# Beam Interlock System Audit

**Report on the Audit held in September 2006**

Stefan Lüders (IT/CO) on behalf of the Auditors

Reiner Denz (CERN AT/MEL), Philippe Farthouat (CERN PH/ATLAS), Stefan Lüders (CERN IT/CO), Javier Serrano (CERN AB/CO), Yves Thurel (CERN AB/PO), Matthias Werner (DESY)

# Scope

**This audit is supposed to verify design and implementation of the BIS:**

- fundamental design decisions
- PCB schematics and layouts & VHDL programming
- mechanics
- interfaces to other systems

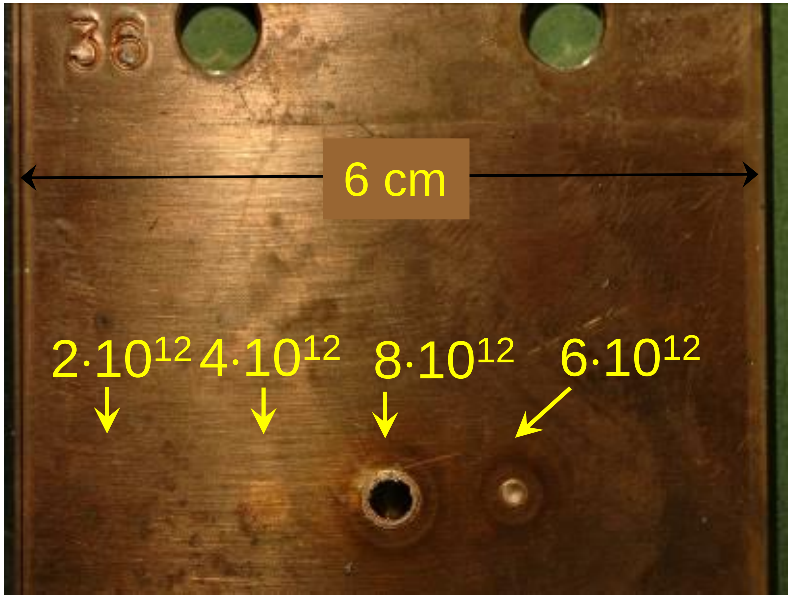
**Particular focus put on safety relevant aspects:**

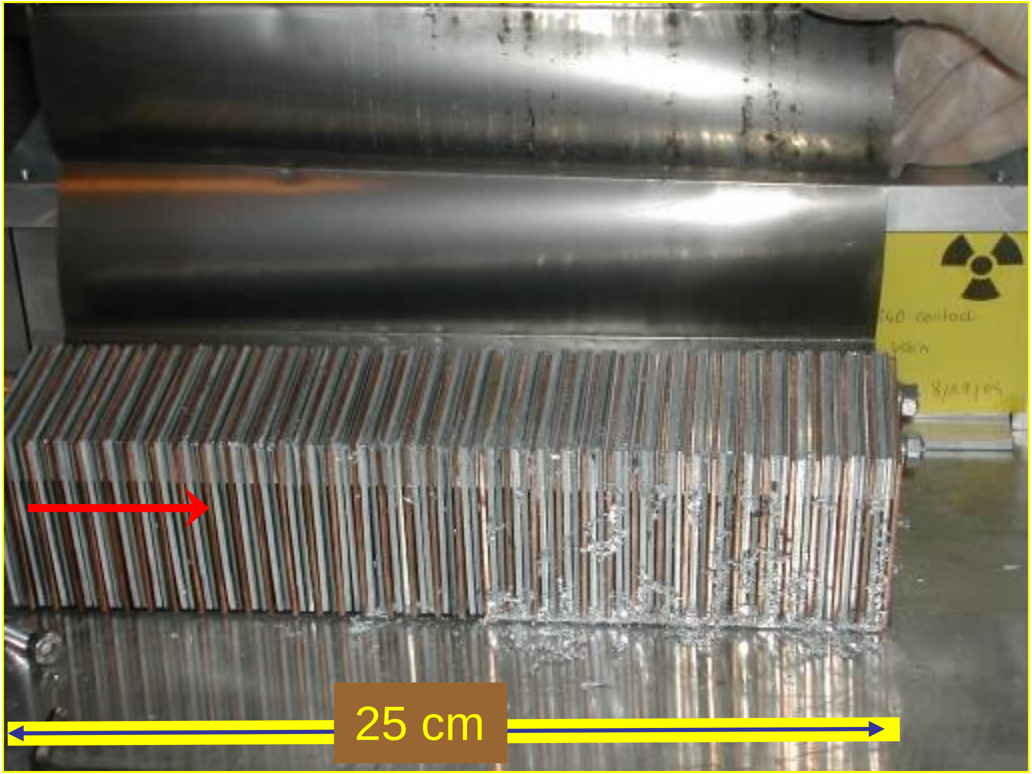
- safe and efficient operation of LHC
- sufficiently high reliability and availability
- single points of failures AND failure modes leading to blind faults

**This audit does not cover**

- system software running on PowerPC
- control aspects & methods for remote diagnostics

# One slide on the “Why”



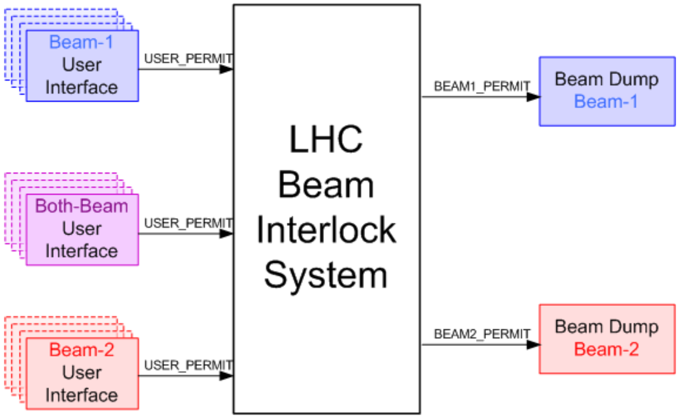


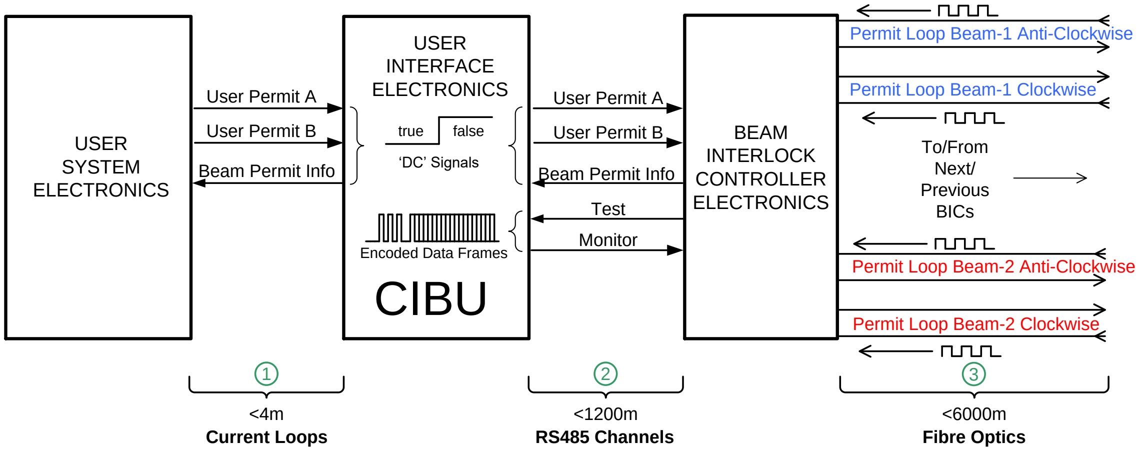
0.1 % of the full LHC beam

$8\cdot10^{12}$ protons

$\sigma_{x/y}$ = 1.1mm/0.6mm

# The BIS Architecture



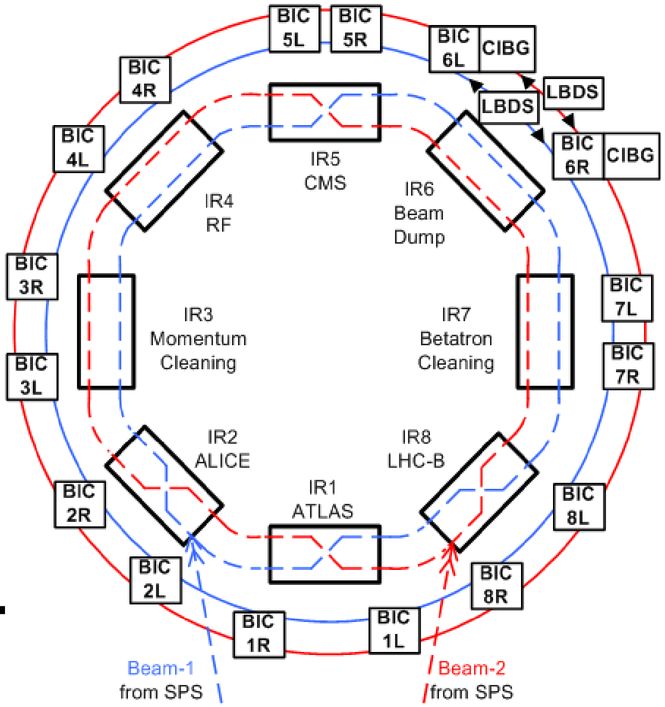


## Three ring-type systems:

- LHC Beam A & Beam B
- SPS

## Four tree-type systems:

- LHC injection (Beam A & B)
- SPS extraction (BA4 & BA6)

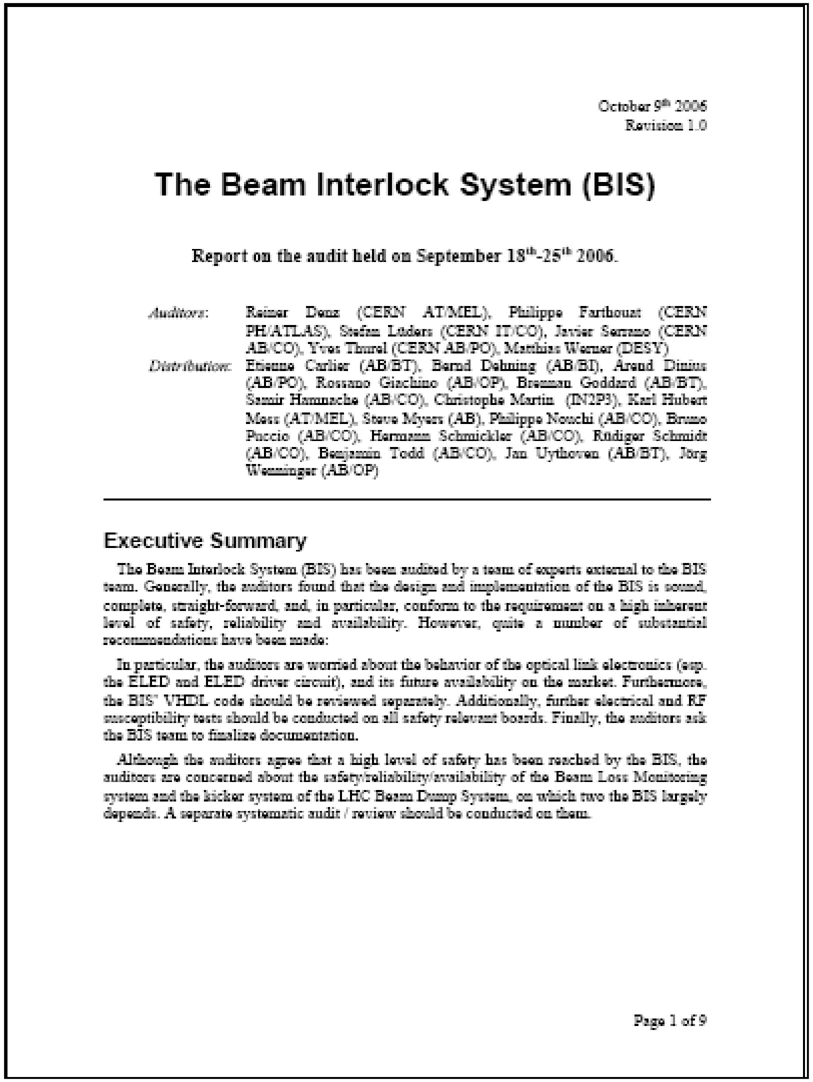


# Auditor’s Recommendations

Recommendations have been distributed to all parties involved.

Focus on major points.

Numbers refer to Audit Report.



October 9th 2006
Revision 1.0

## The Beam Interlock System (BIS)

**Report on the audit held on September 18th-25th 2006.**

*Auditors:* Reiner Denz (CERN AT/MEL), Philippe Farthouat (CERN PH/ATLAS), Stefan Lüders (CERN IT/CO), Javier Serrano (CERN AB/CO), Yves Thurel (CERN AB/PO), Matthias Werner (DESY)

*Distribution:* Etienne Carlier (AB/BT), Bernd Dehning (AB/BI), Arend Dinius (AB/PO), Rossano Giachino (AB/OP), Brennan Goddard (AB/BT), Samir Hamnache (AB/CO), Christophe Martin (IN2P3), Karl Hubert Mess (AT/MEL), Steve Myers (AB), Philippe Nouchi (AB/CO), Bruno Puccio (AB/CO), Hermann Schmickler (AB/CO), Rüdiger Schmidt (AB/CO), Benjamin Todd (AB/CO), Jan Uythoven (AB/BT), Jörg Wenninger (AB/OP)

### Executive Summary

The Beam Interlock System (BIS) has been audited by a team of experts external to the BIS team. Generally, the auditors found that the design and implementation of the BIS is sound, complete, straight-forward, and, in particular, conform to the requirement on a high inherent level of safety, reliability and availability. However, quite a number of substantial recommendations have been made:

In particular, the auditors are worried about the behavior of the optical link electronics (esp. the ELED and ELED driver circuit), and its future availability on the market. Furthermore, the BIS' VHDL code should be reviewed separately. Additionally, further electrical and RF susceptibility tests should be conducted on all safety relevant boards. Finally, the auditors ask the BIS team to finalize documentation.

Although the auditors agree that a high level of safety has been reached by the BIS, the auditors are concerned about the safety/reliability/availability of the Beam Loss Monitoring system and the kicker system of the LHC Beam Dump System, on which two the BIS largely depends. A separate systematic audit / review should be conducted on them.

Page 1 of 9

# General Impression

**Design and implementation of the BIS is**

- **sound,**
- **complete,**
- **straight-forward, and,**
- **conform to requirement on high inherent level of safety, reliability and availability (SIL4) .**

**BIS as such makes a mature and solid impression.**

**Requirements have been adequately defined.**

**The present implementation fulfils completely the requirements.**

# Documentation

**Quite complete set of documentation on EDMS:**

- incl. drawings for PCB schematics, PCB layout and VHDL code
- Additional documents on Bit-Error-Rate of optical link, resistance under EMC, detailed FMECA

1. Consistent set of up-to-date and finalized documents should be provided.

**One of the main actors finishing his thesis soon:**

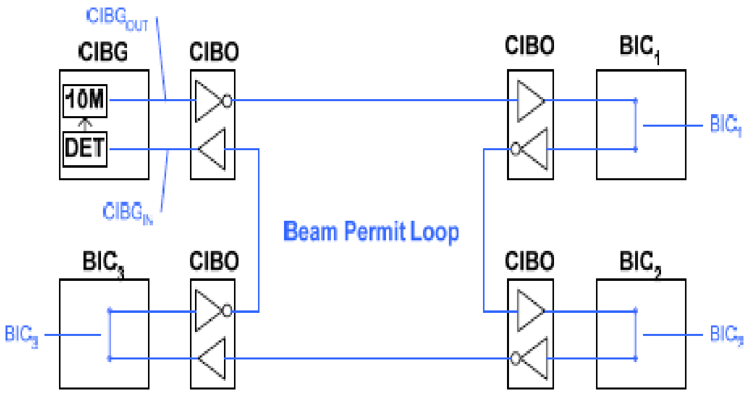
2. Ensure that all information relevant for the project is properly retrieved.

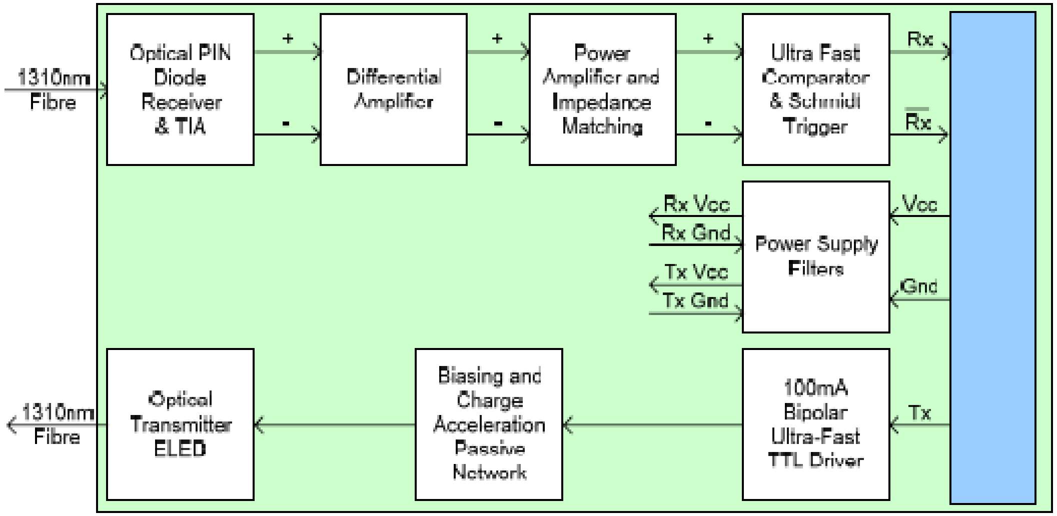
# Optical Loop I

**Severe denial-of-service due to spurious signals on optical fiber link:**

- ELED driver amplified power supply ripples on the “high” state after the signal inversion, transmitted by the ELED, and amplified and shaped by the PIN diode receiver circuit.

13. A solution should be found to avoid this behavior.
14. The availability of the “old-fashioned” ELED seems to present a potential problem.





1310nm Fibre
Optical PIN Diode Receiver & TIA
+
-
Differential Amplifier
+
-
Power Amplifier and Impedance Matching
+
-
Ultra Fast Comparator & Schmidt Trigger
Rx
$\overline{Rx}$
Rx Vcc
Rx Gnd
Tx Vcc
Tx Gnd
Power Supply Filters
Vcc
Gnd
1310nm Fibre
Optical Transmitter ELED
Biasing and Charge Acceleration Passive Network
100mA Bipolar Ultra-Fast TTL Driver
Tx

# Optical Loop II

**Two optical loops at 8.000 and 8.192 MHz:**

4. More separated frequencies like 8.750 and 9.375 MHz should be used.

**For hardwired CCC interlock signals, a CIBU is too distant:**

15. Consistent and safe solution should be found for mitigation.
    The auditors prefer an additional BIC in the CCC.

# Testing & Environment

**Careful functional testing is essential:**

16. Electrical tests of all PCBs
17. Power soak test duration should be justified and adjusted
17. Accelerated thermal aging test of one system
18. “Walkie-Talkie”-type or RF susceptibility test

**BIS depends highly on proper electrical grounding:**

19. Conductivity of unit’s enclosure and earth connection of rack should be tested after installation.

**CIBUs have never been specified to be radiation tolerant:**

27. Radiation tolerance should be defined and verified.
27. Persons responsible for BIS users must be made aware of the situation concerning radiation tolerance.

# Components, Xilinx & VHDL

**Recommendations have been made on choice of components:**

5. Extra power filters for the 230V mains
9. Choice of ceramic capacitors
10. Choice of bi-directional transil suppressor

**Xilinx chip will block once the external clock is missing:**

21. Failure modes and corresponding mitigations should be checked.

**A number of questions came up during reviewing the VHDL code:**

22. VHDL code review should be conducted when the final CIBM design is ready.
23. Storage of VHDL code inside a software repository (e.g. CVS)

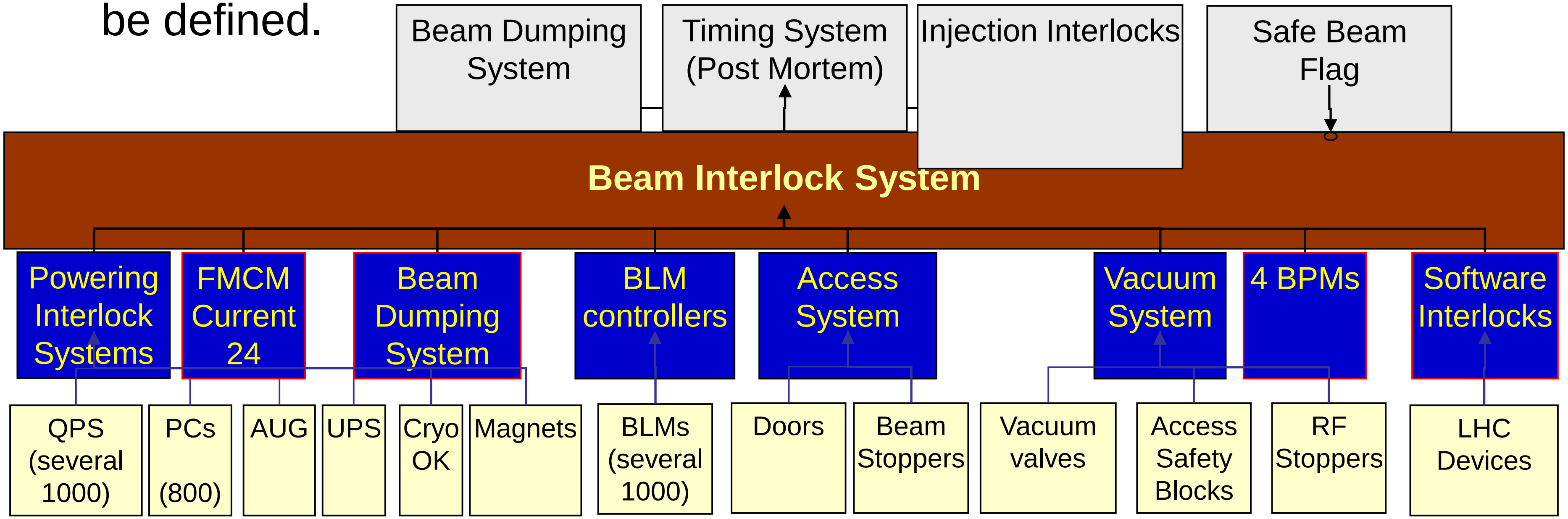
# Interfaces I

**Substantial amount of effort has been put in high reliability and availability of the BIS:**

- Dependence on quite a long list of user systems and on proper functioning of the LDBS

**LHC safety is only as good as its weakest element:**

35. Clear procedures for testing the *full* BEAM_PERMIT-signal chain should be defined.



# Interfaces II (Users)

**LBDS kicker magnet system is essential for LHC safety:**

29. Similar audit should be conducted for LBDS kicker magnets and their trigger mechanism.

**LHC safety relies largely on a small set of monitoring and control systems, e.g. Beam Lifetime Monitors, BLM, FMCM, Powering Interlock, Transverse Feedback System:**

31. Dependencies analysis with regard to LHC safety and of an audit of the major dependencies should be conducted.
32. Procedures are mandatory to guarantee that BIS user systems obey standard safety rules.
32. Awareness discussions & training
33. “Walkie-Talkie”-type or RF susceptibility test on (critical) BIS users
34. Can SOFTWARE_PERMIT sustain high level of reliability and availability of the overall BIS ? Alternatives should be evaluated.

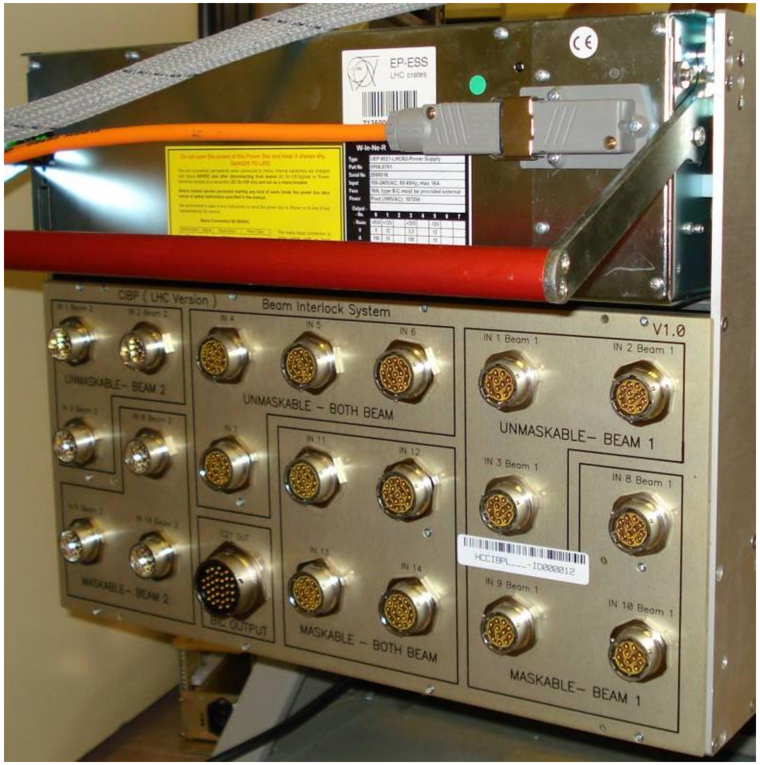
# Safe Beam Mode

**SAFE_BEAM_FLAG allows masking half of the user inputs to the BIC:**

36. No protection mechanism to prevent the exchange of the cables

37. Safe solutions for the implementation of the SLBR board should be investigated.

37. No documentation for the implementation and the SLBR.



**The SAFE_BEAM_FLAG is distributed by the SMP / GMT:**

38. The distribution of the SAFE_BEAM_FLAG should be consistent with reliability / availability / safety of BIS.

# Summary

**Design and implementation of the BIS is sound, complete, straight-forward, and, conform to requirement on high inherent level of safety, reliability and availability (SIL4) .**

**However:**

- To keep reliability high, functional testing on regular basis is vital.
- Worried about the behavior of the optical link electronics (esp. the ELED and ELED driver circuit).
- VHDL code should be reviewed separately.
- Further electrical and RF susceptibility tests should be conducted.
- Concern about the safety/reliability/availability of BLM and kicker system of the LBDS (separate systematic audit / review should be conducted on them).
- Finalize documentation.