On the use of NI PXI platform for High reliability and availability systems:
LHC Collimators low level control a study case

Dr. A. Masi
CERN, Switzerland
EN Dept, STI group
alessandro.masi@cern.ch

BIG PHYSICS Symposium, Austin 2011
Control, Diagnostic and Measurement for Physics Systems and Experiments
Outline

• The LHC collimation system
• Reliability and Availability Requirements
• The control architecture
• Reliability and availability review
• Lessons learnt by the 2010 operation
• Are NI PXI systems suitable candidates for high reliability and availability control systems ???
• Conclusions
The LHC collimation system must carry out 2 main functions:

1. Beam cleaning, i.e. removing stray particles which may induce quenches in SC components. 2 out of 100k particles enough to trigger quench ...

Several types of collimators at multiple locations are required to ensure efficient beam cleaning ...

Very complex system (100+ LHC Collimators)

Total of 108 collimators (100 movable).

Two jaws (4 motors) per collimator!
The collimation system must carry out **2 main functions**:

2. **Machine Protection**, i.e., shielding the other machine components from the catastrophic consequences of beam orbit errors.

LHC beam parameters:

- Stored energy 350 MJ per beam (factor 100 higher than others)
- Beam transverse density ~1 GJ/mm² (factor 1000 higher than others)
- This makes the LHC beam highly destructive

Robustness Test at 450 GeV 3.2x10^{13} protons

Collimator jaws after impact ... no signs of mechanical damage

5 full intensity shots ranging from 1 to 5 mm, 7.2ms ...
Each impact energy equivalent to more than ½ kg of TNT

---

**Carbon/carbon jaw**

**Graphite jaw**
A collimator has two parallel jaws
Each jaw is controllable in position and angle

The jaws positioning accuracy is function of the beam size (1/10 beam size). At top energy 20 um accuracy is required.
**The Motorization Solution**

**Collimator Axes Motor type:** Stepping Motors Controlled in open loop (4 for the jaws` axes + 1 for the vertical axis)

**Steps Loss Detection:** Resolvers (4 for the jaws` axes)

**Positions Survey:** LVDT sensors in redundant number (5 for the axes absolute position and 2 for the jaws` gap)

---

**Road Map**

- The LHC collimation system
- The control architecture
- R&A review
- Lesson learnt by 2010 operation
- NI PXI platforms suitable for high R&A systems
- Conclusions

---

A. Masi,

PXI Platforms for High Reliability and Availability Systems, Big Physics Symposium Austin 2011
### Control system parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axes to control</td>
<td>555</td>
</tr>
<tr>
<td>Positioning sensors to monitor in RT</td>
<td>750</td>
</tr>
<tr>
<td>Resolvers to read synchronously with the motors` steps</td>
<td>400</td>
</tr>
<tr>
<td>Limit switches to acquire</td>
<td>1200</td>
</tr>
</tbody>
</table>

### Control system requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axes positioning accuracy</td>
<td>few μm</td>
</tr>
<tr>
<td>Axes motion synchronization</td>
<td>below 1 ms</td>
</tr>
<tr>
<td>Response delay to a digital start trigger</td>
<td>100 μs</td>
</tr>
<tr>
<td>Position sensors RT survey frequency</td>
<td>100 Hz</td>
</tr>
<tr>
<td>Reliability</td>
<td>Very high</td>
</tr>
</tbody>
</table>
System reliability is “an attribute of any system that consistently produces the same results, preferably meeting or exceeding its specifications.”

Goal: No failure on the control system can put in danger the LHC operation safety. Failures in the collimation system have to be detected and eventually the LHC beam dumped.

Availability:

Accelerator is available (called a mission) for nine months per year 24/7. Short technical stops (5 days) are scheduled in average every 2 months.

Goal:

• Reduce the number of failures in operation and the consequent LHC downtime
• Possibility to mask a failure till the next scheduled technical stop and/or fix it by remote avoiding access to the LHC tunnel
The new Front-End Software Architecture (FESA) is a comprehensive framework for designing, coding and maintaining LynxOS/Linux equipment-software that provides a stable functional abstraction of accelerator devices.

See details at: http://project-fesa.web.cern.ch/project-fesa

network support TCP/IP

(See details at http://dim.web.cern.ch/dim/)

The DIM Server library was successfully compiled for Pharlap

The LHC collimation system

The control architecture

R&A review

Lesson learnt by 2010 operation

NI PXI platforms suitable for high R&A systems

Conclusions
A. Masi,
PXI Platforms for High Reliability and Availability Systems, Big Physics Symposium Austin 2011

The control system synchronization solution

Road Map

- The LHC collimation system
- The control architecture
- R&A review
- Lesson learnt by 2010 operation
- NI PXI platforms suitable for high R&A systems
- Conclusions

Central Control Applications

CMW Infrastructure
CORBA, RDA, JMS
FESA Gateway Linux
DIM CLIENT + Low Level FESA Class

Timing Network

MDC
PRS

Device/Property Model
Topic Model

- The LHC collimation system
- The control architecture
- R&A review
- Lesson learnt by 2010 operation
- NI PXI platforms suitable for high R&A systems
- Conclusions
Redundancy at sensors level:

- Position sensors: 1 LVDT per collimator axis (4) + 2 redundant to measure the collimator gap to easily detect failures
- Stepping motors used in open loop + resolvers used in addition to detect steps lost

Redundancy at system level:

- MDC and PRS: Critical task of positioning and position verification are split on two separated PXI systems
- Position axes monitoring with Energy Limits (network synchronized) and position limits (timing synchronized)

The LHC collimation system

The control architecture

R&A review

Lesson learnt by 2010 operation

NI PXI platforms suitable for high R&A systems

Conclusions
Reliability Review

- Software implementation fail safe:
  
  Dual core processor to:
  - reduce the work load
  - separate the critical tasks from the network communications
  - implement reciprocal watchdog timers

  ✓ Watchdog timers on CPU and FPGA to detect stuck conditions

  ✓ Check of the Compact RIO module working status in the FPGA

  ✓ Watchdog timers to verify Energy limits communication over the network

Road Map

- The LHC collimation system
- The control architecture
- R&A review
- Lesson learnt by 2010 operation
- NI PXI platforms suitable for high R&A systems
- Conclusions
• Improvements on the NI PXI Systems:

  • FTP Socket (RCP)
  • RT platforms diskless with network boot
  • Solid State Drive (SDD) as boot backup
  • PXI diagnostic data monitored (CPU and chassis T, memory usage, CPU load)
  • Remote reset based on safety PLC using the power supply control connector
  • KVM switches to redirect the Keyboard, Video and Mouse over the network

The Linux PXE server ensures the software images coherence on the 106 PXI systems !!!!
The low level control software has been designed to be fully configurable. Proper tools have been developed to make easier the management, the maintenance and the diagnostic of the system:

- The software configuration is performed via a proper Configuration tool fetching the parameters by a Collimators Software Configuration Database
- The coherence of the software images is ensured by a PXE booting system

<table>
<thead>
<tr>
<th>Control system size</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Collimators</td>
<td>108</td>
</tr>
<tr>
<td>MDC</td>
<td>60</td>
</tr>
<tr>
<td>PRS</td>
<td>60</td>
</tr>
<tr>
<td>Gateways</td>
<td>8</td>
</tr>
</tbody>
</table>
Redundancy:

A sensor failure can be easily and quickly bypassed remotely to reduce the downtime to few minutes. The problem will be fixed at the next scheduled technical stop.

Power Supply Redundancy:

All the power supplies of the custom electronics have been designed redundant to make totally transparent to the operation a power supply failure.

The LHC collimation system

The control architecture

R&A review

Lesson learnt by 2010 operation

NI PXI platforms suitable for high R&A systems

Conclusions
• No failure has put in danger the machine safety
• The system availability in 2010 has been of 99.54% (37.55 h/8184 operation hours)
• Many failures registered in 2010 have been definitively fixed
According to the failure data accumulated so far:

- Only 1 FPGA card failed so far.
- The weak part has shown to be the PXI chassis power supply. The MTBF evaluated on 2010 operation time gives 178716 h (20.4 years) comparable with the data provided by NI this means roughly a failure every 2 months and half.

A. Masi,
PXI Platforms for High Reliability and Availability Systems, Big Physics Symposium Austin 2011
Definitively YES but with the following recipe:

- Recommended use of parallel architecture: Multiprocessors and basically FPGA to split the execution of critical tasks on different levels and units.

- Systems diskless with network booting.

- AMT features (remote reboot via network, KVM features, remote bios upload).

- On-line monitoring and verification of the systems critical parameters (CPU and chassis T, CPU load, memory usage).

- High Availability PXI chassis.
Can the 8 Slot PXI 1042 Chassis be considered High Availability ?????

• According to the requirements of the LHC

<table>
<thead>
<tr>
<th>SIL</th>
<th>Low demand mode of operation</th>
<th>High demand or continuous mode of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$10^{-2} &lt; \text{PFD} &lt; 10^{-1}$</td>
<td>$10^{-6} &lt; \text{PFH} &lt; 10^{-5}$ MTBF~23 years</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-3} &lt; \text{PFD} &lt; 10^{-2}$</td>
<td>$10^{-7} &lt; \text{PFH} &lt; 10^{-6}$ MTBF~230 years</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-4} &lt; \text{PFD} &lt; 10^{-3}$</td>
<td>$10^{-8} &lt; \text{PFH} &lt; 10^{-7}$</td>
</tr>
<tr>
<td>4</td>
<td>$10^{-5} &lt; \text{PFD} &lt; 10^{-4}$</td>
<td>$10^{-9} &lt; \text{PFH} &lt; 10^{-8}$</td>
</tr>
</tbody>
</table>

• According to the standard IEC 61508 on the Safety Integrity Levels in continuous mode of operation the PXI 1042 is a SIL 1. For High R&A systems chassis SIL 3 or better 4 is recommended

A. Masi,
PXI Platforms for High Reliability and Availability Systems, Big Physics Symposium Austin 2011
Has NI available PXI chassis High Availability as standard product?

At my knowledge so far NO for the PXI bus but…

A custom development is in progress for the LHC Collimators project

- Redundant power supply hot swappabel
- Redundant Cooling system
- Compact sizes
- Remote reset and monitoring of chassis parameters (T, airflows) via an independent network port

A. Masi, PXI Platforms for High Reliability and Availability Systems, Big Physics Symposium Austin 2011
The LHC Collimators low level control system is characterized by tight requirements in terms of Reliability and Availability

The low level RT platforms chosen are the PXI systems Intel Dual core from NI

Particular design choices are implemented at the architecture level to improve the system reliability as well as technical enhancements of the PXI platforms have been applied

Proper tools have been developed to make easier the maintenance and the management of this challenging control system

The new PXI chassis High Availability will contribute to further improve the system availability
We are indebted to NI for the precious support received. In particular the System Engineering Group (Doug, Brent and Christian) and all the R&D people that were involved in this project as well as the Big Physics team (Stefano, Murali, Joel, Christian).

Last but not least Chris, Matthew and Giuseppe

Eric Brauel and his team for the current work on the High Availability PXI Chassis
Thank you very much for your attention.