LHC Beam Dump System (LBDS)

Report on the Audit held in January/February 2008

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

Richard Jacobsson (PH/LHCB), Stefan Lüders (IT/CO),
Javier Serrano (AB/CO), Benjamin Todd (AB/CO),
Yves Thurel (AB/PO), Matthias Werner (DESY)

Scope

This audit is supposed to verify design & implementation of the LBDS:

- Fundamental design decisions
- PCB schematics & layouts, VHDL & PLC programming
- 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

- Kicker magnet & extraction septum design
- Beam dump dilution and absorption
- Beam aperture issues & protection devices
- System software running on PowerPC & high-level control systems
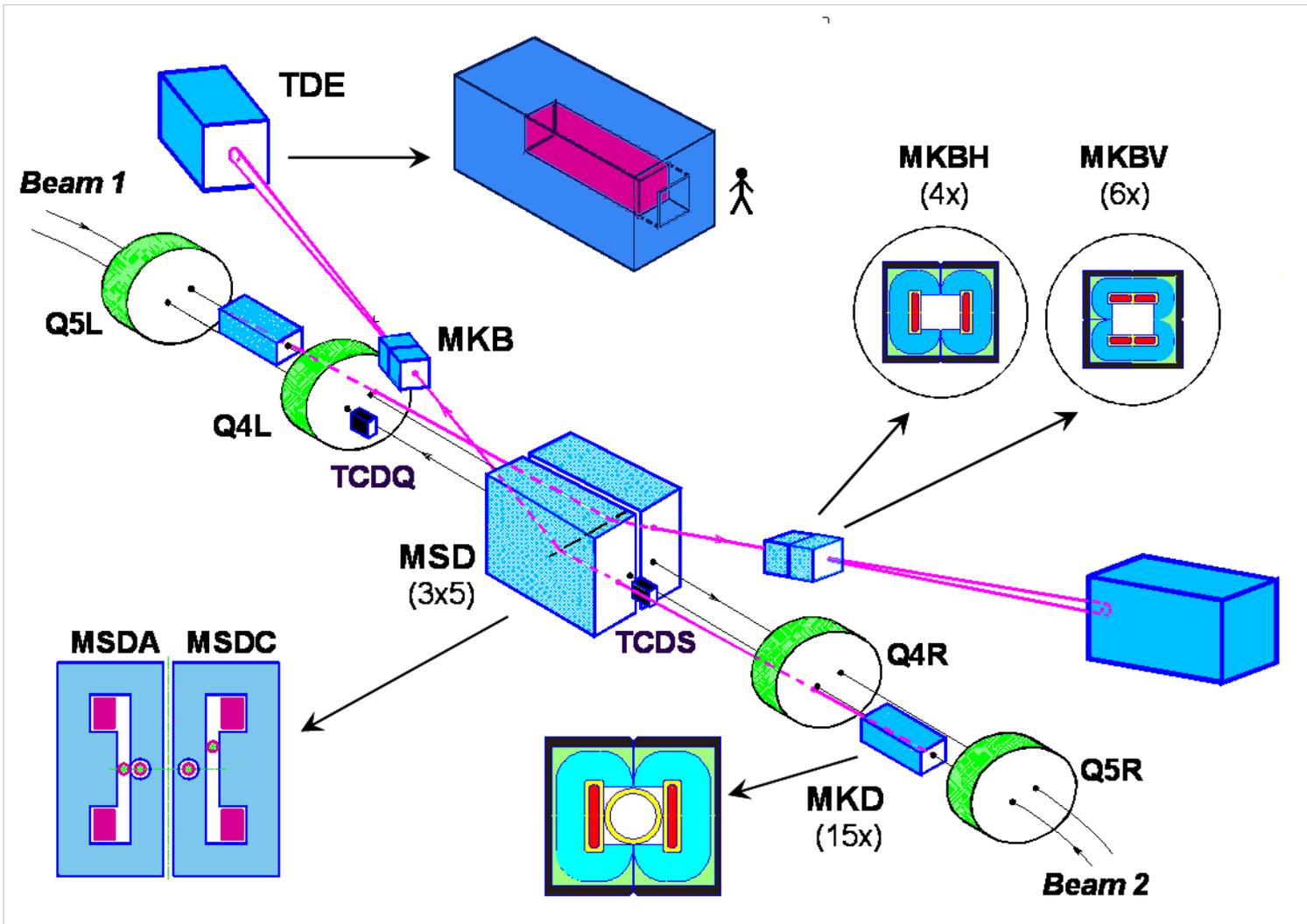
One slide on the "Why"

6 cm

$2 \cdot 10^{12}$ $4 \cdot 10^{12}$ $8 \cdot 10^{12}$ $6 \cdot 10^{12}$
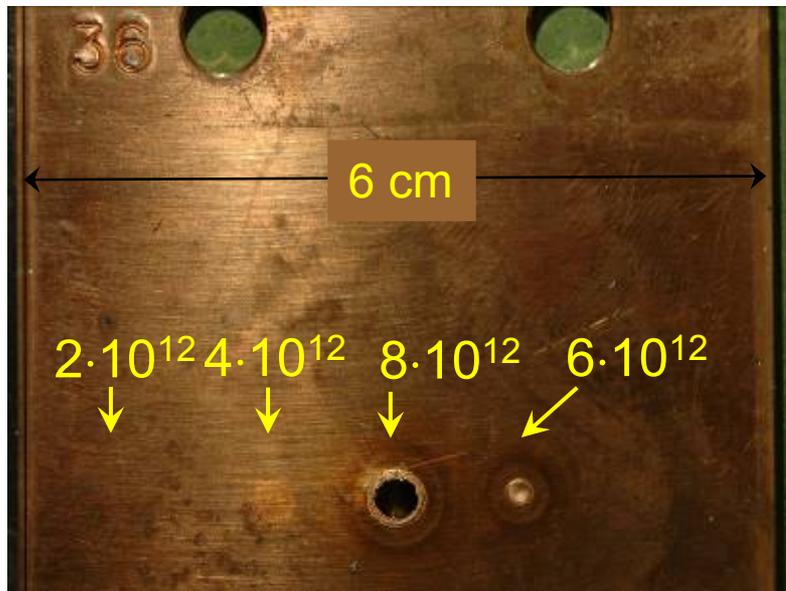
0.1 % of the full LHC beam
$8 \cdot 10^{12}$ protons
$\sigma_{x/y}$ = 1.1mm/0.6mm

25 cm
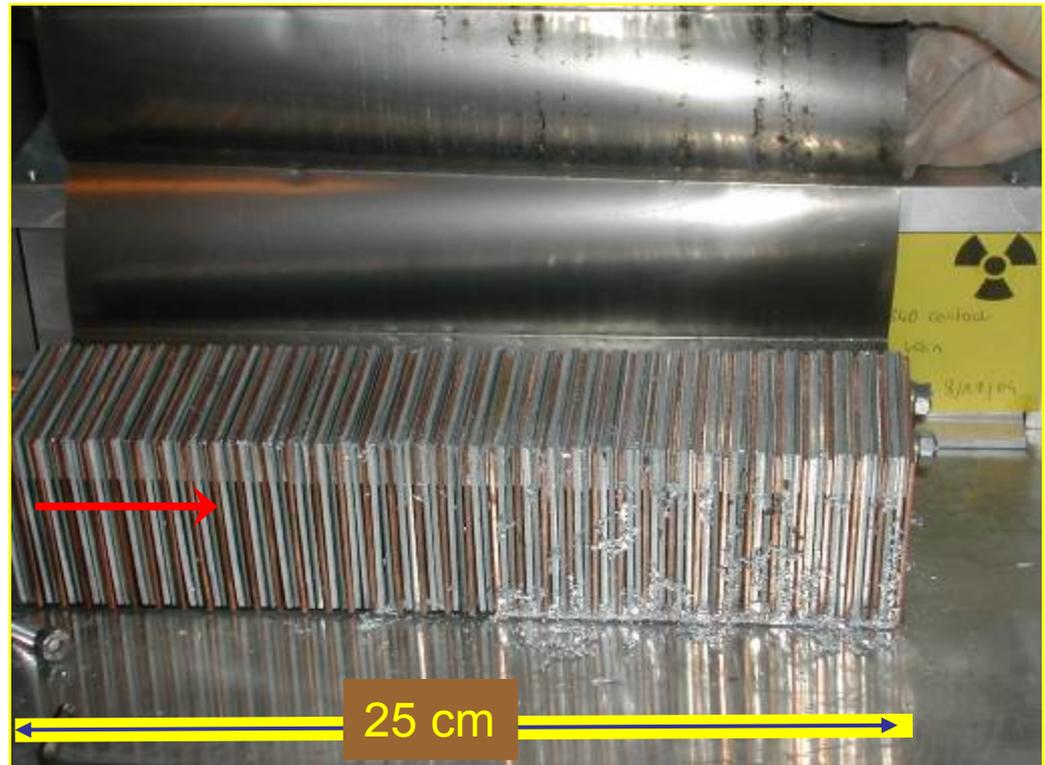
The LBDS Architecture

Auditor's Report

- Lots of good documentation consulted (it lacks a central repository, though)
- Dedicated discussions with experts
- Hands-On on PCBs, VHDL & PLC code
- Visit to point 6
- Participation in CCC dry-run

Recommendations have been distributed to all parties involved.

Focus on major points.

Numbers refer to Audit Report.

February 18th 2008
Revision 1.2

The LHC Beam Dump System

Report on the Audit held on January 28th to February 15th 2008

Auditors: Richard Jacobsson (PH/LHCB), Stefan Lüders (IT/CO), Javier Serrano (AB/CO), Benjamin Todd (AB/CO), Yves Thurel (AB/PO), Matthias Werner (DESY)

Distribution: Etienne Carlier (AB/BT), Laurent Ducimetiere (AB/BT), Brennan Goddard (AB/BT), Verena Kain (AB/OP), Volker Mertens (AB/BT), Steve Myers (AB), Hermann Schmickler (AB/CO), Rüdiger Schmidt (AB/CO), Jan Uythoven (AB/BT), Jörg Wenninger (AB/OP), Wim Weterings (AB/BT)

1 Executive Summary

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

From the auditors' point-of-view, discrepancies in the interface definitions between the BIS and the LBDS, and the LBDS dependency on the RF system's revolution frequency require additional discussion and documentation of the experts involved. Also the energy-dependency of the high-voltage switches has consequences on the complexity of the PLC code, and their degradation in time is worrying. Especially, since this degradation might also (start to) draw from the — already very tight —3µs abort-gap length.

The LBDS requires a high level of safety. An analysis of failure modes, effects and criticality (FMECA) has determined the safety to be SIL 4. The study identified the high power system components dominating the remaining unsafety. Thus, an in-depth study of them should be organized. Furthermore, the overall safety level depends strongly on the "As-Good-As-New"-approach. Clear documentation must be produced of the procedures needed in order to assure the "As-Good-As-New"-state.

The current design does not include special measures to achieve radiation tolerance. However, with regard to the incidents at CNGS and due to the location of the LBDS electronics in the service galleries, a thorough study on radiation effects must be conducted, including both immediate malfunctioning and long-term aging. Long-term radiation effects on the BETS are particularly critical for the LBDS. Also the consequence of EMC on the LBDS electronics and of the high-voltage kicker pulse on other systems must be studied and understood.

Finally, the auditors recommend a more detailed analysis in the form of parallel peer-reviews for the VHDL and PLC code.

General Impression

Design and implementation of the LBDS is

- sound,

- complete,

- straight-forward, and,

- conform to requirement on high inherent level of safety, reliability and availability (>SIL4) .

The LBDS hardware as such makes a mature and solid impression.

Requirements have been adequately defined.
The present implementation fulfils them to a very large part.

However, very high dependence on

- 100% coverage of XPOC & IPOC

- Really random failures

Interface to BIS & RF

Severe DoS due to spurious signals on BIS optical fiber link:

- BIS' 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.

1. Interfaces between BIS and LBDS should be properly discussed, agreed upon, and documented. The resulting solution should minimize the complexity of the overall, combined system without deteriorating overall safety.

2. Measures must be put in place to ensure that the LBDS is always synchronous and in phase with the right and proper beam revolution frequency. This might also require actions from experts of the RF system.

Kicker Generator Switches

The complexity of the kicker generator switches are worrying:

- An impressive effort has been put into ensuring correct timing.

- Reaction time depend on beam energy and is compensated by adjusting kicker energy (i.e. more complex PLC code).

- Indication of degradation.

3. Alternatives for compensation should be discussed.

4. A deeper study must be conducted to understand degradation and alternative solutions must be elaborated.

5. Possibilities to increase the tight time window in order to add some safety margin should be investigated.

"As-Good-As-New"

Special "As-Good-As-New"-tests are crucial for proper functioning:

8. The respective procedures should be carefully elaborated and implemented together with the persons responsible for the RF and BIS systems.

10. Procedures must be established for maintenance and inspection.

11. Procedures have to be put in place for the restart of the LBDS after a beam-dump and after shut-down periods.

   It must be defined and documented when "dry dumps" and "safe beam dumps" are needed, and how this is enforced.

12. An assessment must be conducted on how far the "safe beam dump"-tests resembles operation with full beam and which failures can not be detected by it.

FMECA

A detailed FMEC Analysis has validated the basic design:

13. A second, independent analysis should be conducted to confirm and verify these initial results.

17. A "reliability database" should be set up in order to track failures and to accumulate "real life" statistics.

18. Procedures must be put in place to verify, after a failure, that no safety aspect has been compromised at a design level.

Magnet assemblies account for about 99.5% of the un-safety, while the trigger electronics covers the remaining 0.5%:

14. Since the focus of this review was on the trigger electronics, an independent review of the high power system components should be organised.

EMC

LBDS hardware installed in UA63 and UA67 together with other systems:

20. It is strongly recommended to verify the impact of triggering the kicker magnets onto other, crossing signal lines with respect to cross-talk and EMC.

21. All external cables of the LBDS (e.g. the re-trigger lines) should be tested with burst tests to identify potential susceptibility and verify EMC.
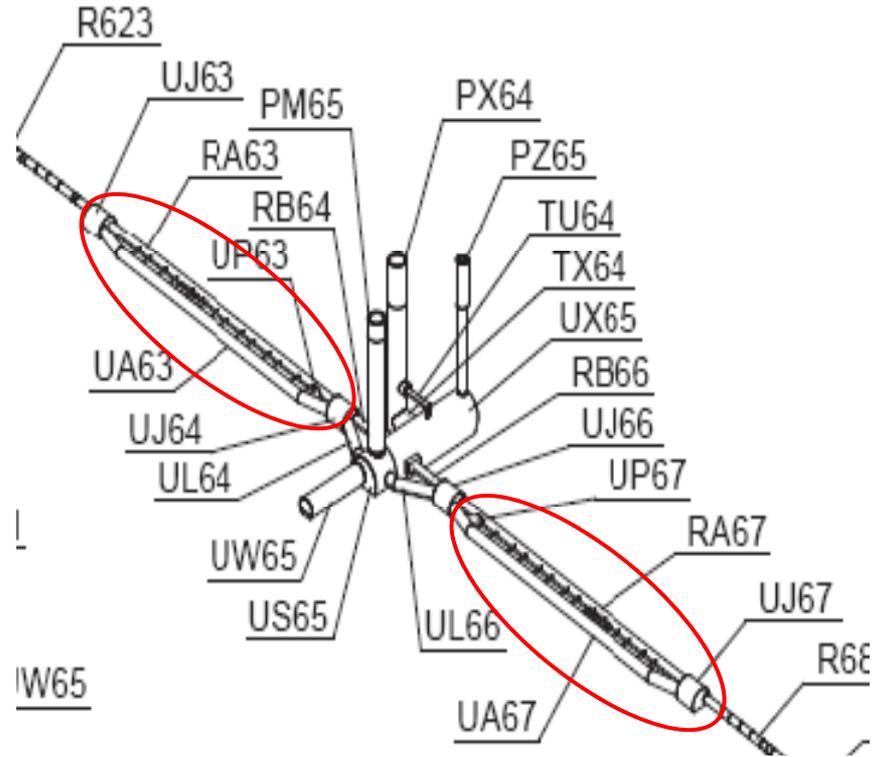
Radiation

LBDS hardware installed in-line with cable ducts to kicker magnets:

- Radiation-tolerance not part of design
- SEEs in CMOS & FPGA hardware, VHDL & PLC code, look-up-tables…

22. Quantify risks due to SEEs & "aging".
23. Simulations to determine expected flux.
24. Create list of susceptible components (e.g. CMOS on the critical signal path).
25. Together with SEE expert, perform irradiation experiments to identify failure modes and cross-sections.
26. Contact Xilinx FAE in order to quantify the risks of FPGA mal-function with the given flux.
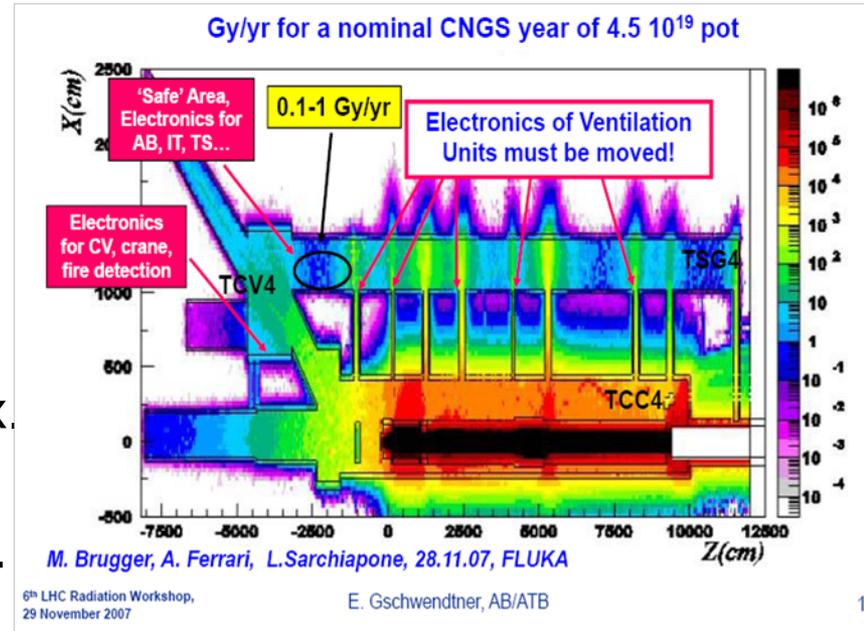
PCBs & Components

Quite a substantial number of components close to their rated limits :

29. An infra red inspection of all PCBs should be done in order to ensure the current high reliability, to verify the power consumption of individual components, and to detect bad components being mounted.

DTACK signal on TSU card may not adhere to complete VME spec:

34. The implementation of the TSU's DTACK should be changed in the next iteration of the design.

Most effective decoupling of FPGA power supplies necessary:

35. The PCB design should consider a proper decoupling of the FGPA to accommodate relatively high power consumption.

Frequent FLASH memory read/write cycles are error prone:

36. It is recommended to use EEPROM instead of FLASH RAM.

VHDL & PLC Code

TSDS and BETS cards are extensively using VHDL code :

37. A tighter collaboration on VHDL programming should be established by the LBDS programmers and other VHDL experts at CERN. A peer-review parallel to the development of the LBDS code should be conducted.

41. Extensive tests must be performed every time a re-design of the FPGA VHDL code is conducted (incl. VHDL compiler changes/upgrades). A robust framework and simulation test bench must be put in place to assure that any upgrades are regression tested.

PLC runs the SCSS and adjust the kicker strength

43. A tighter collaboration on PLC programming should be established by the LBDS programmers and other PLC experts at CERN (e.g. in AB/CO and IT/CO). A peer-review parallel to the development of the LBDS code should be conducted.

Summary

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

However:

- Interfaces to BIS and RF need refinements and verifications.

- Generator switches time-dependency needs re-evaluation and follow up.

- Additional procedures for "As-Good-As-News"-testing needed in order to keep reliability high.

- EMC tests on/from other systems must confirm non-susceptibility.

- Impact & consequences of radiation in UA63/67 must be fully understood.

- Some PCB component need adjustments.

- Deeper external collaboration on VHDL & PLC code recommended.