, India, Italy & Russia
PMD: India
Muon Trigger: France & Italy
ZDC: Italy
not visible, installed next to the beampipe inside the LHC tunnel.
FMD: Denmark & Russia
T0: Finland & Russia
V0: France & Mexico
Muon Absorbers: CERN, France & Russia
TRD: Germany, Russia JINR & Romania
PHOS: China, Czech Rep., France, Norway, Poland & Russia
TOF: Italy, Korea & Russia

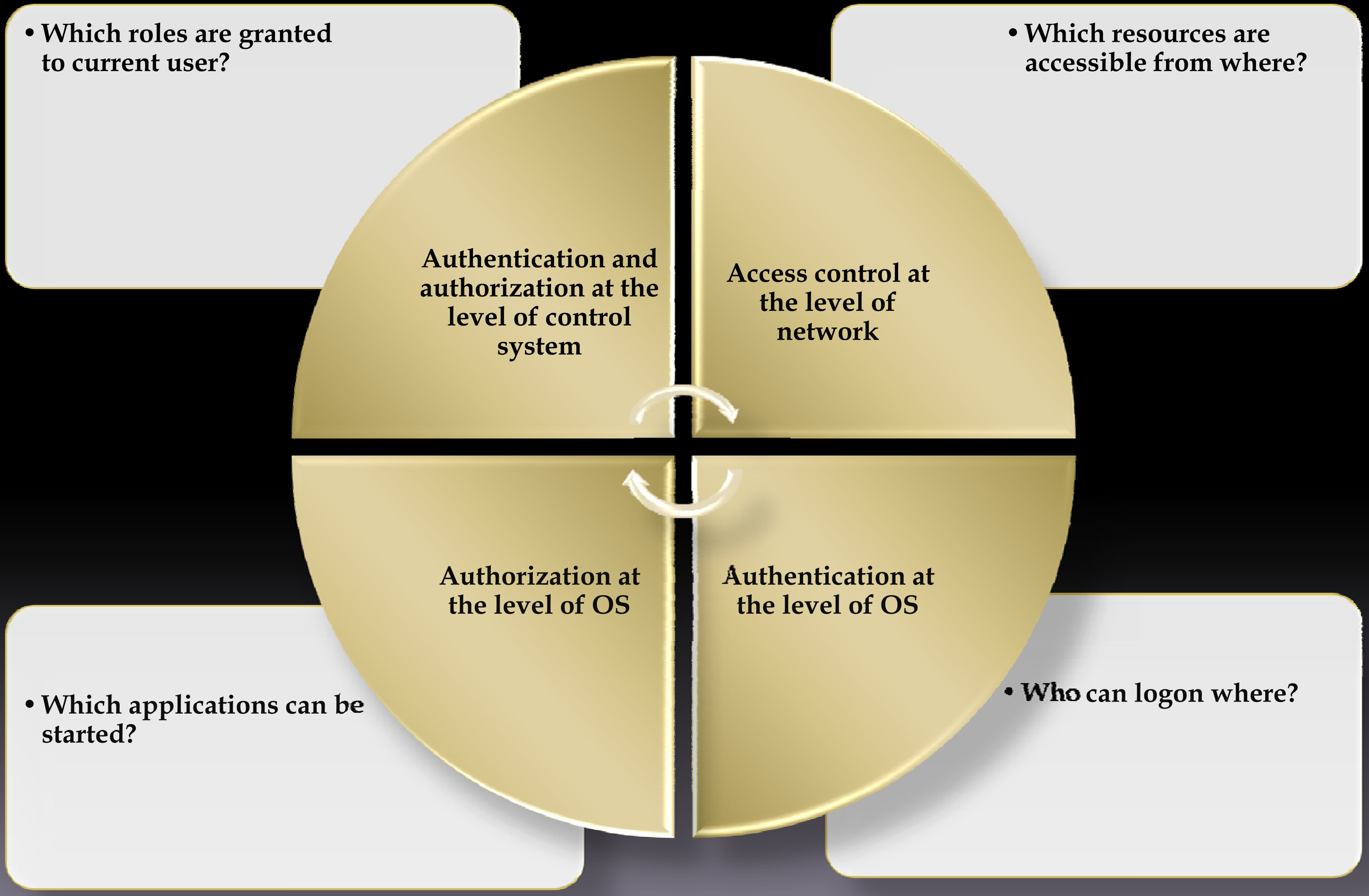
ALICE Detector Controls system





- Responsible for safe operation of ALICE
- Based on commercial SCADA system PVSSII
- Controls 18 sub-detectors and about 150 subsystems
- Directly involved in control of ~300 000 channels
  - About 1 000 000 properties handled by DCS

Security Layers in ALICE DCS



- Which roles are granted to current user?

Authentication and authorization at the level of control system

- Which resources are accessible from where?

Access control at the level of network

- Which applications can be started?

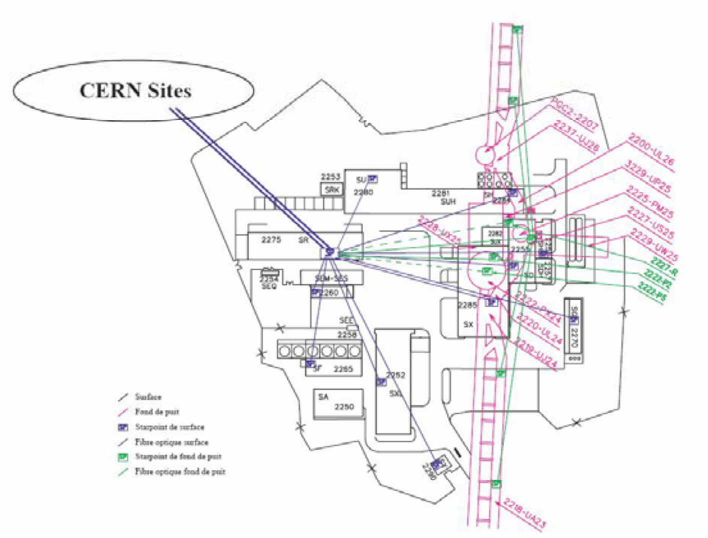
Authorization at the level of OS

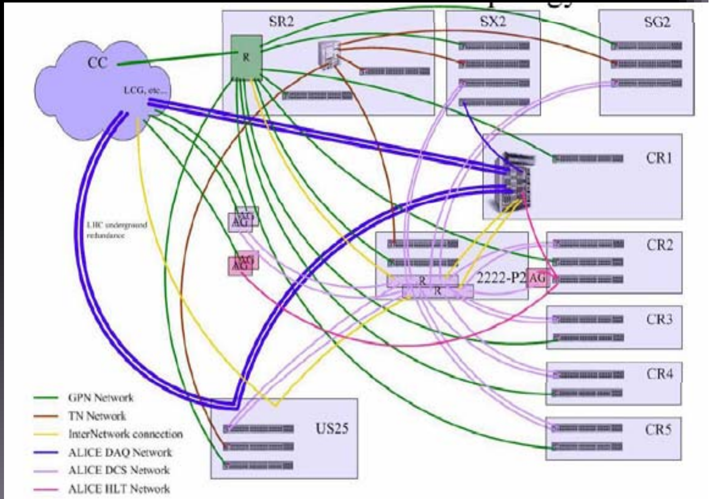
- Who can logon where?

Authentication at the level of OS

ALICE DCS Network

- Covers ALICE cavern and surface buildings
- Based on CNIC recommendations and tools
  (details in talk of Stefan Lueders in this workshop)
  - No direct connection with external networks
  - Host exposed by DCS network are accessible from general purpose network (GPN)
  - Hosts from other (CERN) network are visible from DCS network only if they belong to a set of trusted machines



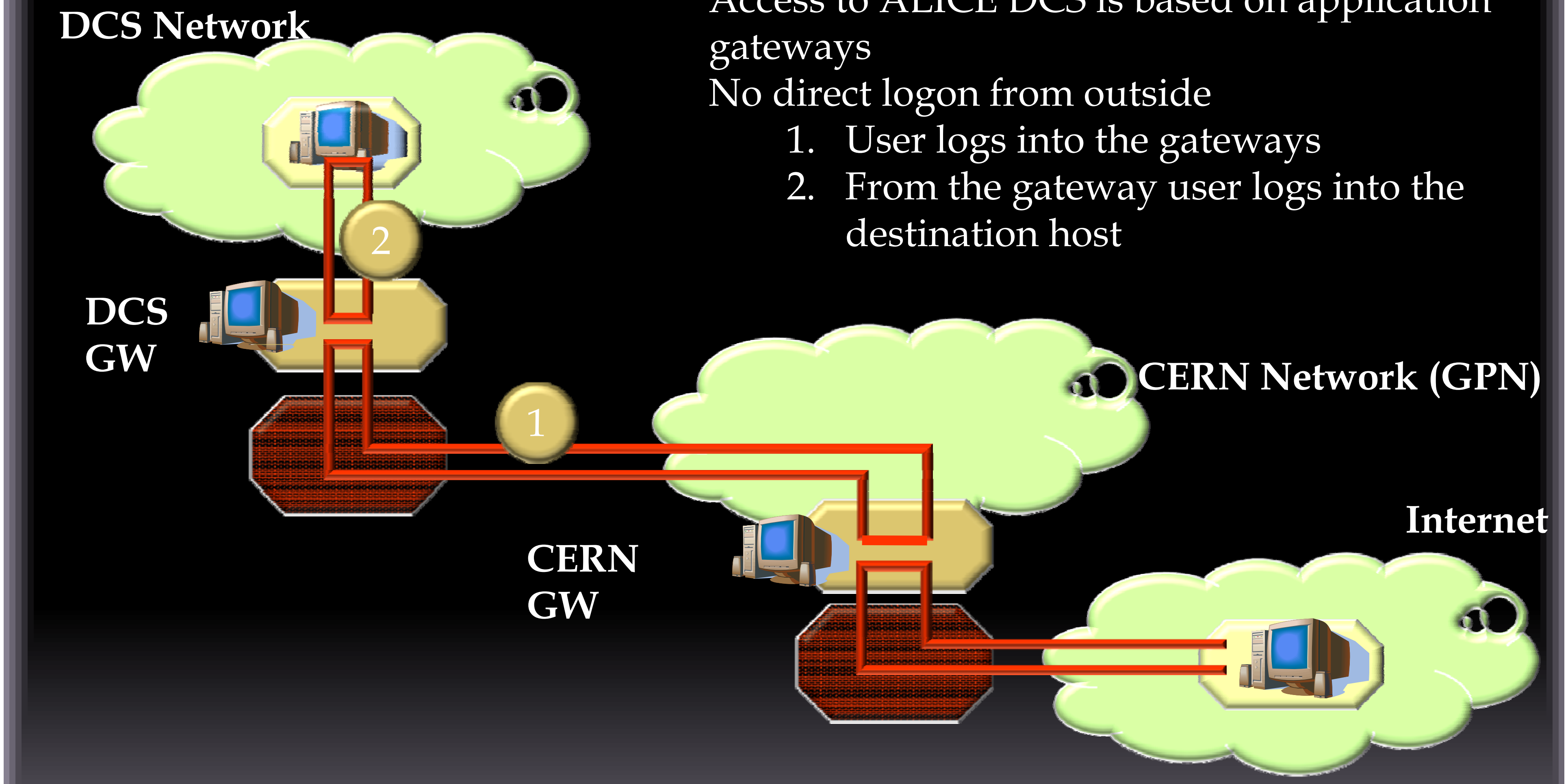


ALICE DCS Computing Infrastructure in Numbers

- DCS Network:
  - 1400 network ports
  - 1200 network attached devices

- DCS Computers
  - 150 DCS servers
  - 800 Single board computers
  - 250 crates

Remote Access to the DCS Network

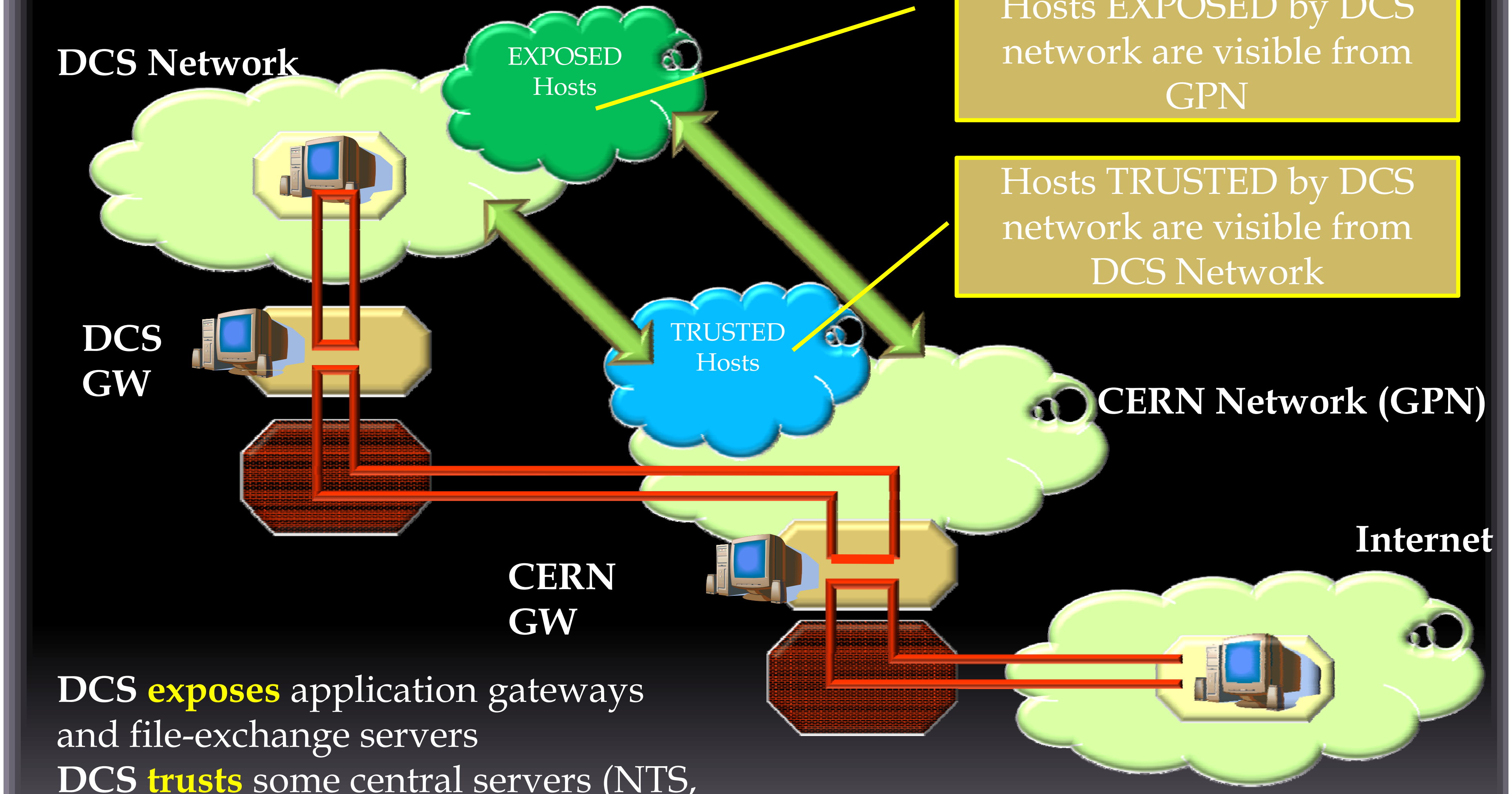


Access to ALICE DCS is based on application gateways

No direct logon from outside

1. User logs into the gateways
2. From the gateway user logs into the destination host

Remote Access to the DCS Network



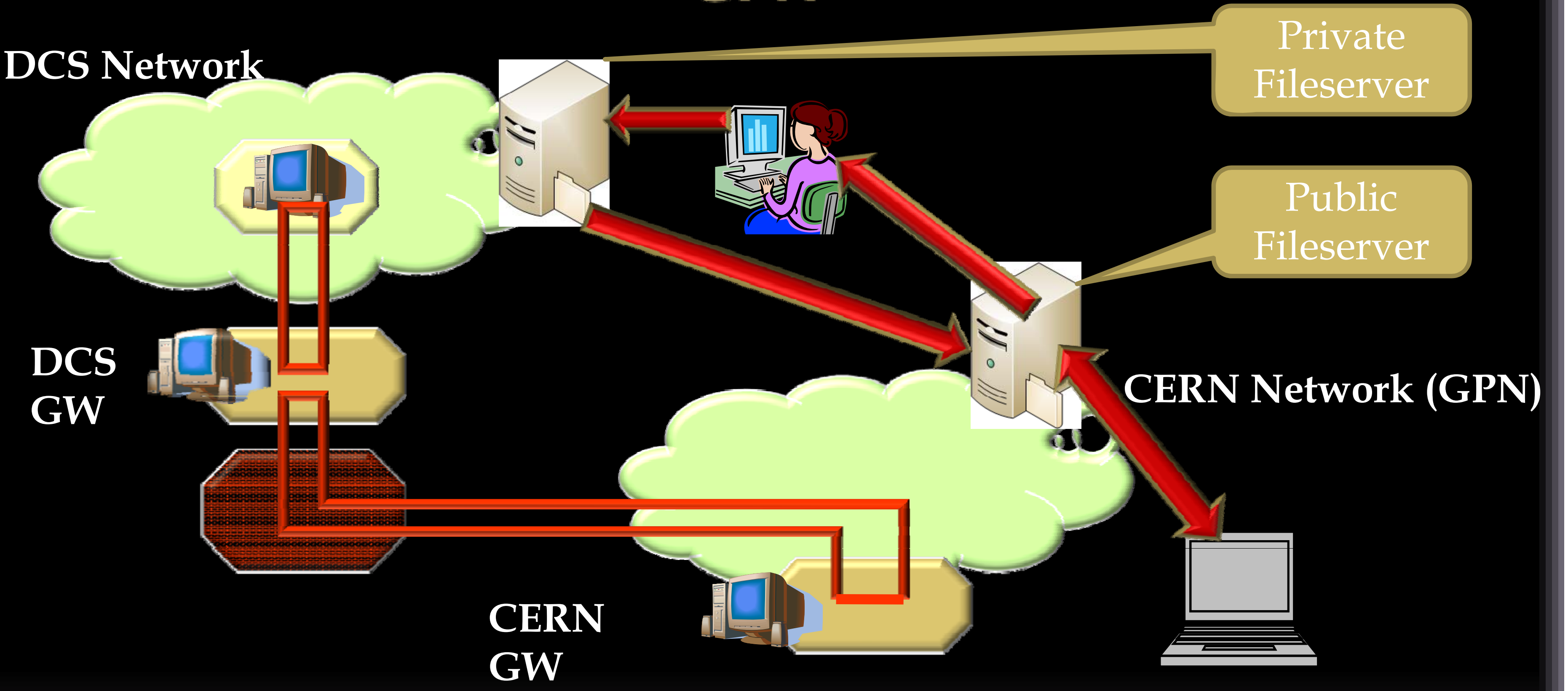
Hosts EXPOSED by DCS network are visible from GPN

Hosts TRUSTED by DCS network are visible from DCS Network

DCS **exposes** application gateways and file-exchange servers

DCS **trusts** some central servers (NTS, DNS, authentication servers…)

Data Exchange Between DCS Network and GPN

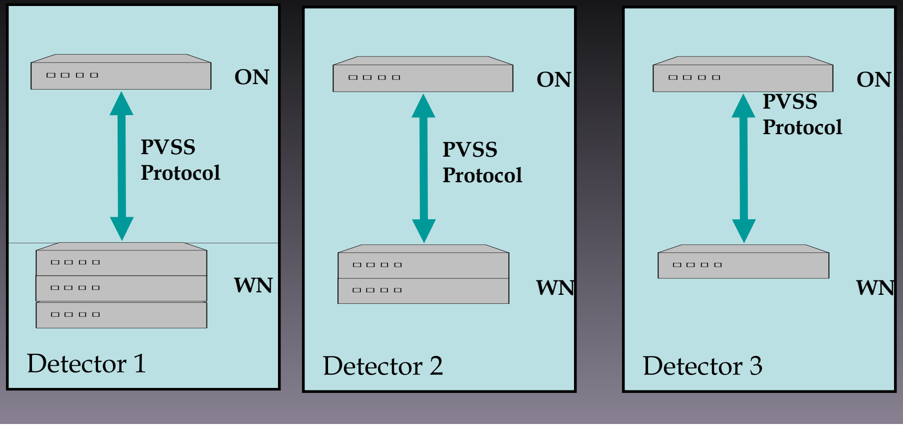


DCS exposes application gateways and file-exchange servers

DCS trusts some central servers (NTS, DNS, authentication servers…)

DCS Computer Roles

- 3 categories of computers
  - Central servers
    - Backend service (DNS, database, …)
    - Engineering nodes
    - Application gateways
  - Operator nodes
    - Run UI
    - Windows Server 2003 and Terminal Service
  - Worker nodes
    - Run DCS software as system service



Security at the level of OS (1)

- DCS computers run different OS according to their roles:
  - 90 Windows XP nodes running PVSSII
  - 27 Servers running Windows Server 2003
    - All configured as terminal servers
  - 6 database servers running RedHat Enterprise Linux
  - 27 front-end servers running SLC4
  - 800 DCS boards runing uCLinux

Security at the level of OS (2)

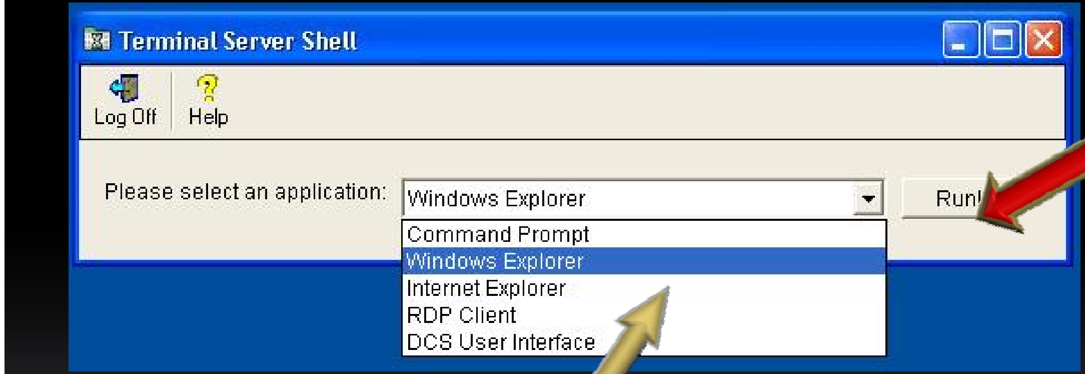
- Users logon only to Windows machines
  - Linux hosts are typically running device drivers
- **Authentication** based on CERN common infrastructure
  - CERN authentication servers are trusted by DCS network
    - Users use own credentials everywhere
  - Few generic service accounts are used to run OS services
- **Authorization** enforced through policies:
  - Users get privileges only on computers belonging to their group and on selected central services (application gateway etc.)
  - Detector users are divided into two groups:
    - **Users**
    - **Experts**

- User actions are restricted to
  - Logon to application gateways
  - Launching basic applications

- Experts are authorized to
  - Logon to application gateways
  - Launch wider range of applications
  - Logon (with elevated privileges) to all computers belonging to their project

Controlling Access to Applications at the OS Level

- On gateways the standard Windows user interface is replaced by custom shell (TSSHELL)
  - User cannot interact with the operating system anymore
  - Only actions granted to user can be performed (standard users can only start the PVSSII UI)

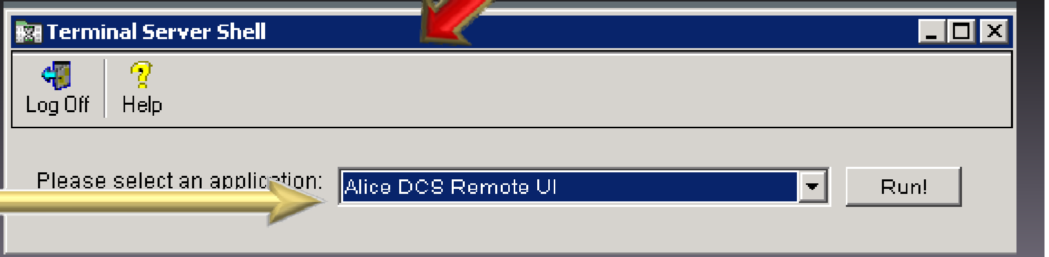


Terminal Server Shell

Please select an application: Windows Explorer

Expert Mode

User Mode



Terminal Server Shell

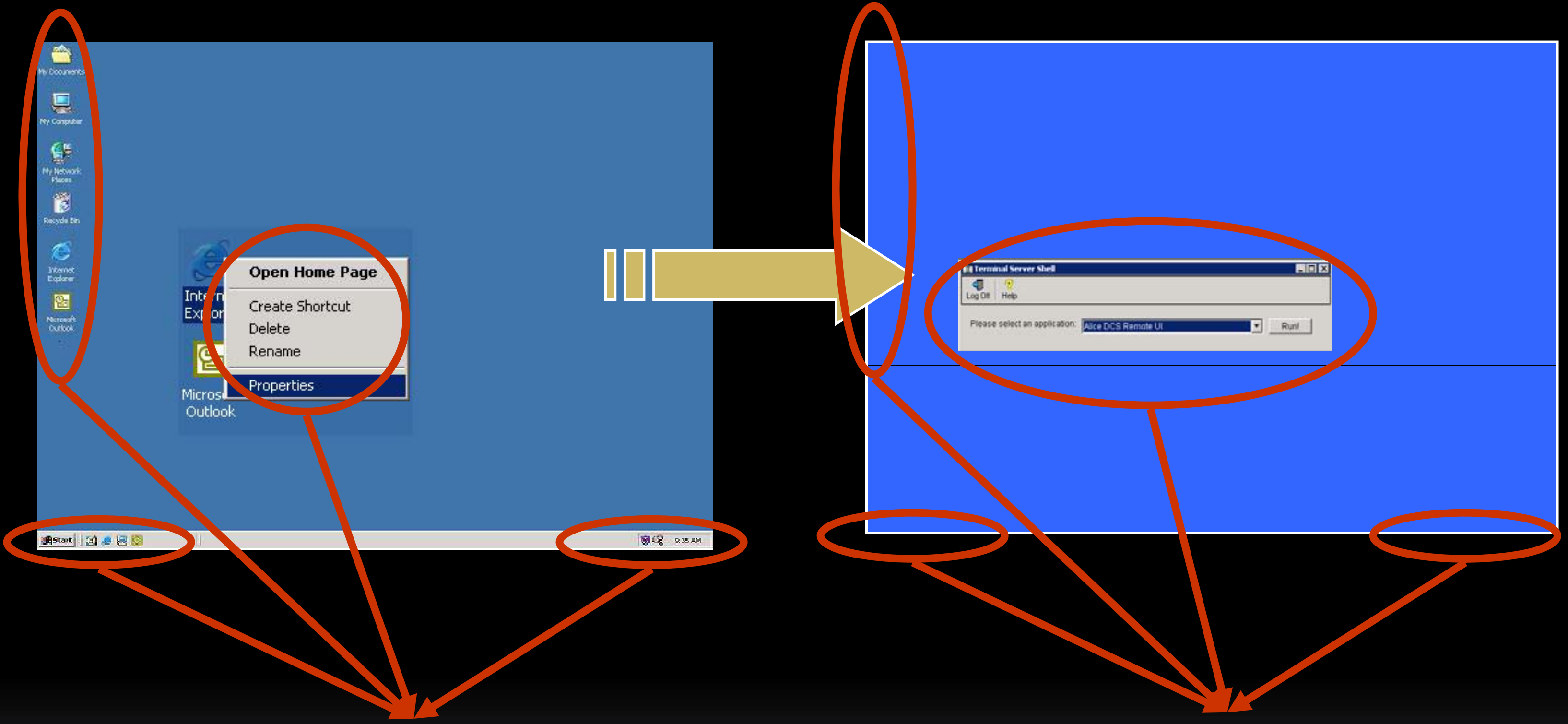
Please select an application: Alice DCS Remote UI

List of **available actions** is generated dynamically by the TSSHELL according to **group membership**

The TSSHELL

Standard Windows Shell

TSShell



Please select an application: Alice DCS Remote UI

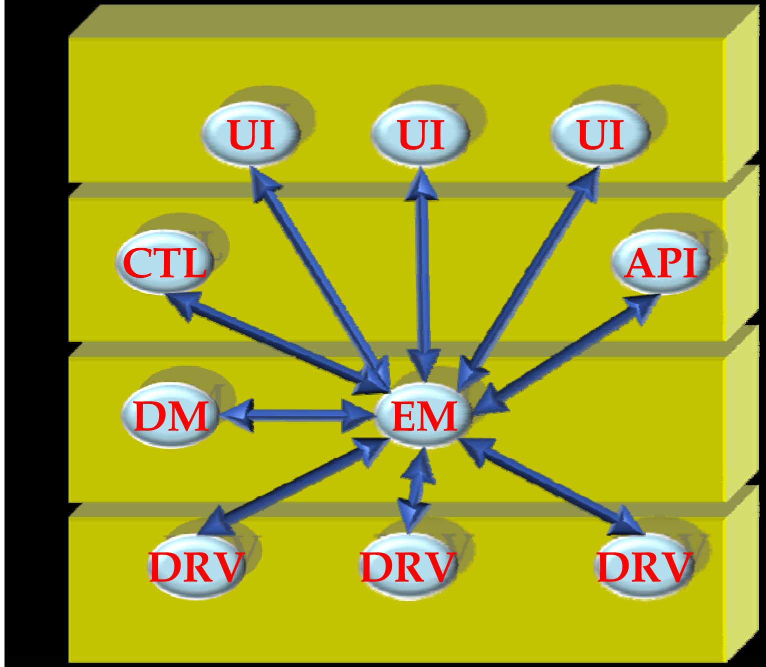
User can interact with system in several ways

User cannot interact with system – TSSHELL is the only available interface

Access Control at the Level of DCS Applications

- Access control to DCS applications is closely tied with DCS architecture
- Core of the DCS is built on commercial SCADA system PVSSII
- Access control implemented at the level of UI provides:
  - Authentication control
  - Authorization
  - Accounting
- Role of the PVSSII access control is to protect the system against the inadvertent errors
  - Protection against the malicious attacks is the role of network security and OS access control

PVSSII Architecture



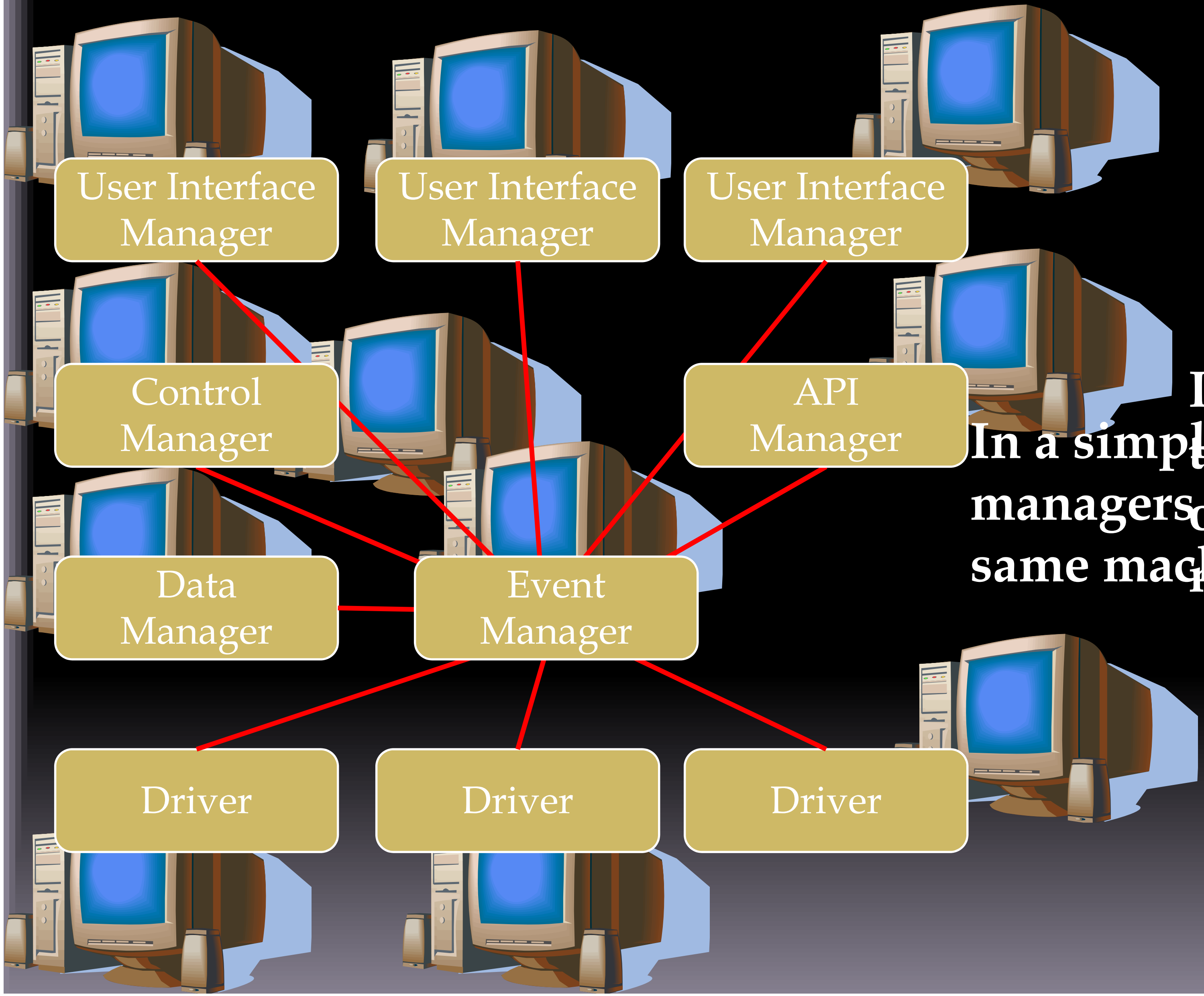
User Interface Layer

Application Layer

Communication and Storage Layer

Driver Layer

- PVSSII system is composed from specialized program modules (managers)
- Managers communicate via TCP/IP
- ALICE DCS is built from 100 PVSS systems composed of 900 managers



User Interface Manager

User Interface Manager

User Interface Manager

Control Manager

API Manager

Data Manager

Event Manager

Driver

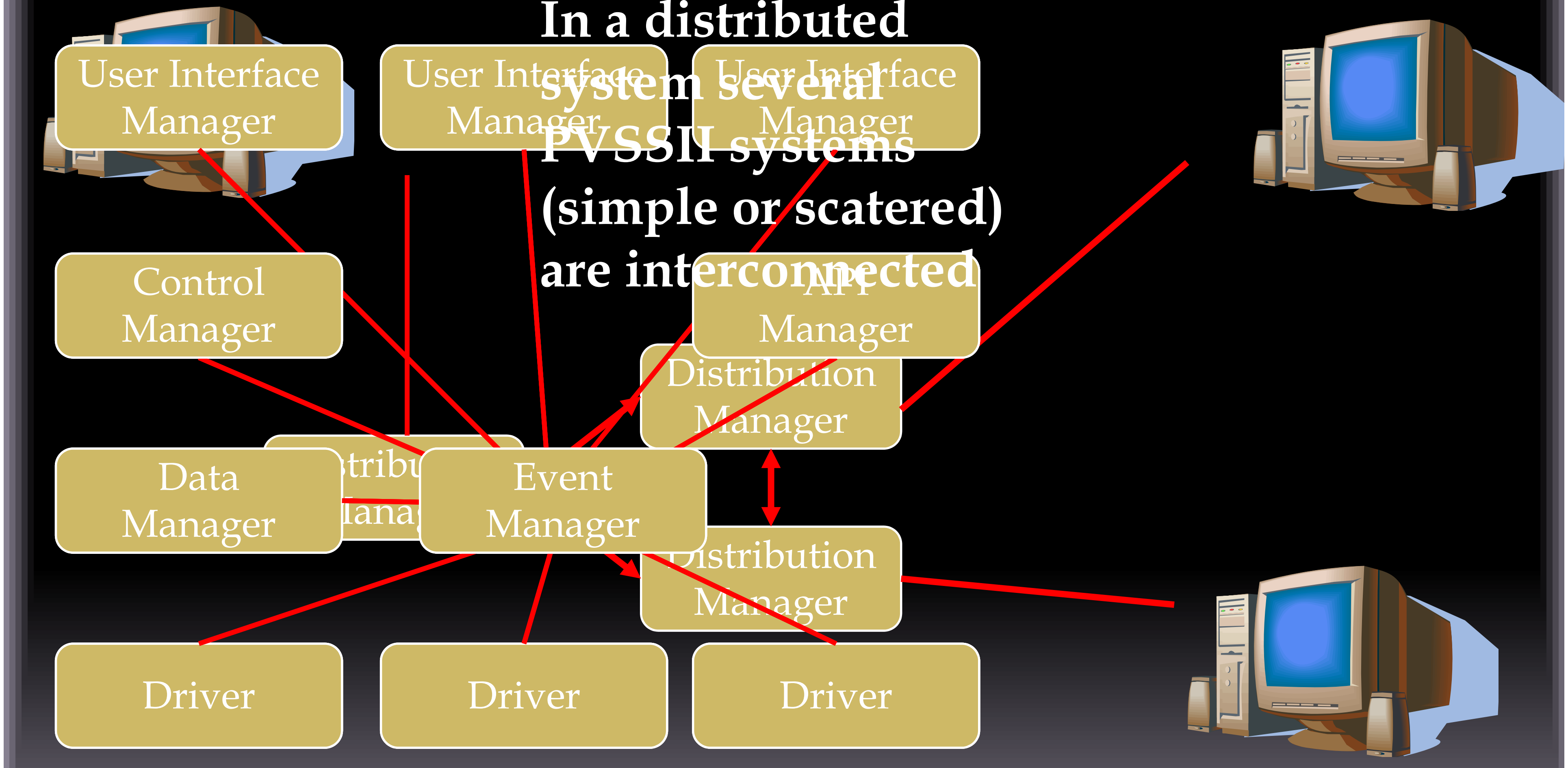
Driver

Driver

In a simple system all managers run on the same machine

In a scattered sy the managers ca on dedicated machines

In a distributed system several PVSSII systems (simple or scatered) are interconnected



User Interface Manager

User Interface Manager

User Interface Manager

Control Manager

API Manager

Distribution Manager

Data Manager

Distribution Manager

Event Manager

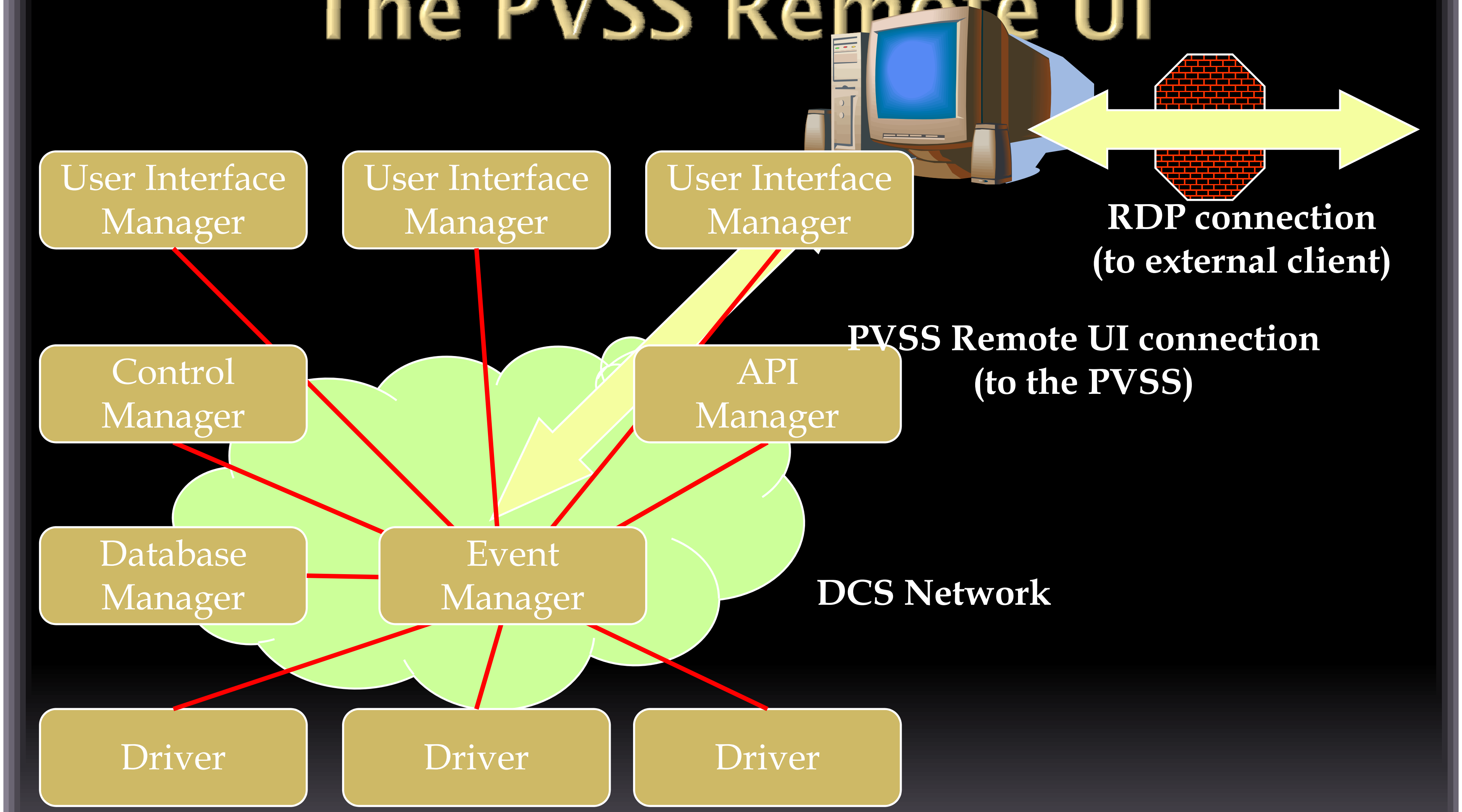
Distribution Manager

Driver

Driver

Driver

The PVSS Remote UI



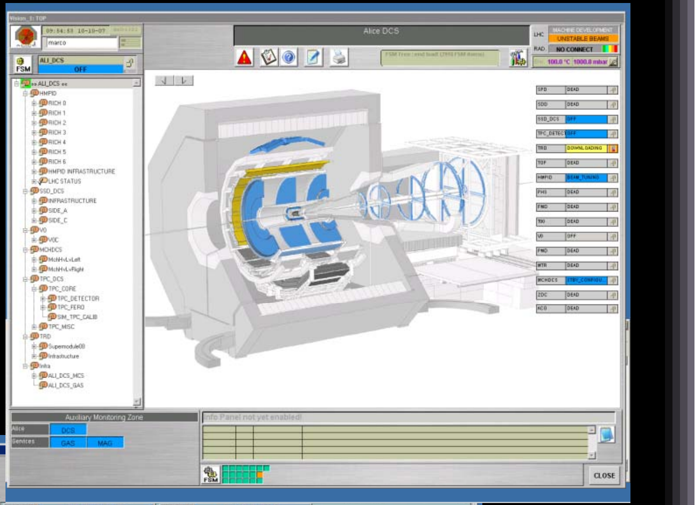
Standard ALICE DCS UI

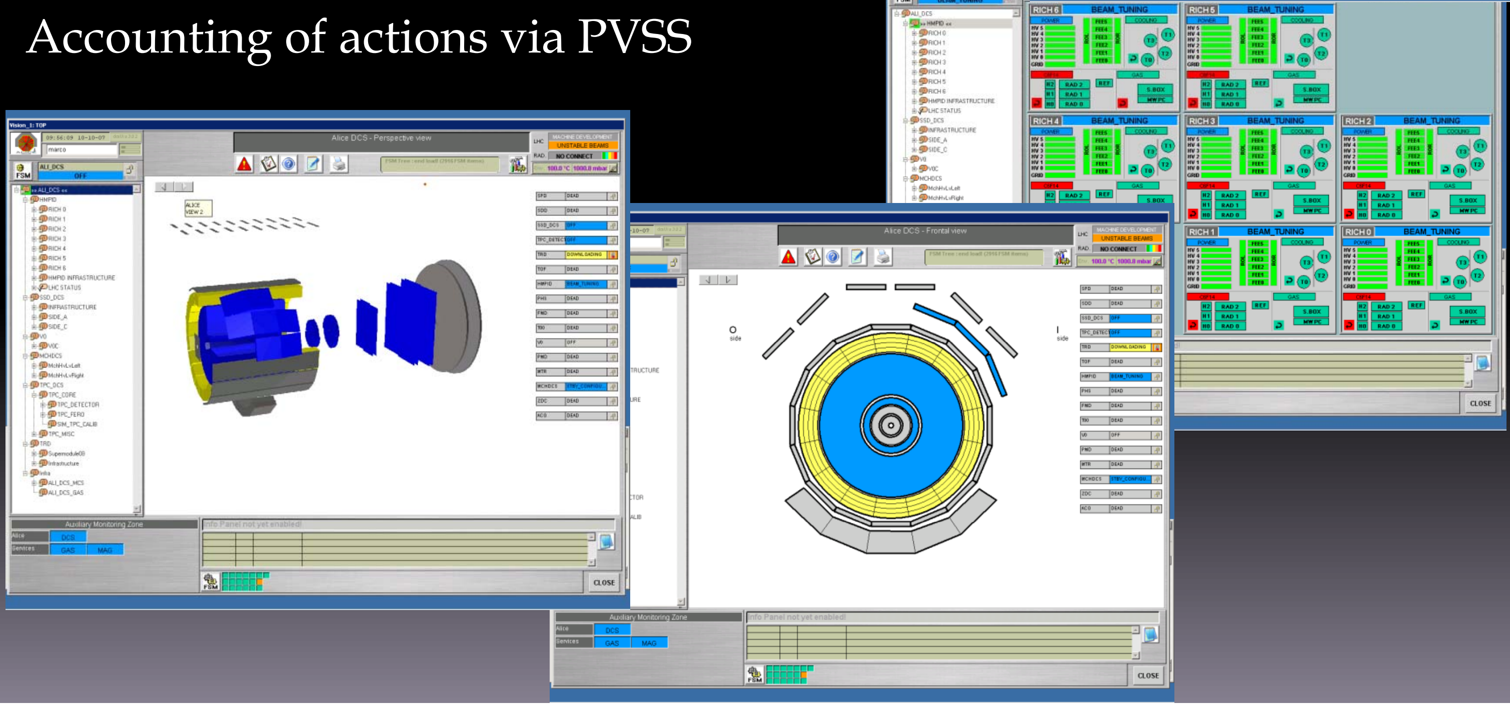
Standard UI is used on all DCS systems

Users must authenticate in each UI session

Actions available to users depend on authorization

Accounting of actions via PVSS





Implementation of the PVSSII Access Control in ALICE

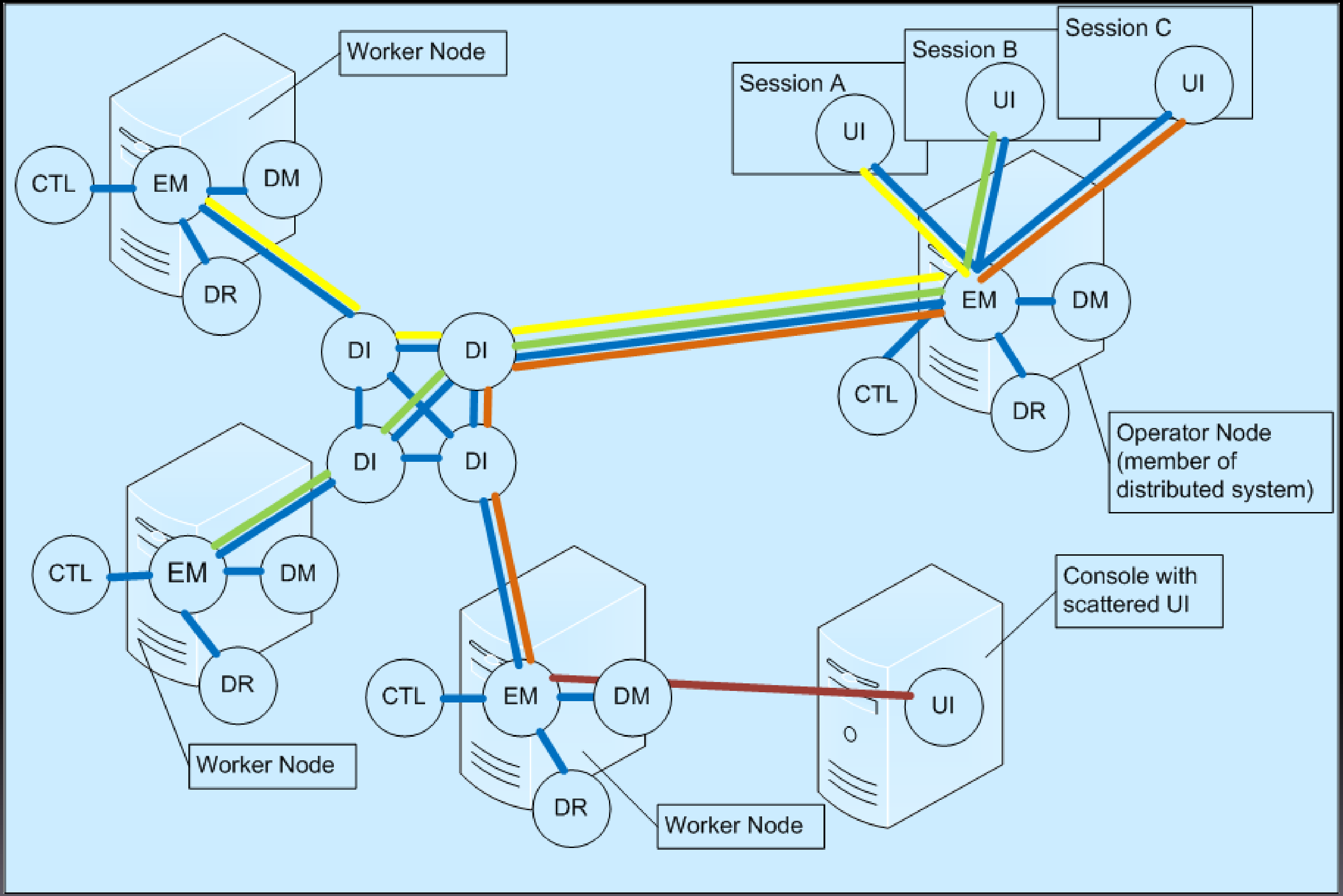
- The ALICE DCS is divided into domains per detector and subsystem
  - Example :
    - Detector domains: SPD, SSD, SDD …
    - Subsystem domains: SPD-HV, SPD-LV, SPD-COO…
- Each user can acquire different privileges for each domain
  - Example: the SPD cooling expert has Expert rights in the cooling sub-domain, but only standard privileges for the front-end sub-domain

Implementation of the PVSSII Access Control in ALICE

- DCS actions accessible in each domain depend on granted rights
  - **Monitor** to get read only access to DCS parameters
  - **Control** to change some parameters (for example to send commands to the detector via the FSM tools)
  - **Debug** to change all parameters, for example the alert or trip limits
  - **Modify** to modify structure of objects (for example to add new device channels or change the structure of datapoints)
  - **Administer** which allows for the administration of domain. This privilege is reserved for DCS administrators

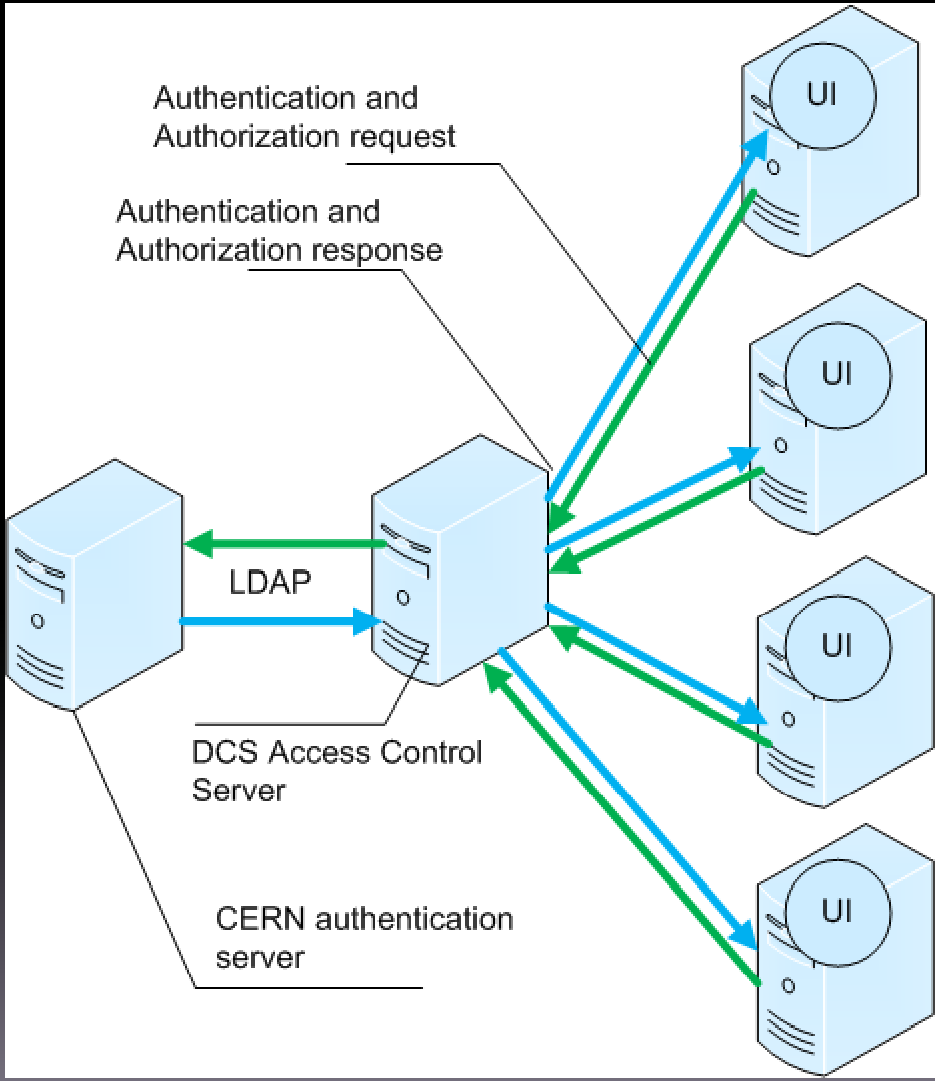
- DCS users are divided into groups according to their roles:
  - **Observers, Operators, Experts, Developers, Administrators**

Distributed and Scattered UIs in ALICE



PVSS Access Control

- Based on CERN JCOP tools and recommendations
  - **FW Access Control** component including Access Control Server
- **NICE Authentication**
  - ALICE runs PVSS only on Windows

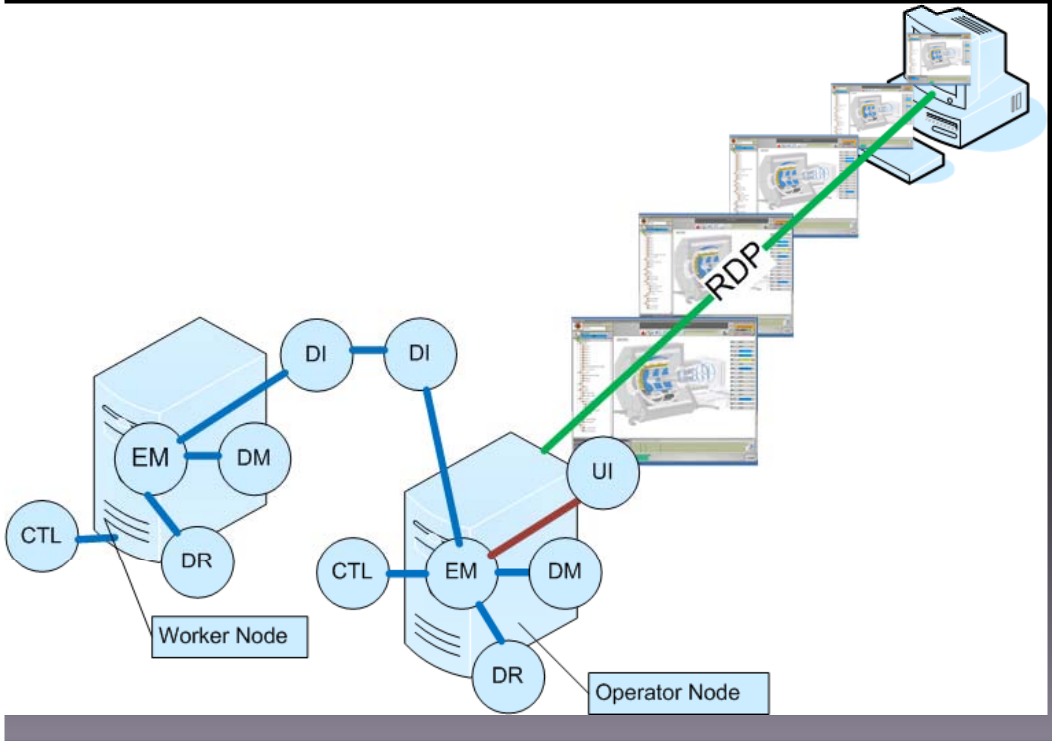

Authentication and Authorization request
Authentication and Authorization response
UI
UI
UI
UI
LDAP
DCS Access Control Server
CERN authentication server

Accessing the DCS UI

Each Operator Node is configured as Terminal Server

Several Users can connect to TS in parallel and launch the UI

Access to ON is established over RDP



ON and WN load for large number of remote clients

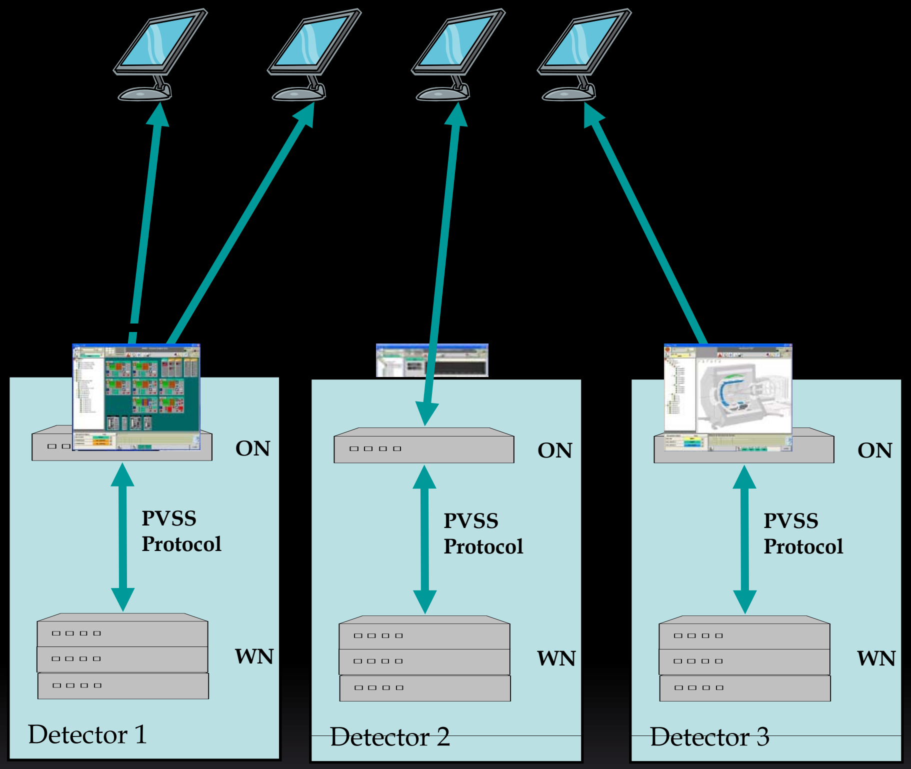
Master project generated 50000 datapoints and updated 3000 /s.
Remote client displayed 50 values at a time

Operator Node		
#clients	Average CPU load [%]	Mem [kB]
60	11.2	2788719
55	11.0	2781282
45	13.8	2790181
35	12.0	2672998
25	9.7	2067242
15	7.2	1448779
5	4.2	934763
0	4.9	666914

Worker Node		
#clients	Average CPU load [%]	Mem [kB]
60	85.1	579666
55	86.6	579829
45	84.9	579690
35	81.3	579405
25	80.9	579384
15	81.4	579463
5	83.0	580003
0	83.7	579691

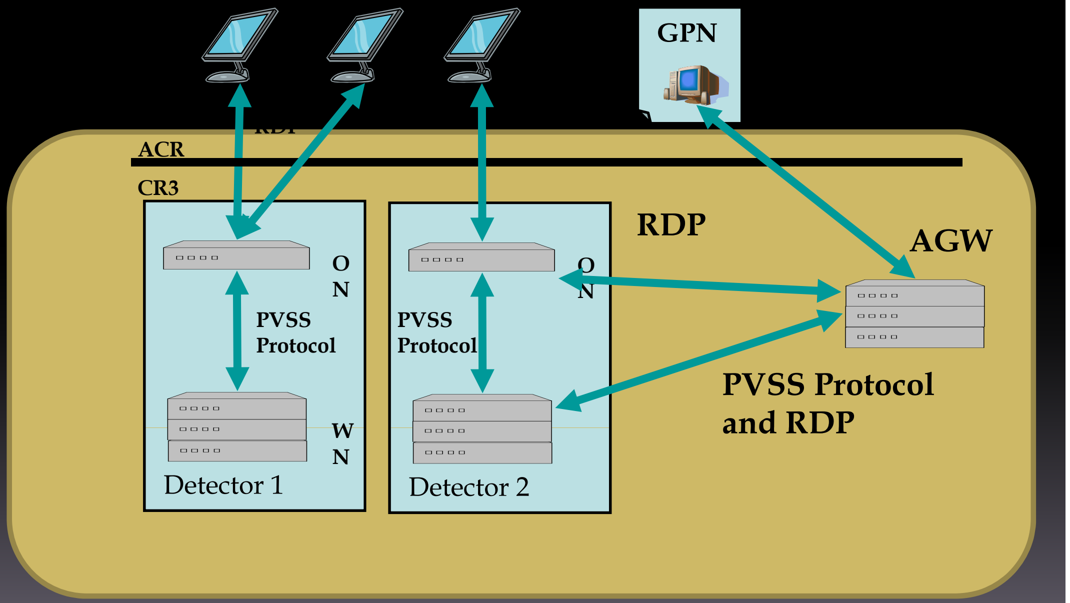
Accessing the DCS from ALICE Control Room

- Consoles in Control Room have access to the DCS network but do not run PVSSII
  - Consoles are detector independent
- User Interface runs on Operator Nodes
- Consoles access the Operator Node via the Remote Desktop Connection
  - The UI executes on the ON and the images are transferred to the console over RDP



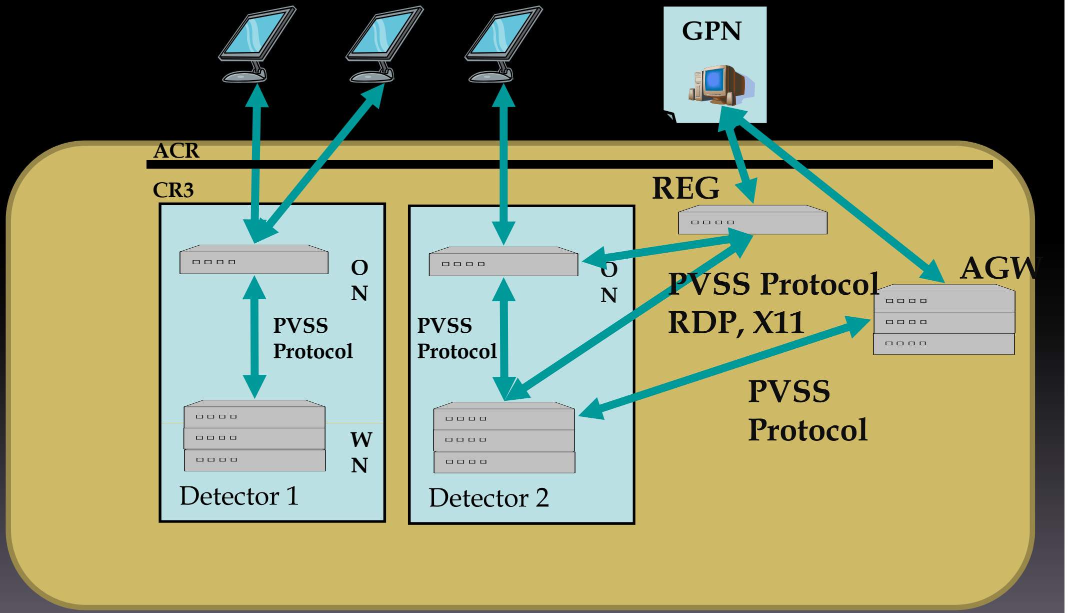
Accessing the DCS During Commissioning

- Access to the DCS from the GPN is granted via a cluster of dedicated application gateways
  - Users can logon to Operator Nodes of their project
  - Experts can logon also to Worker Nodes



Accessing the DCS During Operation

- AGW runs only PVSS UI, no RDP is possible
- Additional remote expert gateway (REG) allows for expert access to the DCS
  - Access only to authorized persons
  - SmartCards required



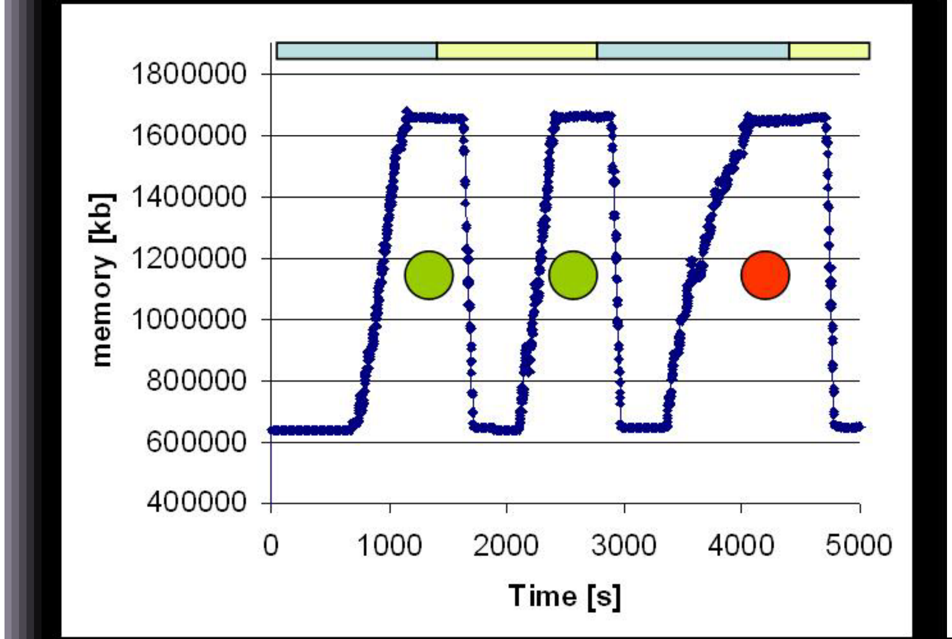
Conclusions

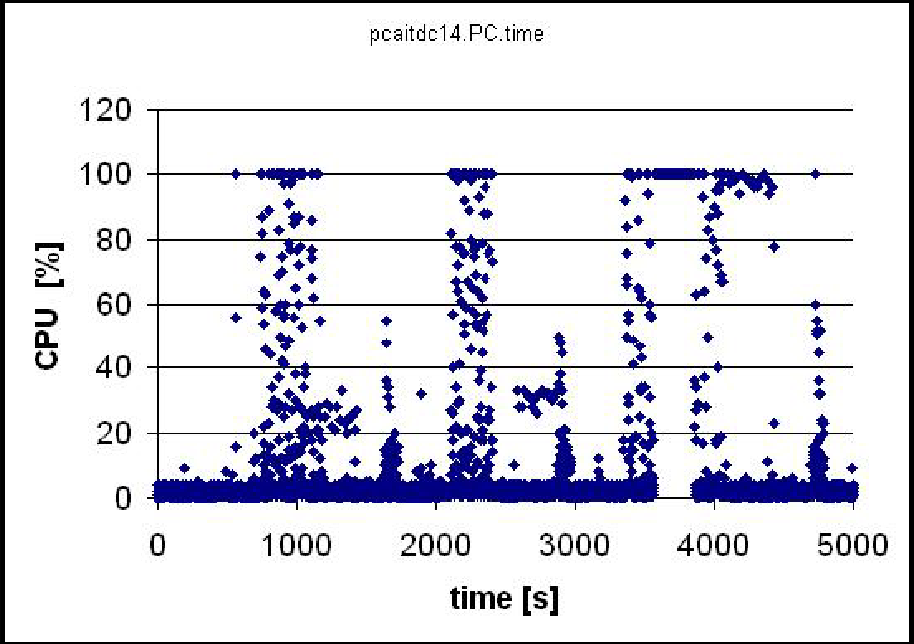
- Security measures are applied at all levels of ALICE DCS computing
- Implemented solution satisfies
  - CERN security rules
  - Collaboration needs
  - Existing infrastructure

backup

Terminal Server Load

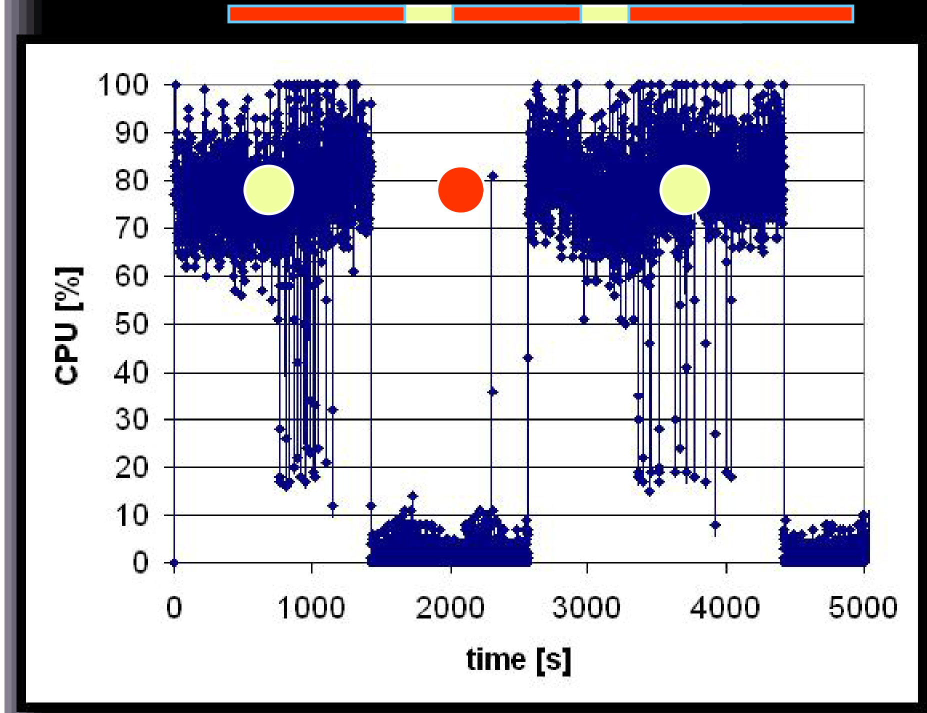
Master project generated 50000 datapoints and updated 3000 /s

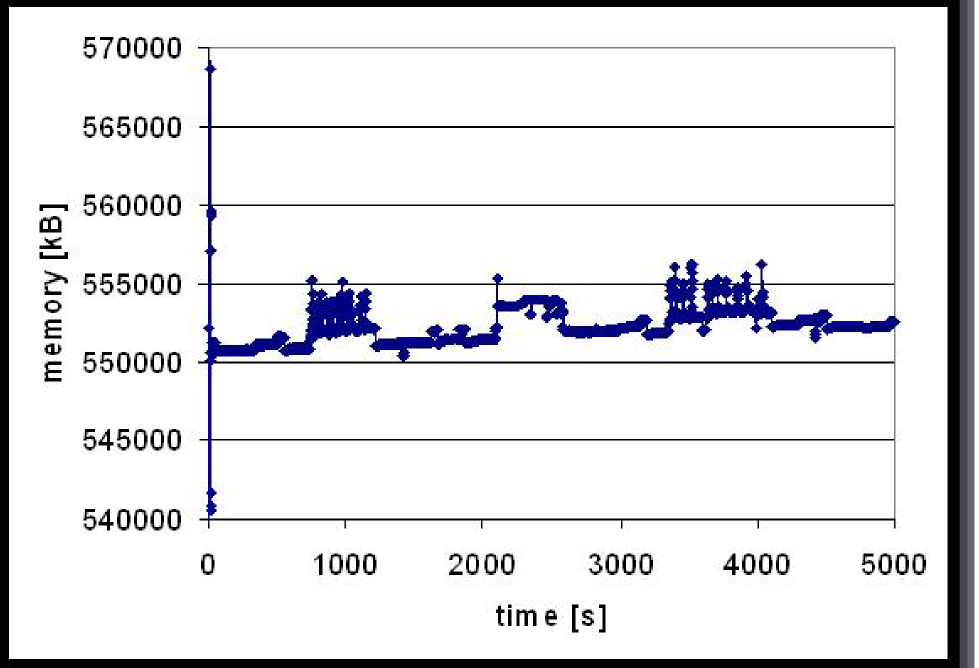




▬	Master project stopped	●	Remote panel displays 50 values
▬	Master project running	●	Remote panel displays 200 values

Load of the workstation running the master project





🟨 Remote client disconected

🟥 Remote client connected

● Master project stopped

○ Master project running

Thin clients for GPN access

- Transtec MYLO clients are used
  - in some areas during the preinstallation (general purpose clients in cavern, etc)
  - Administrator consoles to be trusted from the DCS network

  - Single purpose machines – no unwanted software installed
  - Difficult to infect (OS is in Eprom)

Smartcard Authentication

Smartcards were evaluated in ALICE

- IT infrastructure is in place
- problems with printing CERN artwork on the cards