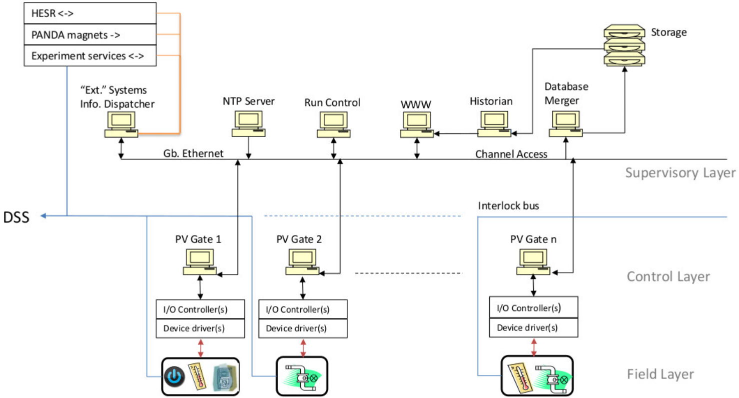
EPICS Channel Access Gateway and Access Security

Florian Feldbauer

Helmholtz-Institut Mainz
Johannes Gutenberg-Universität Mainz

LV. Collaboration Meeting
November 30, 2015

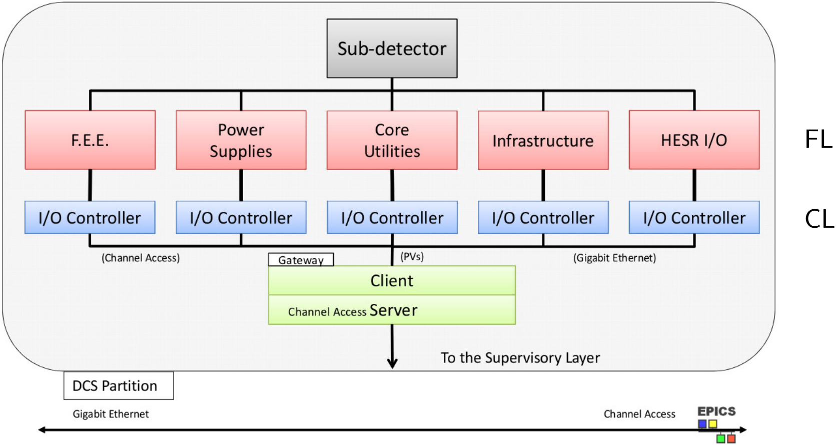
P̄ANDA DCS Overview



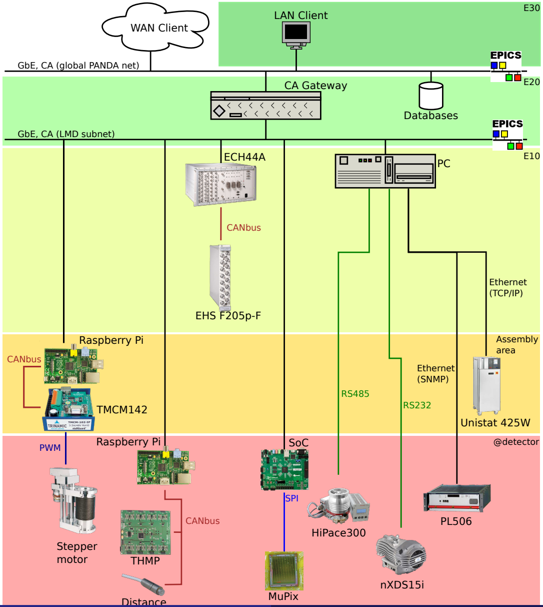
- Each sub-detector has it's own partition
- Separated from each other via CA-Gateways

P̄ANDA DCS Partition

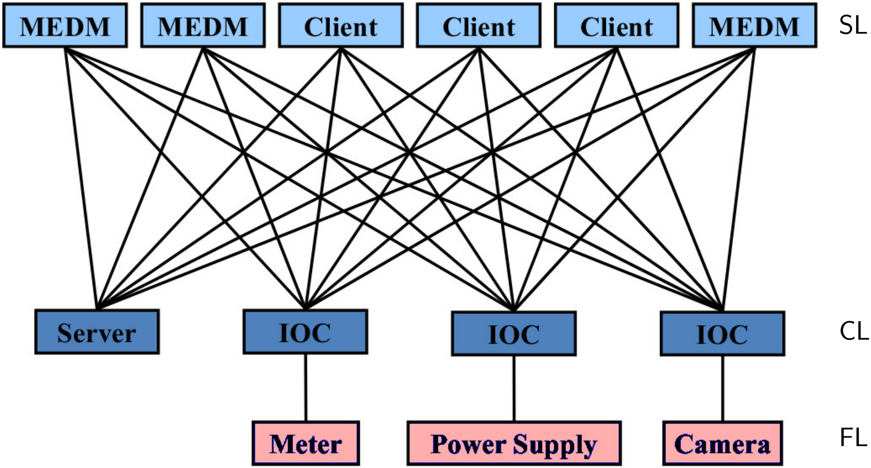
DCS partition for one sub-detector



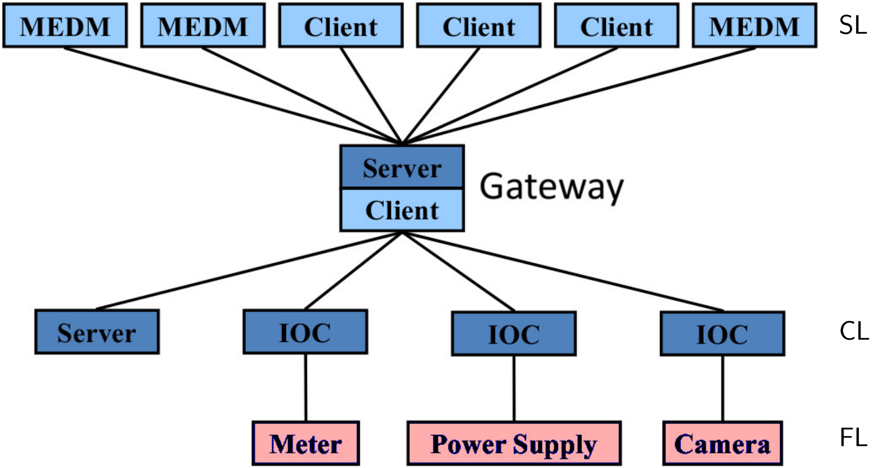
$\overline{\text{P}}$ANDA LMD DCS Partition



EPICS Channel Access



EPICS Channel Access



EPICS Channel Access Gateway

Parts of CA Gateway:

1. CA Access Security
2. PV list
3. Network configuration

CA Access Security

”No attempt has been made to protect against the sophisticated saboteur. Network and physical security methods must be used to limit access to the subnet on which the iocs reside.” [1]

[1] Application Developer’s Guide, c. 8, ”Access Security”, s. 8.3.2, ”Limitations”

CA Access Security - Features

Access security protects IOC databases from unauthorized CA clients, based on

- Who?
  userid of the ca client
- Where?
  Hostid where user is logged on, No attempt to see if user is local or remotely logged on
- What?
  Individual fields of records are protected
- When?
  Access rules can contain input links/calculations

CA Access Security - Definition

ASL Access Security Level

- 0 or 1
- By default all fields are level 1 except VAL, CMD and RES
- Level 1 implies 0

ASG Access Security Group

- Group defining access rights for users/hosts

UAG User Access Group

- List of user names
- User names may appear in more than one UAG

HAG Host Access Group

- List of host names
- Host names may appear in more than one HAG

CA Access Security - Simple Example

PandaLmd.access

```
UAG(uag) {user1,user2}
HAG(hag) {host1,host2}

ASG(DEFAULT) {
  RULE(1,READ)
  RULE(1,WRITE) {
    UAG(uag)
    HAG(hag)
  }
}
```

Provide read access to anyone located anywhere
write access to *user1* and *user2* if located at *host1* or *host2*

PV List

- List of PV names available through gateway
- Combines PVs with access rules
- PV names can be given as pattern

PV List - Simple Example

PandaLmd.pvlist

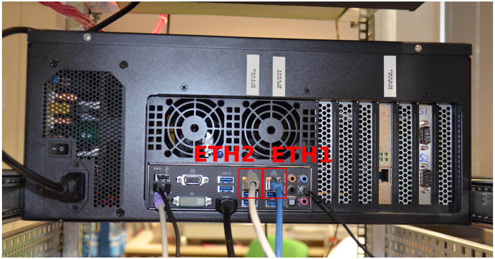
```
## DENY overwrite ALLOW
EVALUATION ORDER ALLOW, DENY

## Allow access by ASG DEFAULT to PVs which
## begin with "PANDA:LMD:"
PANDA:LMD:.*     ALLOW

## Deny access by ASG DEFAULT to PVs which
## begin with "PANDA:LMD:" and end with "__"
PANDA:LMD:.*__   DENY

## Allow access by ASG GatewayAdmin to gateway
## internal PVs
gateway:.*Flag   ALLOW GatewayAdmin
```

Network Configuration



- For CA Gateway PC with two network interfaces is needed
- eth2 connected to local (sub-detector) subnet
- Running local DHCP/DNS server on eth2 (dnsmasq)
- eth1 connected to network of the institue
- If using firewall, ports 5064(udp/tcp), 5065(udp) must be open

Network Configuration

Need to know IP address of eth1, broadcast address of eth2

```
~ > /sbin/ifconfig
[...]
eth1      Link encap:Ethernet  HWaddr 74:d4:35:ec:0c:47
          inet addr:10.32.90.101  Bcast:10.32.90.255  Mask:255.255.255.0
[...]
eth2      Link encap:Ethernet  HWaddr 74:d4:35:ec:0c:45
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
[...]
```

Using the CA Gateway

Starting the CA Gateway

```
˜ > cd /opt/epics/gateway2_0_6_0
˜ > bin/linux-x86_64/gateway          \
      -log /home/panda/cagateway.log  \ # Logfile
      -cip 192.168.1.255              \ # Client IP address
      -sip 10.32.90.101               \ # Server IP address
      -uid 1000 -gid 1000             \ # User id and group
      -server -no_cache               \ # run as daemon
      -home /opt/epics/gateway2_0_6_0 \ # Dir to search for config
      -pvlist PandaLmd.pvlist         \ # File with PV list
      -access PandaLmd.access           # Access Security definition
```

Stopping the daemon

```
˜ > cd /opt/epics/gateway2_0_6_0
˜ > ./gateway.killer
```

BACKUP

Installing the CA Gateway

Dependencies: Epics base 3.14.12 (or newer)

```
~ > wget -q -O - https://launchpad.net/epics-gateway/trunk/2.0.6.0/+
     download/gateway2_0_6_0.tar.gz | tar xzf - -C /opt/epics
~ > cd /opt/epics/gateway2_0_6_0
~ > echo "EPICS_BASE = /opt/epics/base" > configure/RELEASE.local
~ > make -j4
```