CIBU connection Review

BT, BP & IRR   AB/CO/MI   12December 2008

Outline

1st presentation: CIBU Failure in UJ33 *(Benjamin TODD)*

- Background
- Before the incident
- The incident
- Future goals

2nd presentation: Proposal cures on HW side *(Bruno PUCCIO)*

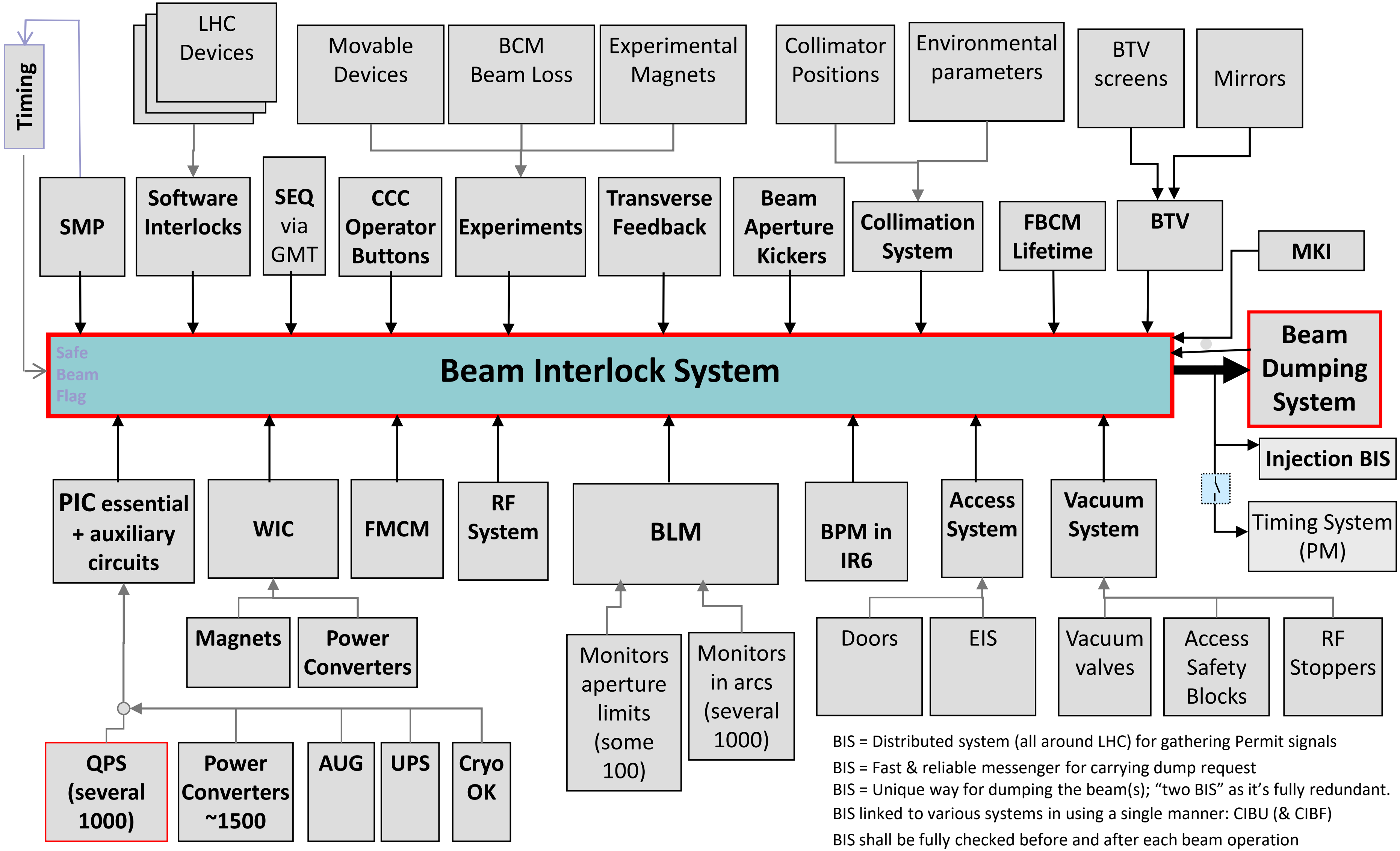
- CIBU connection change
- Redundant signals and independent outputs
- Consequences on the Users side

3rd presentation: Proposal for automated test *(Ivan Romera)*

- The purpose
- First implementation on PIC-BIC interfaces
- Proposal & CMW interface with the Users.

The next steps…

Beam Interlock System: Heart of the Machine Protection



BIS = Distributed system (all around LHC) for gathering Permit signals

BIS = Fast & reliable messenger for carrying dump request

BIS = Unique way for dumping the beam(s); “two BIS” as it’s fully redundant.

BIS linked to various systems in using a single manner: CIBU (& CIBF)

BIS shall be fully checked before and after each beam operation

The connections with User systems will be checked as well

=> Automated tests launched by the LHC Sequencer.

Based on a R.Schmidt’s drawing

Outline

1st presentation: CIBU Failure in UJ33 *(Benjamin TODD)*

- Background
- Before the incident
- The incident
- Future goals

2nd presentation: Proposal cures on HW side *(Bruno PUCCIO)*

- CIBU connection change
- Redundant signals and independent outputs
- Consequences on the Users side

3rd presentation: Proposal for automated test *(Ivan Romera)*

- The purpose
- First implementation on PIC-BIC interfaces
- Proposal & CMW interface with the Users.

The next steps…

CIBU Failure Explanation

1. Background
   - CIBU Input Circuits
   - Installation Rules
   - MI Stance

2. Before the Incident
   - Vacuum System as Tested
   - Conformity
   - Functional Testing

3. The Incident
   - Modified Interconnection
   - Failure in the CIBU
   - Report of Non-Conformities

4. Future Goals
   - Connection Specification
   - Improvements to Interfaces
   - Automated Test Sequences

Background

Machine Interlocks Section

Develop fail-safe dependable hardware
Testing / failure modes analysis of all critical hardware
Audited / reviewed internally and externally

We commit to

Be open and honest with you about our work
Share our experiences openly (both bad & good)
Be completely open to critique / criticism
Optimise the balance safety versus physics

If ever we find weaknesses in our designs effecting safety
We will present the findings to MPP and stop the LHC until issues can be solved
Every experience is fed back into the design
Everyone's opinion counts.

This is an example of this commitment to you – no blame to be assigned!
Quite the opposite!
We can use this to improve our designs - Let's take a look…

The User Interface (CIBU)

User System to Beam Interlock System connection

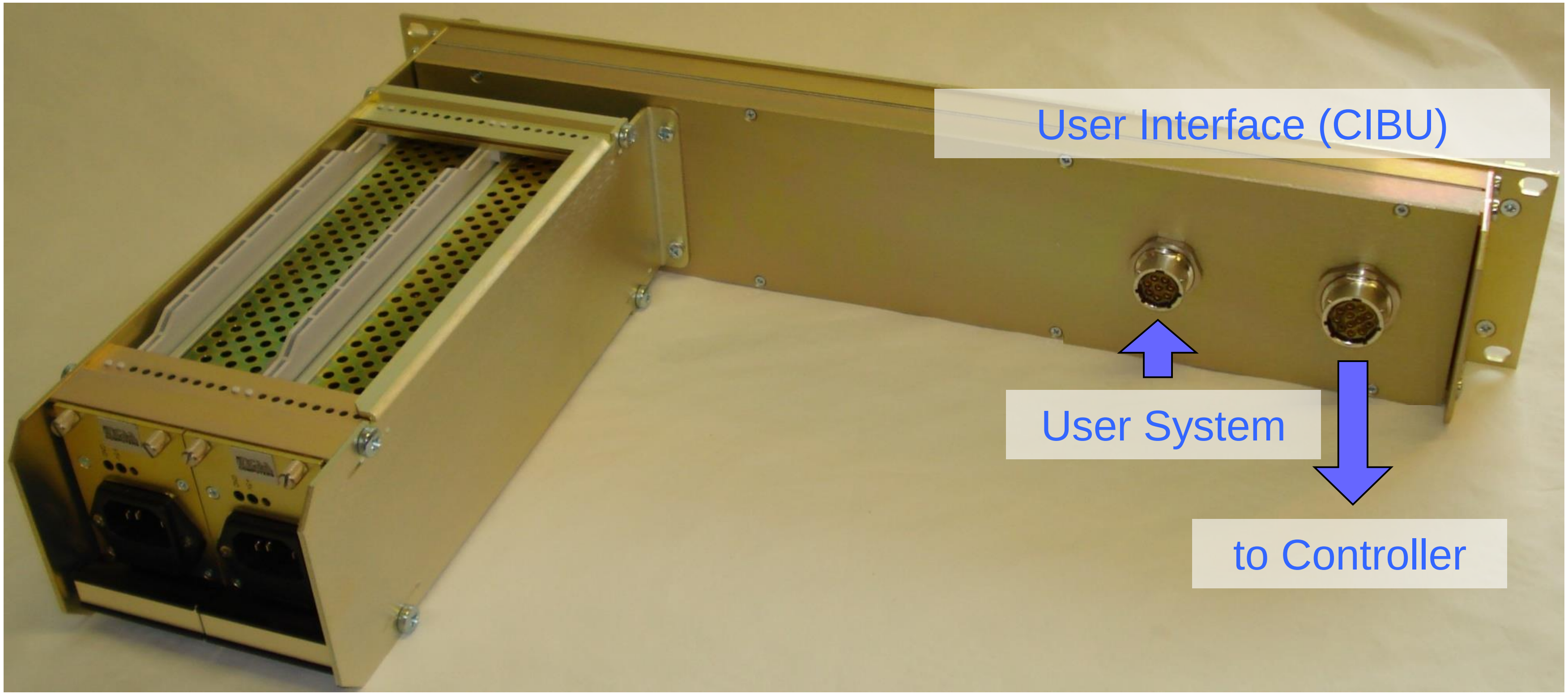
1. Unique Hardware for All Users
2. Current Loops
3. Redundant Circuits
4. Tested to CIBU Output Connector Internally using BIS TEST
5. Need USER SYSTEM Test for full coverage

CIBU is used in the whole accelerator complex
Many CIBU-Hours of operation for statistics
Around 2e6 unit-hours - SPS since 2006

Link Specified in:
https://edms.cern.ch/document/636589/1.4

Until this year – NO failures on critical paths

The User Interface (CIBU)

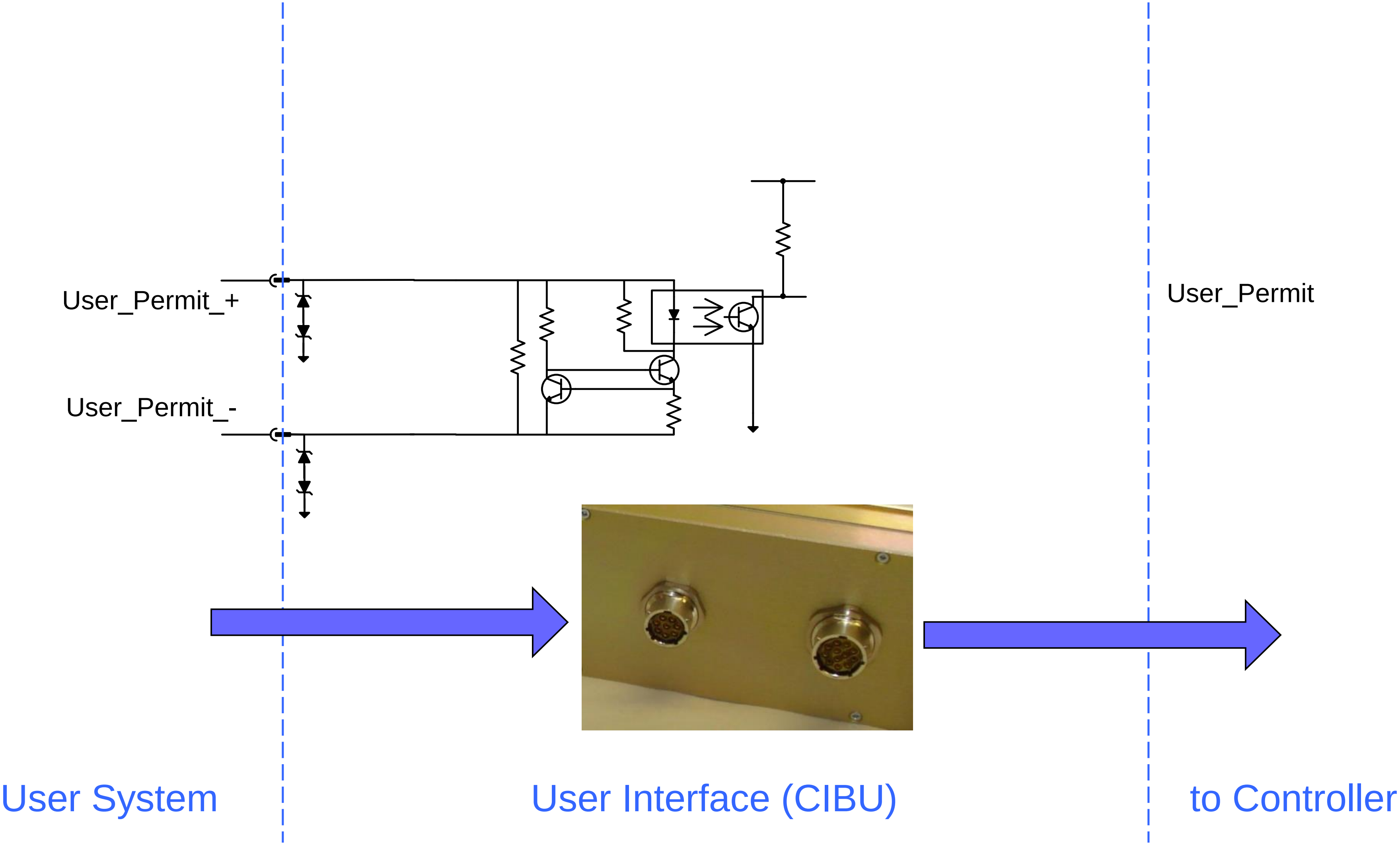


User Interface (CIBU)

User System

to Controller

CIBU Input Circuit



User_Permit_+

User_Permit_-

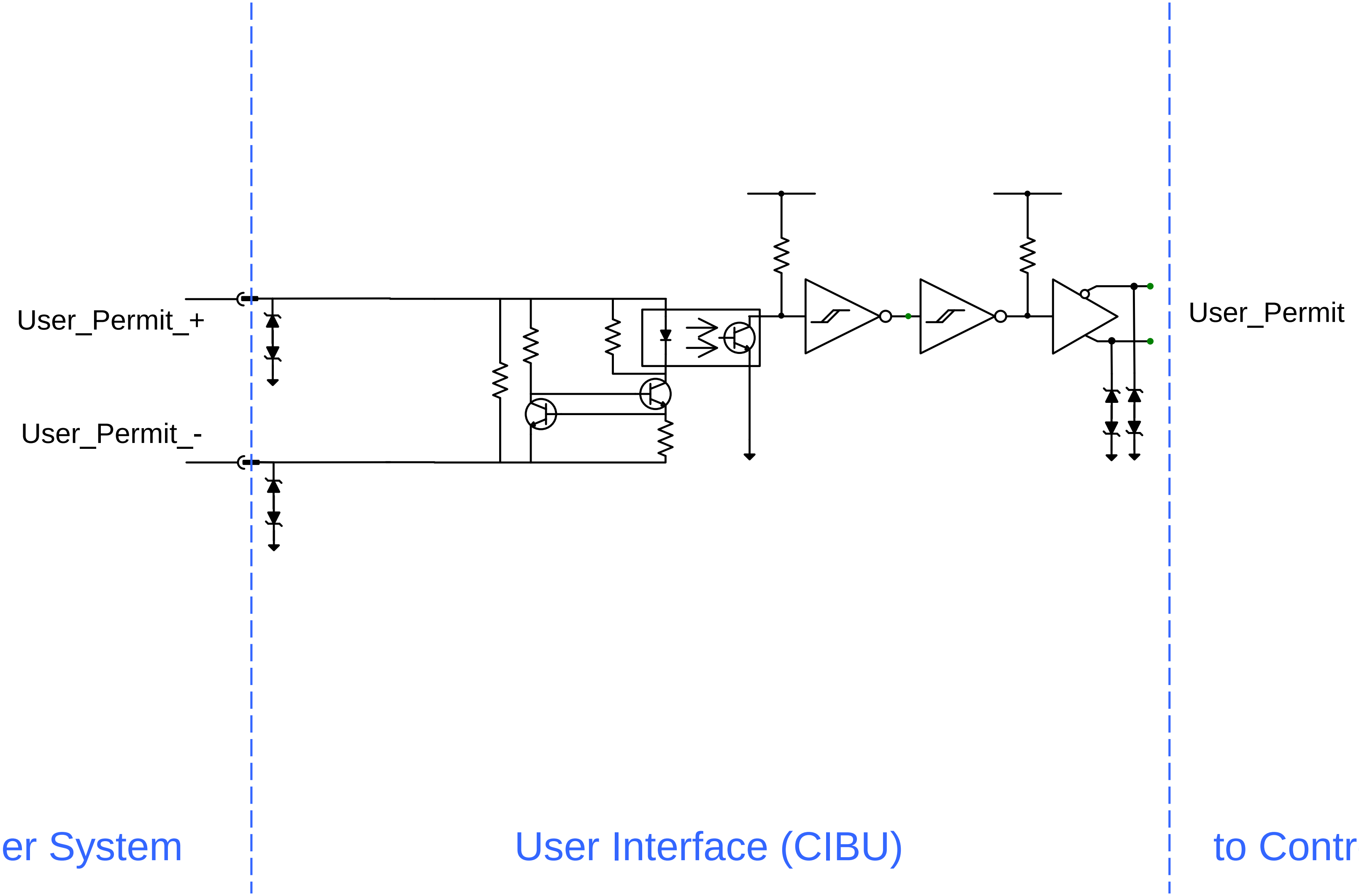
User_Permit

User System

User Interface (CIBU)

to Controller

CIBU Input Circuit

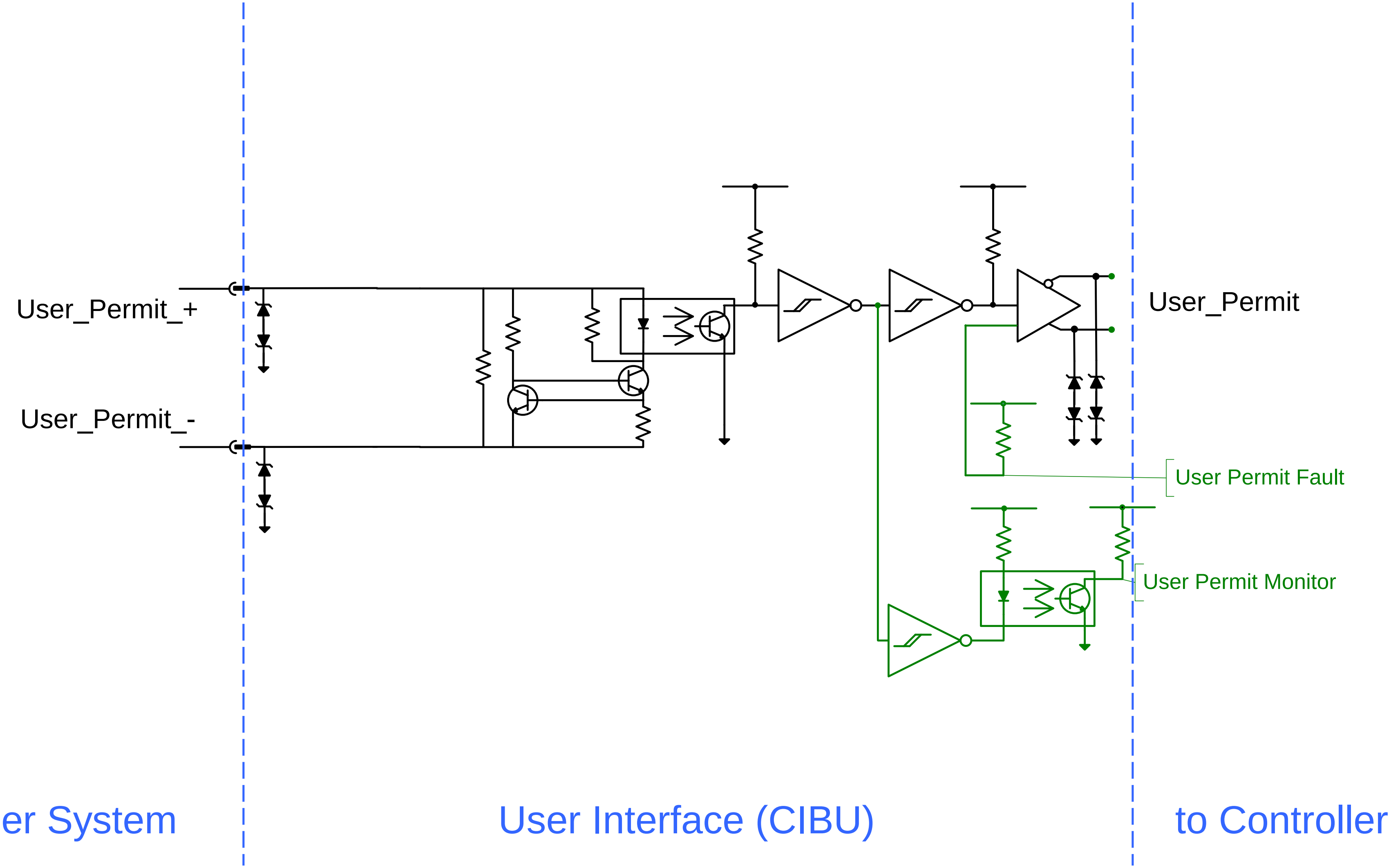


User System

User Interface (CIBU)

to Controller

CIBU Input Circuit

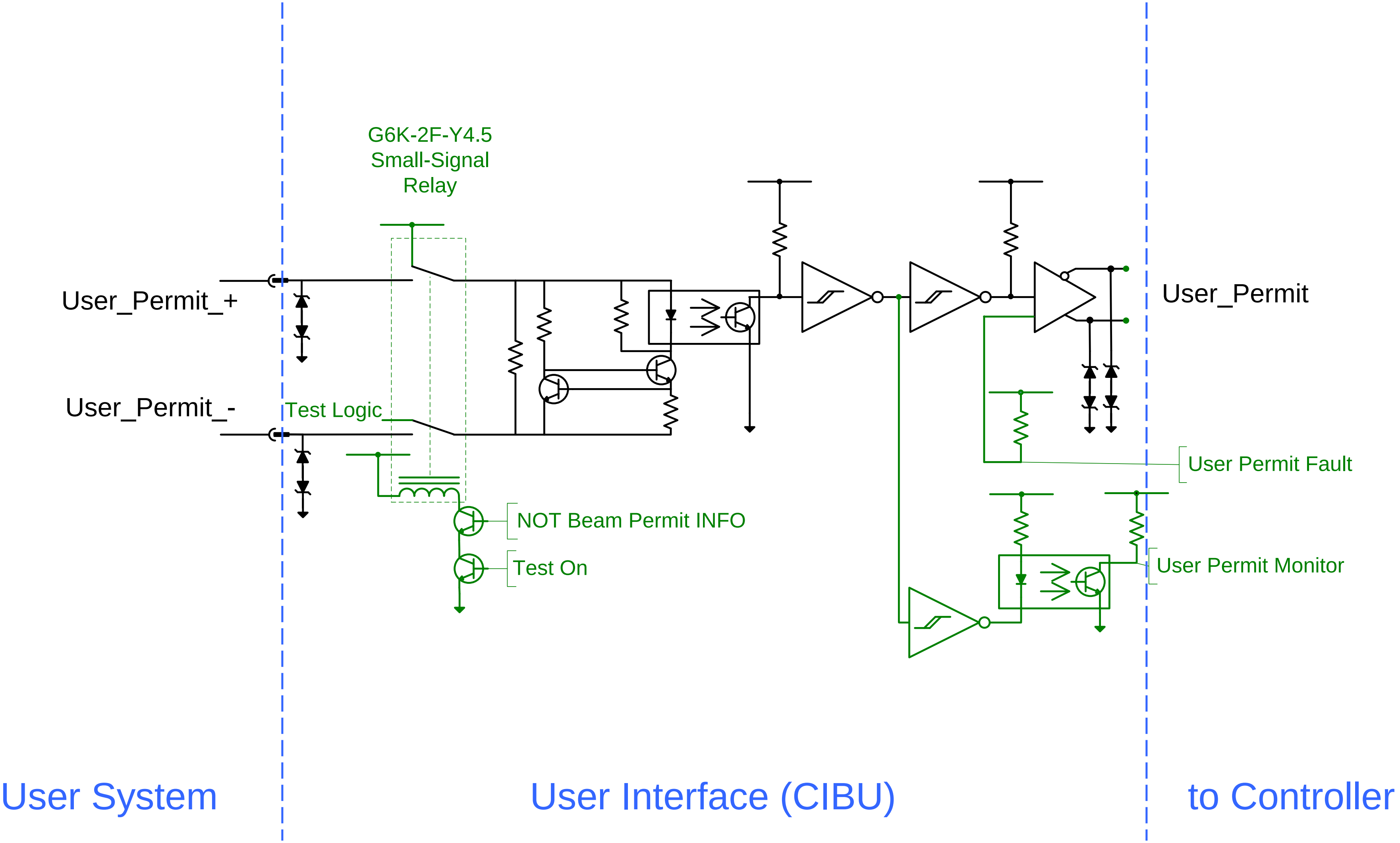


User System

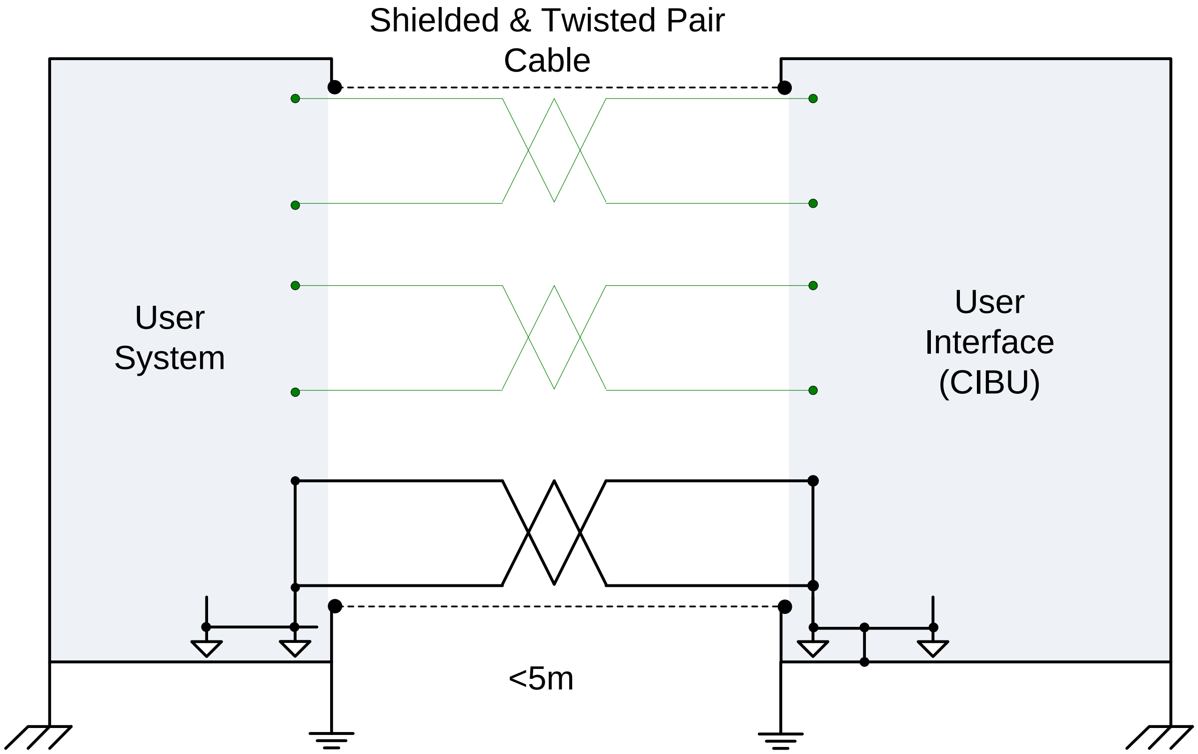
User Interface (CIBU)

to Controller

CIBU Input Circuit



CIBU Input Circuit



Mandatory Circuit
1. All ground / earth / 0V connected
2. Spare wires grounded
3. Shield 360° at both ends
4. No pig-tails
5. More than 5m = FORBIDDEN
6. Cable should be:
a. Twisted Pair NE8/NF8
b. LEMO 00 from VME FP

Timescale

7th August 2008

No Beam In the Machine
Final Commissioning Vacuum System to Beam Interlock System

1. Vacuum Valves moved IN around IR3
2. Vacuum UJ33 USER_PERMIT_A stayed TRUE
3. Vacuum UJ33 USER_PERMIT_B stayed TRUE
4. BIC Test Mode showed ALL OK

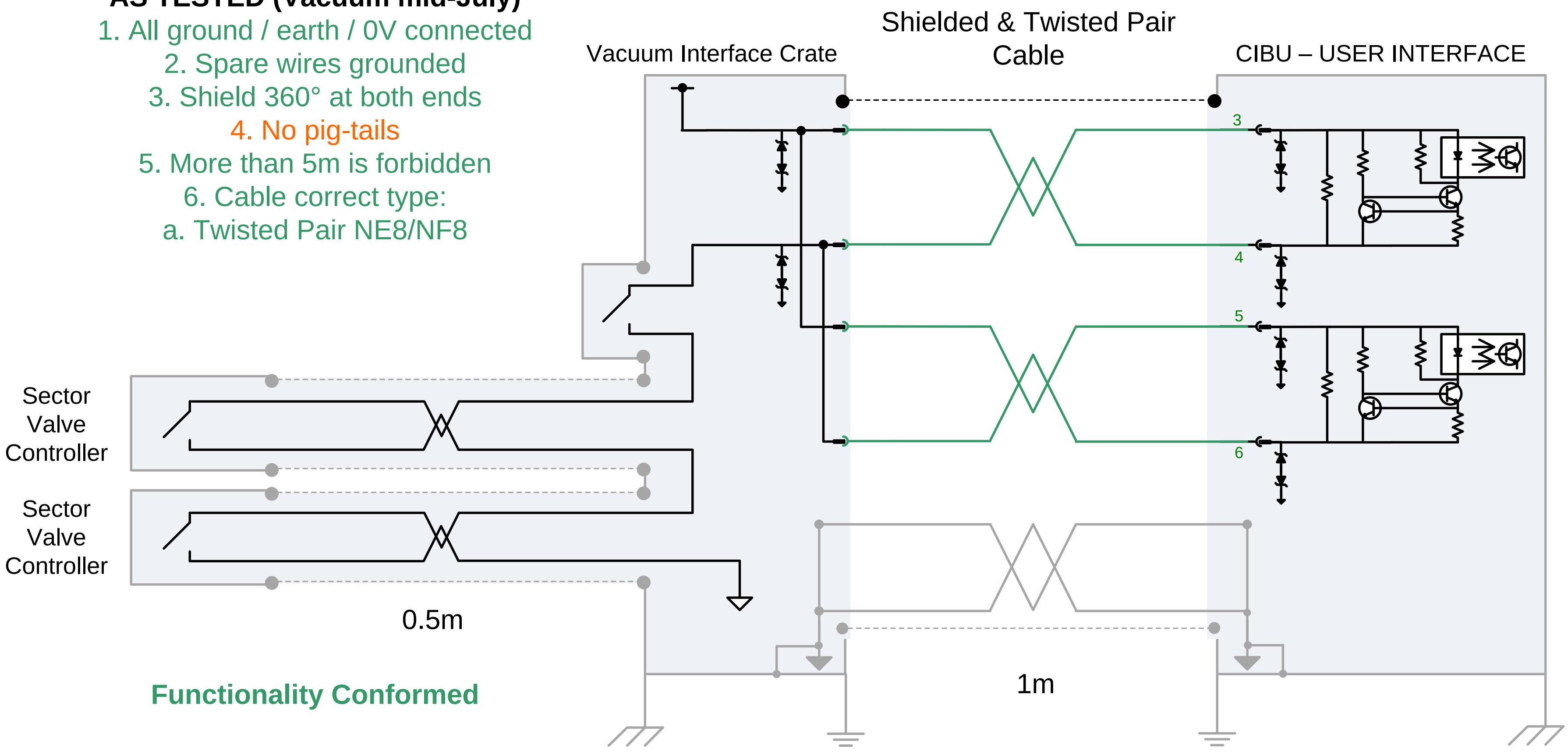
Commissioning Fail

As Tested July 08

AS TESTED (Vacuum mid-July)

1. All ground / earth / 0V connected
2. Spare wires grounded
3. Shield 360° at both ends
4. No pig-tails
5. More than 5m is forbidden
6. Cable correct type:

a. Twisted Pair NE8/NF8



Functionality Conformed

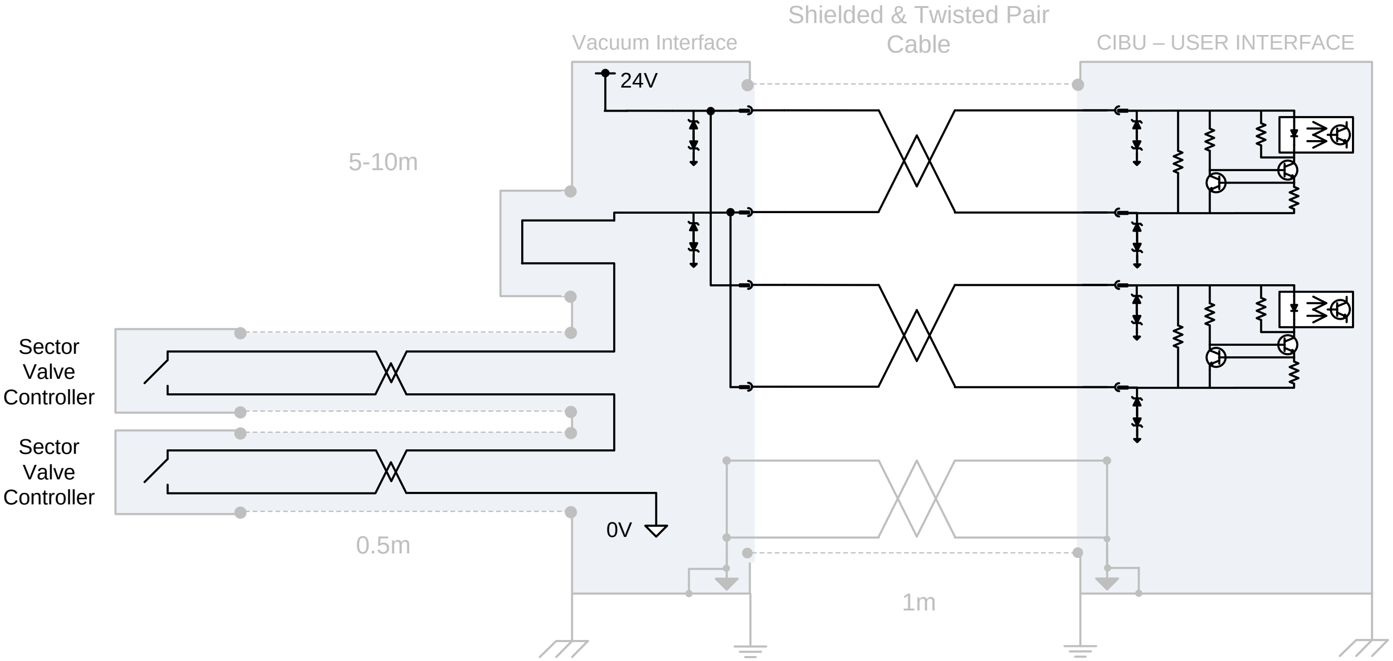
Between July and August

EIS (Elément Important de Sécurité)

1. Added to Interlock Logic
2. EIS controlled by Access System (Personnel Protection Device)
3. Access System connected to BIS via Vacuum System

MI were not aware of this cabling change

August 08 - After Incident

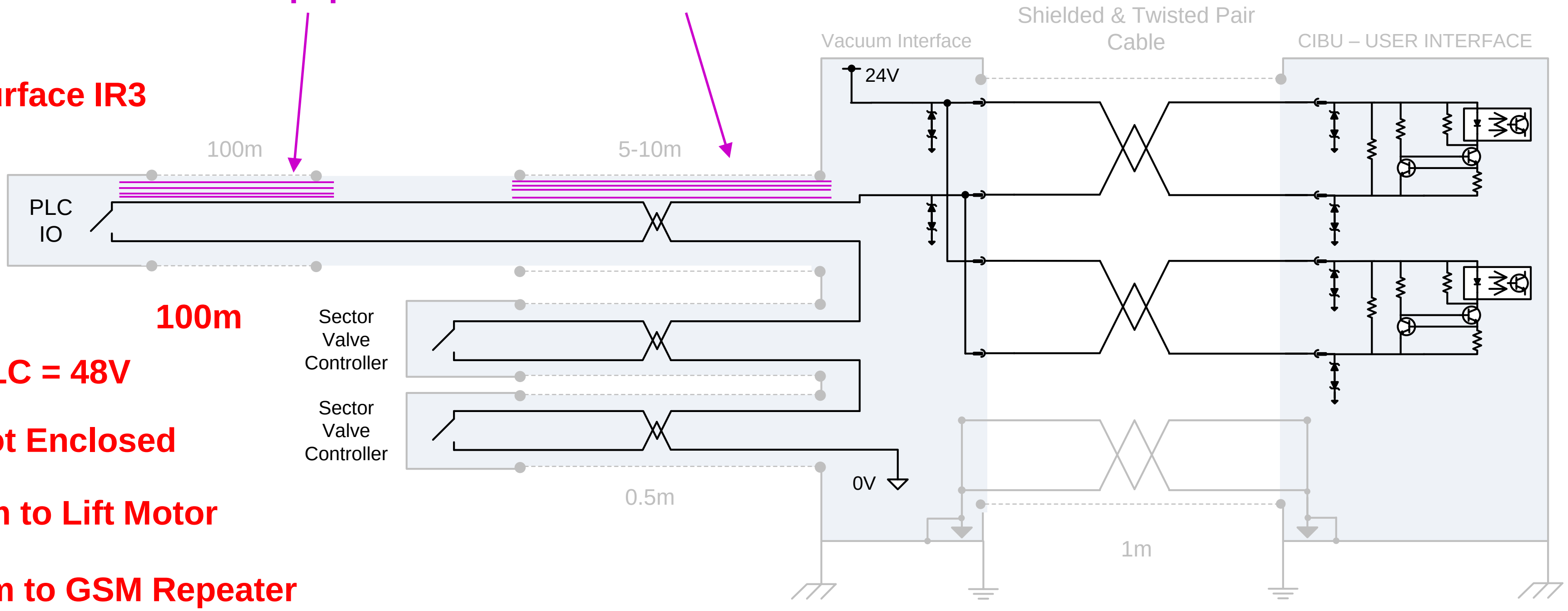


August 08 - After Incident

46 Signals From other equipment

6 floating wires

Surface IR3



100m

PLC = 48V

Not Enclosed

2m to Lift Motor

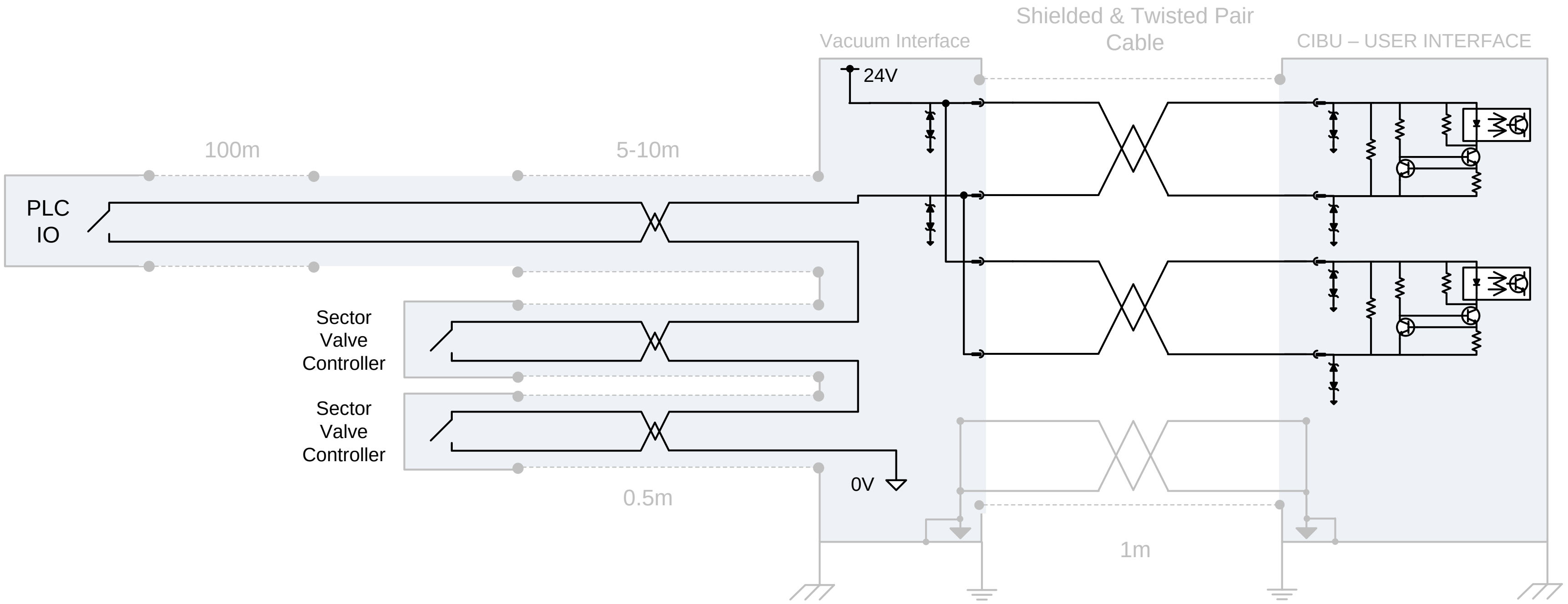
1m to GSM Repeater

WHEN CONNECTED
CIBU ALWAYS TRUE
(next slides)

What was the mechanism?

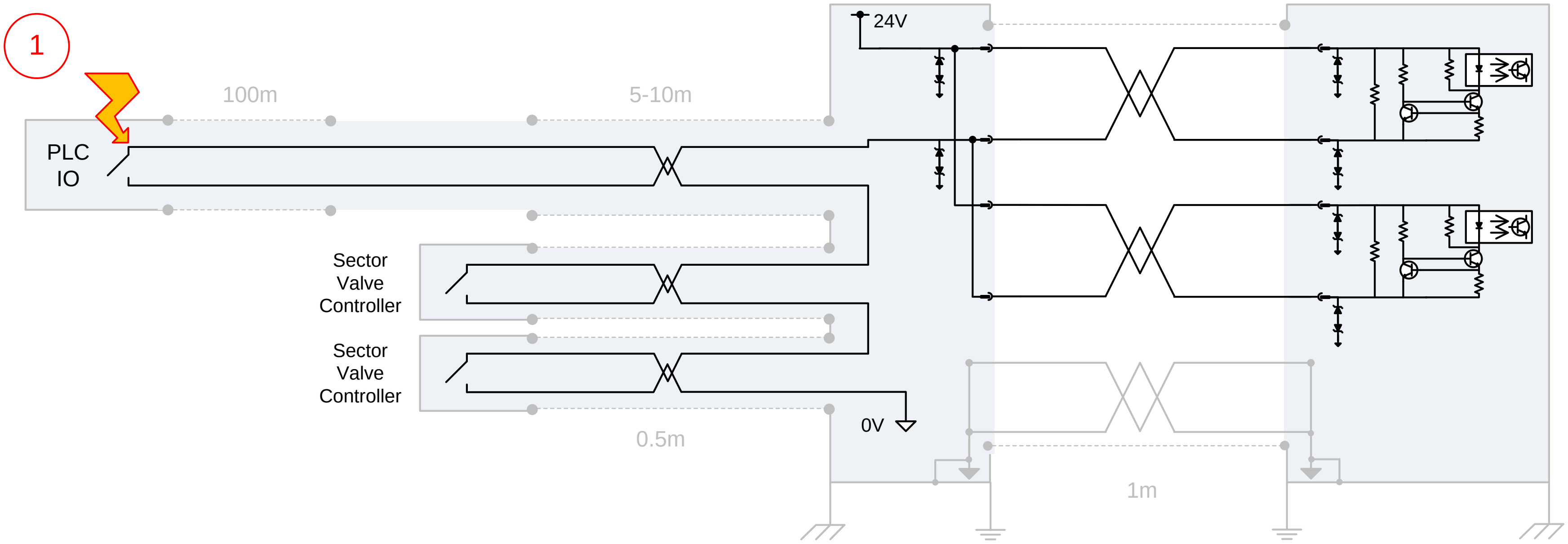
Access – Connected Panel to Surface PLC incorrectly initially

…took several attempts …



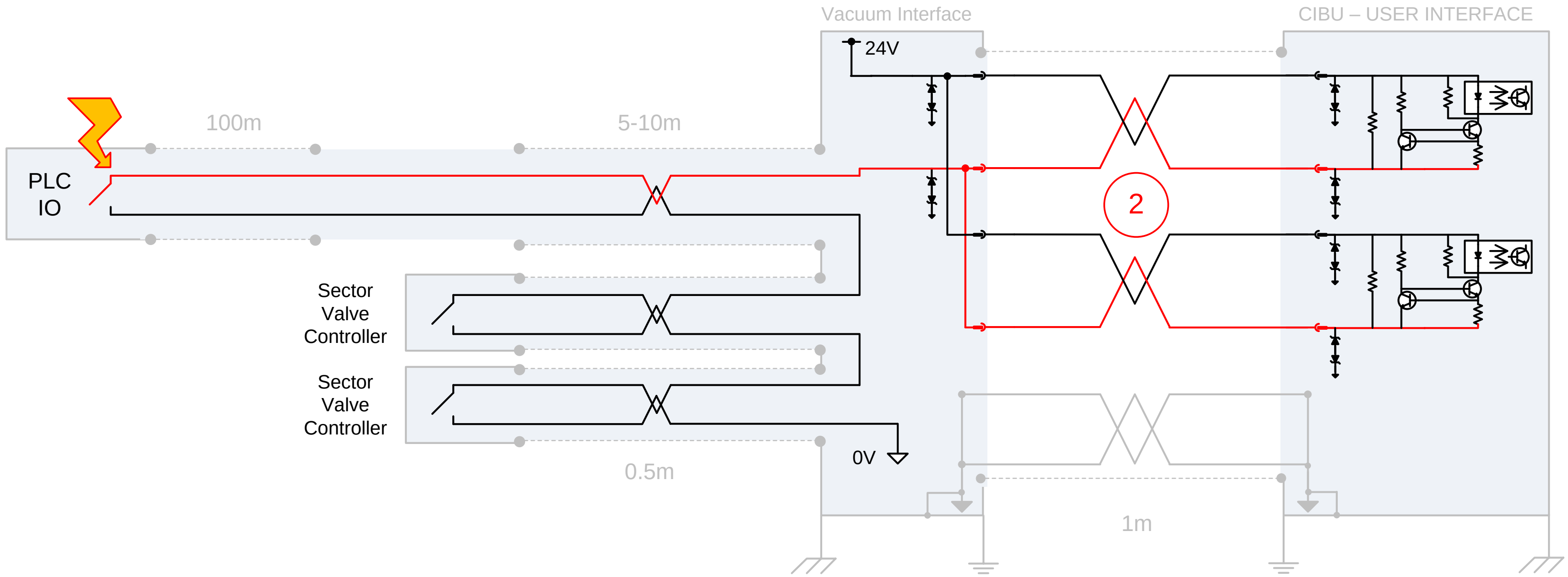
What was the mechanism?

Presumed Failure
1. Excessive Voltage
Is applied in the Access System PLC rack, due to erroneous cabling

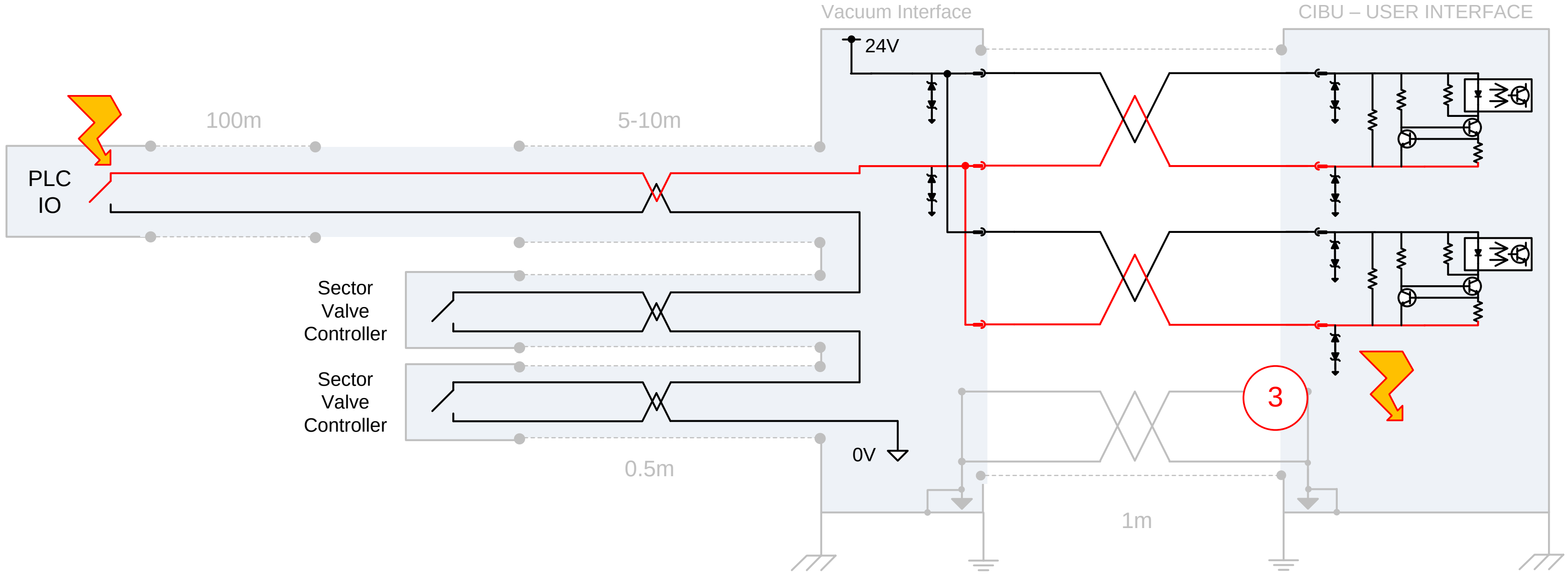


What was the mechanism?

2. This subjects the CIBU negative current loop to an excessive voltage (48V)



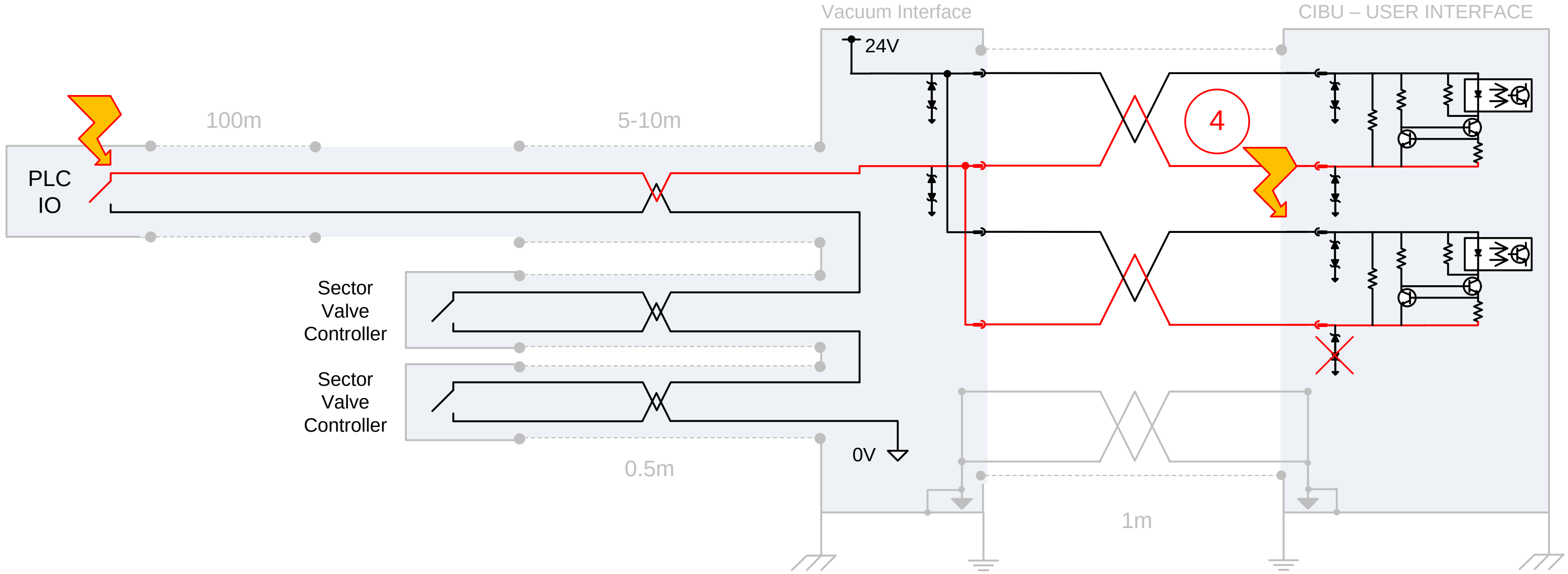
What was the mechanism?



3. The Transient Voltage Supressor (SM6T30CA) Clamps the voltage and dissipates the energy

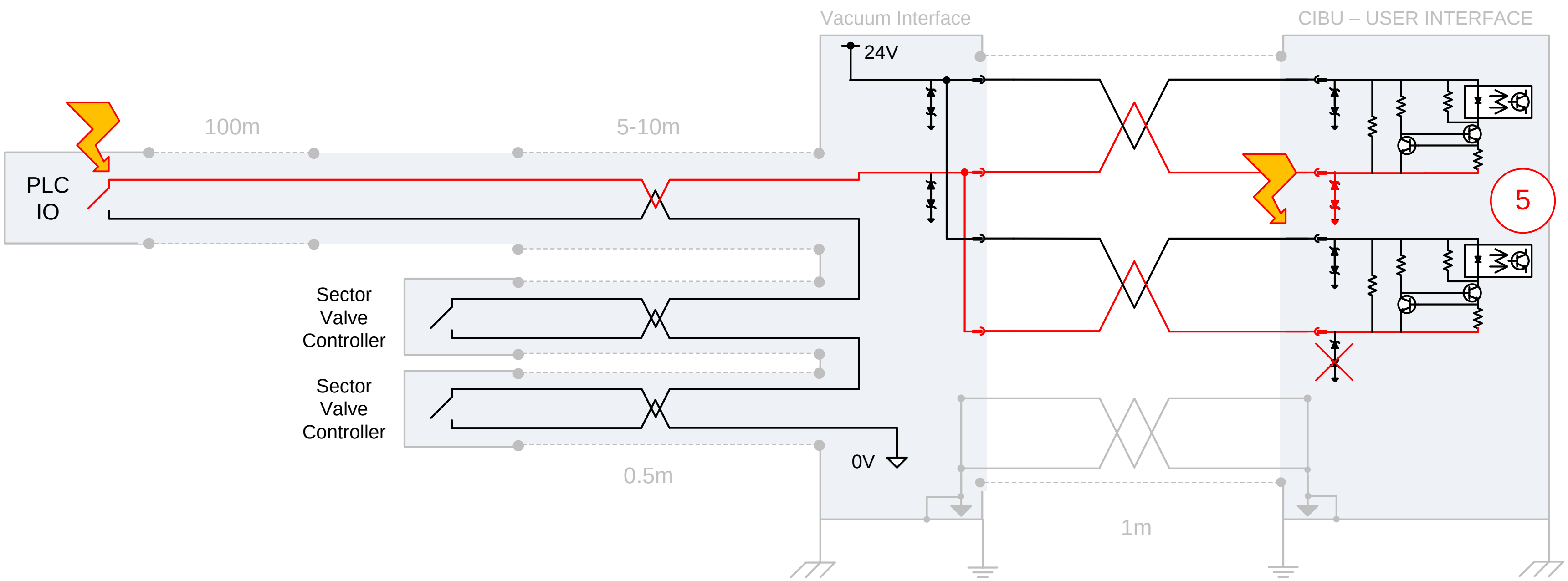
What was the mechanism?

4. Experiments show that after 1-2 seconds the TVS will fail, this TVS fails open-circuit The ‘A’ loop TVS now absorbs the excess



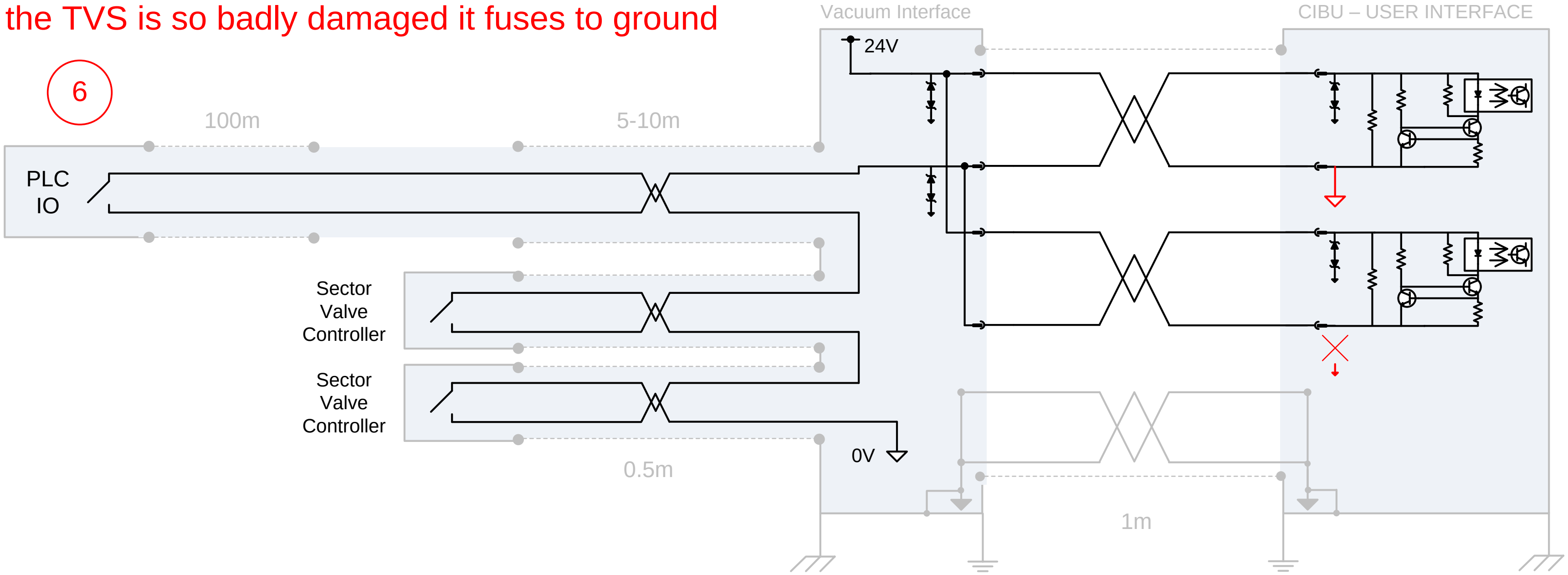
What was the mechanism?

5. 1-2 seconds later this TVS fails short-circuit



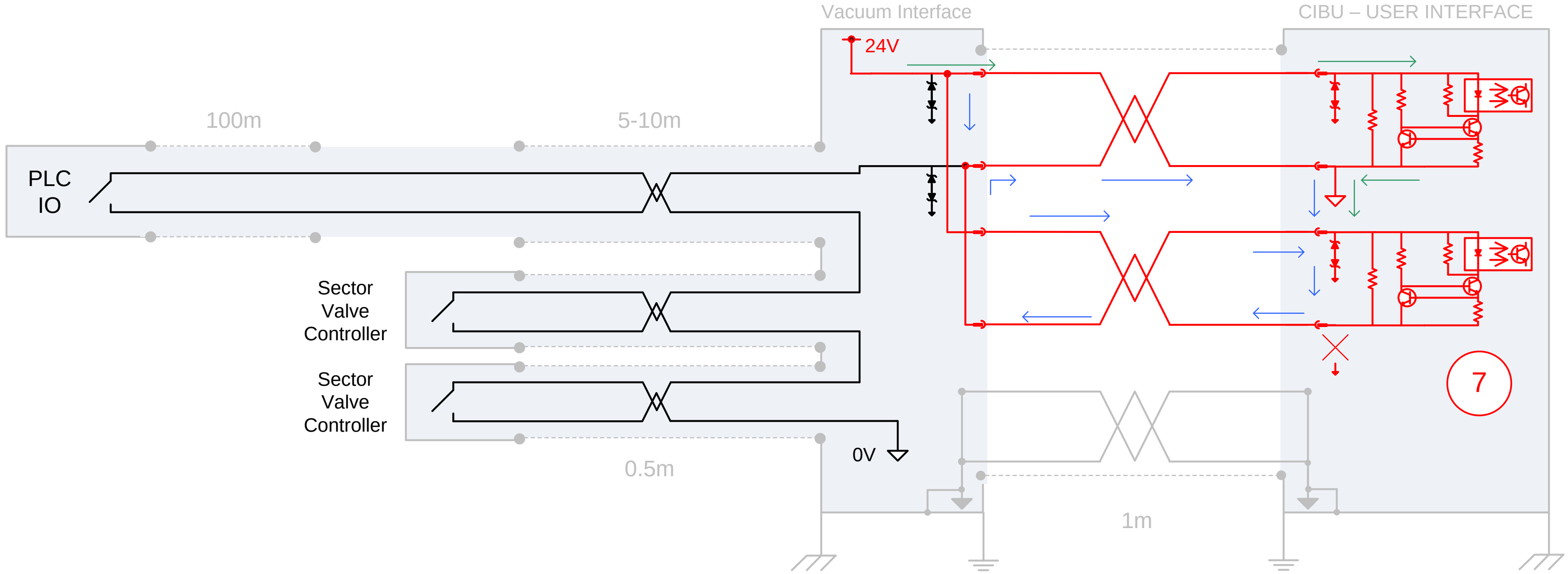
What was the mechanism?

6. The fault is discovered in the ACCESS system and is removed
But the TVS is so badly damaged it fuses to ground



What was the mechanism?

7. At this point both USER PERMIT A and B are stuck TRUE as current flows to ground through A (green) and B (blue) using the damaged TVS



In Summary

Several events = complete Blind Failure

1. Two Equipment systems sharing the same channel
2. PLC Voltage against rules
3. TVS Blocked Short-Circuit
4. Inputs were not redundant
5. Not re-commissioned by MI after a significant change

In addition…

a) Cable length against rules
b) EMC would have been a show-stopper anyway!

Future Work

Shows weaknesses in the interconnection conception:

1. No redundancy = No SIL
2. Can a GND short be mitigated?
3. Human Error can never be 100% eradicated – Testing before each fill should be possible if in doubt!

For each User System

1. Change to use full redundancy
2. Change so a GND fault doesn't fail blind

2nd presentation

3. Automated Test from User Side A /= B

3rd presentation

Intentionally blank (end of 1st part)

Outline

1st presentation: CIBU Failure in UJ33 *(Benjamin TODD)*

- Background
- Before the incident
- The incident
- Future goals

2nd presentation: Proposal cures on HW side *(Bruno PUCCIO)*

- CIBU connection change
- Redundant signals and independent outputs
- Consequences on the Users side

3rd presentation: Proposal for automated test *(Ivan Romera)*

- The purpose
- First implementation on PIC-BIC interfaces
- Proposal & CMW interface with the Users.

The next steps…

Proposed cures

Several events has led to a complete Blind Failure

1. Two different Equipment systems sharing to the same channel → *Vacuum "hosted" E.I.S. connections in 2008*. E.I.S. (managed by Access system) will have theirs **dedicated** channels on 2009

2. PLC Voltage against rules → No additional protection possible with existing design... (only regular tests can "protect")

3 .TVS Blocked Short-Circuit → Slight change of the interface (on User system side) for each connection *(see next slide)*

4. Inputs were not redundant → Redundant signals should be supplied It will become mandatory in 2009. *(see following slide)*

5. Not re-commissioned after change

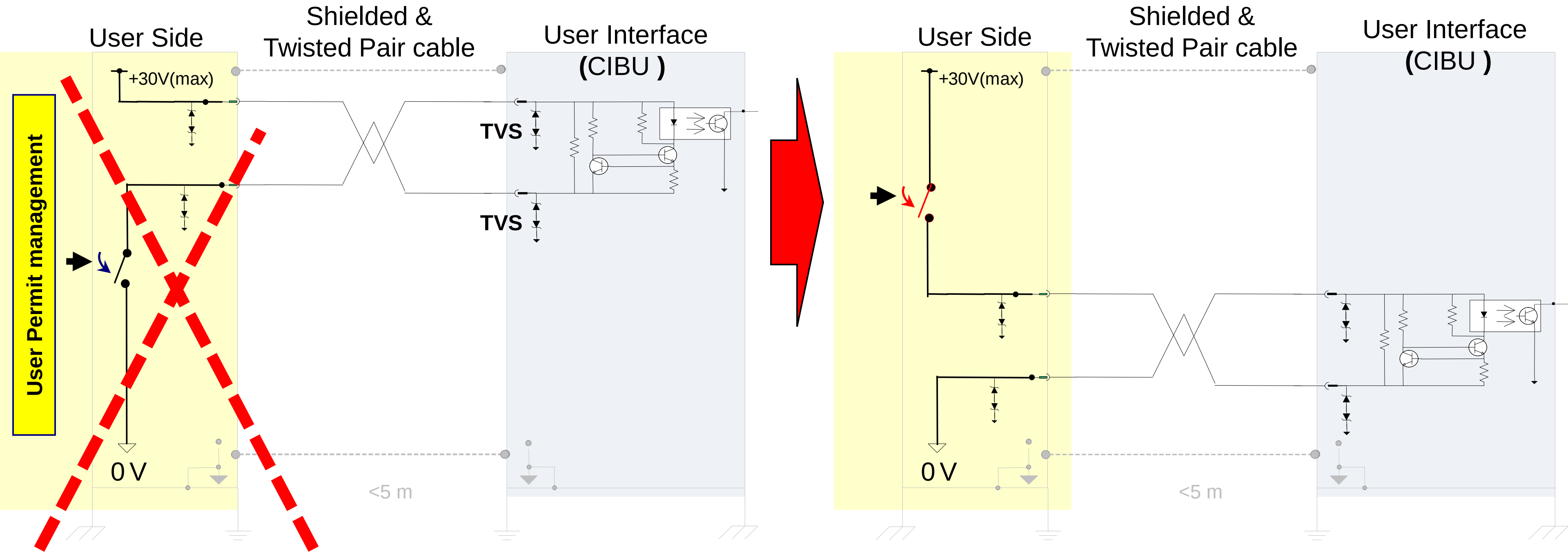
+ Human errors…

+ possible Hardware failure….

→ *Tests, tests and tests…*
in other words: regular tests.
"as frequently as possible" .
Every fill will be the best option
*=> implementation of **Automatic tests***
(see next presentation)

Cure#1: Connection change

On User side, the connection should be modified in order to avoid a fail blind if GND short (i.e. a damaged TVS fuses to ground)



(Same for Input #B)

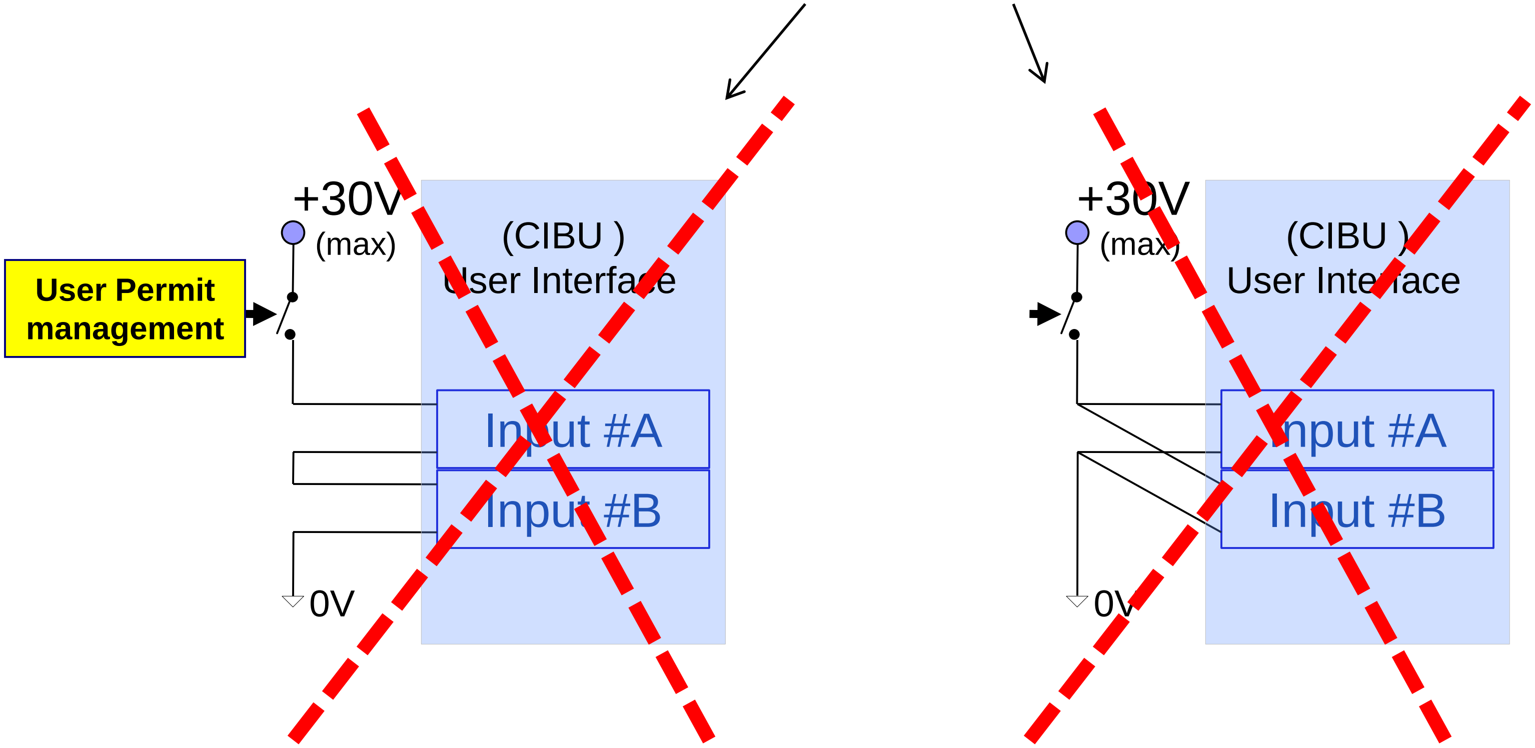
(Same for Input #B)

Cure#2: Redundant signals

1/4

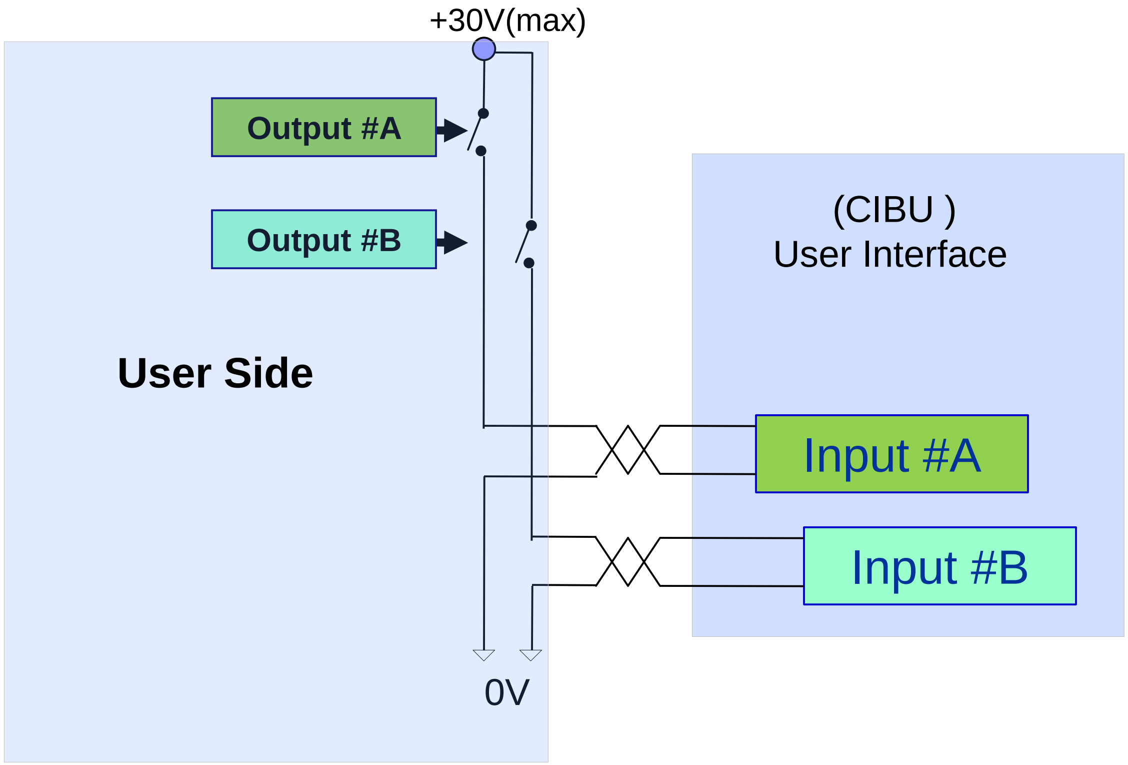
The BIS is fully redundant from CIBU inputs to the outputs to Dump Kickers.

In order to avoid/minimize the single mode failure:
the two CIBU inputs should be no longer linked together
(neither in series nor in //)



Cure#2: Redundant signals

each User system has to provide two independent signals to the CIBU

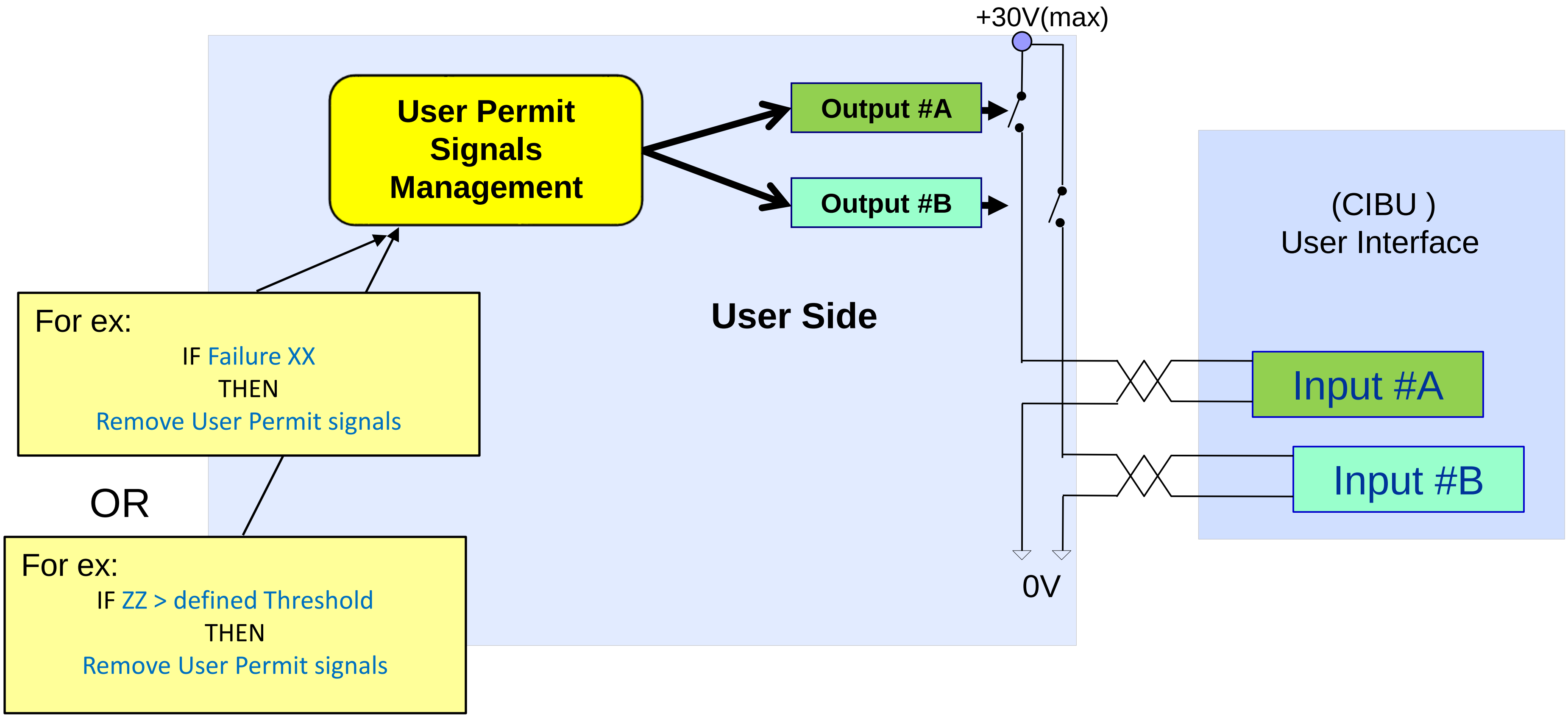


Cure#2: Redundant signals

3/4

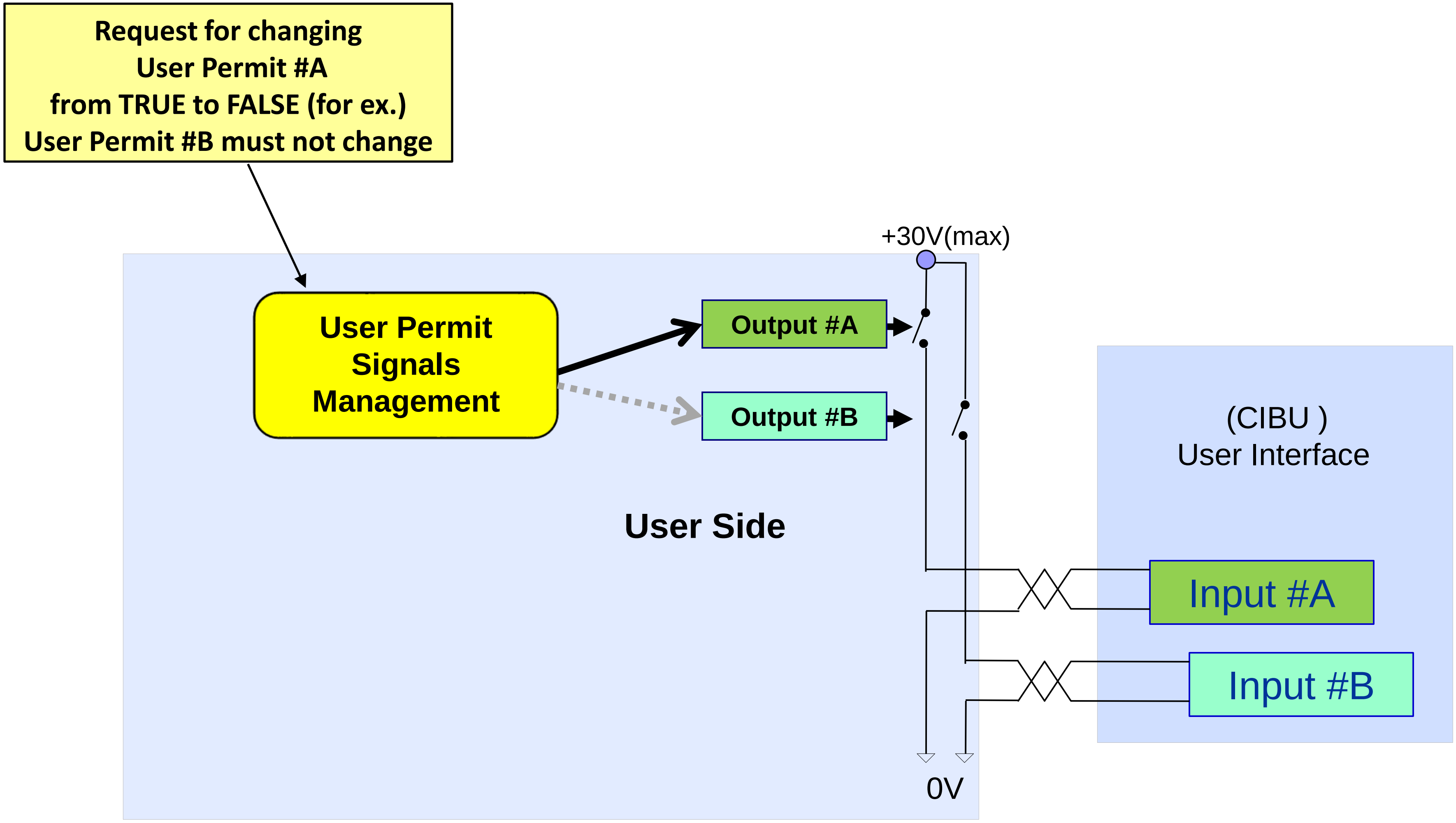
Despite there is a single decision maker…

The aim is to make two physical connections….



Cure#2: Redundant signals

Will be required for automated tests…



Consequences for the Users?

For the redundancy constraint:

As far as we know *(information gathered during the 2008 commissioning)*:
the following systems are not delivering redundant signals:

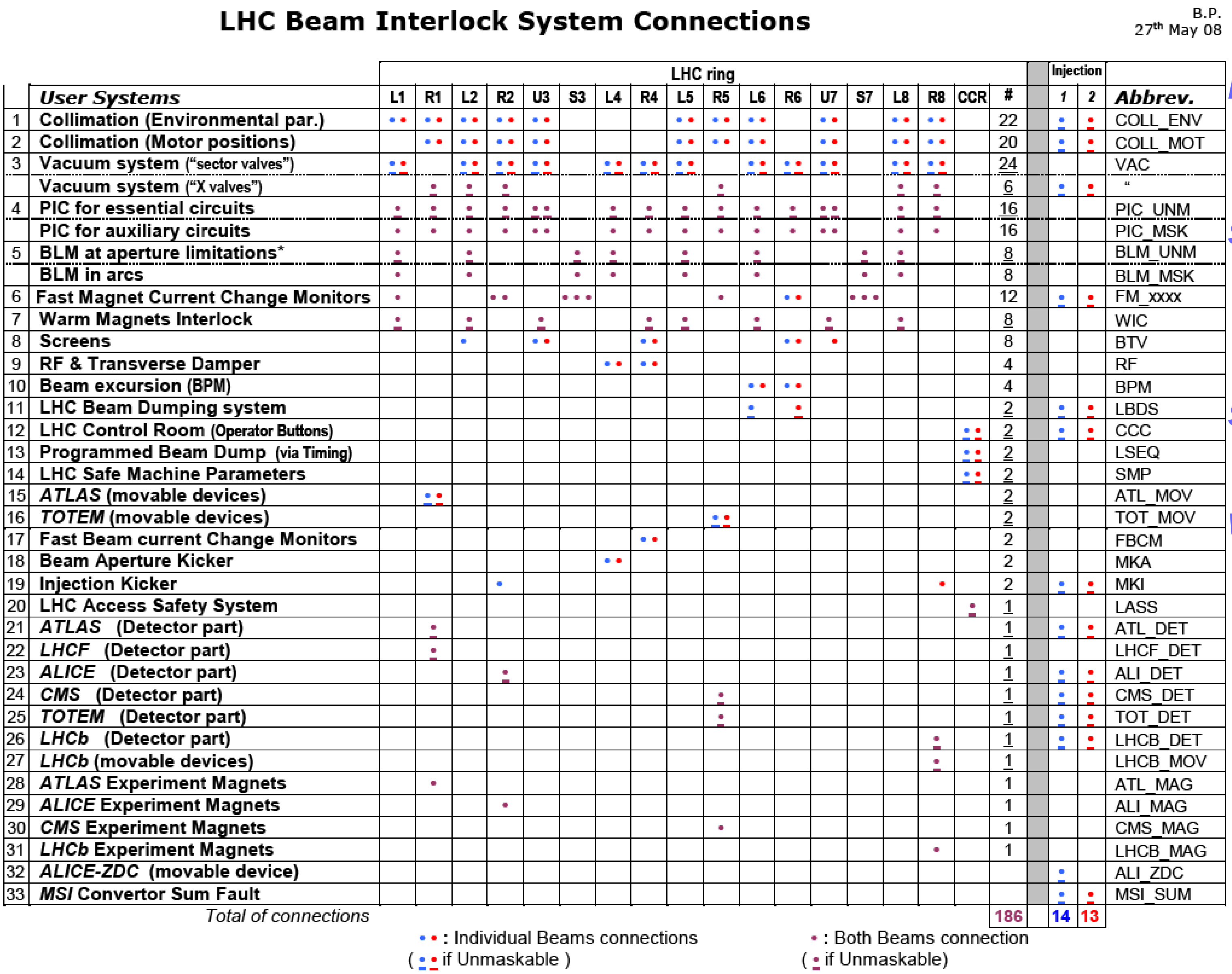
- ALICE magnet, ALICE ZDC
- BPM (Beam Excursion)
- BTV
- CMS (Detector part)
- TOTEM
- MKI2 & MKI8
- PO for the MSI Converter Sum Fault
- RF
- VAC

For the independency of the two outputs activation
and
For the connection change (i.e. move of the “switch”)

We cannot identify because basically
we do not know how it is currently implemented...

Only BLM has kindly sent us the corresponding schematics.

Diversity of BIS Users…



LHC Beam Interlock System Connections

B.P.
27th May 08

		LHC ring																		Injection		
	User Systems	L1	R1	L2	R2	U3	S3	L4	R4	L5	R5	L6	R6	U7	S7	L8	R8	CCR	#		*1*	*2*	***Abbrev.***
1	Collimation (Environmental par.)	🔵🔴	🔵🔴	🔵🔴	🔵🔴	🔵🔴				🔵🔴	🔵🔴	🔵🔴		🔵🔴		🔵🔴	🔵🔴		22		🔵	🔴	COLL_ENV
2	Collimation (Motor positions)		🔵🔴	🔵🔴	🔵🔴	🔵🔴				🔵🔴	🔵🔴	🔵🔴		🔵🔴		🔵🔴	🔵🔴		20		🔵	🔴	COLL_MOT
3	Vacuum system (“sector valves”)	🔵🔴		🔵🔴	🔵🔴	🔵🔴		🔵🔴	🔵🔴	🔵🔴		🔵🔴	🔵🔴	🔵🔴		🔵🔴	🔵🔴		24				VAC
	Vacuum system (“X valves”)		🟣	🟣	🟣						🟣					🟣	🟣		6		🔵	🔴	“
4	PIC for essential circuits	🟣	🟣	🟣	🟣	🟣🟣		🟣	🟣	🟣	🟣	🟣	🟣	🟣🟣		🟣	🟣		16				PIC_UNM
	PIC for auxiliary circuits	🟣	🟣	🟣	🟣	🟣🟣		🟣	🟣	🟣	🟣	🟣	🟣	🟣🟣		🟣	🟣		16				PIC_MSK
5	BLM at aperture limitations*	🟣		🟣			🟣	🟣		🟣		🟣			🟣	🟣			8				BLM_UNM
	BLM in arcs	🟣		🟣			🟣	🟣		🟣		🟣			🟣	🟣			8				BLM_MSK
6	Fast Magnet Current Change Monitors	🟣			🟣🟣		🟣🟣🟣				🟣		🔵🔴		🟣🟣🟣				12		🔵	🔴	FM_xxxx
7	Warm Magnets Interlock	🟣		🟣		🟣			🟣	🟣		🟣		🟣		🟣			8				WIC
8	Screens			🔵		🔵🔴			🔵🔴				🔵🔴	🔴					8				BTV
9	RF & Transverse Damper							🔵🔴	🔵🔴										4				RF
10	Beam excursion (BPM)											🔵🔴	🔵🔴						4				BPM
11	LHC Beam Dumping system											🔵	🔴						2		🔵	🔴	LBDS
12	LHC Control Room (Operator Buttons)																	🔵🔴	2		🔵	🔴	CCC
13	Programmed Beam Dump (via Timing)																	🔵🔴	2				LSEQ
14	LHC Safe Machine Parameters																	🔵🔴	2				SMP
15	*ATLAS* (movable devices)		🔵🔴																2				ATL_MOV
16	*TOTEM* (movable devices)										🔵🔴								2				TOT_MOV
17	Fast Beam current Change Monitors								🔵🔴										2				FBCM
18	Beam Aperture Kicker							🔵🔴											2				MKA
19	Injection Kicker				🔵												🔴		2		🔵	🔴	MKI
20	LHC Access Safety System																	🟣	1				LASS
21	*ATLAS* (Detector part)		🟣																1		🔵	🔴	ATL_DET
22	*LHCF* (Detector part)		🟣																1				LHCF_DET
23	*ALICE* (Detector part)				🟣														1		🔵	🔴	ALI_DET
24	*CMS* (Detector part)										🟣								1		🔵	🔴	CMS_DET
25	*TOTEM* (Detector part)										🟣								1		🔵	🔴	TOT_DET
26	*LHCb* (Detector part)																🟣		1		🔵	🔴	LHCB_DET
27	*LHCb* (movable devices)																🟣		1				LHCB_MOV
28	*ATLAS* Experiment Magnets		🟣																1				ATL_MAG
29	*ALICE* Experiment Magnets				🟣														1				ALI_MAG
30	*CMS* Experiment Magnets										🟣								1				CMS_MAG
31	*LHCb* Experiment Magnets																🟣		1				LHCB_MAG
32	*ALICE-ZDC* (movable device)																				🔵		ALI_ZDC
33	*MSI* Convertor Sum Fault																				🔵	🔴	MSI_SUM
	Total of connections																		186		14	13	

🔵🔴 : Individual Beams connections
(🔵🔴 if Unmaskable)

🟣 : Both Beams connection
(🟣 if Unmaskable)

Difficult to evaluate the impact on the Users.

Same for the implementation of Automated tests.

Should be seen case by case.

We are obviously willing to help and to collaborate.

Intentionally blank (end of 2ndpart)

Outline

1st presentation: CIBU Failure in UJ33 *(Benjamin TODD)*

- Background
- Before the incident
- The incident
- Future goals

2nd presentation: Proposal cures *(Bruno PUCCIO)*

- CIBU connection change
- Redundant signals and independent outputs
- Consequences on the Users side

3rd presentation: Proposal for automated test *(Ivan Romera)*

- The purpose
- First implementation on PIC-BIC interfaces
- Proposal & CMW interface with the Users.

The next steps…

The purpose

1. BIS side:

Test that all HW links from User Systems to CIBUs are working correctly

- ensure that each User system is able to give/remove both Permits
- guarantee no blind failures (electronic part)
- Forms part of BIS pre-operation checks
- will be launched by the LHC Sequencer
- Frequency not yet decided (every month? every week? every fill?...)

2. Machine protection side:

Test could be also used in order to check that the full chain is working correctly

The way to perform the test will be different for each system

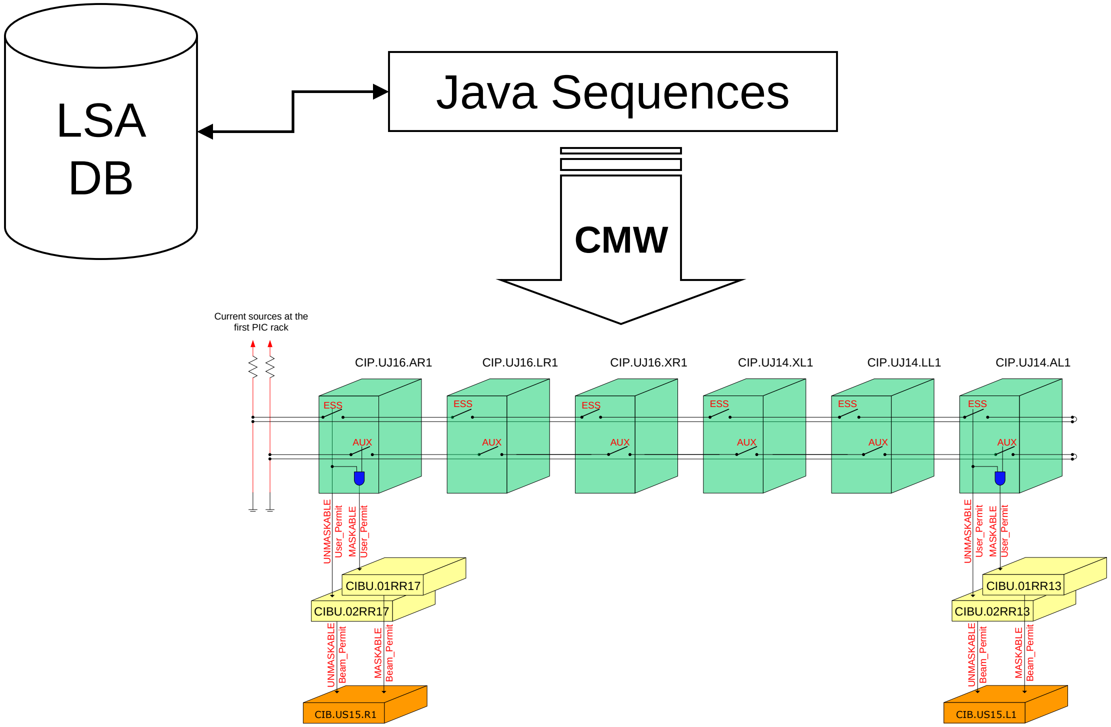
(for ex: how to proceed with thousands of BLMs channels?

in addition, not possible to move each vacuum valves, etc…)

Should be discussed case by case => chosen solution endorsed by MPP.

BIC-PIC first experiences

- Automated tests successfully developed and tested during the HWC
- Integration in the Sequencer Framework
- BICs communication already implemented
- LSA database for configuration and storing results



Automated tests proposal

1. Request to the User from external system (SEQ) to enter in Test Mode

2. User in Test Mode?

   acknowledge by checking the Beam Permit Info (if connected)

3. Loop through all the Users involved in the test:

   3.1. Initial conditions OK for BIC and User? (both Channels A/B are FALSE)

   3.2. Set Channel A and Channel B independently on User side

   3.3. Verify consistency on the BIC side

   3.4. Reset failure conditions

   3.5. Save results to Database (LSA?)

CMW Interface with users

1. Name of the property CibuTest.

2. Property should allow setting and getting - set/get type.

2. Fields of the property: A, B, Test - all boolean type.

3. Partial set should be implemented.

4. Server action implementation of this property, should ensure boolean complementary, that means when the A field is set, B isn´t and viceversa when the B field is set, A isn´t.

5. When user try to set both A and B at the same state in one call then an exception should be thrown and nothing should be changed.

Intentionally blank (end of 3rd part)

The next steps

1. Give time to evaluate the proposals

2. Discussion for the feasibility and the timescale with each User

3. Summary of requests/issues presented in the framework of coming MPP meeting (possibly on 2nd or 3rd week of Feb.09)

4. Setting up of schedule for re-commissioning

5. Give support and discuss in case of issue

FIN