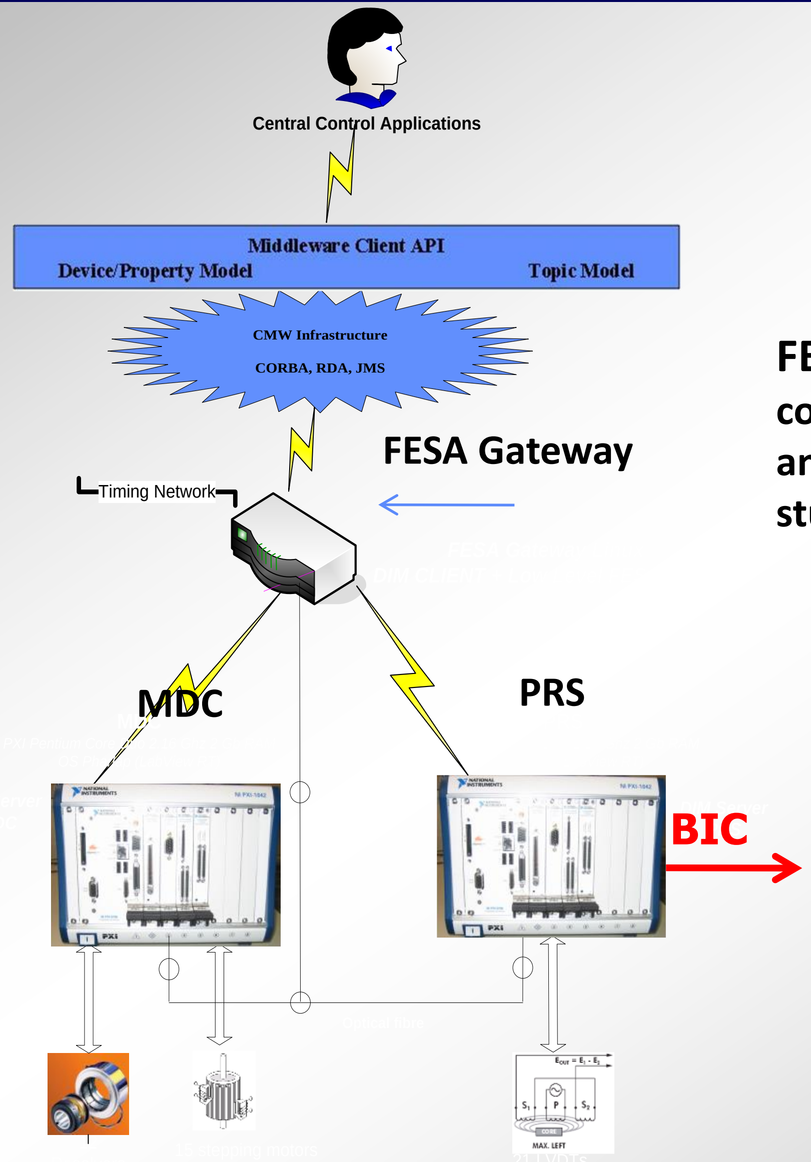
SEU Risk Analysis of the LHC Collimators low level control rack in UJ14,UJ16,UJ56

A. Masi

Contents

1. The LHC Collimator Low level Control system control architecture
2. The electronics location
3. SEU effects and probability according to the CNRAD results
4. SEU effects: Risks Analysis
5. How SEU can be detected
6. Improvements of the control system reliability against SEU
7. Conclusions

1–The LHC Collimator Low level Control system control architecture



Collimators Control System Architecture

FESA server constantly monitors the communication with the low level systems and receives errors if CPU and FPGA are stuck

MDC is responsible for the motors drive and control.

✓*Control is open loop.*
✓*Resolvers are used to detect steps lost.*
✓*The jaw movement is blocked if the difference resolver/controller exceed 50 um*

PRS is responsible for the positioning Readout and Survey

Only the PRS is connected to the BIC system

1st remark:

Only the PRS is part of machine protection. Failure of the MDC does not compromise machine safety, and operation can generally continue without interruption if the collimators do not need to be moved.

- We have experience of failures of the motor drivers in stable beams
  - *TCP.D6L7.B1*
    - *Event Timestamp: 26/08/11 06:30:10.776 Fill Number: 2056 ,*
    - *Event Timestamp: 19/09/11 23:59:01.024 Fill Number: 2127 ,*
    - *Event Timestamp: 20/09/11 01:22:17.718 Fill Number: 2127*):

-The jaws retract because of the auto-retraction system (MDC cannot stop the jaws !!!!!!)

- The PRS must dump the beam if the position limit thresholds are violated (i.e. The ones function of the time and/or of the energy and/or of the ß*)

The failures analysis is focussed only on the PRS system

1–The LHC Collimator Low level Control system control architecture

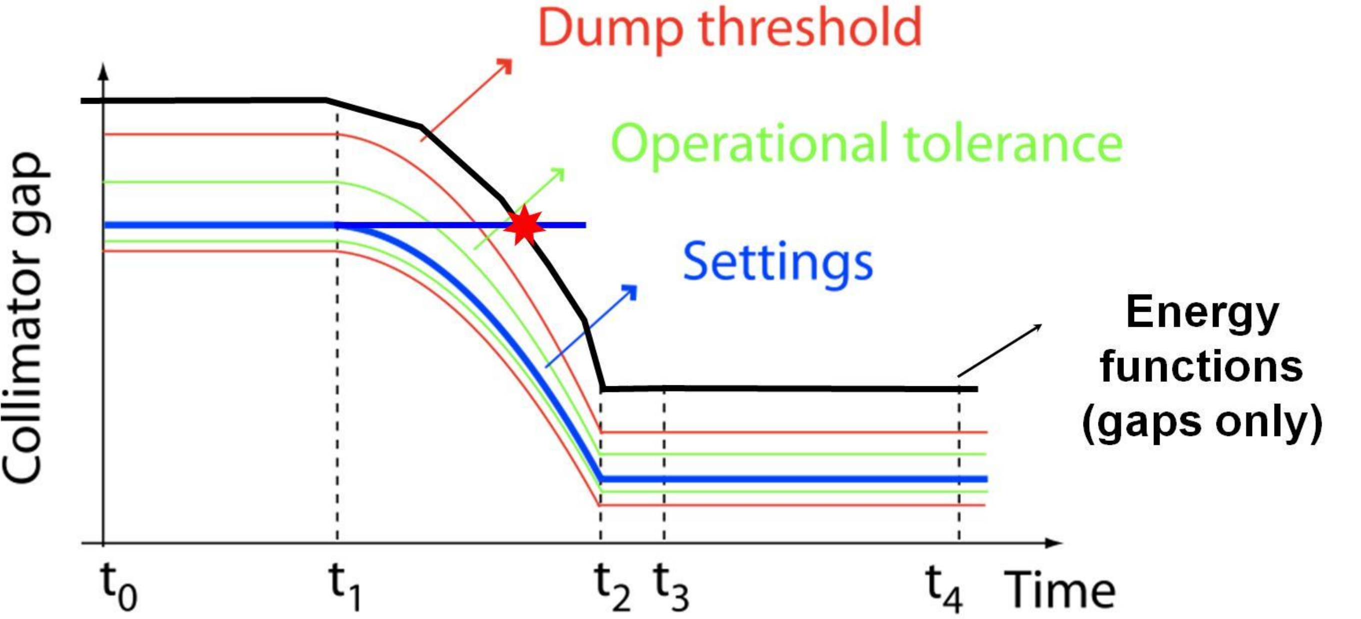
2st remark:

The LHC Collimator control system is an “alive” system. Every year improvements and new functionalities are applied on the base of the experience of the previous year operation.

Engineering specifications are not updated anymore

We have started a complete review of the engineering specifications of the low level control system “as built”. This should help to well classify anomalous behaviours and dissipate unjustified worries

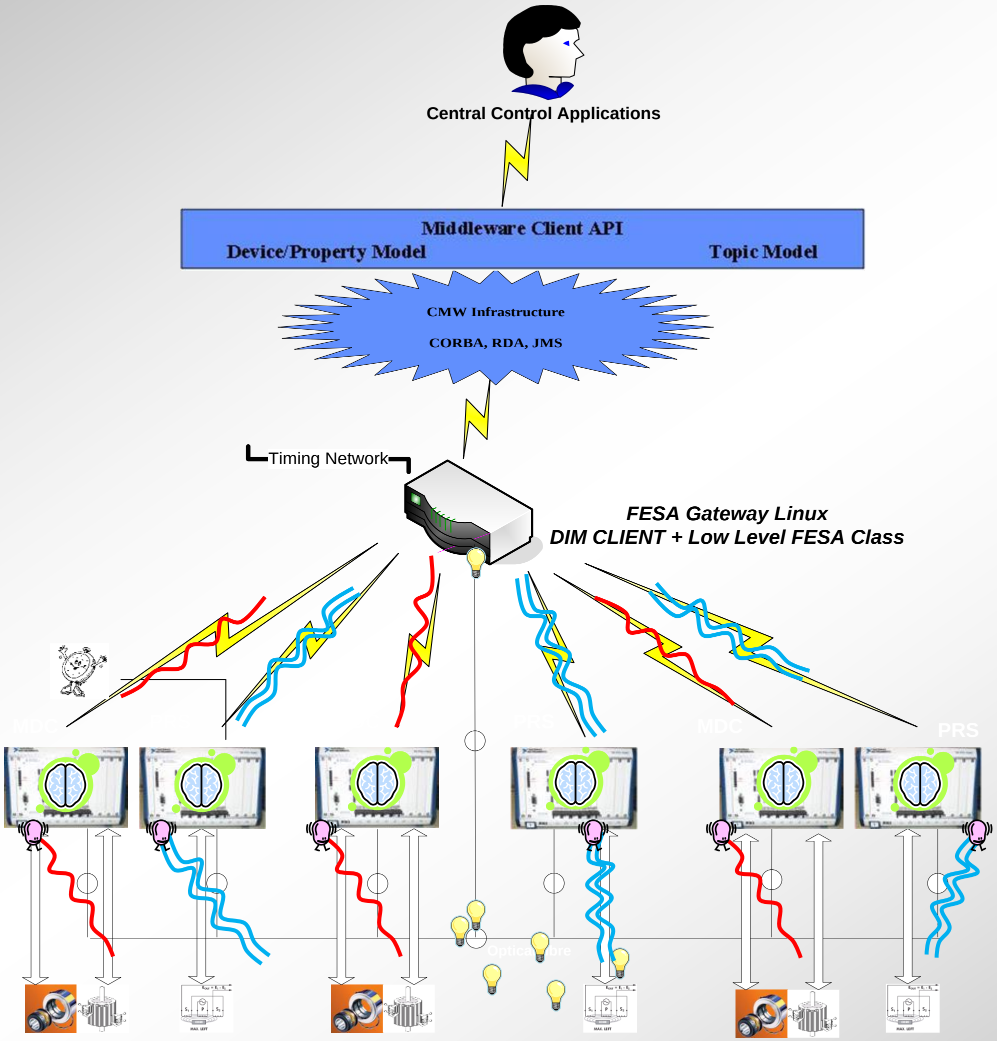
PRS: the protection features for the machine



© S. Redaelli

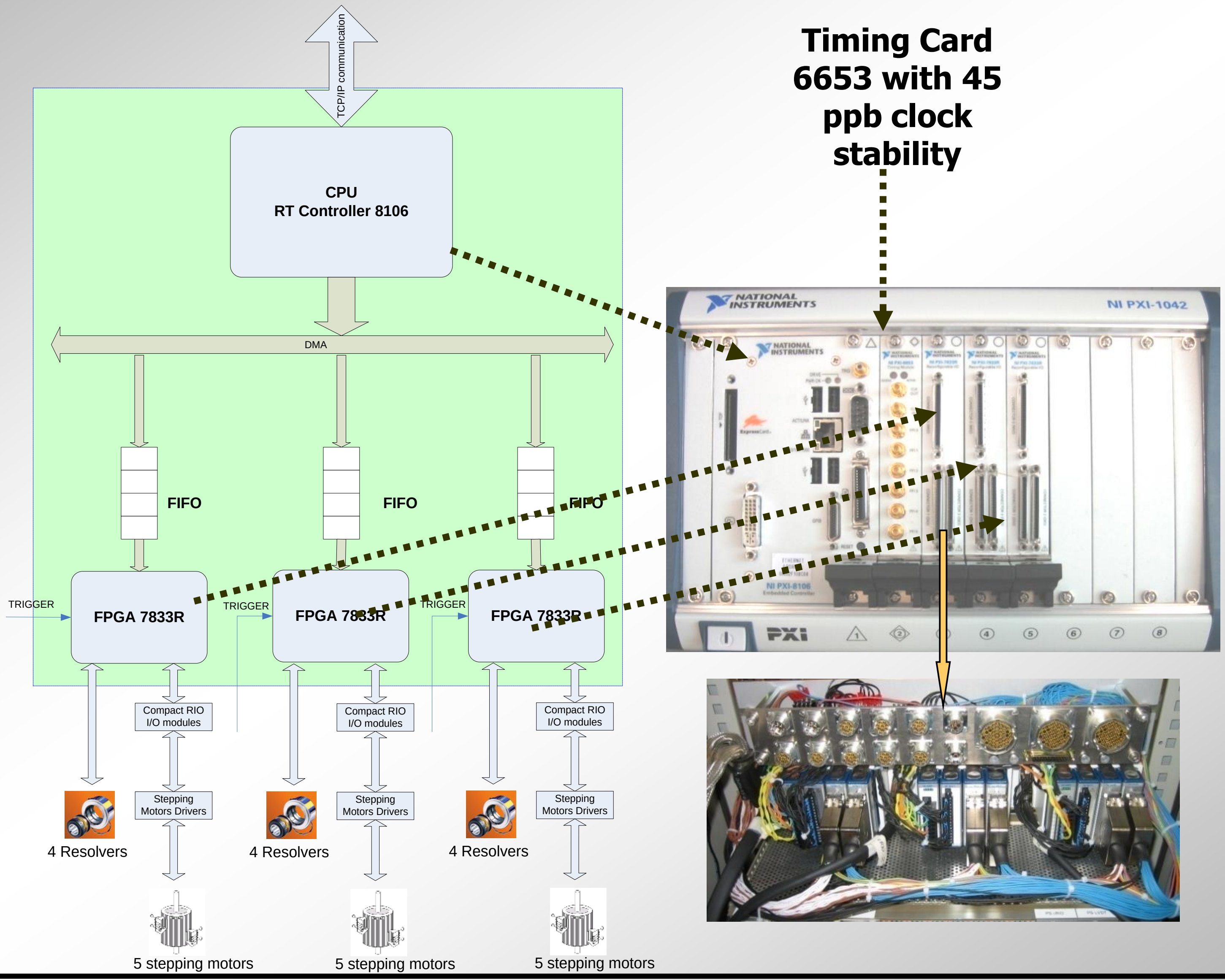
- ☑ Two regimes: discrete (“actual”) and time-functions *(100 Hz survey frequency)*
- ☑ **Inner** and **outer thresholds** as a function of **time** for each motor **axis** and **gap** (24 per collimator). Triggered by timing event (e.g. start of ramp).
- ☑ “Double protection” → BIC loop broken AND jaw stopped
- ☑ Redundancy: **maximum allowed gap versus energy** (2 per collimator). Interpolation performed on the FESA gateway and on fly values sent via network
- ☑ Redundancy: **beta-squeeze factor** for TCT interlocking. Interpolation performed on the FESA gateway and on fly gap values sent via network

1–The LHC Collimator Low level Control system control architecture



1-The LHC Collimator Low level Control system control architecture

MDC control architecture



TCP/IP communication

CPU
RT Controller 8106

DMA

FIFO

FIFO

FIFO

TRIGGER

FPGA 7833R

TRIGGER

FPGA 7833R

TRIGGER

FPGA 7833R

Compact RIO I/O modules

Compact RIO I/O modules

Compact RIO I/O modules

Stepping Motors Drivers

Stepping Motors Drivers

Stepping Motors Drivers

4 Resolvers

4 Resolvers

4 Resolvers

5 stepping motors

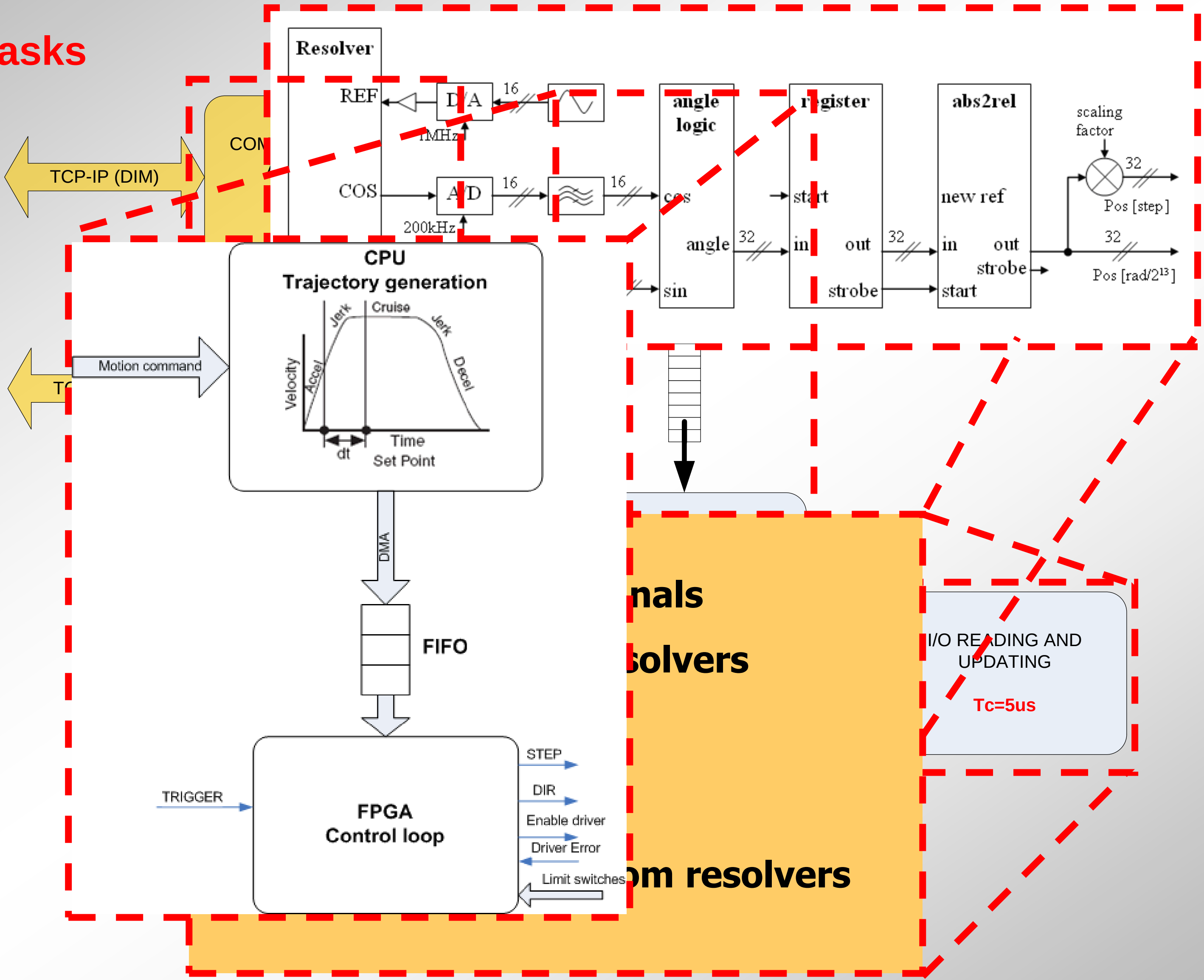
5 stepping motors

5 stepping motors

Timing Card 6653 with 45 ppb clock stability

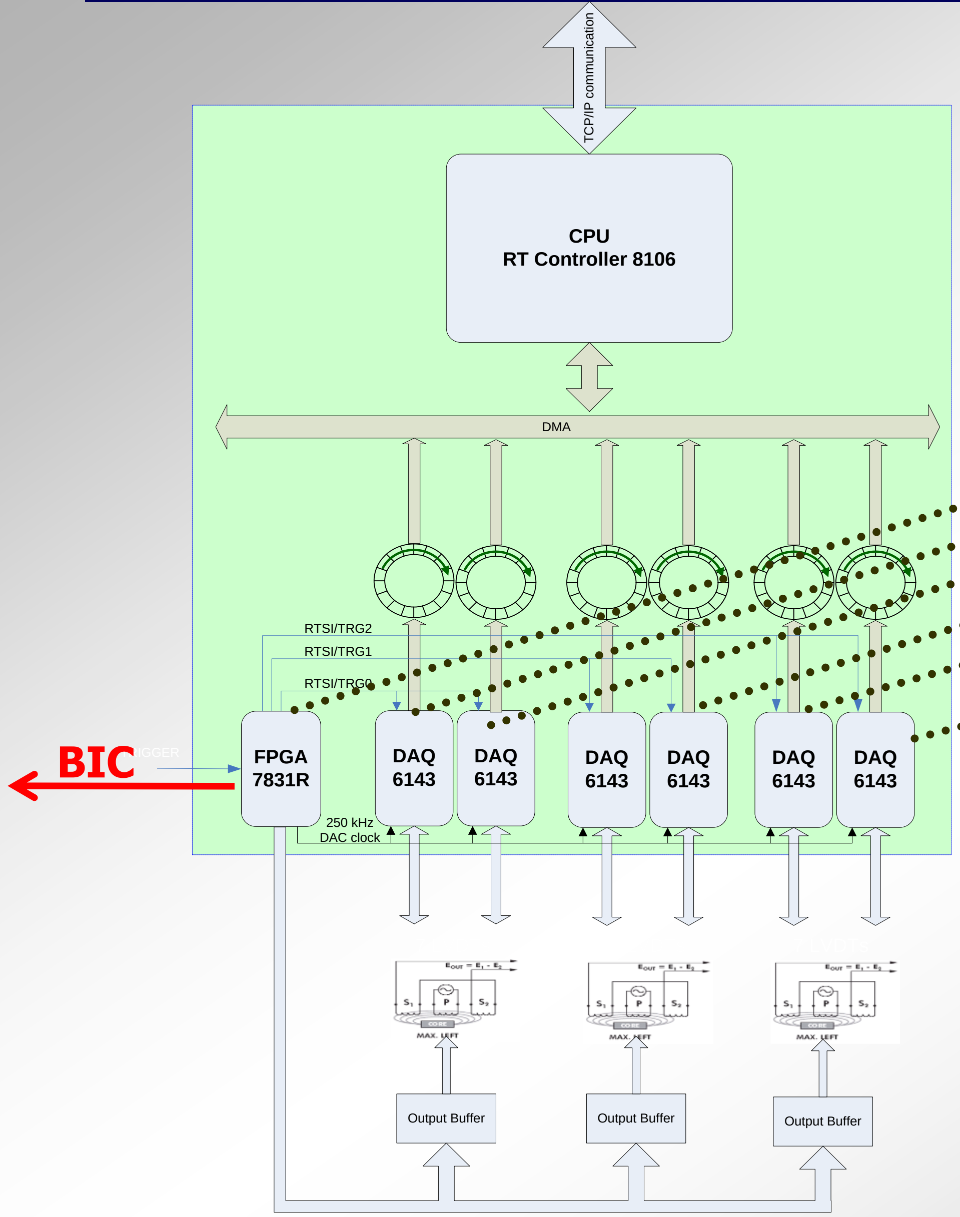
1-The LHC Collimator Low level Control system control architecture

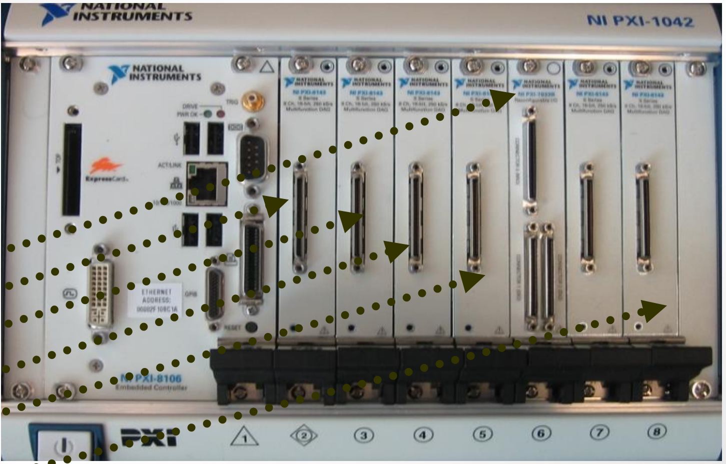
MDC RT tasks



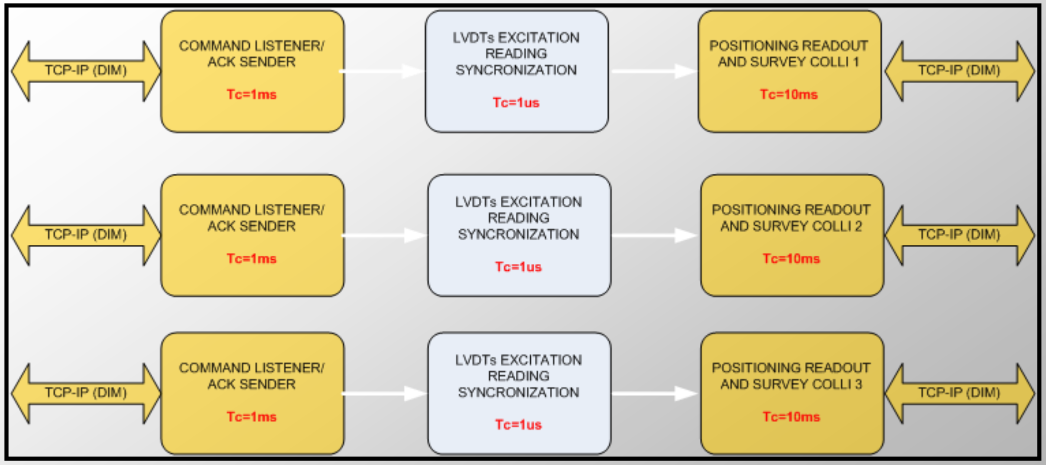
1–The LHC Collimator Low level Control system control architecture

PRS control architecture

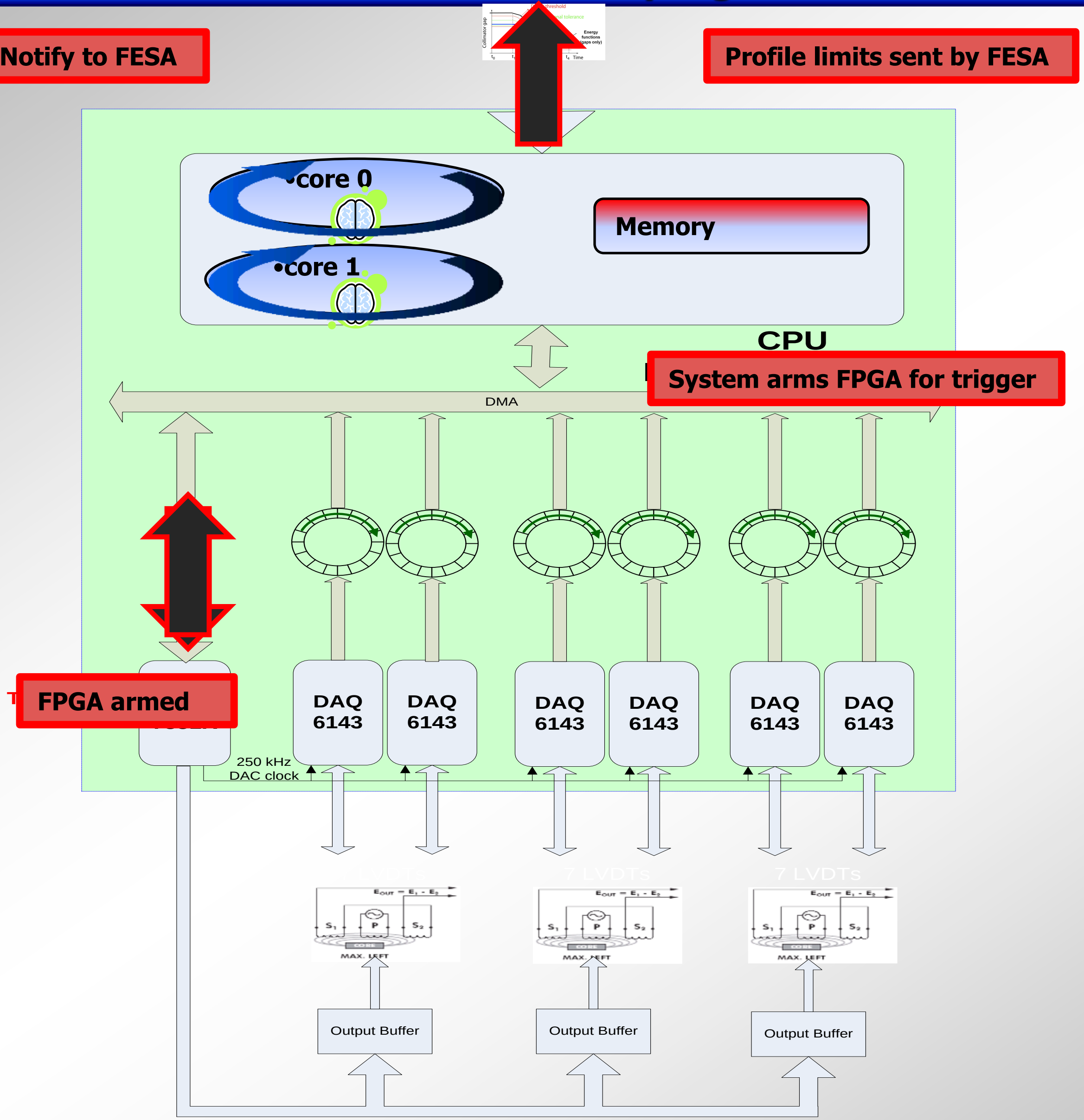




Software Tasks architecture



PRS limit survey logic



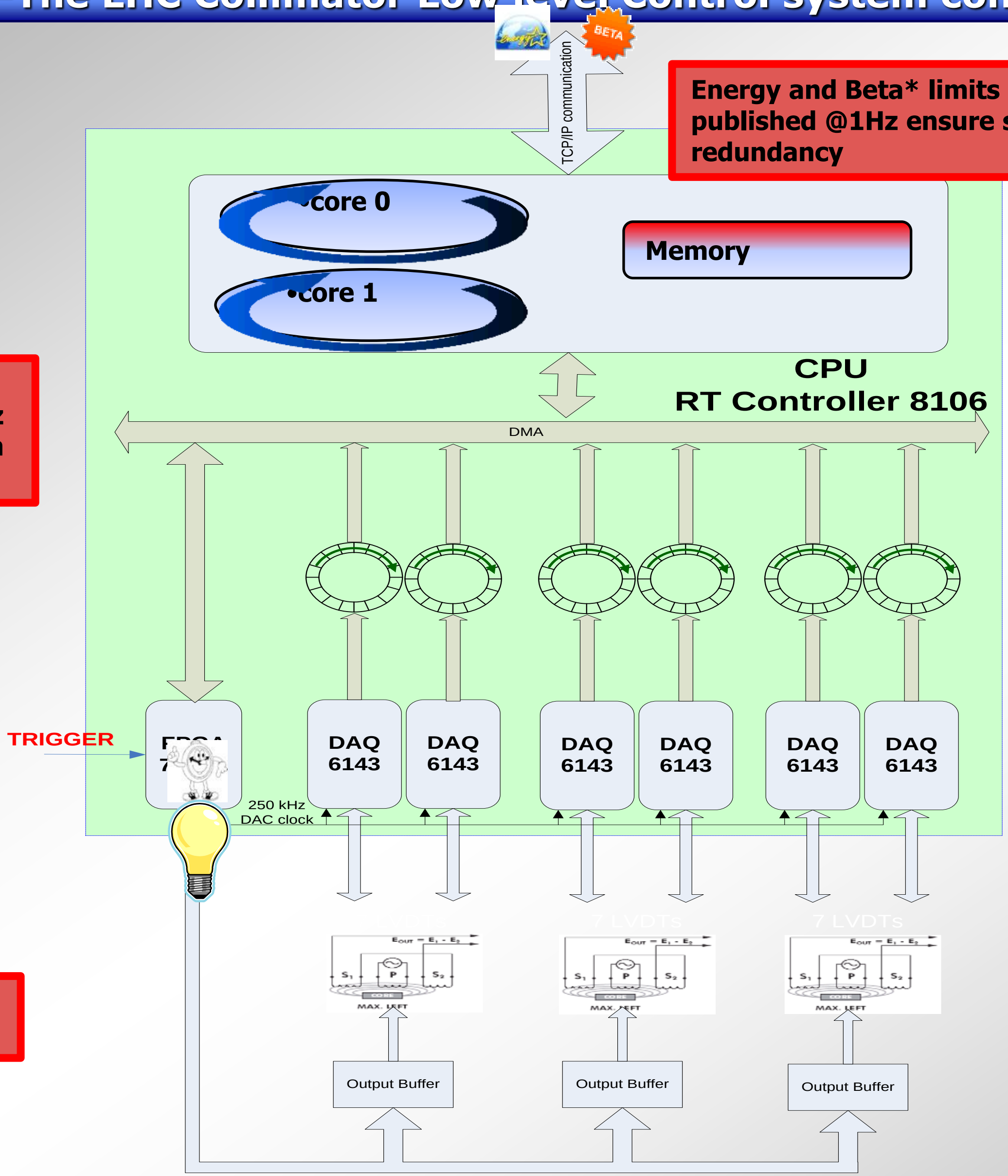
Notify to FESA

Profile limits sent by FESA

System arms FPGA for trigger

FPGA armed

1–The LHC Collimator Low level Control system control architecture



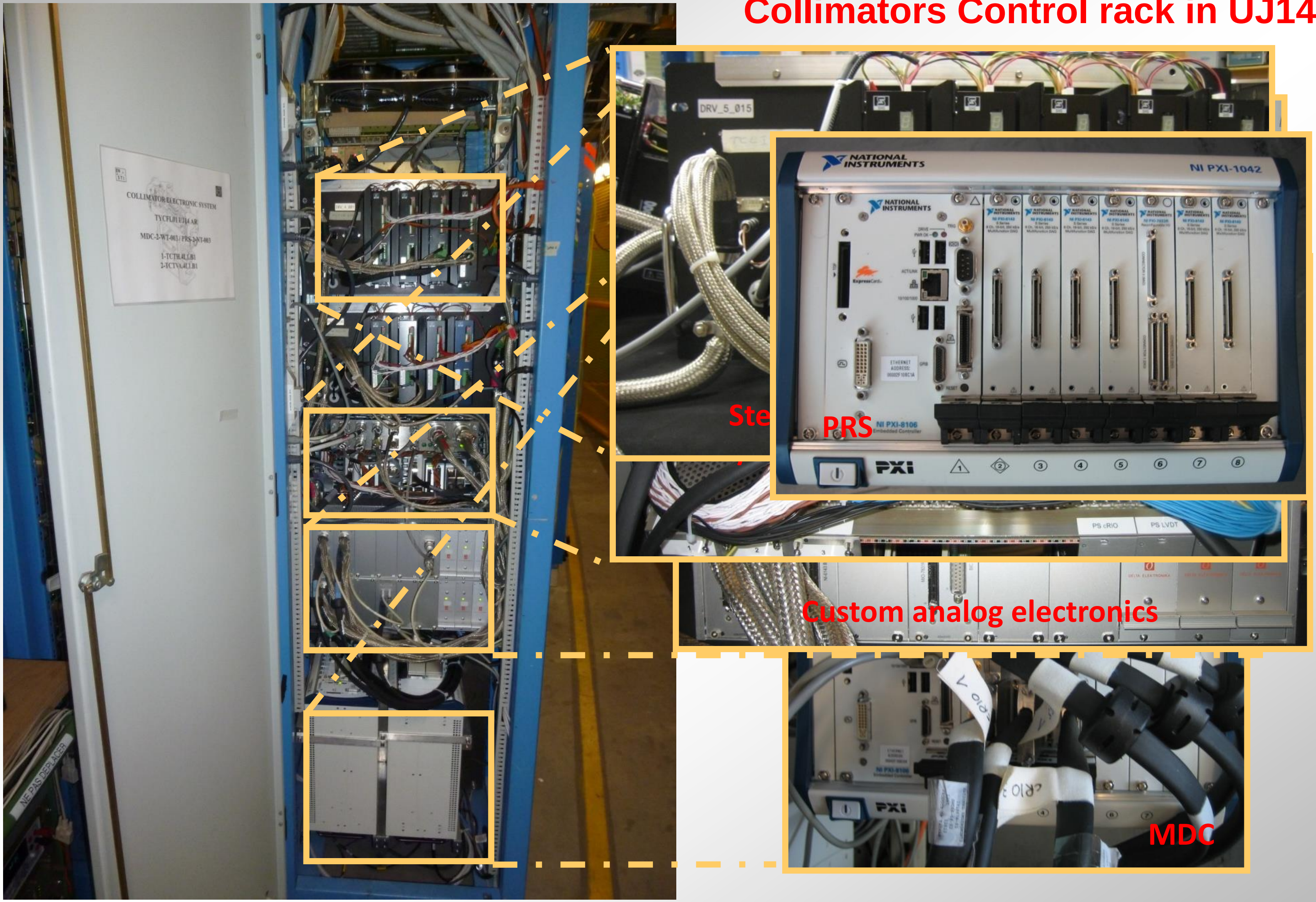
Energy and Beta* limits published @1Hz ensure safety redundancy

Profile limits interpolated @100Hz with timestamp from FPGA

Trigger starts profile monitoring

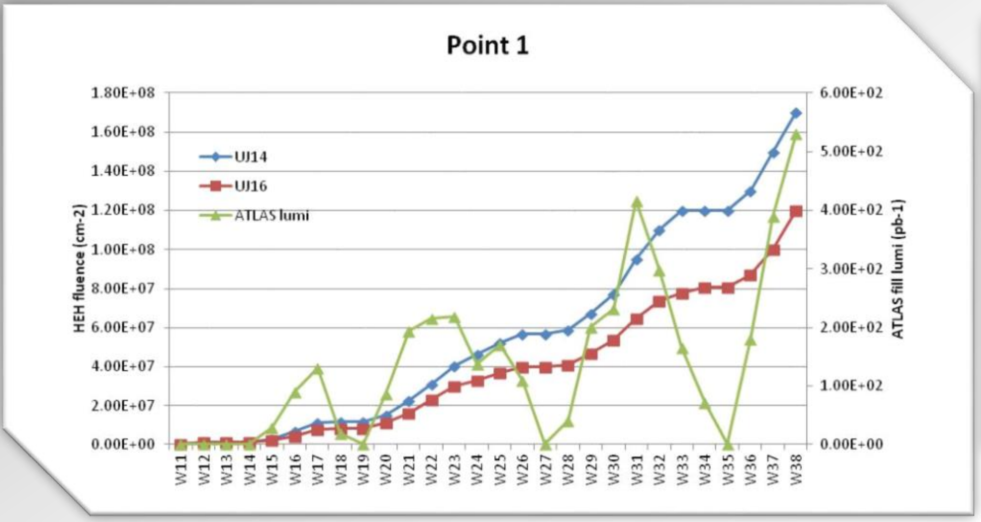
2–The electronics location

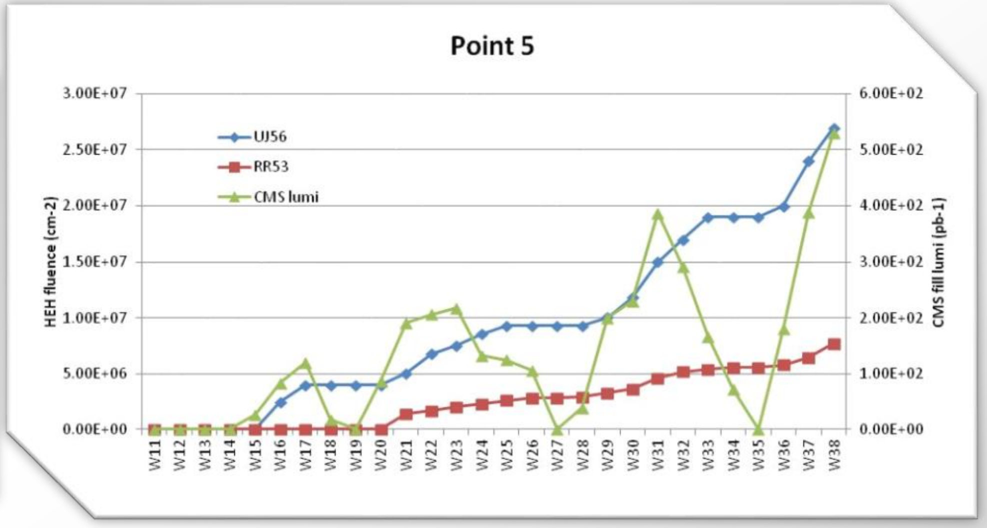
Collimators Control rack in UJ14



2–The electronics location

The Collimators Control Electronics racks exposed to radiation effects are located in the sensitive areas UJ14, UJ16, UJ56

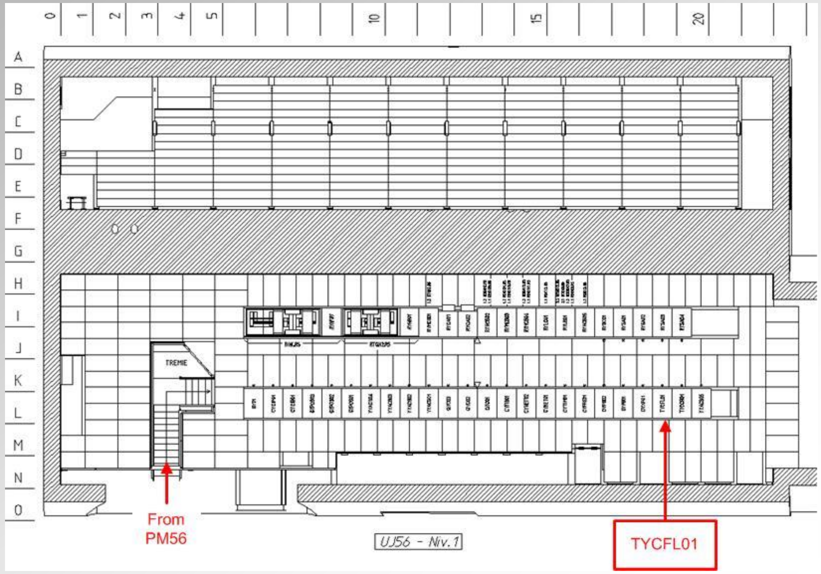


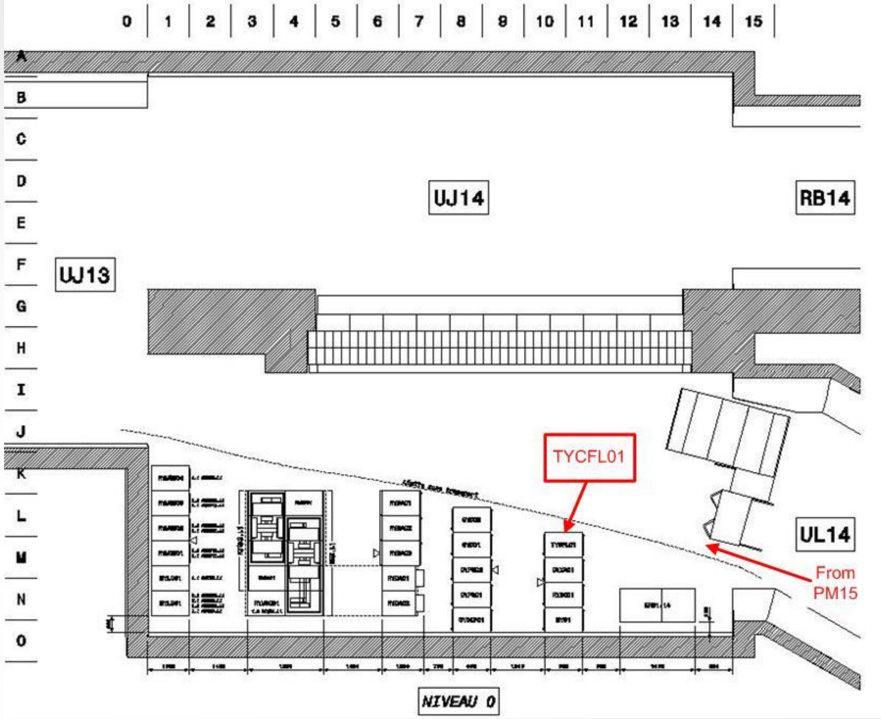


LHC point	Rack Name	Place	PXI Name (MDC)	PXI Name (PRS)	Collimator
Point 1 L	TYCFL01	UJ14	MDC-1-NT-001	PRS-1-NT-001	TCL.5L1.B2
					TCLP.4L1.B2
			MDC-2-WT-003	PRS-2-NT-003	TCTH.4L1.B1
					TCTVA.4L1.B1
Point 1 R	TYCFL01	UJ16	MDC-2-WT-004	PRS-2-NT-004	TCTVA.4R1.B2
					TCTH.4R1.B2
			MDC-1-NT-002	PRS-1-NT-002	TCLP.4R1.B1
					TCL.5R1.B1
Point 5 R	TYCFL01	UJ56	MDC-2-WT-012	PRS-2-NT-012	TCTVA.4R5.B2
					TCTH.4R5.B2
			MDC-1-NT-010	PRS-1-NT-010	TCLP.4R5.B1
					TCL.5R5.B1

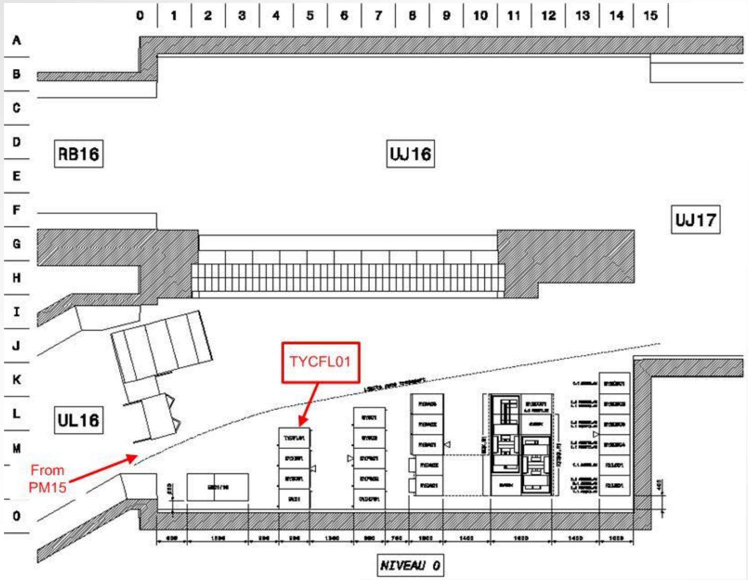
2–The electronics location

Collimators Control rack in UJ56





Collimators Control rack in UJ14



Collimators Control rack in UJ16

3–SEU effects and probability according to the CNRAD results

✓ According to the radiation tests performed in CNRAD last April-May 2010 different failures on a PXI control system have been observed already starting from a fluence of some 10^6 p/cm^2 up to 3.92 p/cm^2 :

- **Operational errors (e.g. register or memory cells value corrupted)**
- **CPU stuck**
- **FPGA errors (e.g. a bit stuck or flip)**
- **PXI rebooted itself**
- **Network communication temporarily lost**

✓ Those failures can be quickly fixed via a remote intervention but can provoke on a MDC:

- **Collimator operation not possible**

✓ Those failures can be quickly fixed via a remote intervention but can provoke on a PRS:

- **Collimator operation not possible**
- **False dumps**
- **Collimator survey out of order (machine protection impact)**

4–SEU effects: Risk analysis

LHC Collimators control in IP1 risk analysis

Legend

Risk probability:

- **High: more than 100 events experienced during the CNGS test**
- **Medium: between 10 and 100 events experienced during the CNGS test**
- **Low: less than 10 events experienced during the CNGS test**
- **Really low: only 1 event experienced during the CNGS test**

Severity:

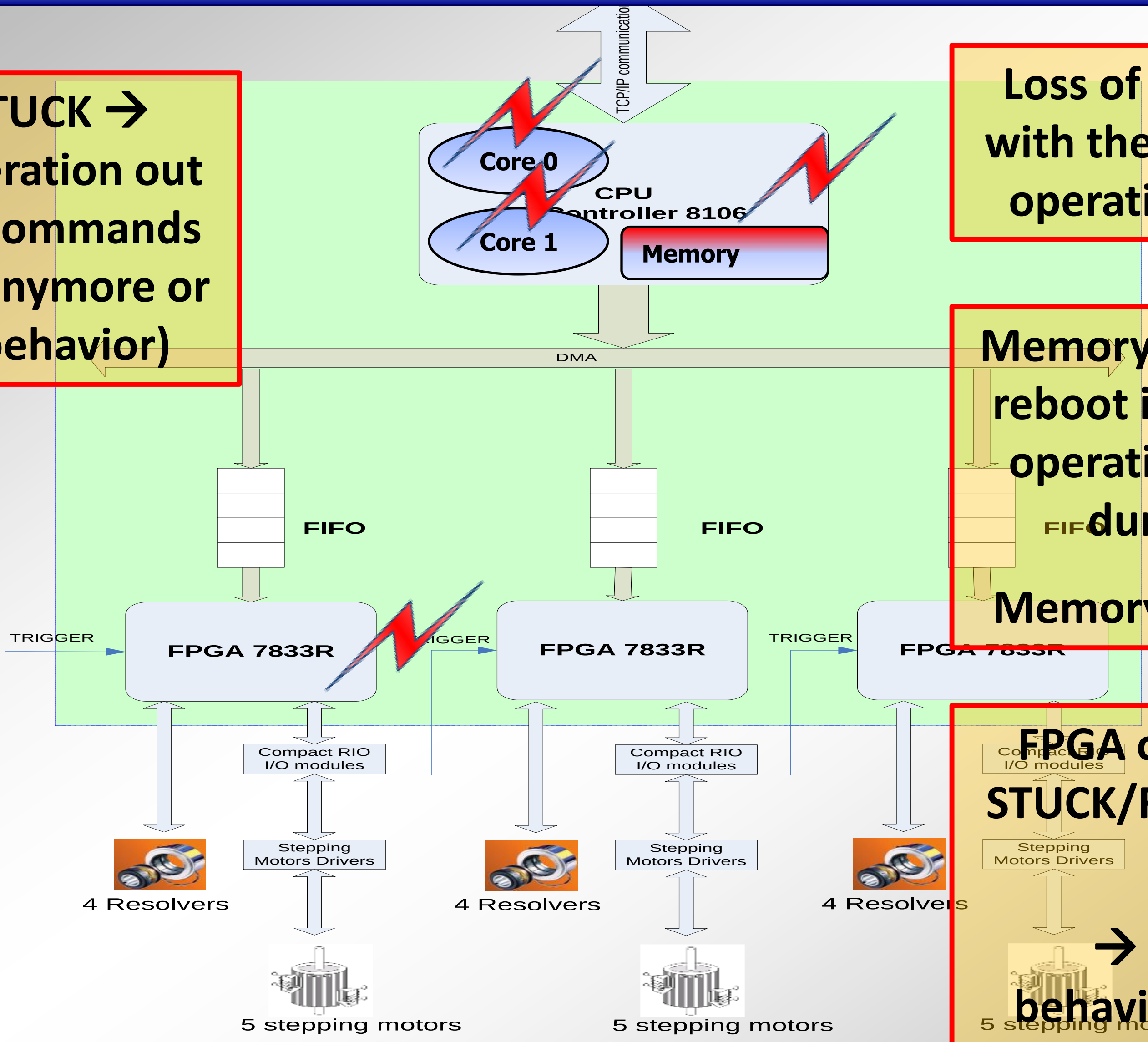
- **Low: Collimator operation not possible**
- **Medium: False dumps**
- **High: Collimator survey out of order (machine protection impact)**

Corrective action: *action to take to restore the correct control system operation*

System downtime: *The time the control system is not operational/ out of order*

4–SEU effects on the MDC

CPU Core STUCK → collimator operation out of order (i.e. Commands not accepted anymore or anomalous behavior)



Loss of communication with the PXI- Collimators operation out of order

Memory page fault →PXI reboot itself (Collimator operation out of order during reboot)

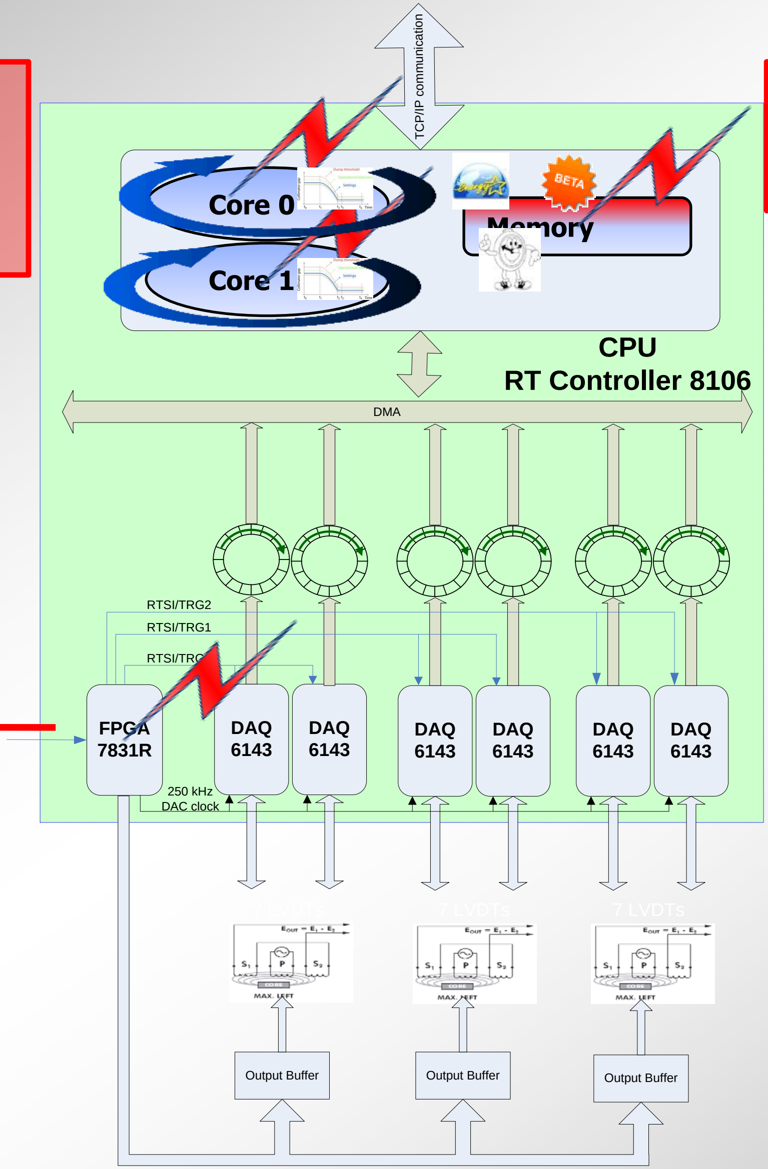
Memory cells corrupted

FPGA communication STUCK/FPGA bit stuck or flip

→ unexpected behaviour/ collimator operation out of order

4–The worst case (PRS): SEU Critical effect for the machine safety

CPU Core STUCK → collimator survey out of order



Loss of communication with the PXI but collimator survey still working

Memory page fault →PXI reboot itself (false dump)

CPU Core STUCK → collimator survey out of order

Memory value corrupted→The limit values are redundant (6 lvdts, Beta* and energy limits)

FPGA communication STUCK → ability to dump the beam/ interlock logic out of order

4–SEU effects: what we experienced so far

Date	IP	SEE type	Beam dumped	PXI system	Collimator names	Fill number	Problem
27/04/2011	UJ14	Soft SEE	NO	MDC-2-WT-003	TCTH.4L1.B1 TCTVA.4L1.B1	1740	Communication lost with the MDC
01/05/2011	UJ14	Soft SEE	YES	PRS-2-NT-003	TCTH.4L1.B1 TCTVA.4L1.B1	1753	PRS rebooted by itself
01/06/2011	UJ56	Hard SEE	YES	PRS-2-NT-010	TCL.5R5.B1 TCLP.4R5.B1	1835	PRS power supply failed
13/06/2011	UJ14	Hard SEE	YES	MDC-2-WT-003	TCTH.4L1.B1 TCTVA.4L1.B1	1865	MDC power supply failed/ rack circuit breaker off
30/07/2011	UJ16	Hard SEE	YES	MDC-2-WT-004	TCTH.4R1.B2 TCTVA.4R1.B2	1992	MDC power supply failed/ rack circuit breaker off
12/09/2011	UJ16	Soft SEE	NO	MDC-2-WT-004	TCTVA.4R1.B2	2102	Bit stuck in the counter register likely on the FPGA output register

4–SEU effects: Risk analysis

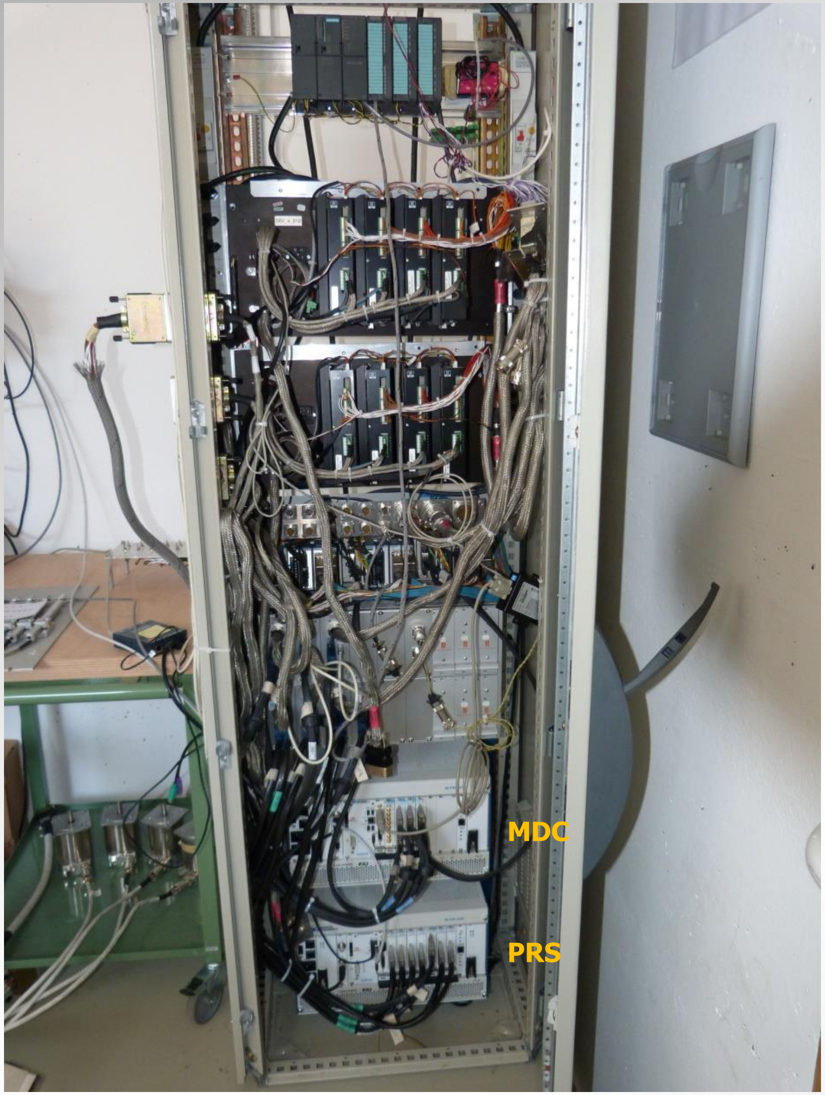
Risk Probability	Failure Scenario	Severity	Coll. not operational	False Beam dumped	Machine un-protected	Corrective action	System Downtime
High	*MDC* FPGA error	L	X			FPGA remote reset	15`
High	*MDC* CPU error	L	X			MDC remote reboot	15`
Medium	*MDC* rebooted itself	L	X				2`
Medium/high	*MDC* power supply failure	L		X		Power supply replacement	2 h
Really Low	Stepping motor driver failure	M		X		Stepping motor driver replacement	2 h
Low	*PRS* CPU communication lost but survey loops still running	M		X		Remote PRS reboot	15`
Medium/high	*PRS* power supply failure	M		X		Power supply replacement	2 h
Medium/low	*PRS* rebooted by itself	M		X			2`

4–SEU effects: Risk analysis

Risk Probability	Failure Scenario	Severity	Coll. not operational	False Beam dumped	Machine un-protected	Corrective action	System Downtime
Really low	*PRS* memory values corrupted	M		X		Remote PRS reboot	15`
Really low	*PRS* FPGA interlock logic corrupted	H		X	X	Remote PRS reboot	15`
Really Low	*PRS* CPU stuck	H			X	Remote PRS reboot	15`
Really low	*PRS* FPGA errors/ communication lost	H			X	FPGA remote reset/ Remote PRS reboot	15`

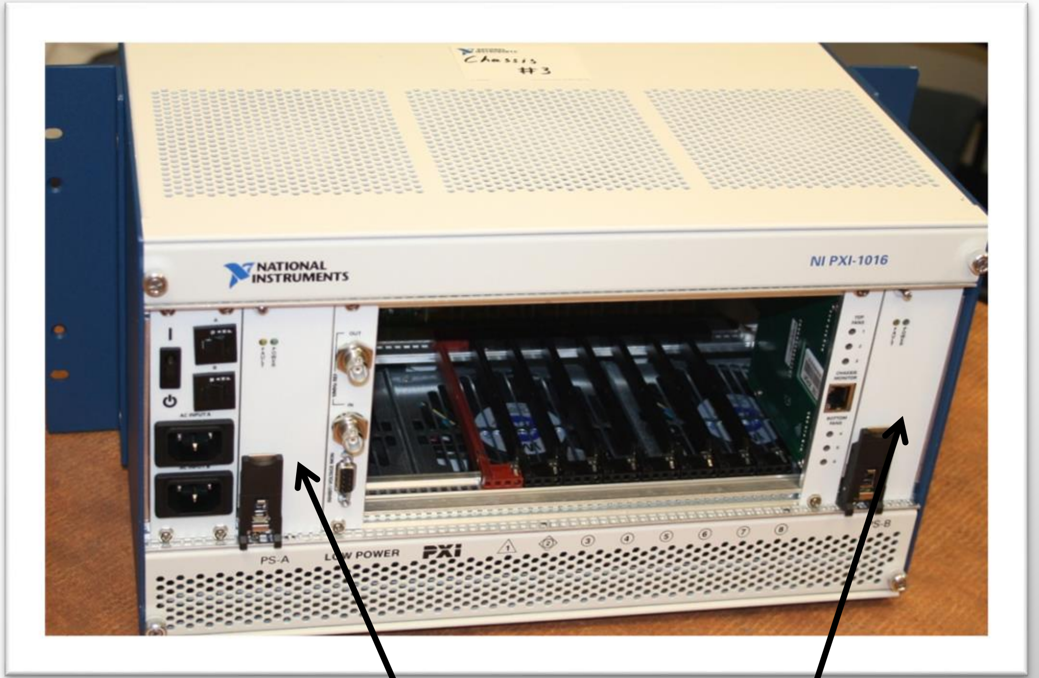
Even if really rare these effects must be detected and mitigate…

5-How the SEU critical effects can be prevented: PXI power supplies failure



Two prototypes of the new PXI chassis successfully tested in a lab collimator rack

The 12 PXI chassis in the sensitive area will be likely replaced with new High Reliability PXI chassis during next Xmas break

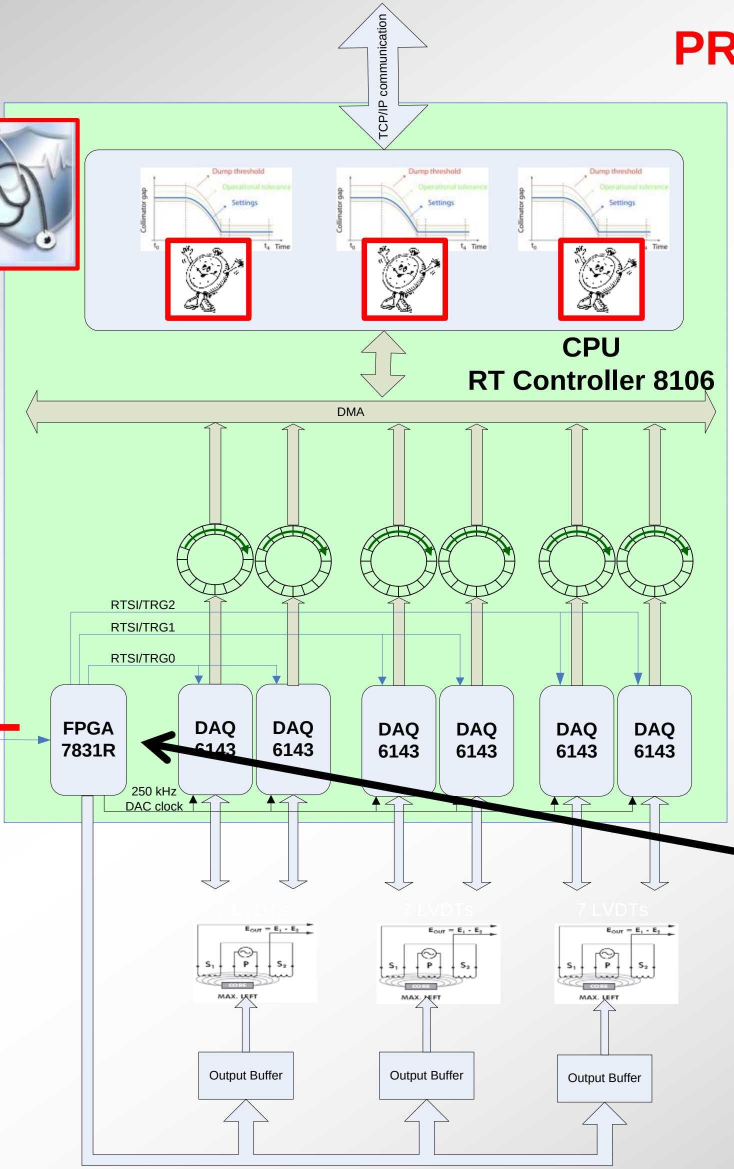


Two redundant hot swappable power supplies and 6 redundant fans

5-How the SEU critical effects can be prevented: PRS unsafe states

PRS architecture

Watch dog timer on the CPU to check FPGA communication status



BIC

Watch dog timer on FPGA to verify CPU activity and survey loops stuck conditions

Implementing the TMR (Triple Modular Redundancy) on the interlock logic on the FPGA

6–Improvements of the control system reliability against SEU

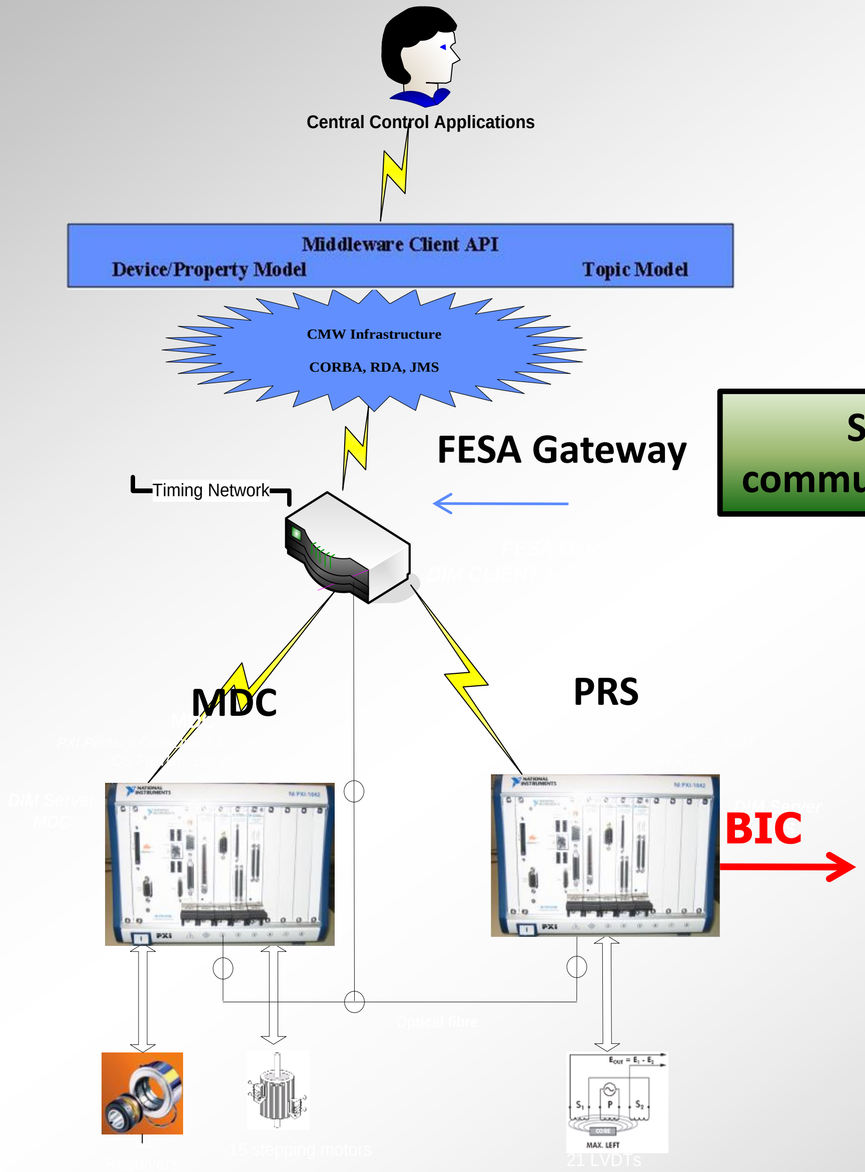
Assumptions:

- ✓ The probability of experiencing on the same system at the same time a CPU and FPGA stuck is negligible....
- ✓ On the PRS system if the CPU is stuck the collimator positions survey is compromised
- ✓ On the PRS system if the FPGA is stuck or affected by errors the beam dump functionality can be compromised

Proposal:

- ✓ The CPU watch dog timer on the PRS FPGA should be able to trigger an interlock
- ✓ A Software Interlock can be added at the FESA level on the PRS FPGA stuck error and communication time out

6–Improvements of the control system reliability against SEU



Software interlock in case of PRS communication lost and/or FPGA stuck error

PRS software mitigation techniques:

1. CPU and Survey loops watch dog timers implemented on FPGA triggering a dump in case of time out
2. FPGA stuck watch dog timer implemented on the CPU arising an error to the FESA server
3. TMR on the interlock logic on the FPGA

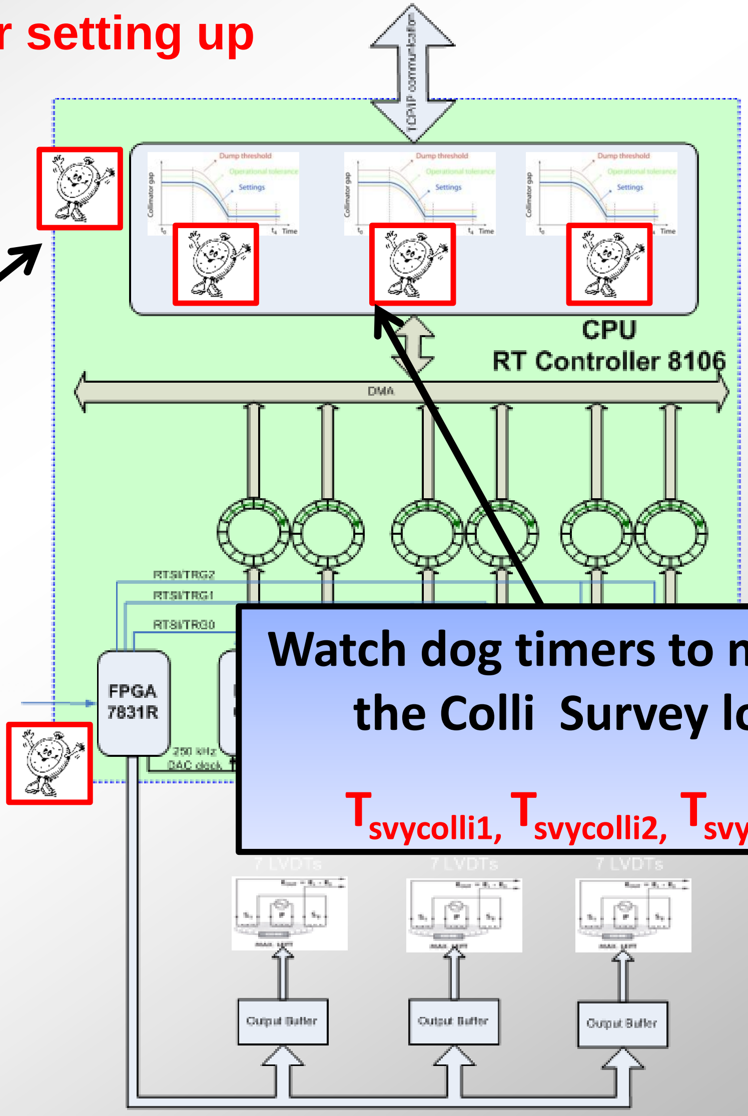
7–Conclusions and timelines

- ✓ In the failure analysis of the SEU effects on the collimator electronics the worst cases have been taken into account (PRS in unsafe state)
- ✓ The sensitivity of the PXI power supply to hard SEU has been proved in radiation test at PSI. We will install during the next Xmas break some new high availability PXI chassis. If the test is successful we will replace all during LS1.
- ✓ Improvements to the PRS software on the collimator control systems in UJ14, UJ16, UJ56 have been proposed to mitigate the SEU effects reducing the impact on the machine protection
- ✓ The proposed improvements are being tested and preliminary results confirm the choice of the time out values as good compromise between detecting dangerous situations for the machine protection and avoiding false dumps
- ✓ The software will be ready to be deployed in the tunnel for the next technical stop
- ✓ An update of the engineering specifications of the low level control system taking into account the last upgrades is in progress
- ✓ We propose to perform a detailed specification and software review performed with the help of an external company to dissipate any doubt on possible weaknesses on the low level control system.

6–Improvements of the control system reliability against SEU

PRS Watch dog timer setting up

The CPU Watch dog time out values must be accurately set to avoid from one side false dumps in the cases of CPU overcharge conditions and on the other side to not compromise the machine safety. The values to set up are:



Watch dog timer to monitor the CPU activities and the network communication T_{CPU}

Watch dog timer to monitor the FPGA communication T_{FPGA}

Watch dog timers to monitor the Colli Survey loop

$T_{svycolli1}$, $T_{svycolli2}$, $T_{svycolli3}$

6–Improvements of the control system reliability against SEU

PRS Watch dog timer setting up

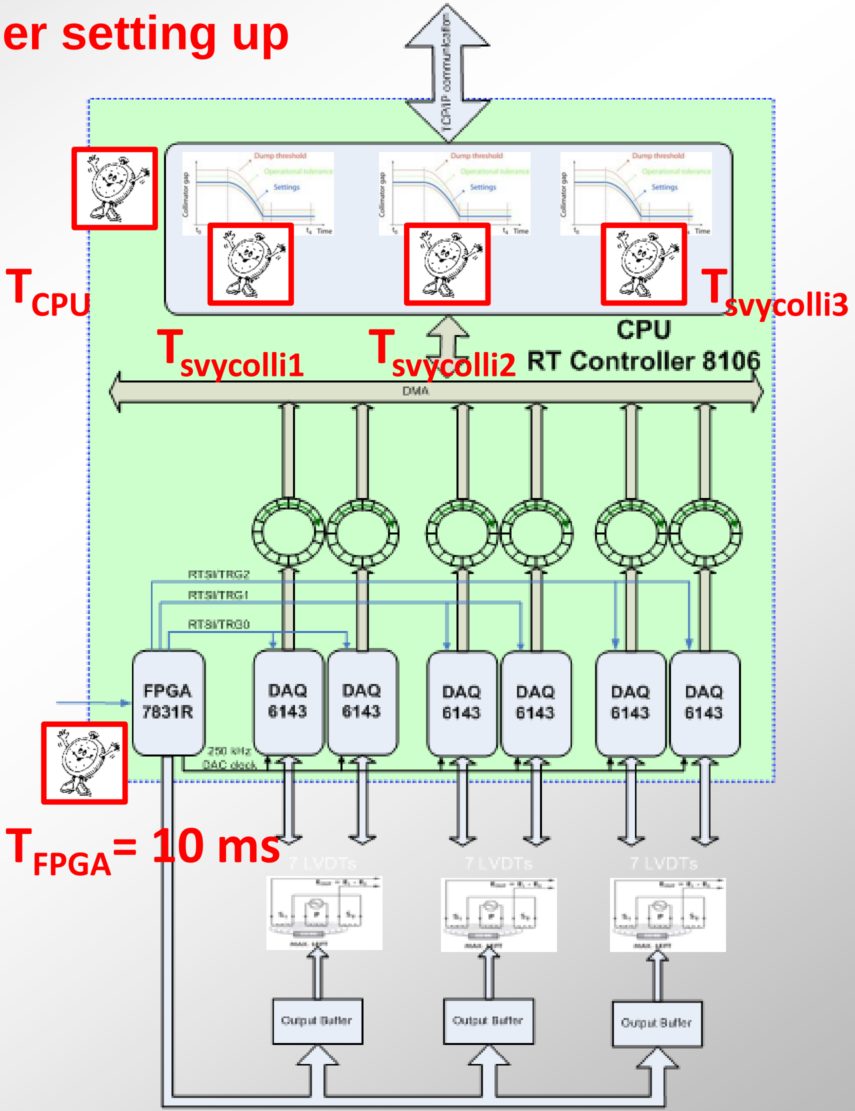
T_{FPGA} : 10 ms equal to the reading period on the Host

$T_{CPU}, T_{svycolli1}, T_{svycolli2}, T_{svycolli3}$:

1. These time out values should ensure the detection of an axes positioning error greater than 100 um

2. This time depends on the maximum speed the axes can move.

   In normal operation the maximum speed is 2 mm/s but the worst case is the autoretraction .....



6–Improvements of the control system reliability against SEU

PRS Watch dog timer setting up

2.

When does the autoret

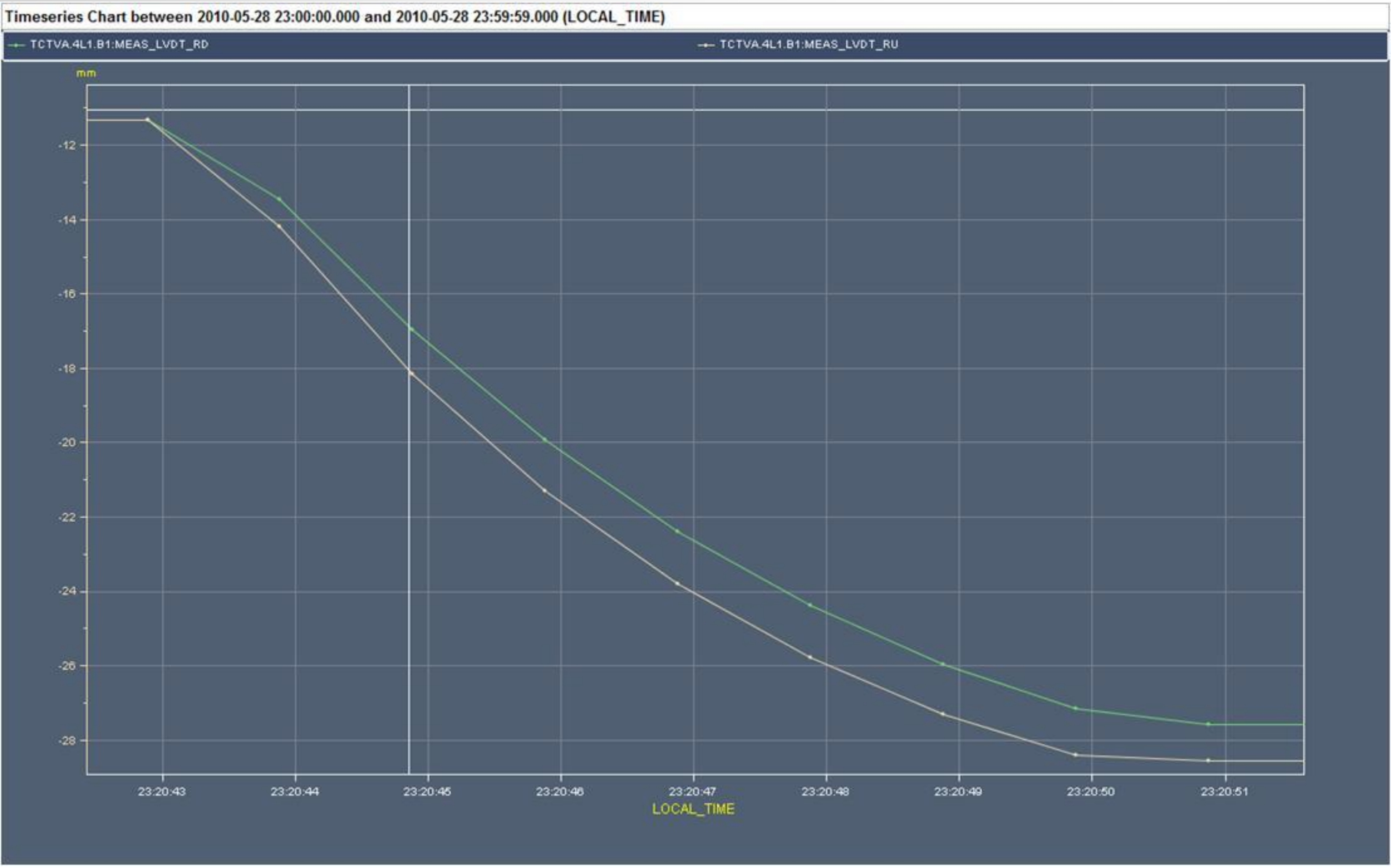
The auto-retraction g
a power cut in the t

Which is the probabilit

From January 2010 y
in UJ14/UJ16 and 9

Which is the maximum

Depend on the coll st
case is represented er
the effect of the gr s.
We can assume as


Timeseries Chart between 2010-05-28 23:00:00.000 and 2010-05-28 23:59:59.000 (LOCAL_TIME)

TCTVA.4L1.B1 autoretraction following the power cut on 28-05-2010

V max = 4 mm/s → $T_{CPU}, T_{svycolli1}, T_{svycolli2}, T_{svycolli3}$ = 30 ms