UNIVERSITÄT
HEIDELBERG

Slow-Control Progress

Schaltungstechnik
und Simulation

Michael Ritzert

michael.ritzert@ziti.uni-heidelberg.de

6th Belle II PXD/SVD Workshop

Pisa

03.10.2014

Overview

- Software Updates
- Interlock Implementation Details
- Access Control
- Outlook

Software Updates are Coming In

- By the time we start installing in Tsukuba:
  - Scientific Linux will be in major version ≥7
    - SL7 beta 4 is out (16.09.), final release later this year
  - EPICS 3.15 will be the latest stable release
    - First stable 3.15 release expected for December
  - CSS 4 is mainstream
    - All development has moved to 4.x.
    - Now based on recent Eclipse 4.
    - First VXD CSS version 4 build at https://sussrv01.ziti.uni-heidelberg.de/~ritzert/PXD/CSS4
- We want to follow the upgrades to continue to receive bug fixes.
- We have enough time to follow the upgrades.
- None of the updates should require larger changes to our code.

⇒ Give each of the updates time to mature, prepare early test versions of our software before finally switching for good.

Interlocks for Data Verification

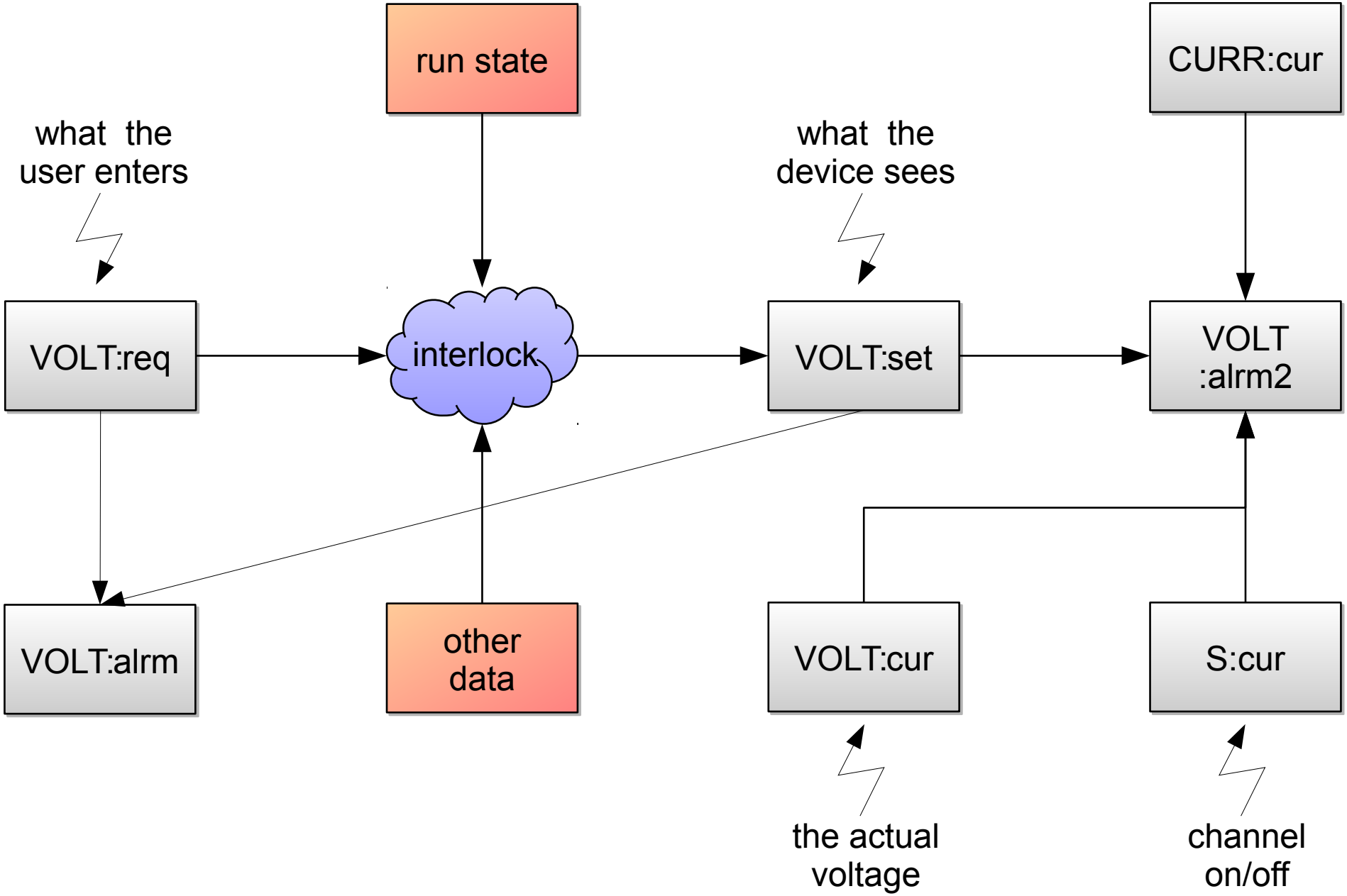
Interlocks protect

- against operator errors.
- from changing environmental conditions.

Typical interlocks for a power supply (voltage):

- Absolute limits for the output voltage.
- Maximum voltage difference to other channel.
  ⇒ The limits may be variable.

Voltage Interlocks



Sample Voltage Interlock EPICS DB

to device

```
record( ao, "$(PV):set" ) {
}
```

from user

```
record( ao, "$(PV):req" ) {
   field( VAL,  "0" )
   field( PINI, "1" )
}

record( calcout, "$(PV):calcset" ) {
   field( INPA, "$(PV):req CPP" )
   field( INPB, "$(PV):high" )
   field( INPC, "$(PV):low" )

   field( DOPT, "Use OCAL" )
   field( OCAL, "A" )
   field( OUT,  "$(PV):set PP" )

   field( OOPT, "When Non-zero" )
   field( CALC, "(A>=C) && (A<=B)" )
}
```

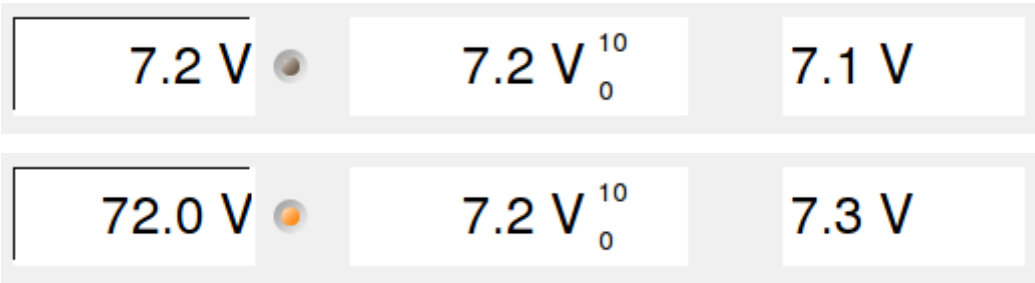
```
record( calcout, "$(PV):calclimit" ) {
   field( INPA, "$(PV):set" )
   field( INPB, "$(PV):high CPP" )
   field( INPC, "$(PV):low CPP" )
   field( DOPT, "Use OCAL" )
   field( OCAL, "MIN(MAX(A,C),B)" )
   field( OUT,  "$(PV):set PP" )
   field( OOPT, "When Non-zero" )
   field( CALC, "(A<C) || (A>B)" )
}

record( calcout, "$(PV):calcalarm" ) {
   field( INPA, "$(PV):req CPP" )
   field( INPB, "$(PV):set CPP" )
   field( CALC, "A!=B" )
   field( DOPT, "Use CALC" )
   field( OUT,  "$(PV):alrm PP" )
}

record( bo, "$(PV):alrm" ) {
}
```

Translated to Pseudo-Verilog Code

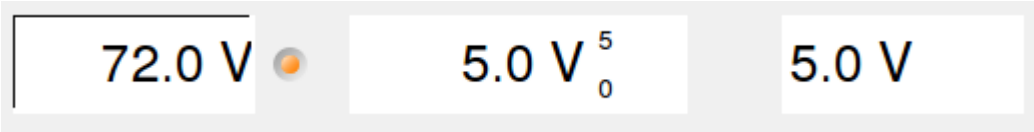
```
always @(req)
   if ((req>=low) && (req<=high))
      set <= req;

always @(high, low)
   if ((set<low) || (set>high))
      set <= min(max(set, low), high);

always @(req, set)
   alrm <= (req != set);
```

Functionality

- When users enter data, it is only activated if `low ≤ req ≤ high`.
  - Everything else is **ignored**. No clamping to the limits.
  - Note: CSS interprets „7.2“ as 7.2 or 72, depending on the locale (decimal point).
    ⇒ plenty of potential for accidents
    ⇒ using text inputs should be discouraged



- When the `low`, `high` limits change, the set voltage is clamped to the new limits.



- In addition, the alarm system monitors current voltage – set voltage.

Hardware Protection Interlocks

- Complement pure hardware interlocks (cf. Livio's talk).
- Power-off on unsafe conditions.
- Inputs:
  - Run State
  - **Environment Conditions** (esp. from FOS)
- Output:
  - enable signal for power supplies
  - slow abort signal for SuperKEKB
- Implementation purely inside EPICS DBs

Heartbeats

- It has to be ensured that the communication between IOCs is permanently alive.
  - Trigger the interlock, when the input data is not accessible.
  - Also trigger, when the interlock signal is no longer received by the device driver.
- The connection timeout is 30 seconds, too long for interlock purposes.
  ⇒ A faster algorithm is required
  ⇒ Heartbeat signals
- The sender sends a 0/1 oscillation with 1 s period
- The receiver samples with 0.5 s period.
  In the receiver, the link is assumed lost, when the same value (0 or 1) is received x times in a row ($x \geq 3$).
  ⇒ Handled in the same way as if the input goes to bad values / the interlock signals an abort.

Sample EPICS DB to Send/Receive Heartbeats

```
# Sender
record(calc, "$(IOC):heartbeat") {
   field(SCAN, ".5 second")
   field(CALC, "a=0?1:0")
   field(INPA, "$(user):heartbeat NPP
   NMS")
}

# Check for 0 value in heartbeat, if not
   detected increment by 1
record(calc, "$(IOC):hb_0s") {
   field(DESC, "Counter of 0 states" )
   field(SCAN, ".5 second")
   field(CALC, "a=0?0:b+1")
   field(INPA, "$(IOC):heartbeat NPP NMS")
   field(INPB, "$(IOC):hb_0s NPP NMS")
}

# same for 1...
record(calc, "$(IOC):hb_1s") {}
```

```
# Calculates if heartbeat is present
record(calc, "$(IOC):hb_calc") {
   field(SCAN, "1 second")
   field(CALC, "((a<g)&(b<g))?1:0")
   field(FLNK, "$(IOC):hb_check PP NMS")
   field(INPA, "$(IOC):hb_0s NPP NMS")
   field(INPB, "$(IOC):hb_1s NPP NMS")
   field(INPG, "$(IOC):dead_hb_tolr NPP
   NMS")
}
```

=3

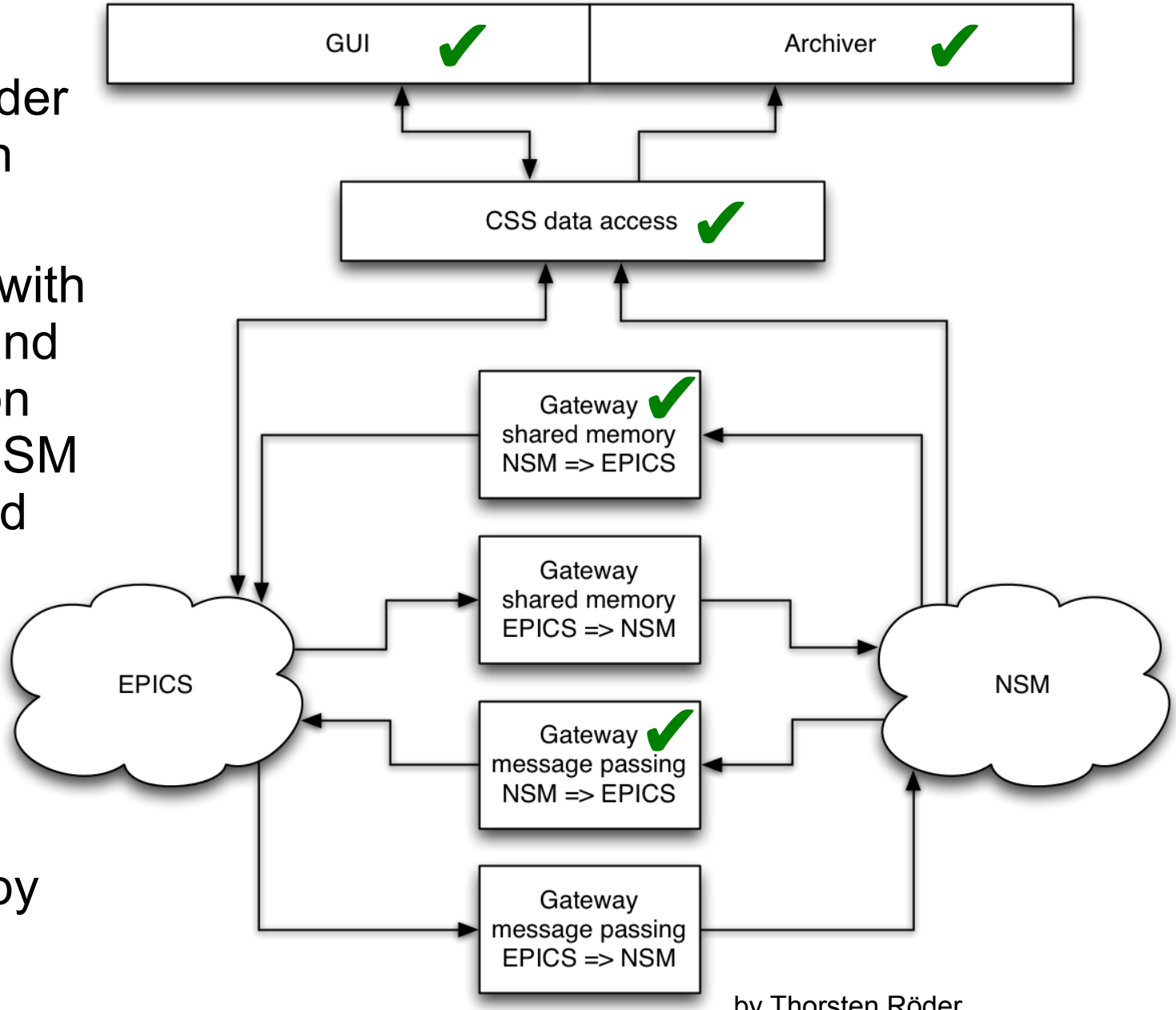
```
record(bi, "$(IOC):hb_check") {
   field(SCAN, "Passive")
   field(PINI, "1")
   field(INP , "$(IOC):hb_calc")
   field(ZNAM, "Dead" )
   field(ONAM, "Live" )
   field(ZSV,  "MAJOR")
   field(OSV,  "NO_ALARM")
}
```

Access Control

- Goals:
  - Establishing several different user levels:
    readonly, shifter, admin, etc.
  - Protection against operator errors (writing to wrong PV)
- EPICS provides:
  - CA Gateway: Filtering by hostname / PV name.
    Can restrict internal PVs to the EPICS network, hide from the control room network.
  - In the IOC: Access control by hostname / user name / PV name.
    The full set of restrictions can be implemented here.

Integration with NSM

- Visit to KEK by Thorsten Röder and myself in September.
- Intensive work with Nakao-san and Konno-san on integrating NSM into CSS, and interfacing between NSM and EPICS.
- To be finished by November.



by Thorsten Röder

Milestones Ahead

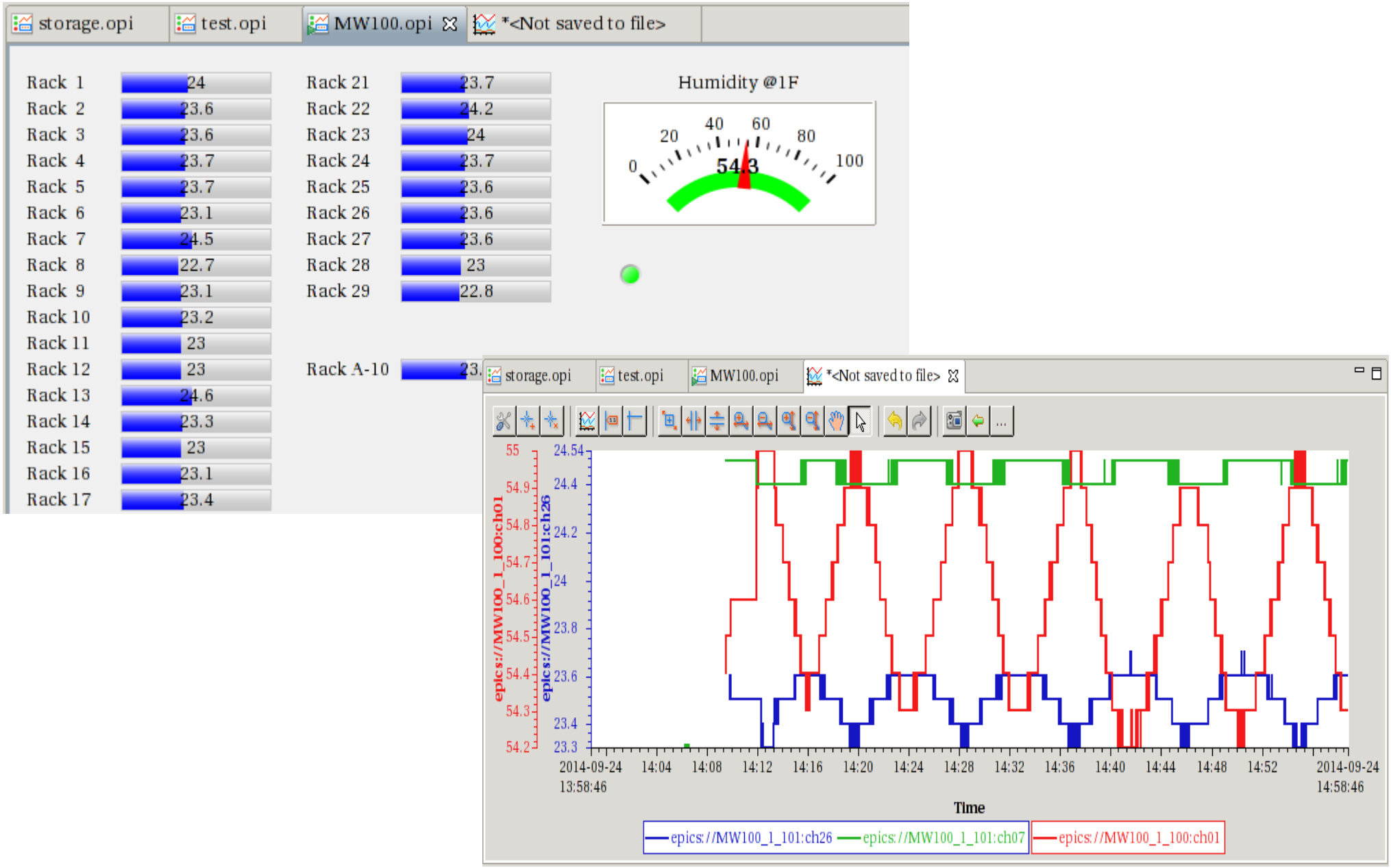
- **Autumn 2015 T**estbeam @ DESY!
  - PXD + SVD + (Pocket-)DAQ, full electronics + SC
- **Autumn 2015** IBBelle commissioning @ MPI
  - Have the UNICOS port ready.
- **2016** Assemble PXD @ MPI
- **Summer 2016 Full PXD SC**
- **late 2016** Start of BEAST phase II operation
  - Before, make the SC servers available, install them and the software, verify.
- **02/2017** PXD @ KEK
- **Autumn 2017** Start of Physics run
  - VXD Installation into Belle II during summer
  - SC should be ready…

Open Major Tasks

- UNICOS
  - PLC-based control system used at CERN. To be ported from WinCC OA (PVSS) to EPICS. Used for IBBelle CO_2 cooling.
  - integration of PLC and CSS alarms
- OPI Guidelines + Implementation
  - consistent look-and-feel of all GUIs
- Configuration Management
  - pre-requisite for any advanced use cases
  - test version of a database exists
- Startup Sequence
  - simplifies the operators' lives a lot
- Run-/PS-Control
  - important for any operation with other subdetectors (VXD @ DESY)
- Integration of env. sensors
  - FOS IOC update for new readout device
  - readout + integration in the interlock logic
- Alarm / Interlock System

Thank you!

MW100 @ E-Hut Integrated into EPICS



What is an Alarm?

Naïve approach:
If what comes out is not what I commanded, that's a problem.
=> This is what would happen:

Power Supply

Set Voltage	Current Voltage	
1.8V	1.8V	all well
1.8V	2.0V	wrong voltage
1.8V	1.5V	wrong voltage
1.8V	0V	wrong voltage

Very simple to implement: Set != Current (±ε) => Alarm.
But this doesn't always highlight the cause of the problems.

What is an Alarm?

Power Supply

Channel	Set Voltage	Set Current	Current Voltage	Current Current	
on	1.8V	100mA	1.8V	10mA	all well
on	1.8V	100mA	2.0V	10mA	wrong voltage
on	1.8V	100mA	1.5V	10mA	wrong voltage
on	1.8V	100mA	1.5V	100mA	wrong current
off	1.8V	100mA	0V	0mA	all well

=> even in this simple case, the condition is complex:
The voltage is in error,

- if it is lower than the set voltage, but not
  - if the PS is switched off, or
  - if the PS is in the current-limit mode.
- or if it is higher than the set voltage.

=> important: what is **expected** to happen? In current-limit mode, the voltage is expected to drop. The problem is only in the current. (Overvoltage is propably an interlock condition due to possible damage)