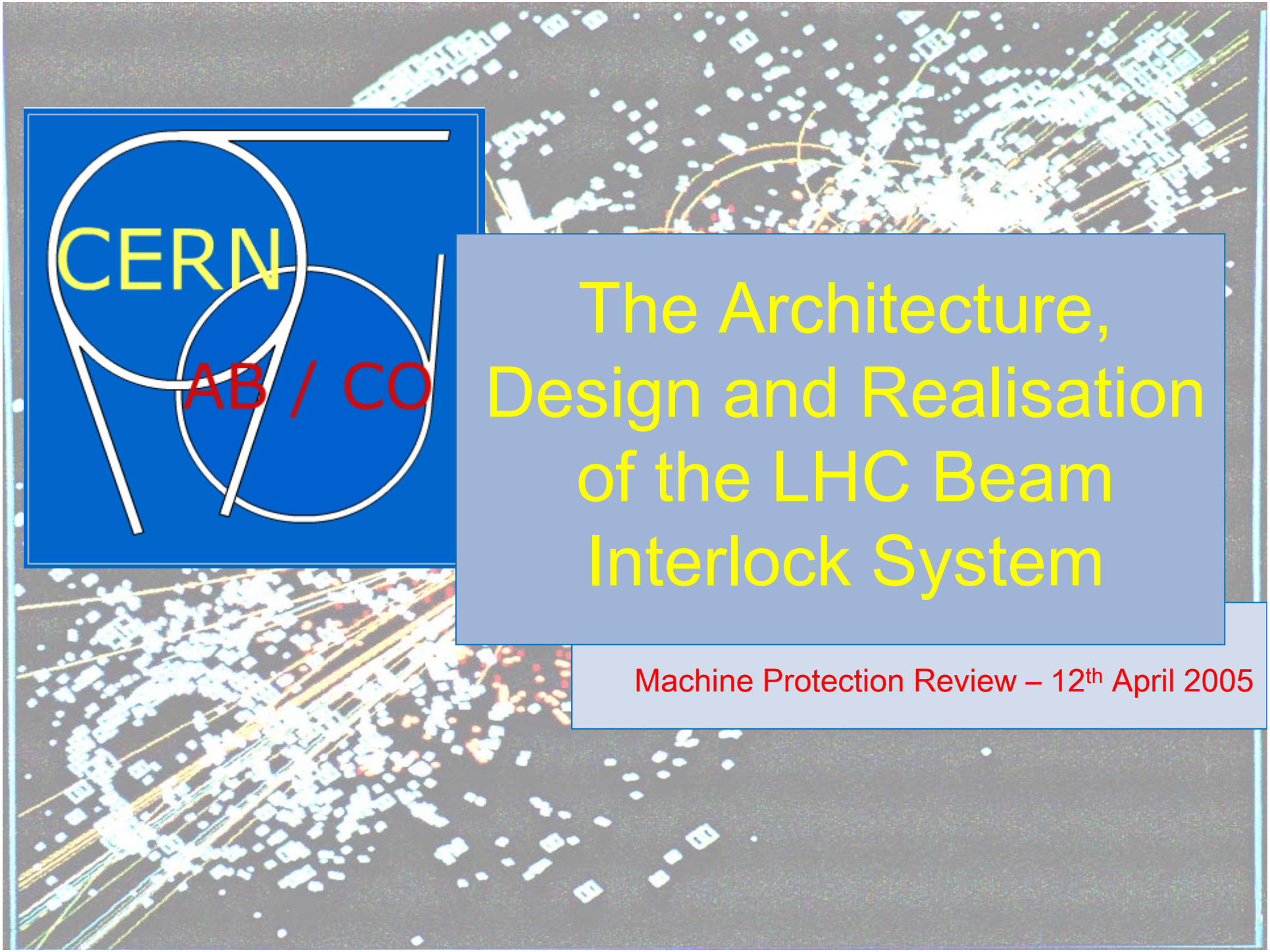


The Architecture, Design and Realisation of the LHC Beam Interlock System

Machine Protection Review – 12th April 2005

The LHC Beam Interlock System

1. Overview and Architecture
   - History
   - Specification
   - BIS Design
   - Communication strategies
   - EMC
   - Testing, Installation, Commissioning and Starting LHC

2. Dependability Analysis
   - Reliability, Safety and Maintainability
   - Typical Figures

3. Summing Up
   - Typical Response
   - Next goals

The LHC Beam Interlock System

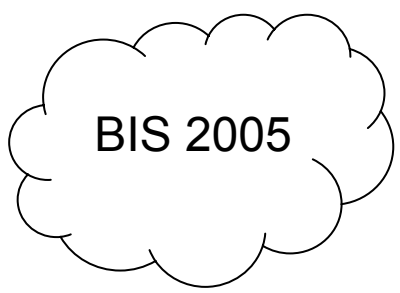
1. Overview and Architecture
   - History
   - Specification
   - BIS Design
   - Communication strategies
   - EMC
   - Testing, Installation, Commissioning and Starting LHC

2. Dependability Analysis
   - Reliability, Safety and Maintainability
   - Typical Figures

3. Summing Up
   - Typical Response
   - Next goals

A bit of history

2001	Beam Interlock System Proposed	BNL / DESY systems used as a basis
2002-2003	System architecture Basic development	Tested in TI8 AUTUMN 2003
2004	Current Loops Fibre Optic 'Permit Loops' Masking	Tested in TI8 AUTUMN 2004
2005	Dependability & EMC Programmable Logic	Testing in SPS AUTUMN 2005
2006	SPS, CNGS, Sector 7-8 Installation & Commissioning	
2007	Remaining LHC Installation & Commissioning	

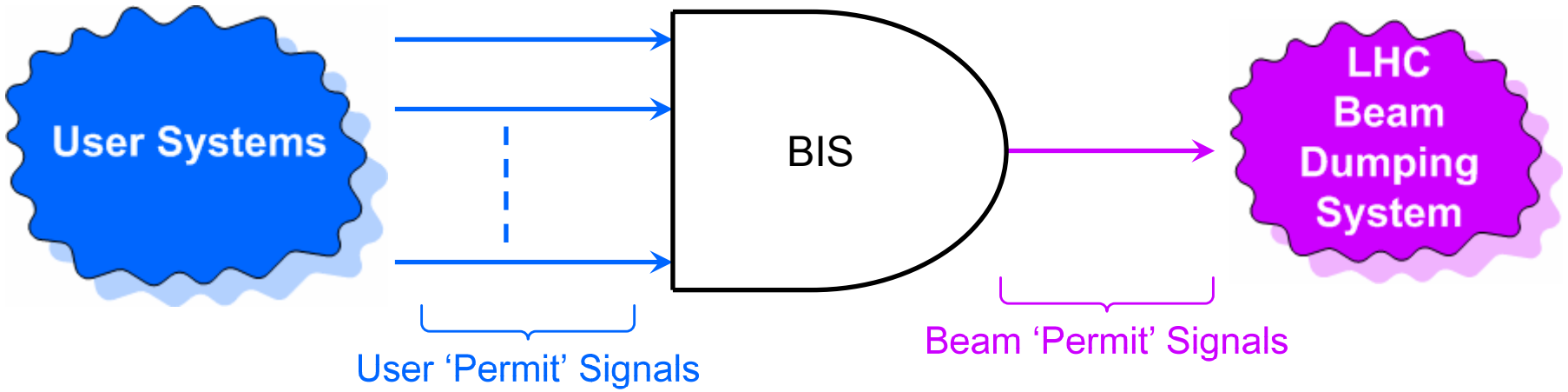


Design Specification

1. A CERN-wide generic Beam Interlock System — LHC, SPS, CNGS etc.
2. Fast — ~70μs over 28km
3. Safe — Requesting Beam Dump = SIL 3
4. High Test Coverage — On startup – 'As Good As New'
5. Maintainable — Low repair time
6. Monitorable — Self-Diagnosing
Provides first Post Mortem info
7. Cost Effective — Protects $$$ but need not be $$$
8. Deterministic — Know what it's going to do & when

This presentation considers only the **LHC** BIS!

Function



153 User Systems distributed over 28kms

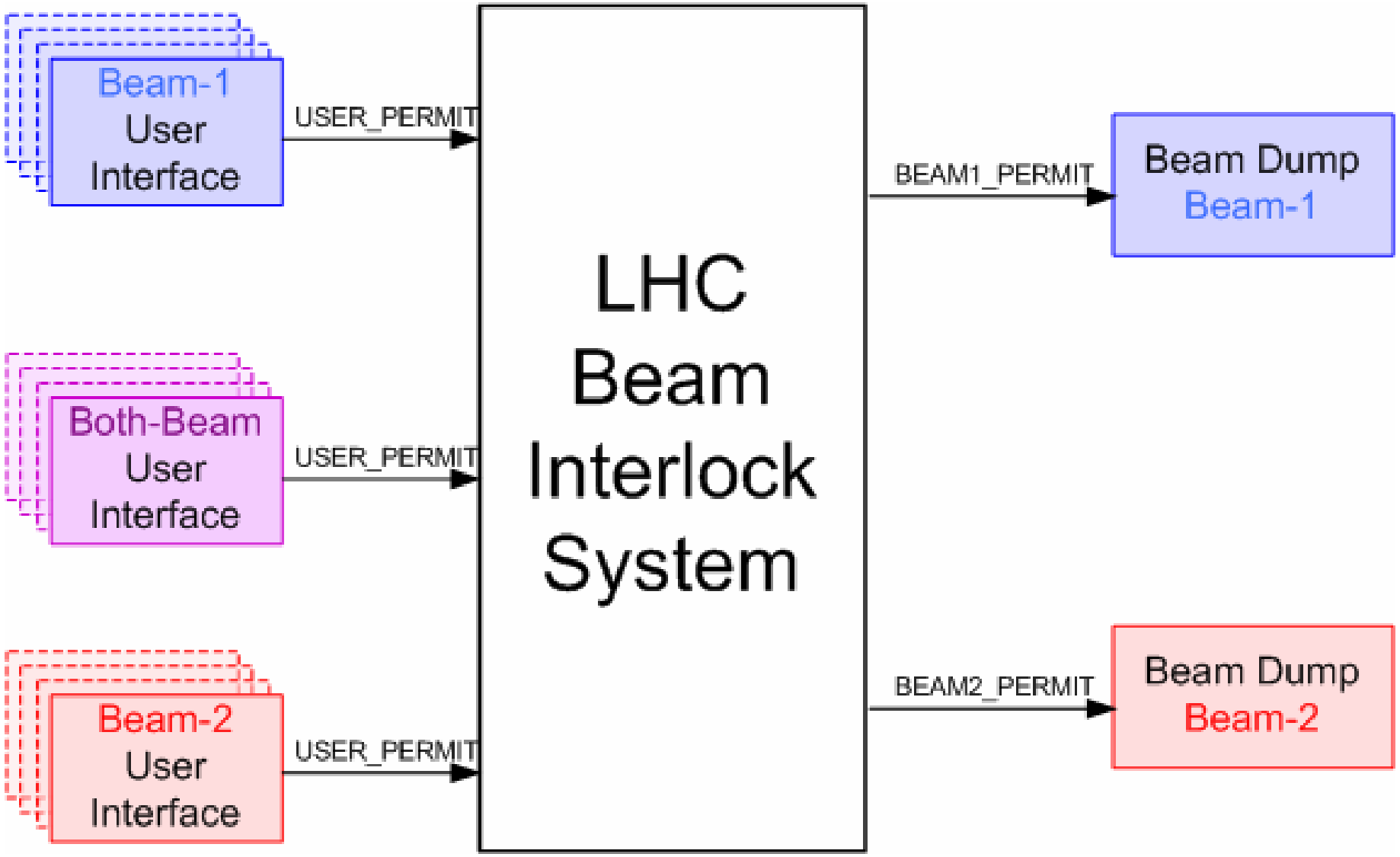
LHC has 2 Beams

Some User Systems give simultaneous permit — Both-Beam

Others give independent permit — Beam-1, Beam-2

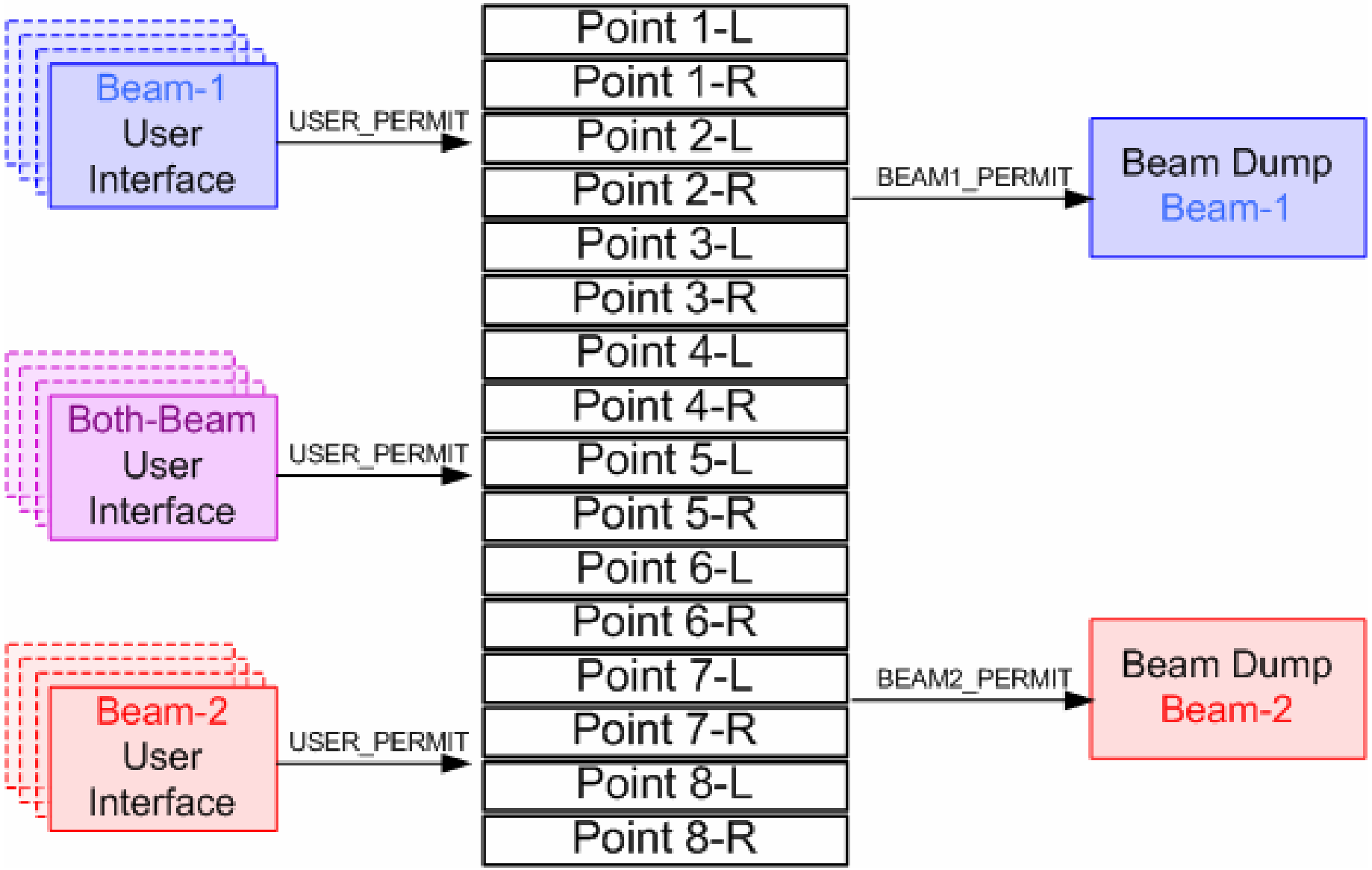
Types of User

In LHC, BIS forms a transparent layer from User System to Beam Dump



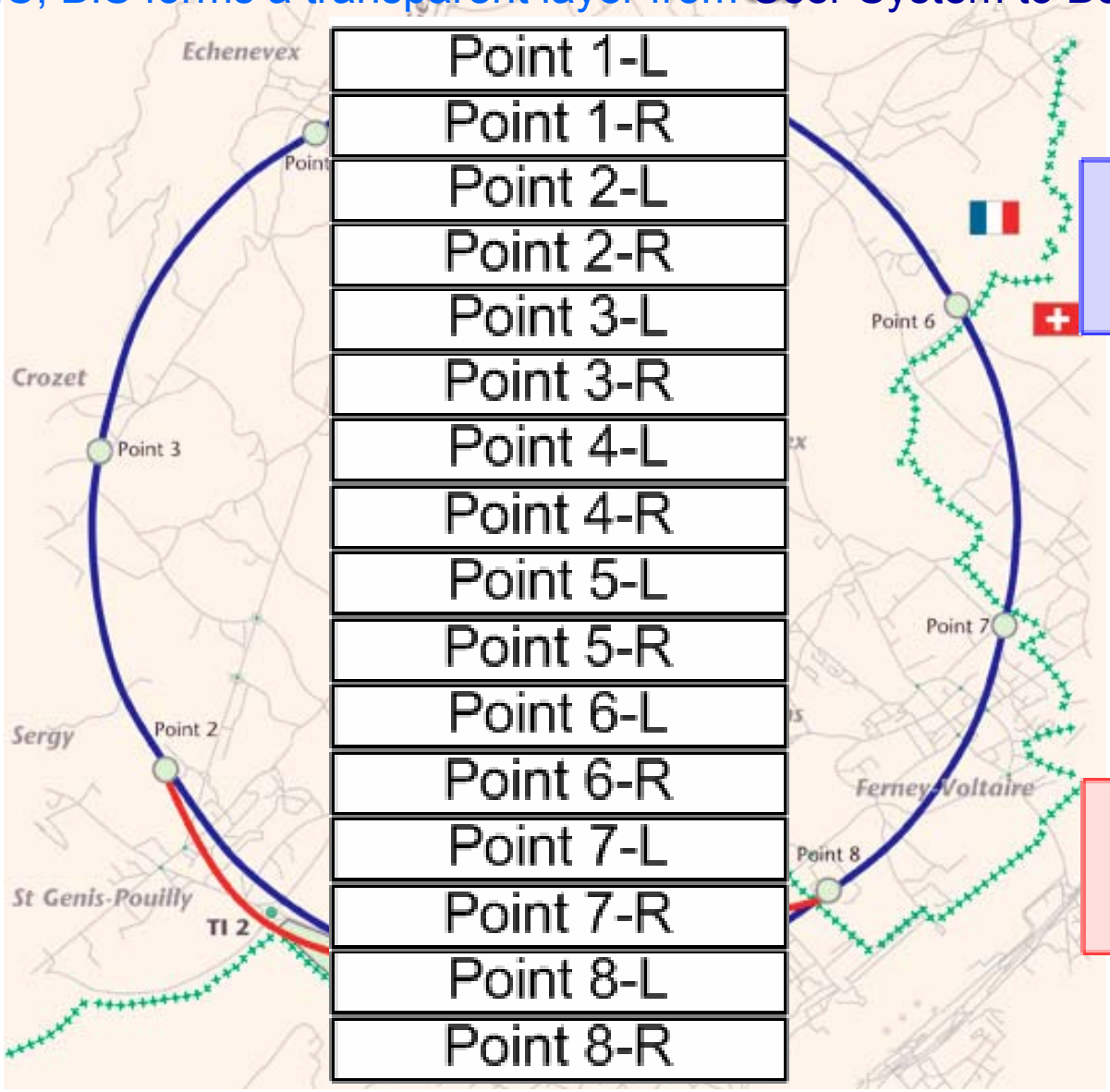
Types of User

In LHC, BIS forms a transparent layer from User System to Beam Dump



Types of User

In LHC, BIS forms a transparent layer from User System to Beam Dump



Beam Permit Loops & BICs

4 fibre-optic channels from Point 6
1 clockwise &
1 anticlockwise for **each** Beam

10MHz Square wave generated at IP6
-Signal can be cut by any Controller
-Signal can be monitored by any Controller

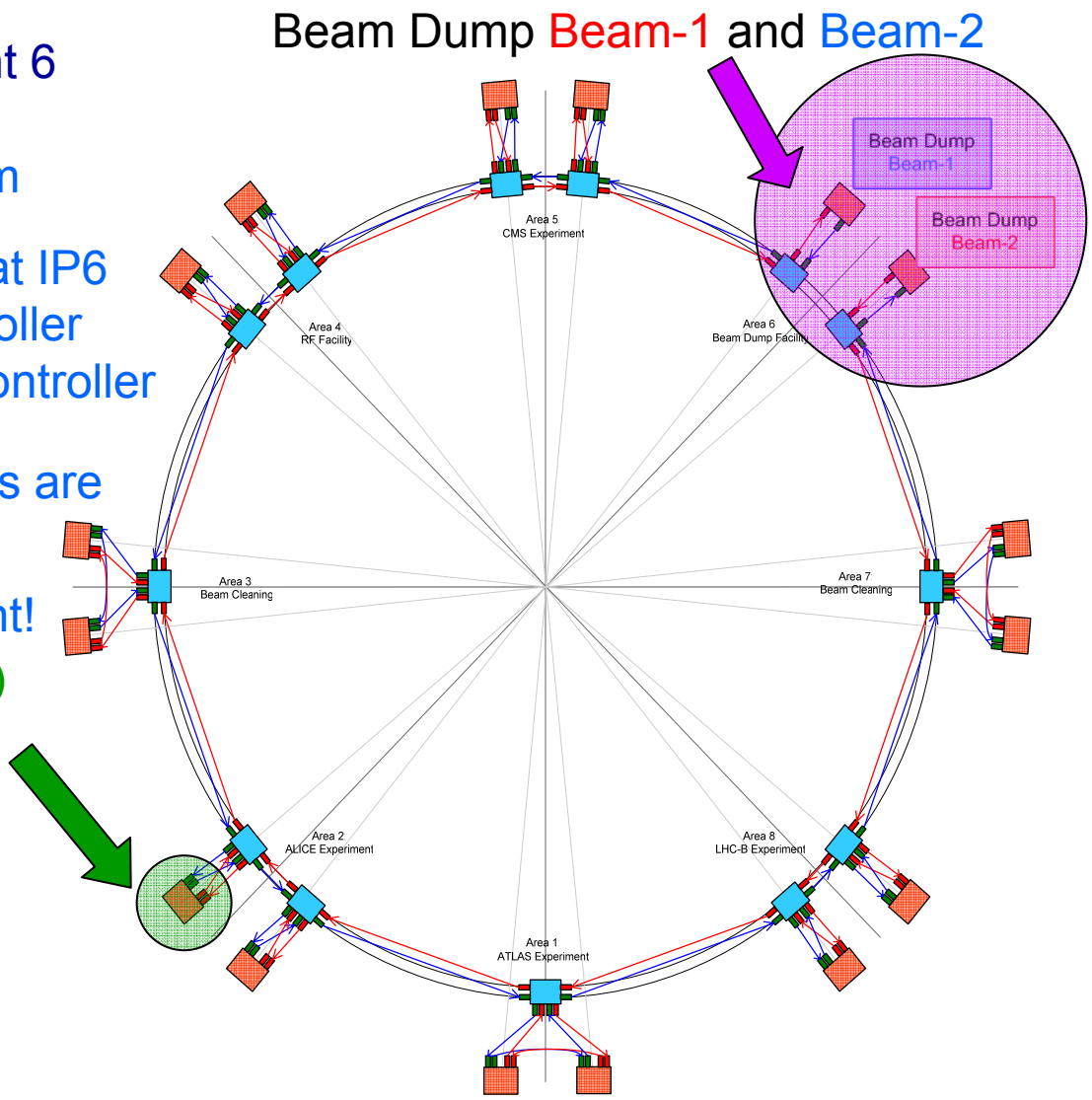
When any of the four 10MHz signals are absent at IP6, BEAM DUMP!

Beam-1 / Beam-2 are Independent!

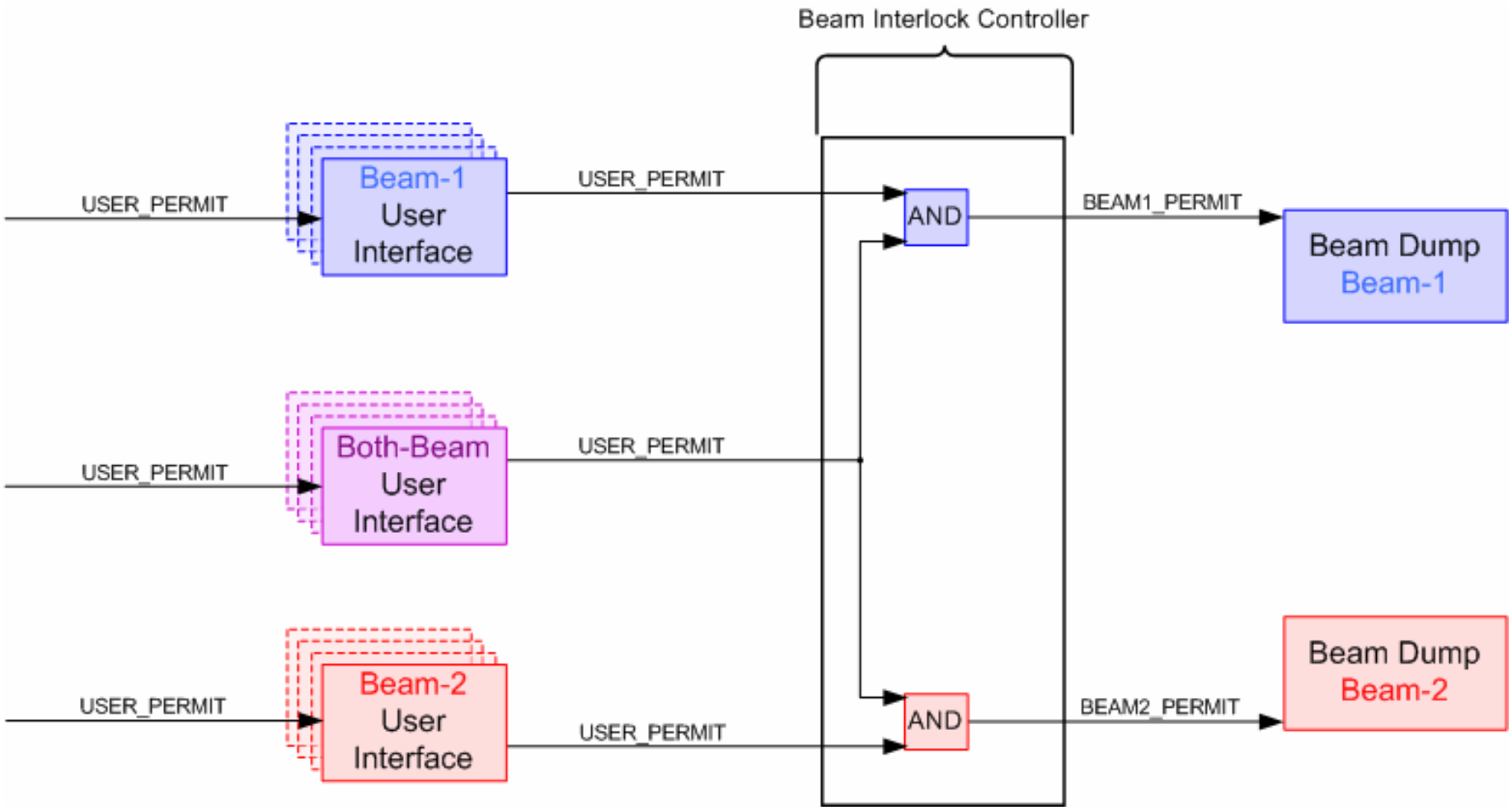
Beam Interlock Controllers (BIC)

16 BICs
- Two at each Insertion Point

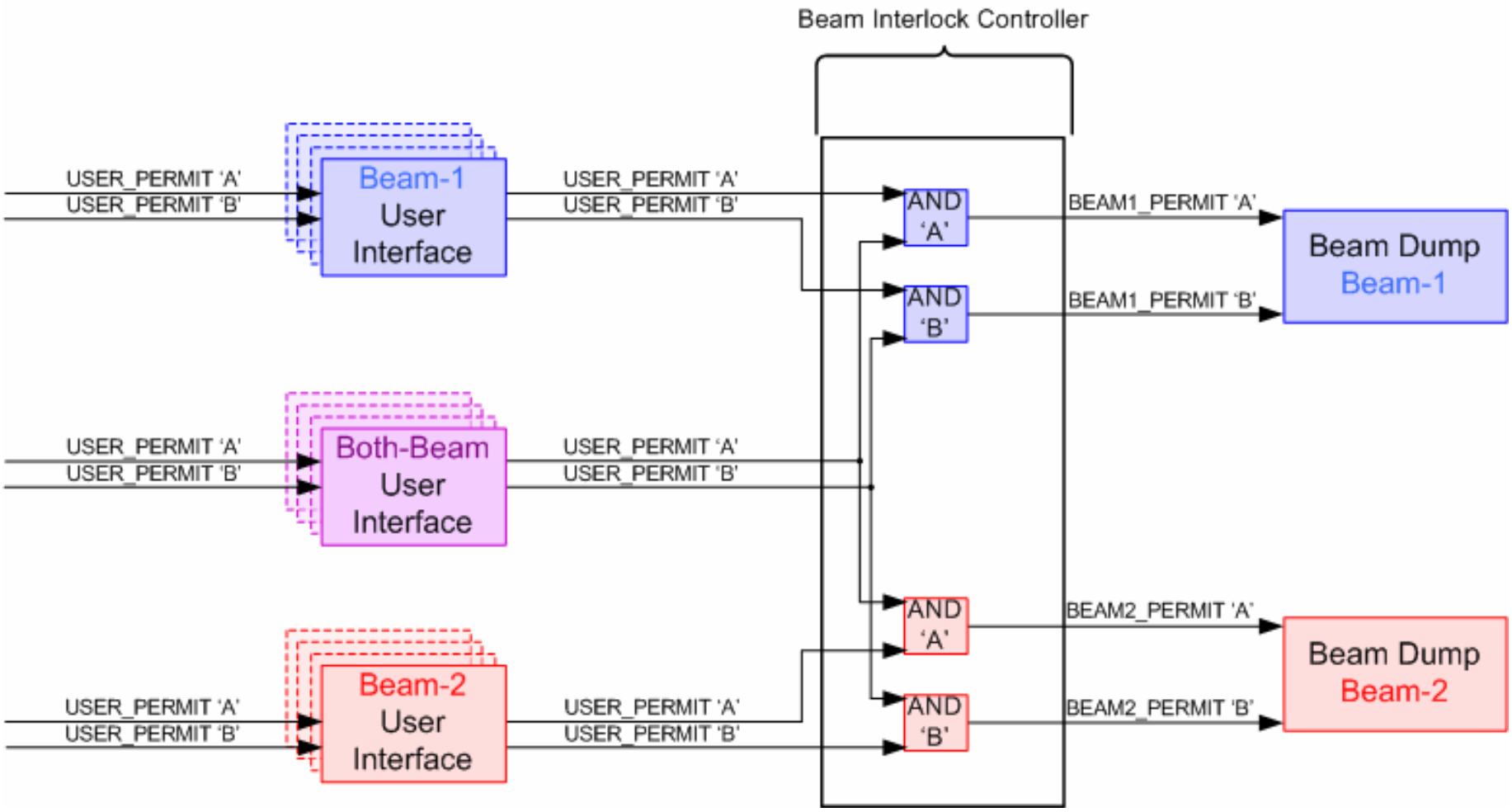
Up to 20 User Systems per BIC
6 x Beam-1
8 x Both-Beam
6 x Beam-2



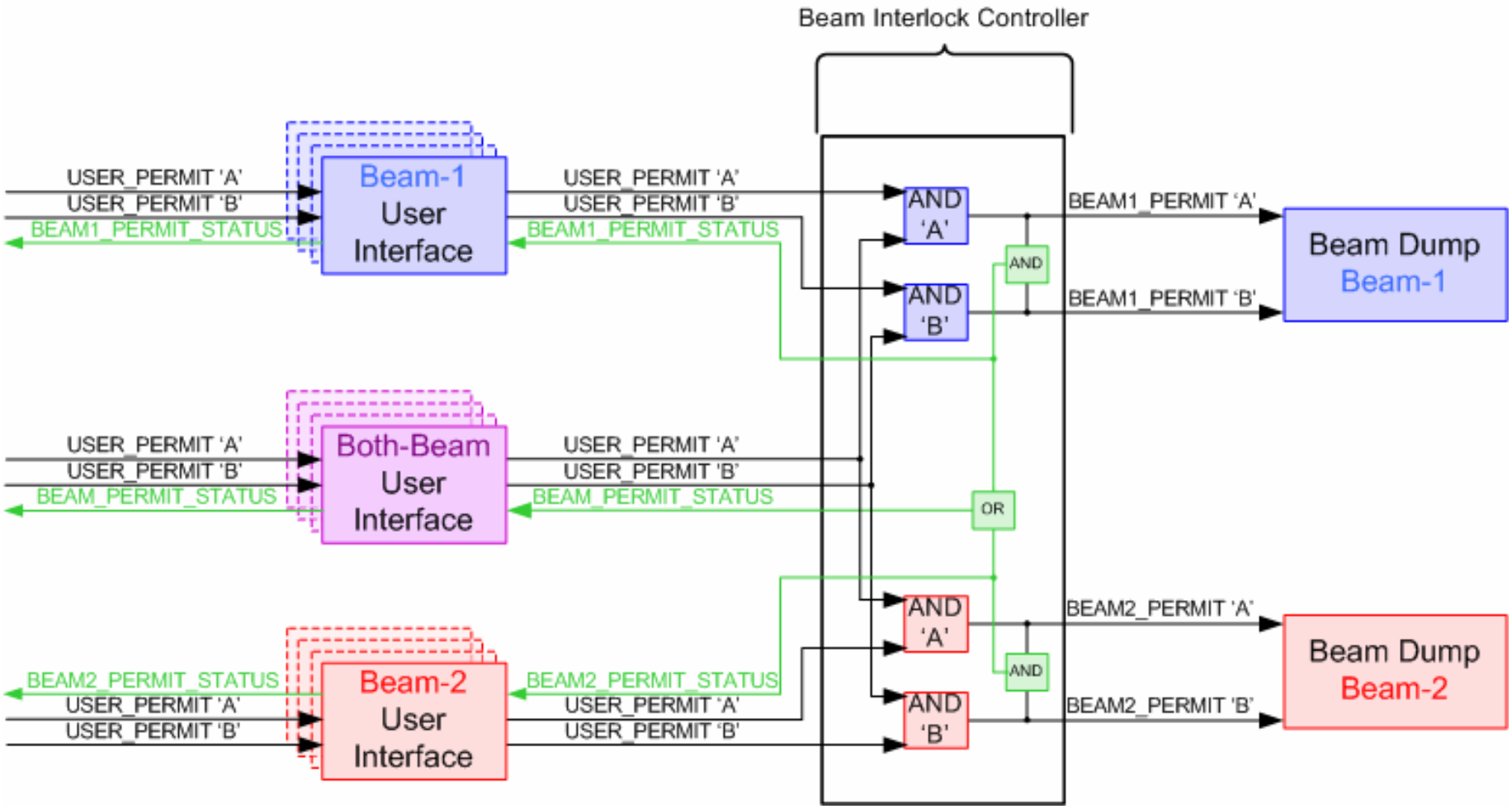
Controller Block Diagram



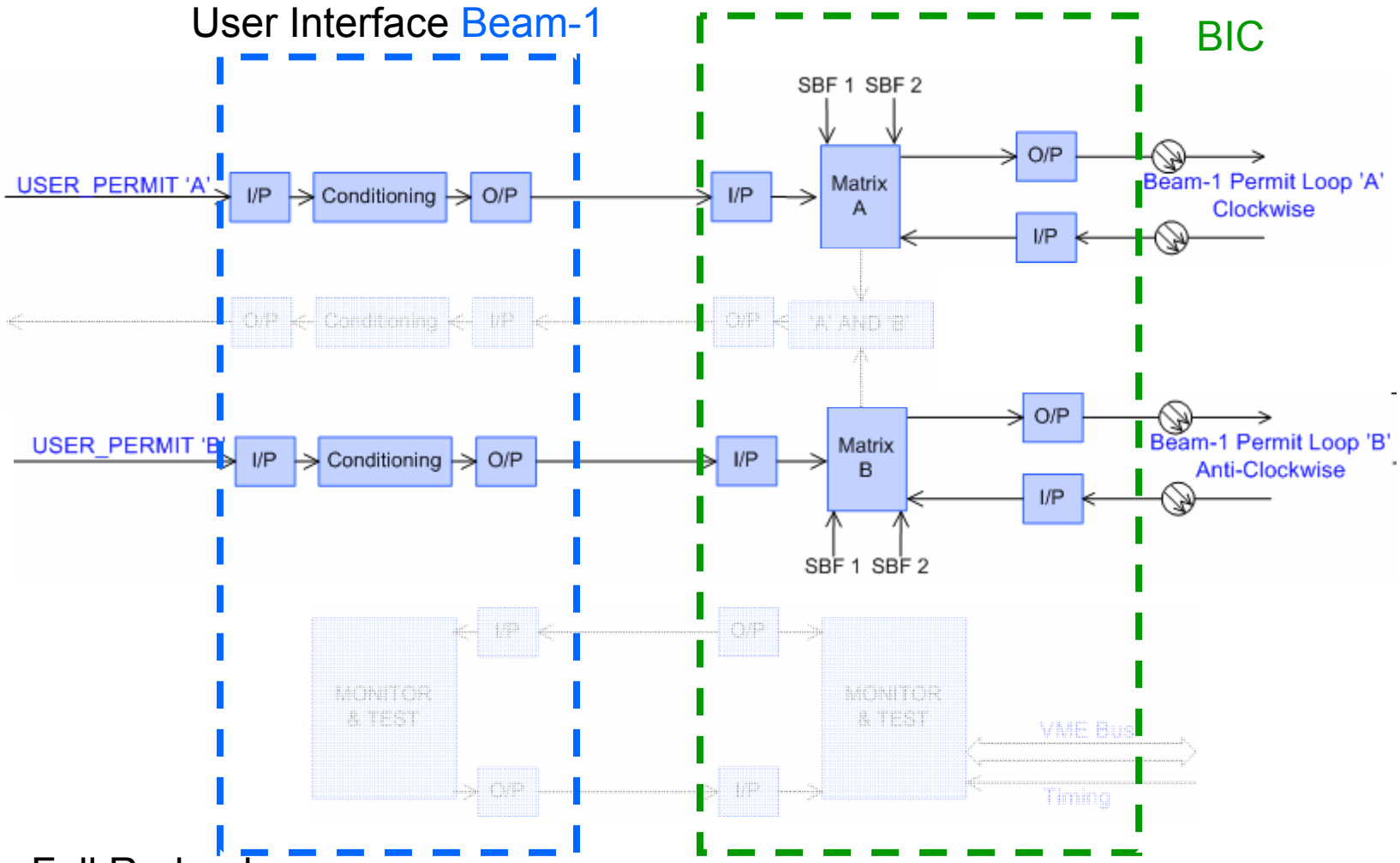
Controller Block Diagram



Controller Block Diagram



Mission Critical Information Flow

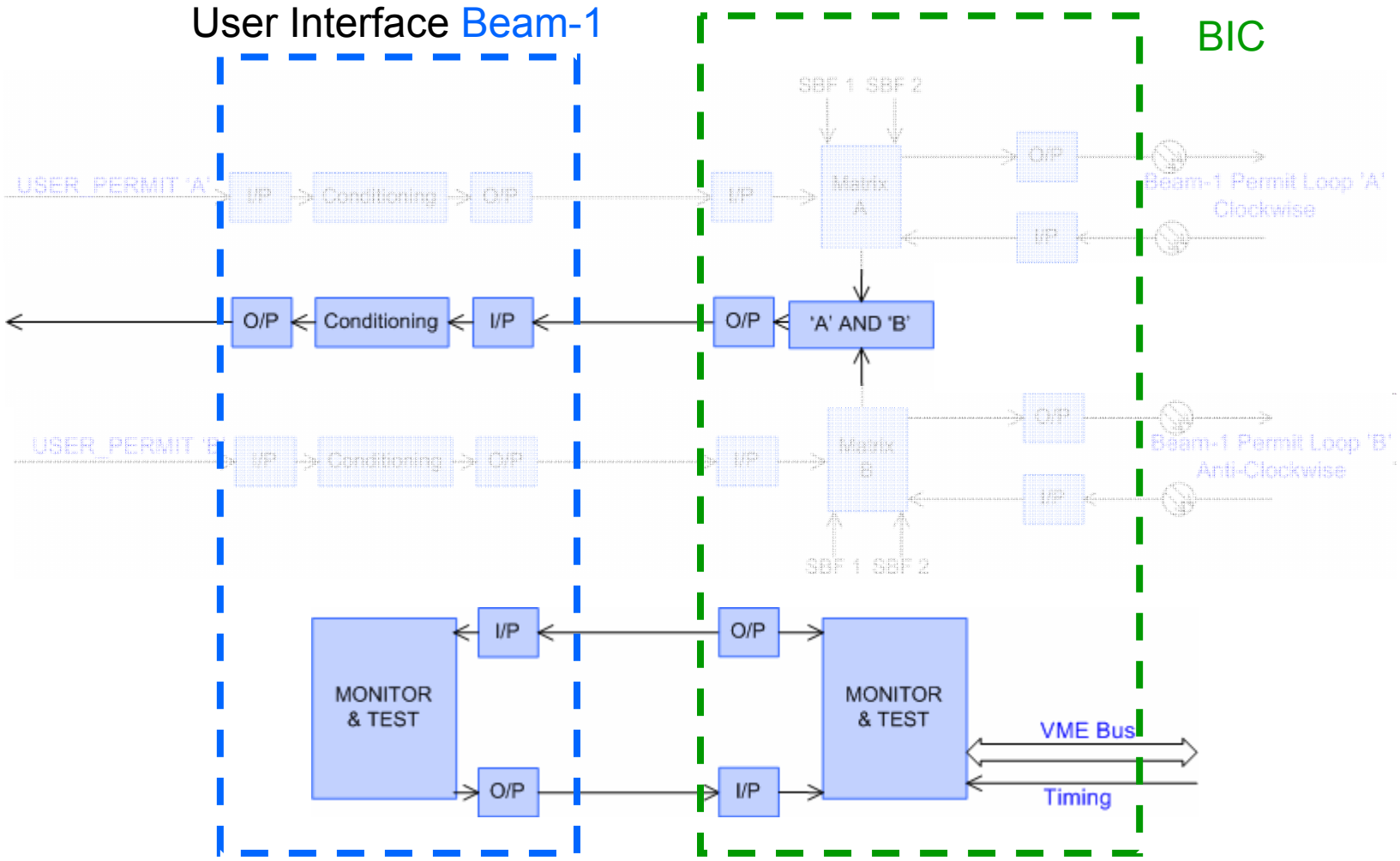


Full Redundancy…

2 User Permits PER BEAM - Treated Identically, in SEPARATE HARDWARE

Safe Beam Flag Redundant – if in doubt NOT SAFE

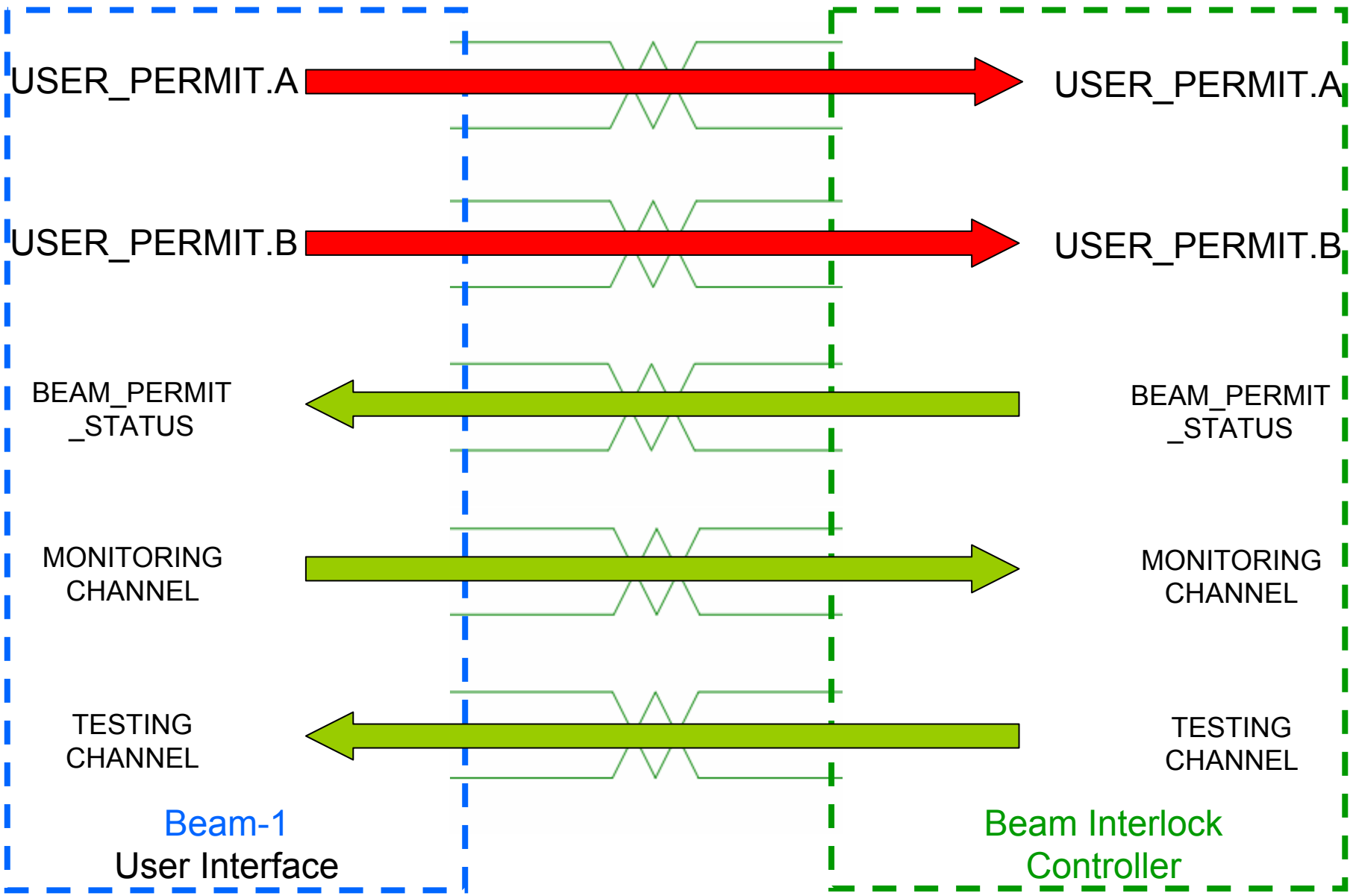
Mission Critical Information Flow



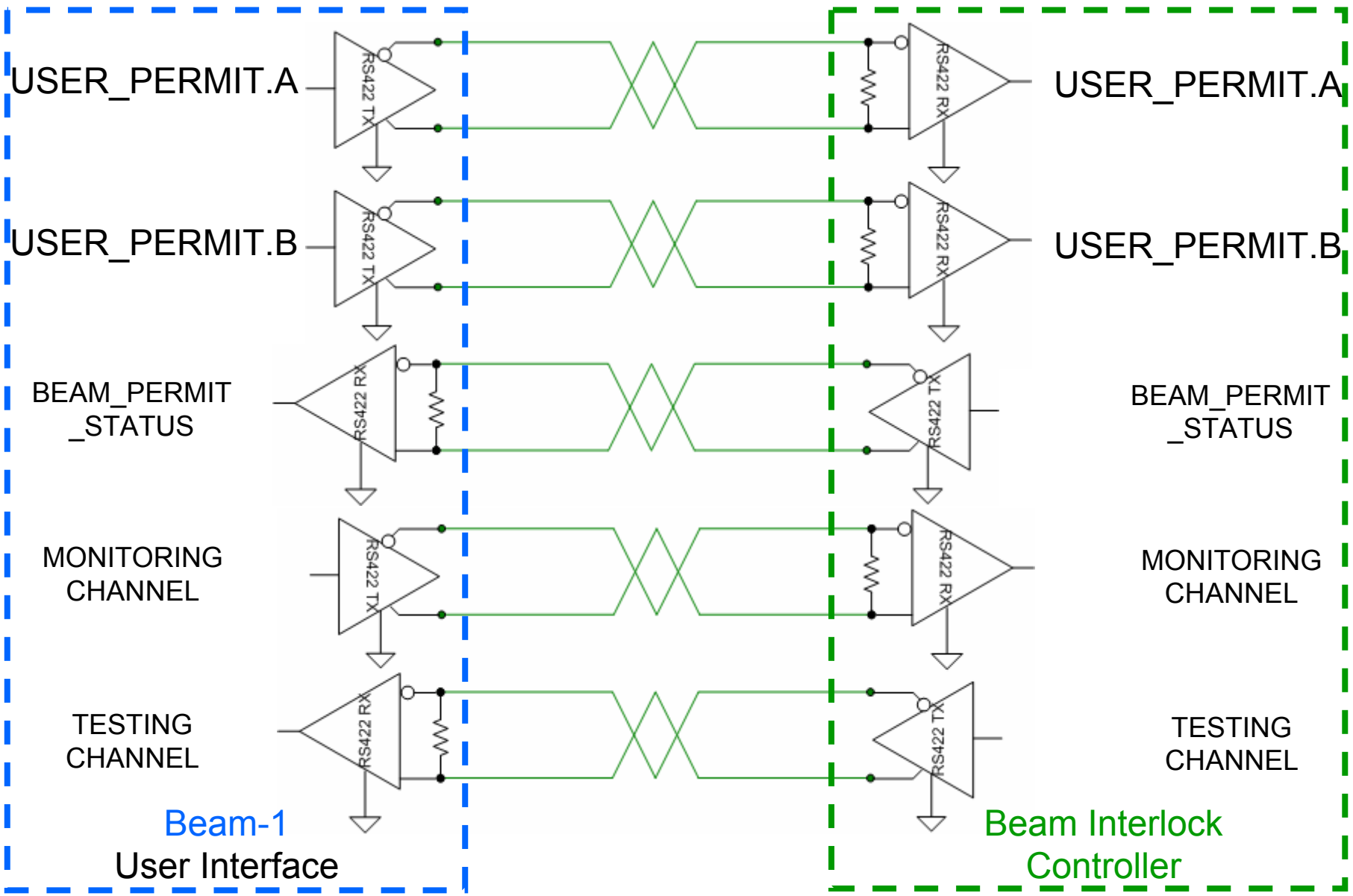
User Interface has Unique ID Number

Different connector genders & sizes are used for safety

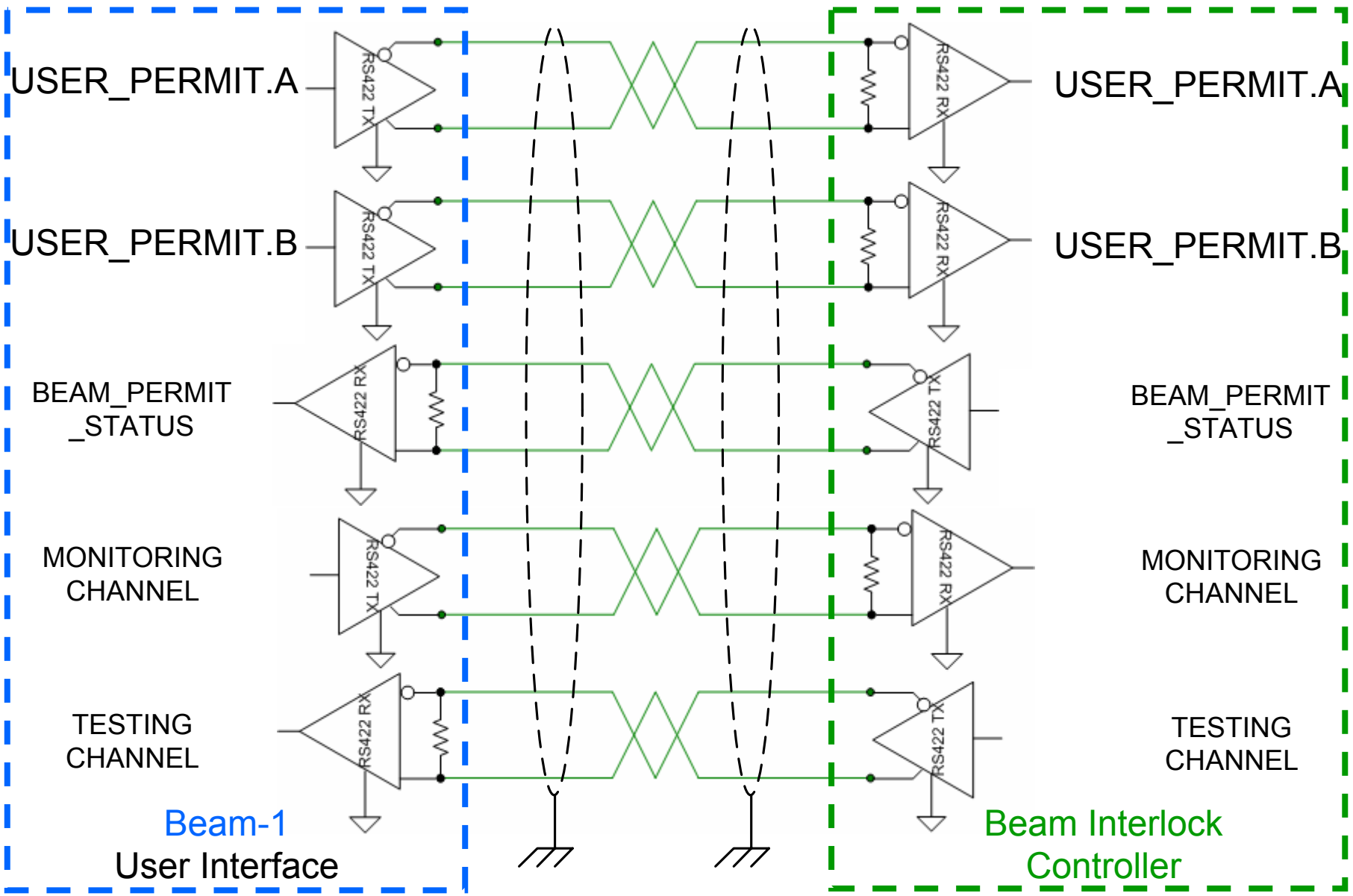
RS422 communication to User



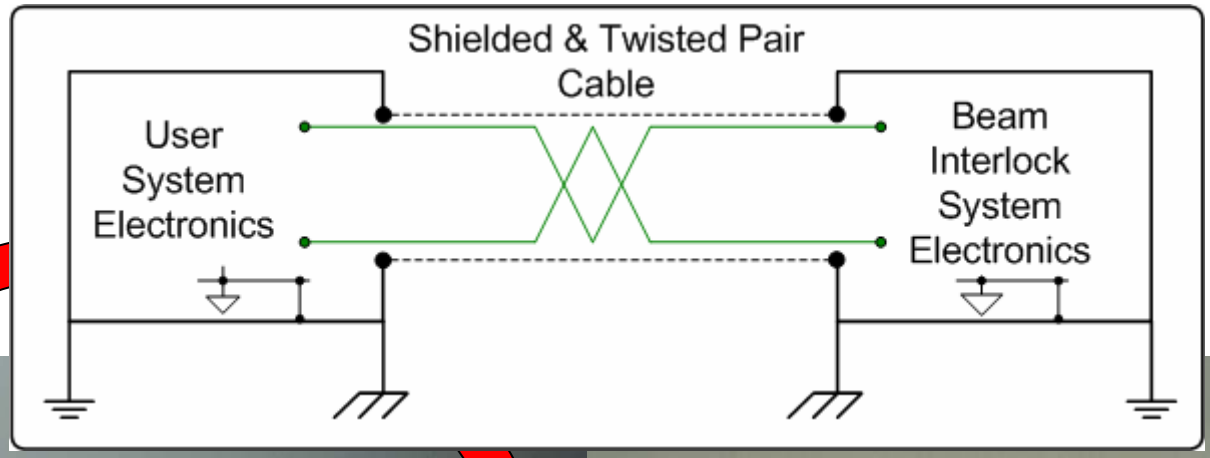
RS422 communication to User

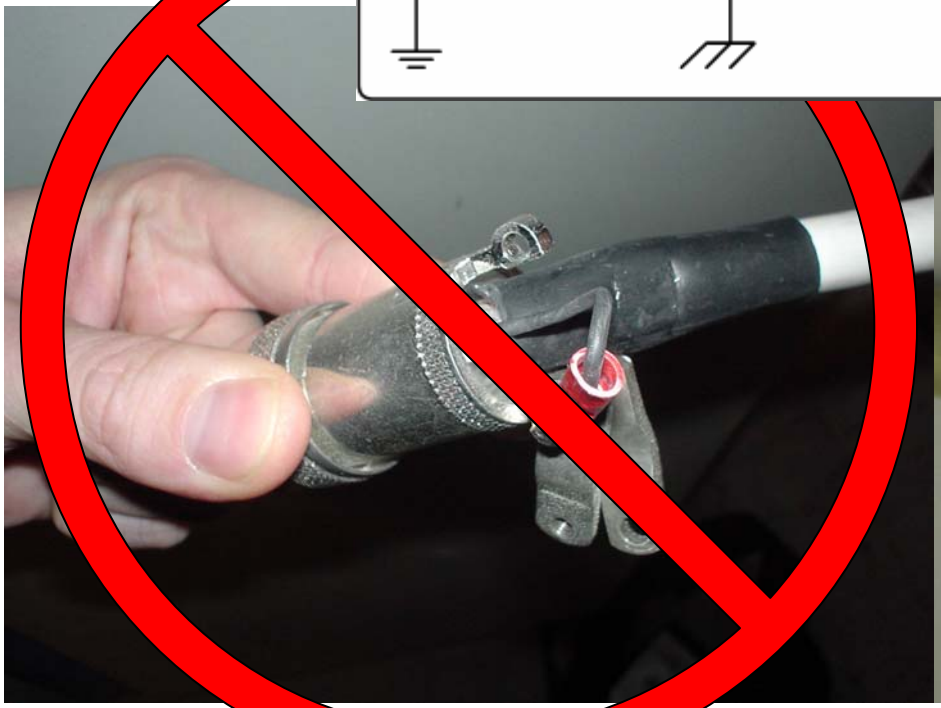


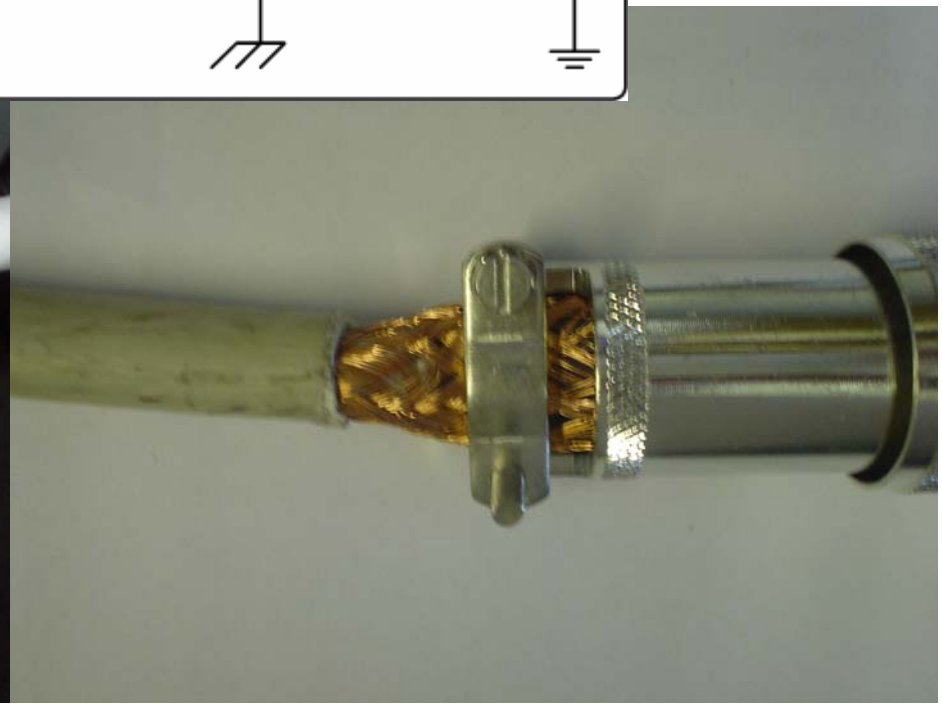
RS422 communication to User



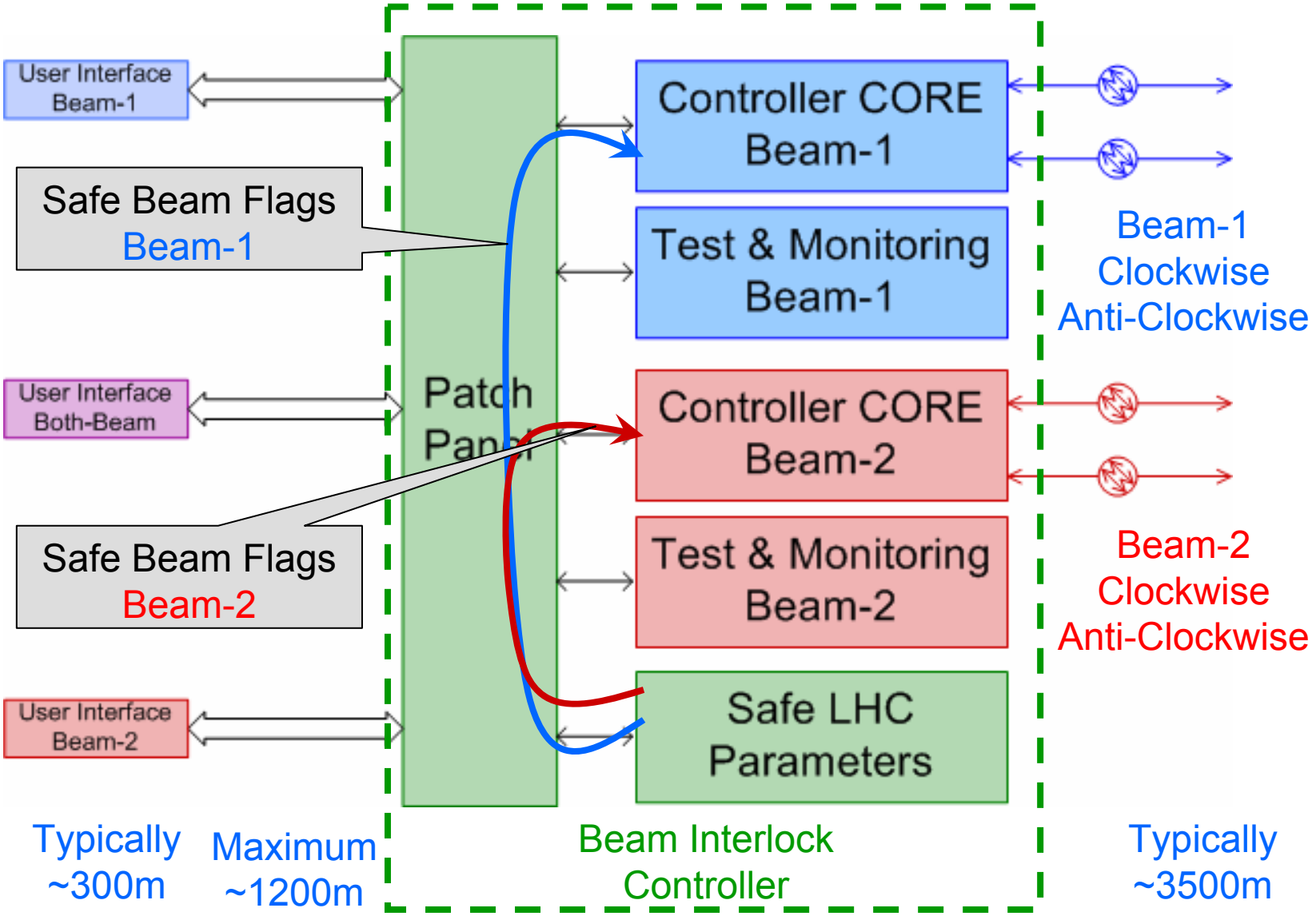
EMC Combat…


Shielded & Twisted Pair
Cable
User
System
Electronics
Beam
Interlock
System
Electronics





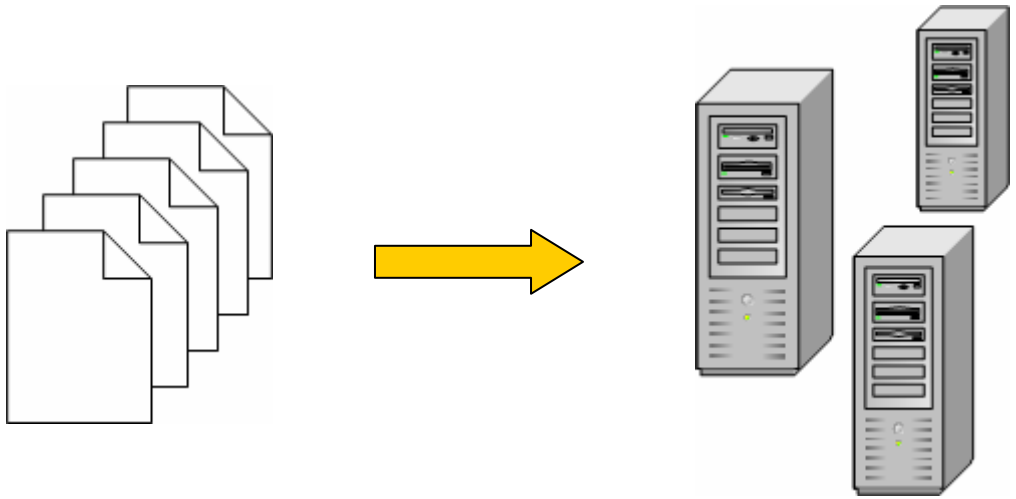
Sub-System Block Diagram



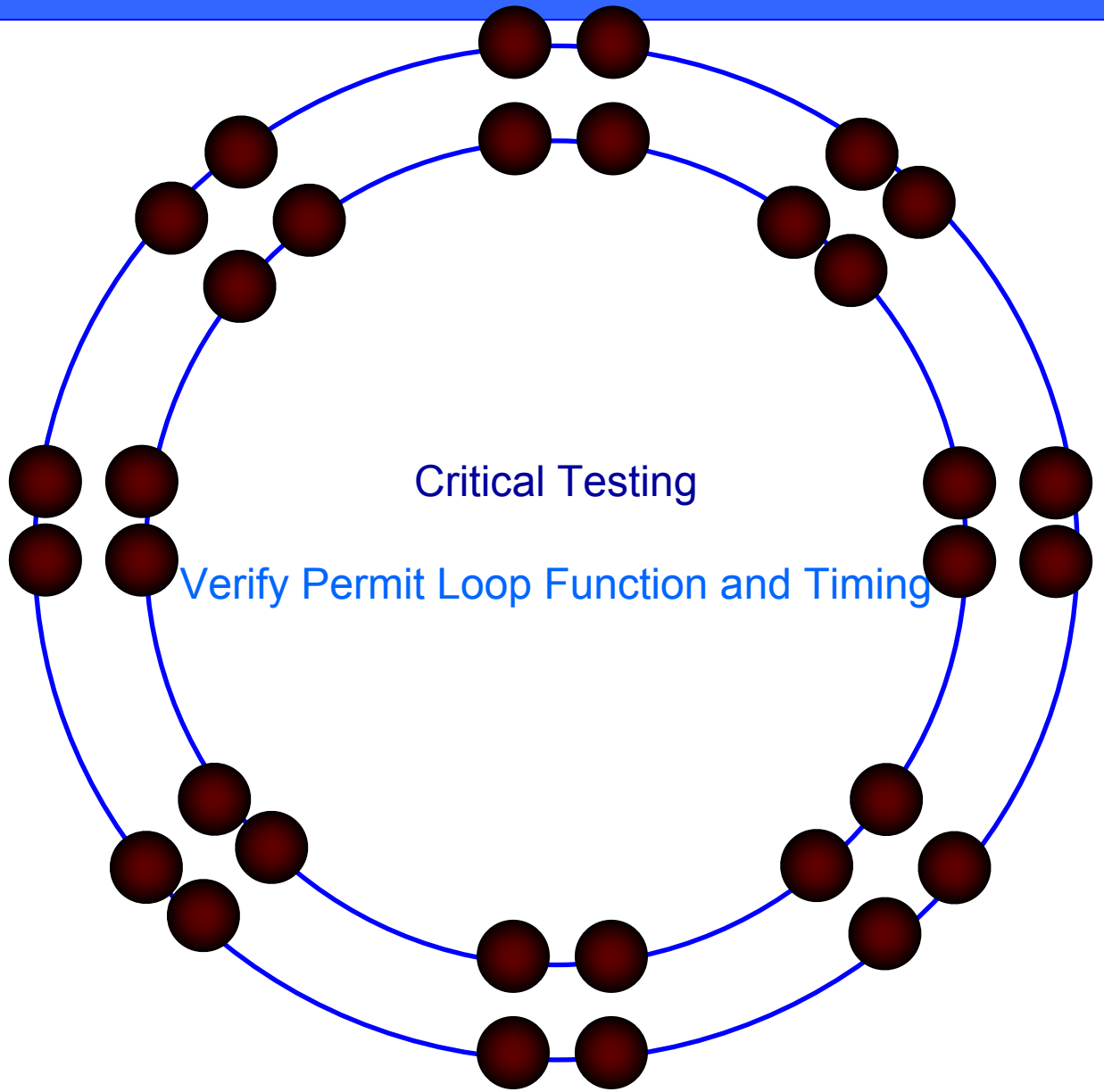
HW Test, Install & Commission

Installation & Commissioning of LHC BIS

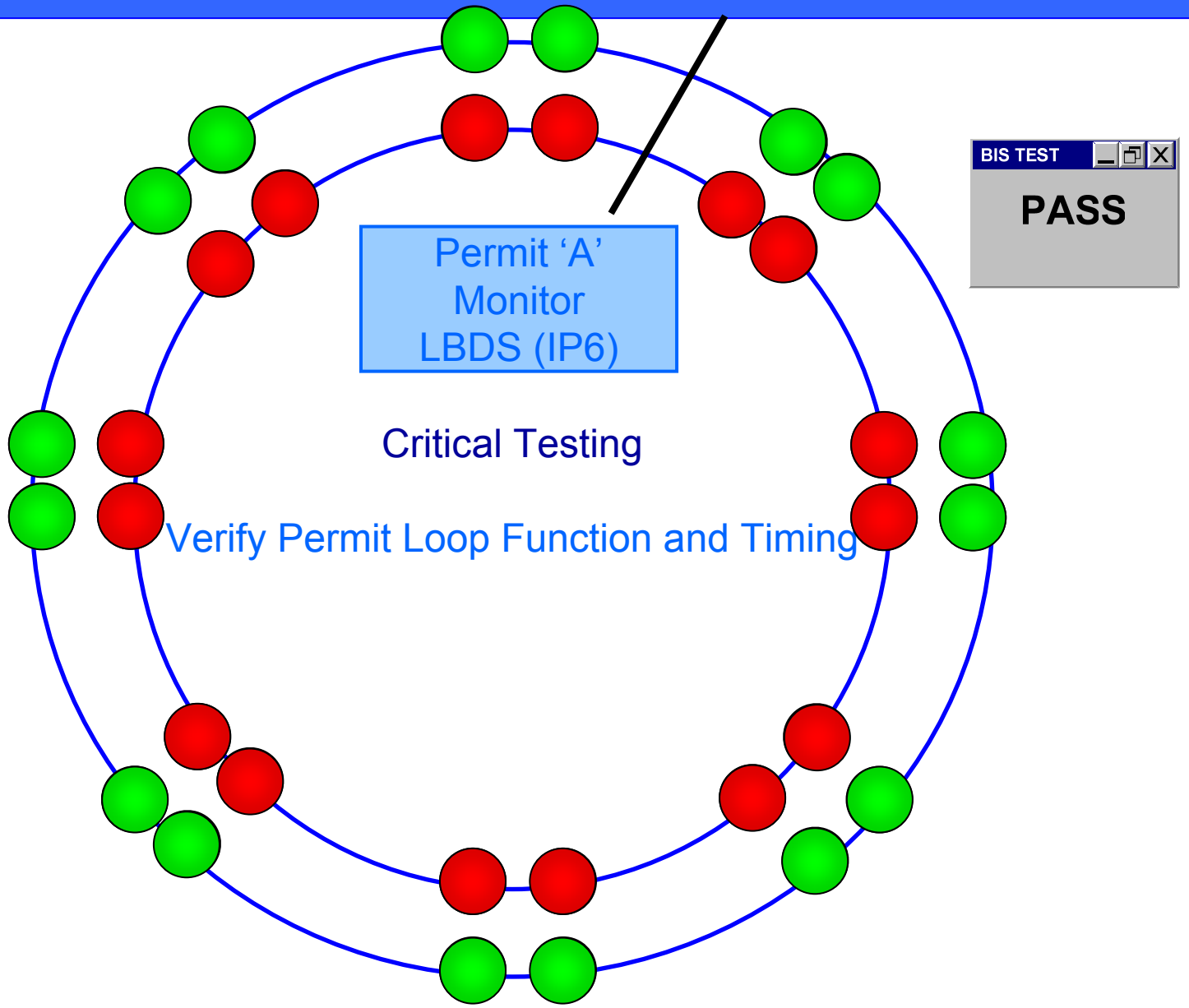
1. Power-Soak (Run-In/Burn-In)
2. Installation in Machine
3. Users can switch USER_PERMIT = FALSE on request
4. Locally verified
5. Once Point complete, information stored in a Data-Base for on-line testing



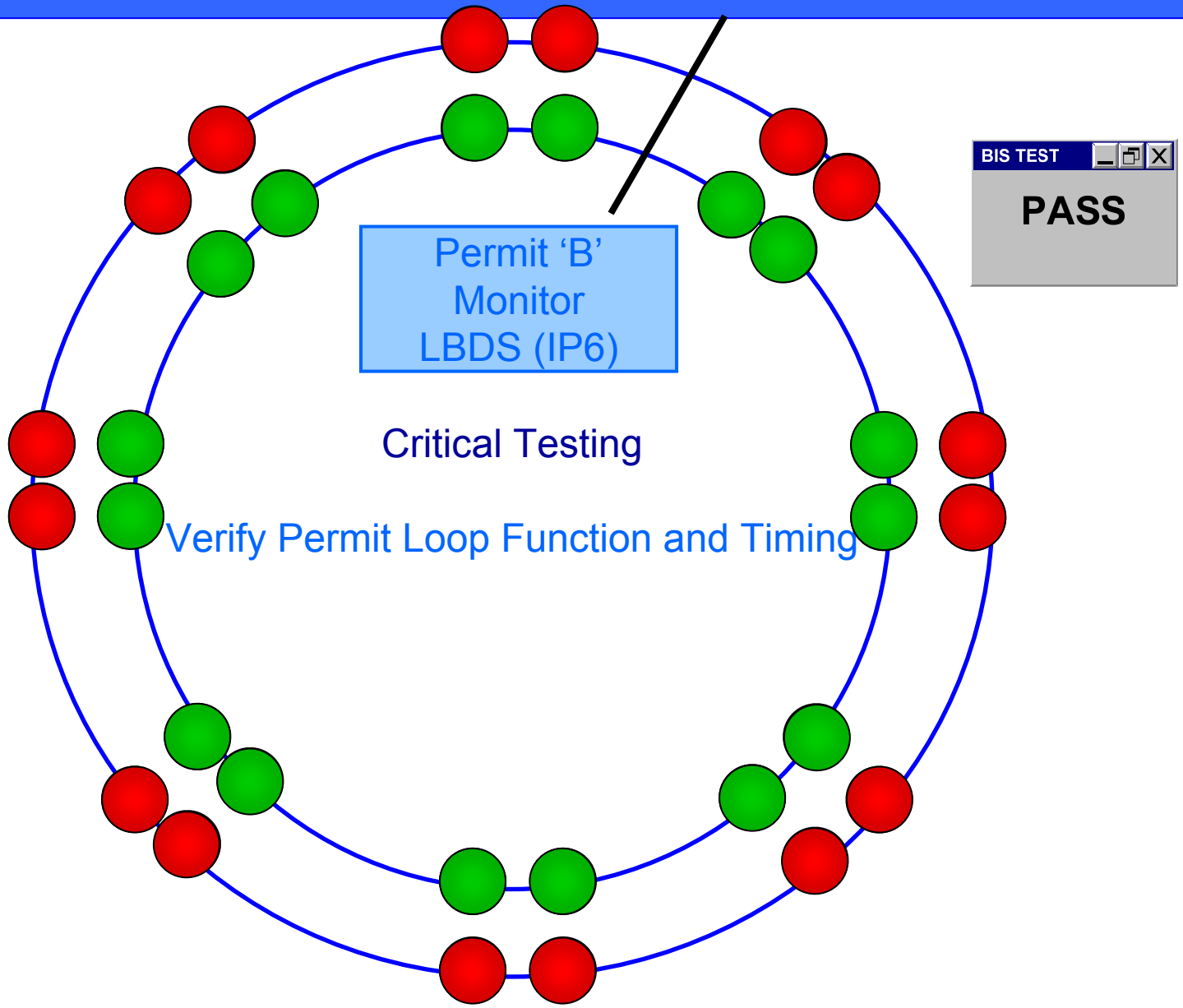
Online Test



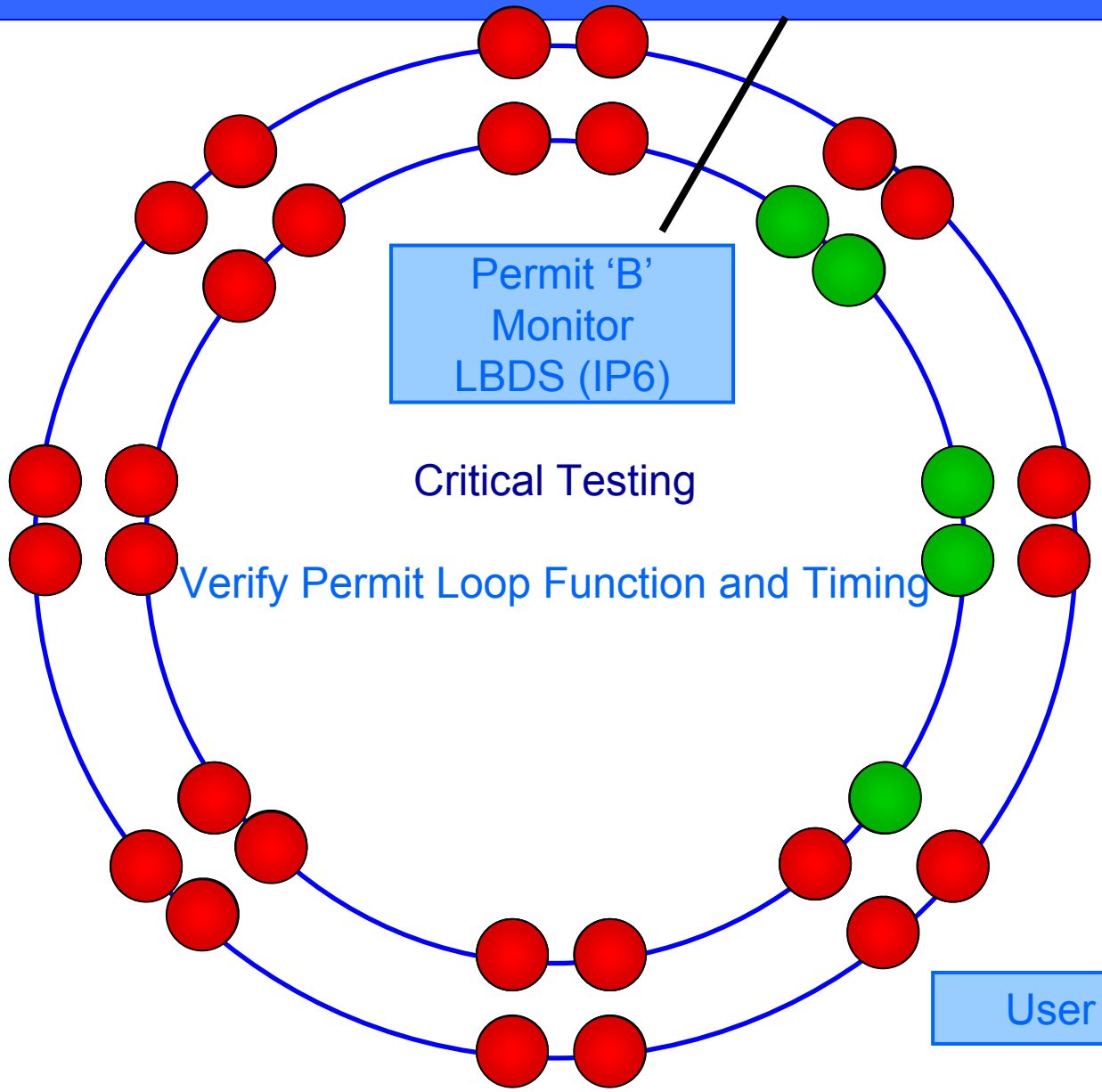
Online Test


Permit ‘A’
Monitor
LBDS (IP6)
Critical Testing
Verify Permit Loop Function and Timing
BIS TEST
PASS

Online Test


Permit 'B'
Monitor
LBDS (IP6)
Critical Testing
Verify Permit Loop Function and Timing
BIS TEST
PASS

Online Test



BIS TEST

Time 78us

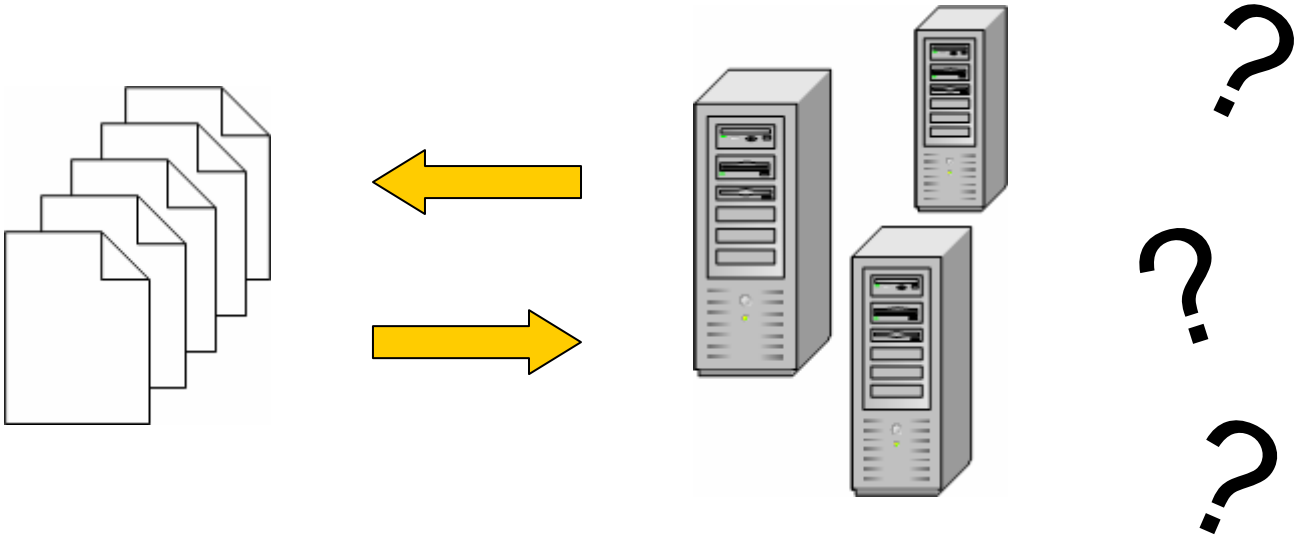
PASS

User #100

Online Test

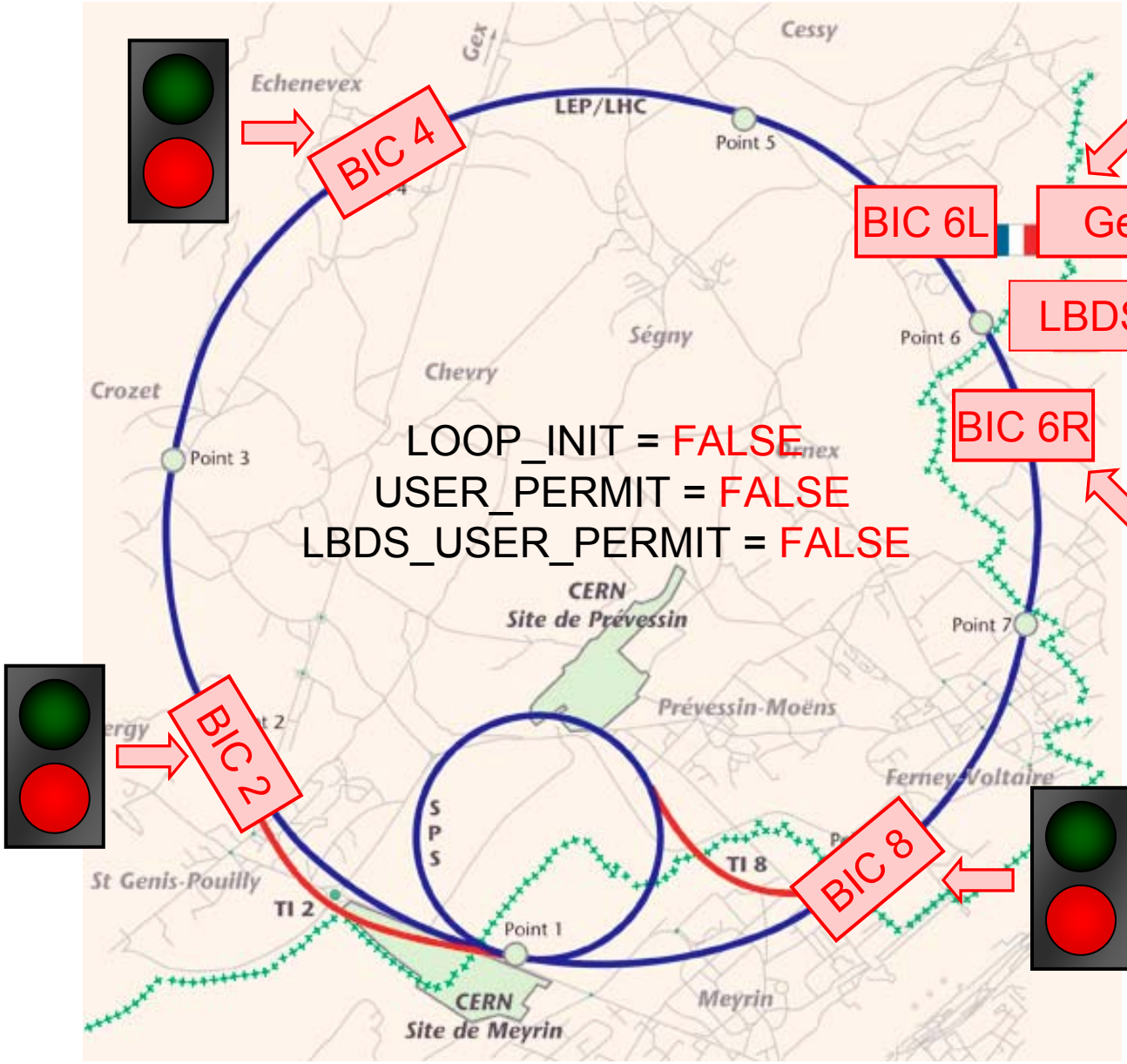
Non-critical Testing

1. Re-built and verify Database – Cabling
2. Verify secondary circuits, power supplies etc.

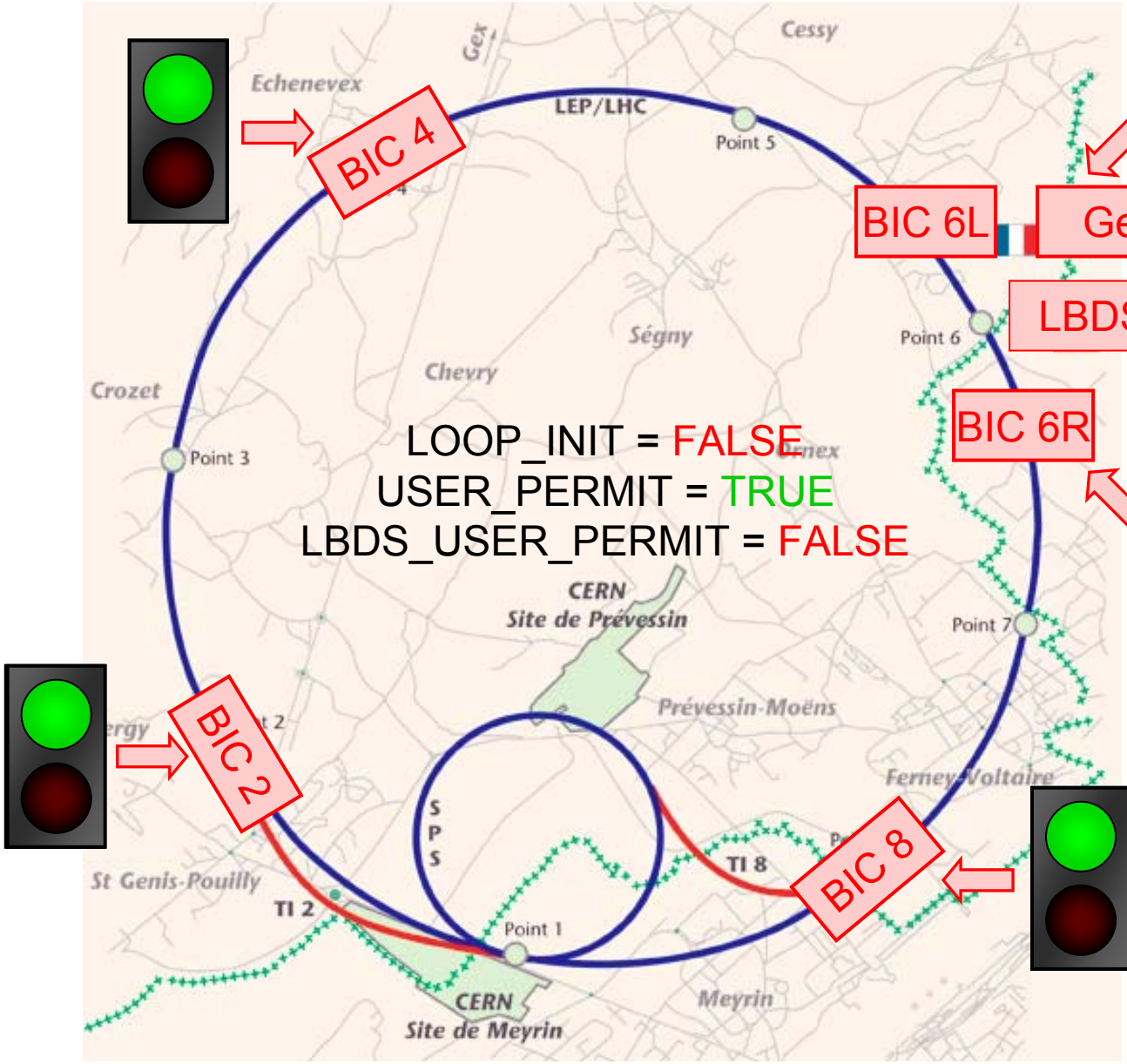


All part of ensuring system is ‘As Good As New’ on startup.

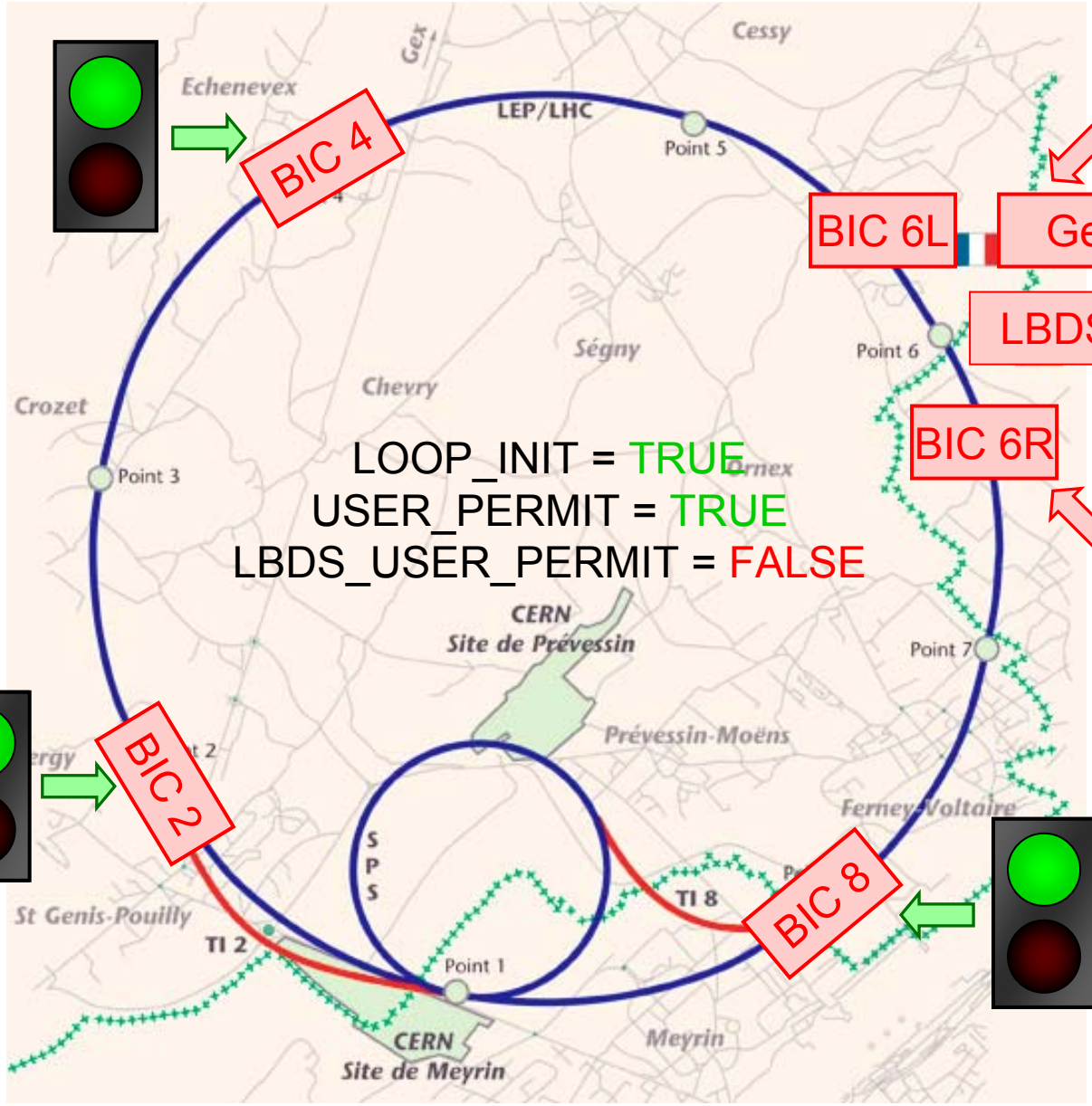
Startup


Gex
Cessy
Echenevex
LEP/LHC
Point 5
BIC 4
BIC 6L
Generator
INITIALISE_LOOP
LBDS
PERMIT 'A'
Point 6
Ségny
Chevry
Crozet
Point 3
BIC 6R
LOOP_INIT = FALSE
USER_PERMIT = FALSE
LBDS_USER_PERMIT = FALSE
LBDS_USER_PERMIT
CERN
Site de Prévessin
Point 7
Prévessin-Moëns
BIC 2
BIC 8
S
P
S
TI 8
St Genis-Pouilly
TI 2
Point 1
CERN
Site de Meyrin
Meyrin

Startup


Gex
Cessy
Echenevex
LEP/LHC
Point 5
BIC 4
BIC 6L
Generator
INITIALISE_LOOP
LBDS
PERMIT 'A'
Point 6
Ségny
Chevry
Crozet
Point 3
BIC 6R
LOOP_INIT = FALSE
USER_PERMIT = TRUE
LBDS_USER_PERMIT = FALSE
LBDS_USER_PERMIT
CERN
Site de Prévessin
Point 7
Prévessin-Moëns
BIC 2
Ferney-Voltaire
S
P
S
TI 8
BIC 8
St Genis-Pouilly
TI 2
Point 1
CERN
Site de Meyrin
Meyrin

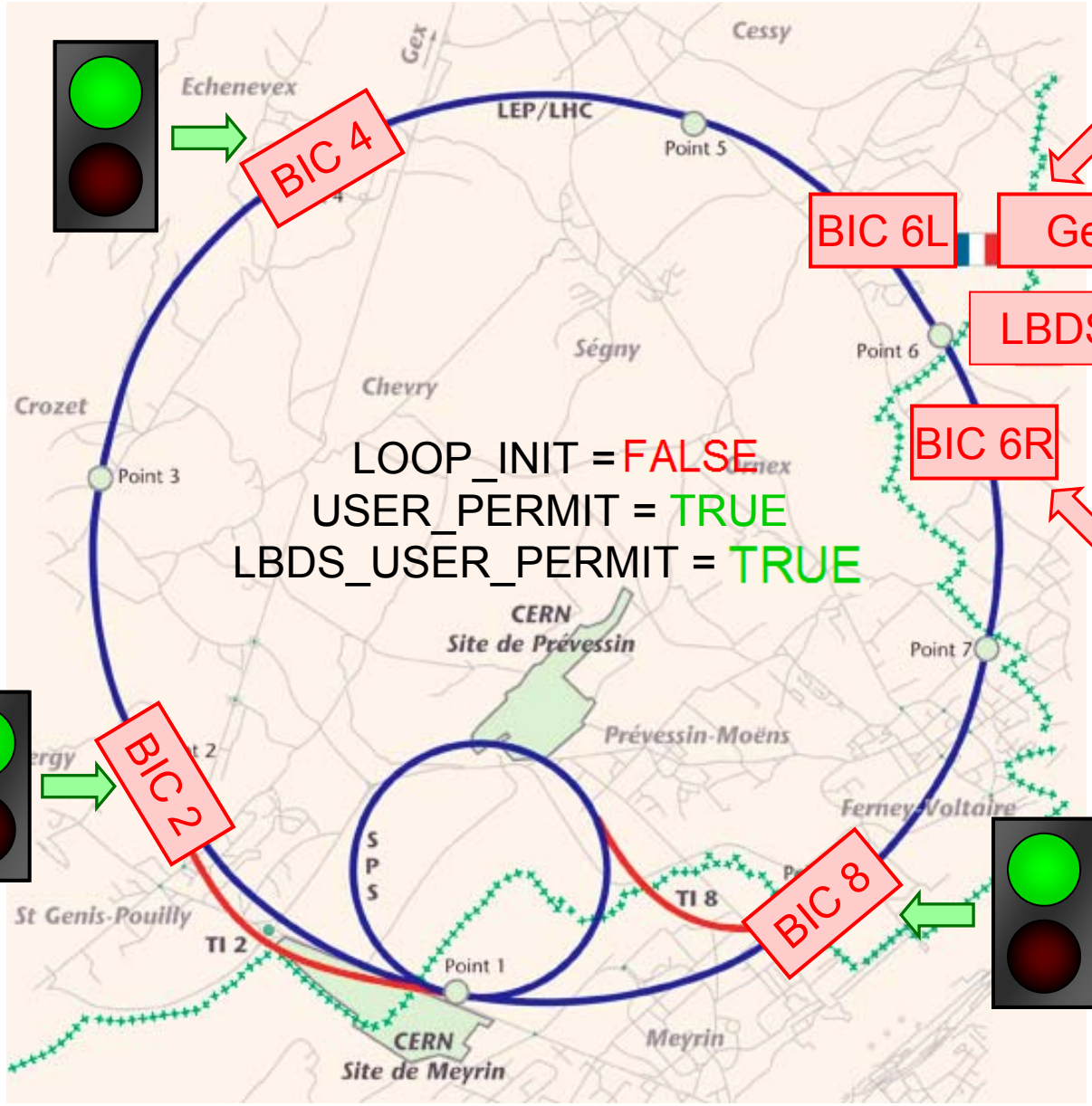
Startup



Generator needs 10MHz INPUT to Latch-On

ONLY set for ~250us HARDWARE INTERNAL RESET

Successful Startup



Generator needs 10MHz INPUT to Latch-On

ONLY set for ~250us HARDWARE INTERNAL RESET

The LHC Beam Interlock System

1. Overview and Architecture
   - History
   - Specification
   - BIS Design
   - Communication strategies
   - EMC
   - Testing, Installation, Commissioning and Starting LHC

2. Dependability Analysis
   - Reliability, Safety and Maintainability
   - Typical Figures

3. Summing Up
   - Typical Response
   - Next goals

Failure Modes, Effects and Criticality Analysis

In what way can something go wrong?…

…when it does go wrong, what happens to the system?…

…and just how much of a problem does this cause?

MIL-STD-1629 MIL-HDBK-338 FMD-97 MIL-HDBK-217

FMECA starts at the Component Level of a system

FMECA Conclusions User Interface

75 Simultaneous Beam Dump User Interfaces
39 Independent Beam Dump User Interfaces
10 Hour LHC mission
400 Missions per year

	CIBU B1&B2 or Half CIBU B1/B2	ALL LHC	One Year ALL LHC
P(Fail) Any Failure	3.82E-05	5.84E-03	2.34
P(Fail) Blind A Failure	4.91E-07	7.51E-05	3.00E-02
P(Fail) Blind B Failure	4.91E-07	7.51E-05	3.00E-02
P(Fail) Blind A&B Failure	2.41E-13	3.68E-11	1.47E-08
P(Fail) Beam Dump	7.82E-06	1.20E-03	0.48
P(Fail) Maintenance	2.01E-05	3.07E-03	1.23

During one year it's probable that for all User Interfaces

0-1 will fail during a mission causing a Beam Dump

1.47E-08 is Probability of a both channels failing blind in the same User Interface

SIL 3

FMECA Conclusions

75 % Analysed System

	COMBINED AND AJUSTED TOTALS		
	BIS	BIS	Safety Integrity
	One Mission	One Year	Level IEC61508
P(Fail) Any Failure	1.84E-02	7.378	
P(Fail) Blind Failure	3.68E-11	1.473E-08	SIL 3
P(Fail) Beam Dump	2.85E-03	1.140	

Redundancy

Remove All Redundancy…

	COMBINED AND AJUSTED TOTALS	NO REDUNDANCY	
	BIS One Mission	BIS One Year	Safety Integrity Level IEC61508
P(Fail) Blind Failure	7.51E-05	3.003E-02	< SIL 1

Remove User Input Redundancy…

	COMBINED AND AJUSTED TOTALS	NO USER REDUNDANCY	
	BIS One Mission	BIS One Year	Safety Integrity Level IEC61508
P(Fail) Blind Failure	3.08E-06	1.230E-03	< SIL 1

All User Interface Power Supplies are REDUNDANT

REDUNDANT VME Power Supplies are anticipated… 1 False Beam Dump p.a. less

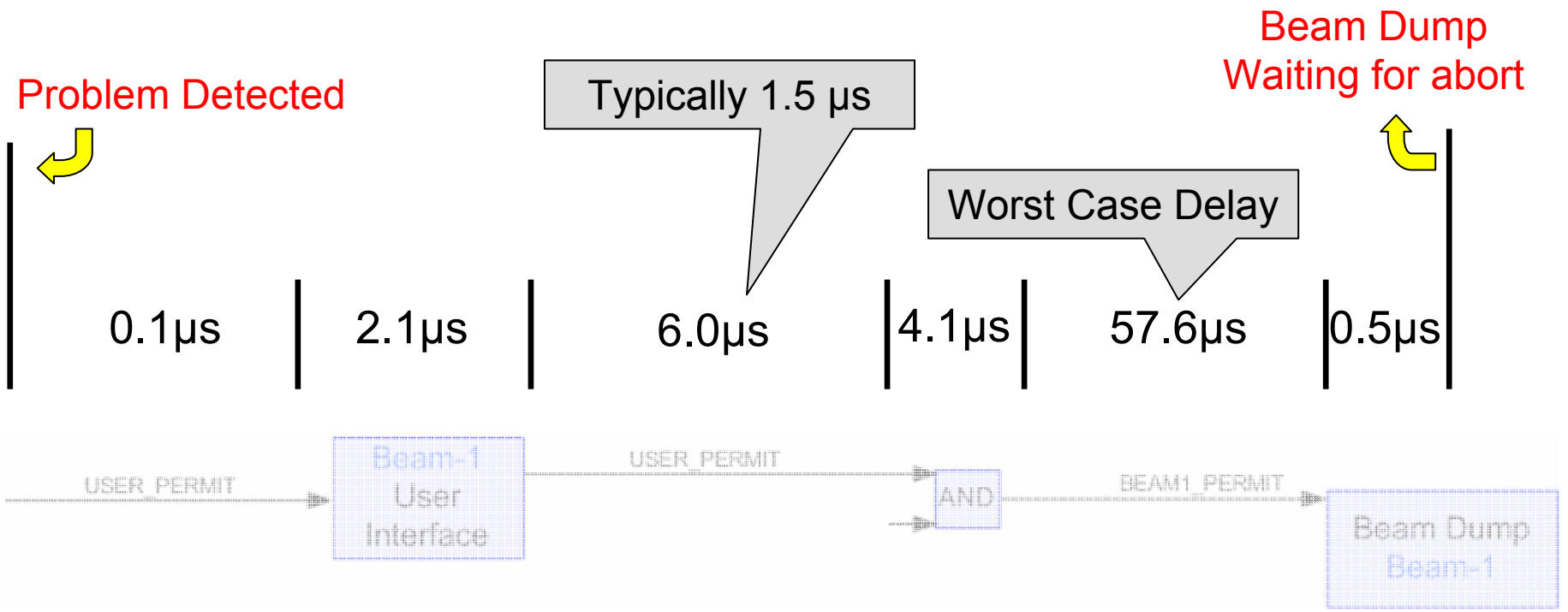
The LHC Beam Interlock System

1. Overview and Architecture
   - History
   - Specification
   - BIS Design
   - Communication strategies
   - EMC
   - Testing, Installation, Commissioning and Starting LHC

2. Dependability Analysis
   - Reliability, Safety and Maintainability
   - Typical Figures

3. Summing Up
   - Typical Response
   - Next goals

Delta-t for a Point 2 Beam Loss



~70µs MAXIMUM

A bit of history

2001	Beam Interlock System Proposed	BNL / DESY systems used as a basis
2002-2003	System architecture Basic development	Tested in TI8 AUTUMN 2003
2004	Current Loops Fibre Optic 'Permit Loops' Masking	Tested in TI8 AUTUMN 2004
2005	Dependability & EMC Programmable Logic	Testing in SPS AUTUMN 2005
2006	Long Term testing Further Analysis of Dependability	
2007	Mass Produce Commission Install	3 SPS BICs by November

2007 – LHC BIS installed, commissioned, ready.

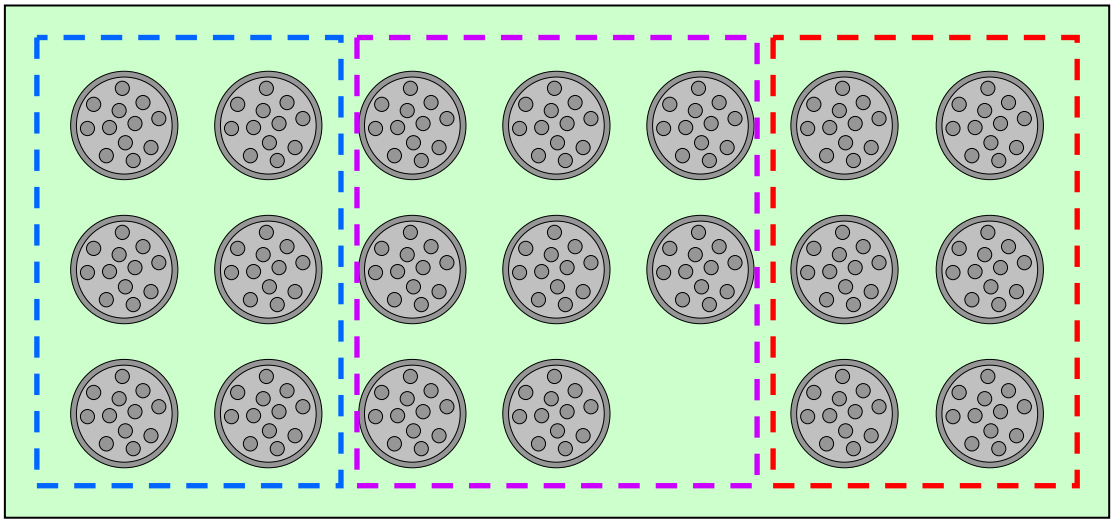
FIN

BIC Patch Panel Cabling

Burndy 12
Female

Burndy 12
Male

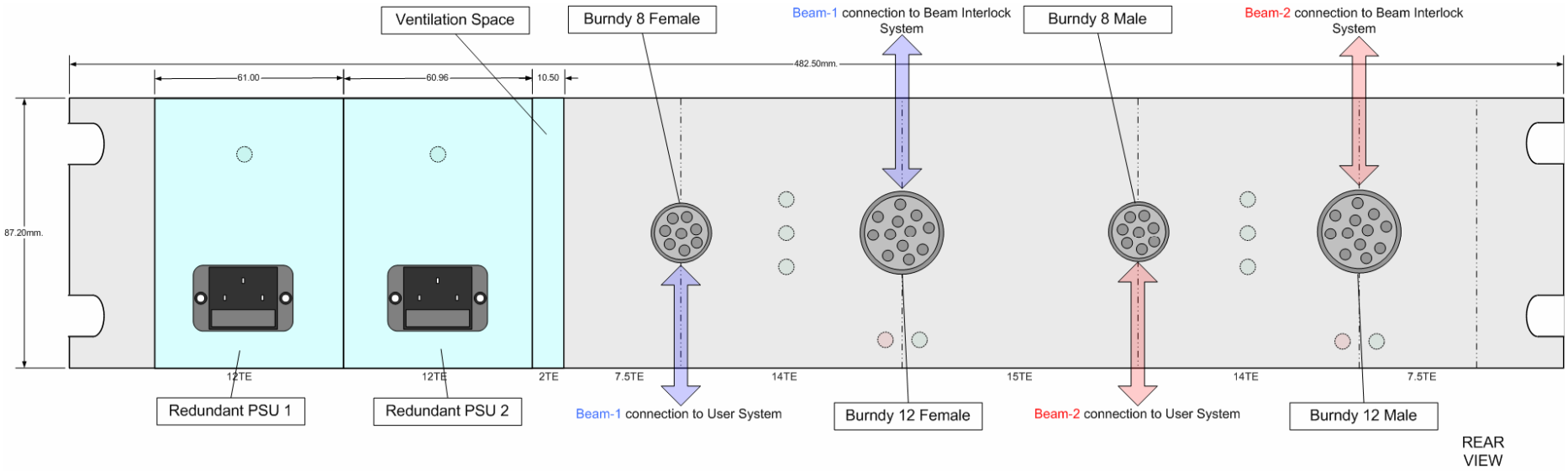
Rear View
Of VME
Chassis



Burndy 19
Female

Connected DIRECTLY to the rear of the P2 VME connector (extender)
Securely fastened in place, vibration of fans no problem
DEPENDABLE, one of the best architectures for reliable design
PCBs not wires - No risk of cross connection / bad cables
Genders

User Interface & Cabling



CIBU Details

A single User Interface exists for simultaneous and independent operation – saves space – more reliable

DUAL power supplies, redundant, monitorable

INPUT Configuration

A user gives 2 signals for each beam – small current loops

Accommodates all the different user hardware 5V 12V 24V etc etc

Diagnosis & Standard Functions

Direct data from CIBU by Monitoring

Test Mode Status (1 bit)
Test Channel Status (1 bit)
Test Logic Status (1 bit)
Unique CIBU ID (10 bits)
Number of Reception Errors (8 bits)
Permit A State (1 bit)
Permit B State (1 bit)
Beam Permit Status State (1 bit)
Permit A RS422 Fault (1 bit)
Permit B RS422 Fault (1 bit)
Beam Status RS422 Fault (1 bit)
CIBUT (Tester) Attached (1 bit)
PSU 1 Status (1 bit)
PSU 2 Status (1 bit)

Commands to CIBU by Testing

Test Mode (1 bit)
Test Channel (1 bit)
Test Logic (1 bit)
Soft Reset (1 bit)

Direct data from CIBT

CIBT Alive (1 bit)
Boxes Alive (14 bits)
Cumulative BER per CIBU (14 x 16 bit)
Cable Delay (Calc.) per CIBU (14 x 16 bit)

Direct data from CIBC

Current State Permit As (14 bits)
Current State Permit Bs (14 bits)
Beam Permit Loop States (4 x 3 bit)
RS 422 faults (60+ bits)
Core Beam Number (2 bits)
History Buffer (??)

All data is moved to the Controller Core and can be read out by VME access

Software has to reassemble the information correctly

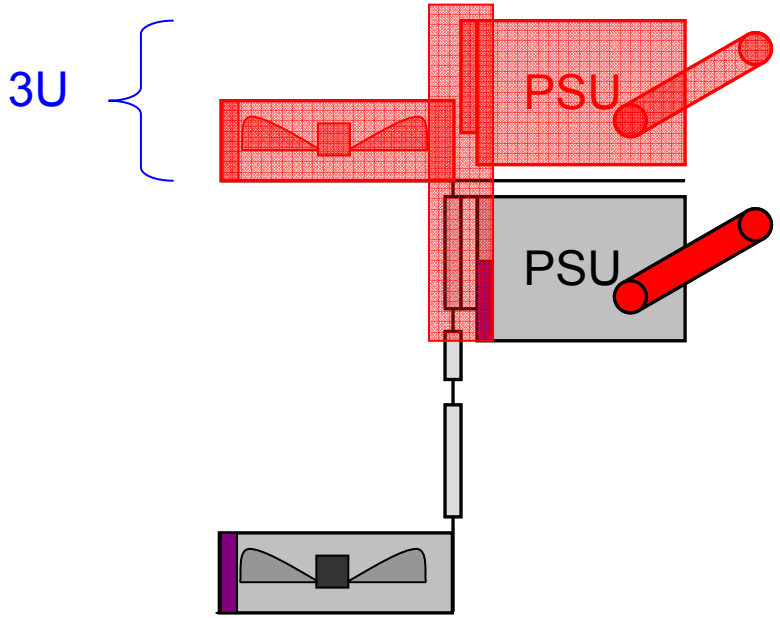
Provides initial Post Mortem Diagnosis

PSU Redundancy = AVAILABLE

Add Redundant VME PSU…

	COMBINED AND AJUSTED TOTALS		
	BIS One Mission	BIS One Year	Safety Integrity Level IEC61508
P(Fail) Any Failure	2.00E-02	8.017	
P(Fail) Blind Failure	3.68E-11	1.473E-08	SIL 3
P(Fail) Beam Dump	1.82E-03	0.729	
P(Fail) Maintenance	1.67E-02	6.698	
Maintance OR Beam Dump	1.86E-02	7.427	

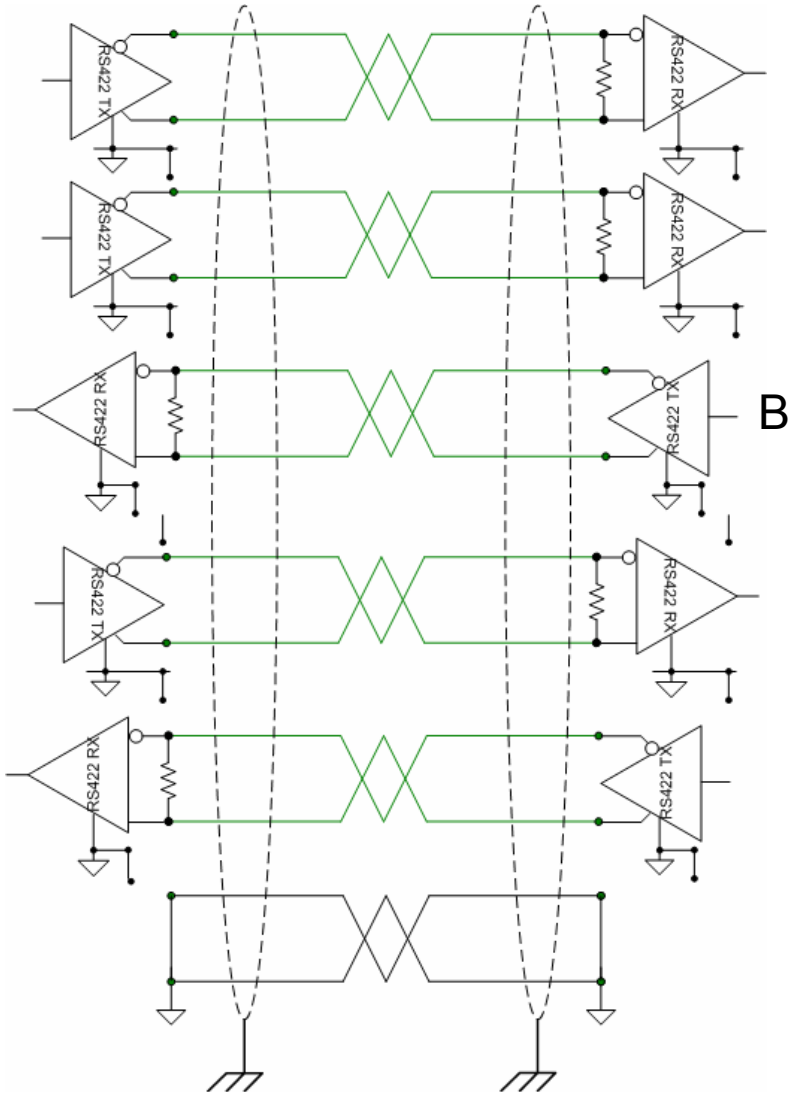
About **1 less** False Dump p.a.



RS422 communication to User

MAX3440E
EMC Excellent
Slew Rate Limited
Fail Safe
Short Circuit Proof
Fault Pins
DC Mode - Simplex

MAX489E
Full Duplex Comms
~60-80kbps
Manchester Encoded
DC Balanced
Monitoring Channel
Testing Channel



USER_PERMIT.A

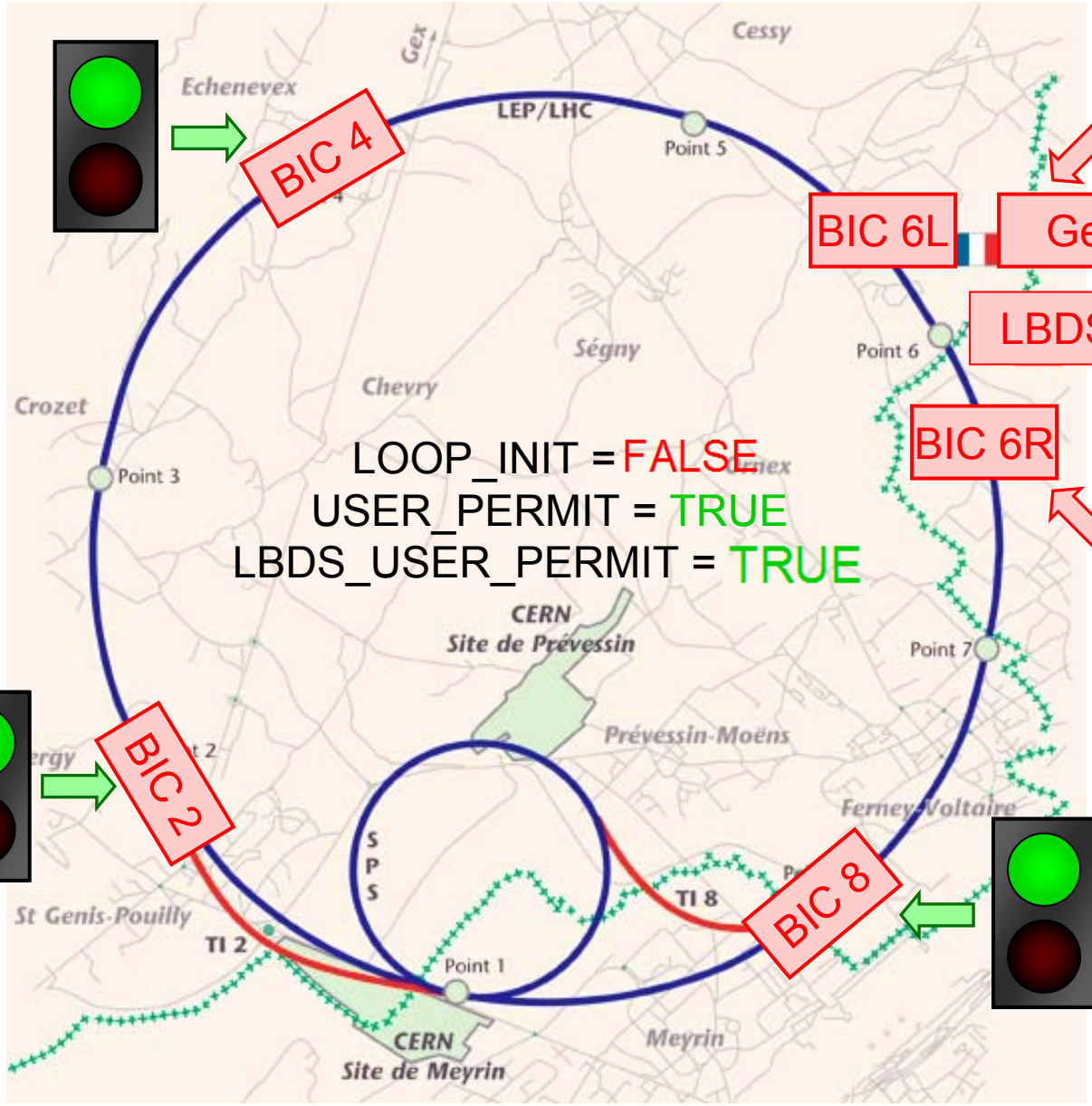
USER_PERMIT.B

BEAM_PERMIT_STATUS

CIBU_MONITORING

CIBU_TEST

INIT



Generator needs 10MHz INPUT to Latch-On

ONLY set for ~250us HARDWARE INTERNAL RESET