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.

2 Contents

3 Scope

This audit is supposed to verify the design and implementation of the LHC Beam Dump System (LBDS). It should cover the fundamental design of the Trigger Synchronization and Distribution System (TSDS) electronics as well as the electronics used for the Beam Tracking System (BETS), i.e. design decisions and documentation, PCB schematics and layouts, VHDL programming, mechanics, as well as the interfaces to other systems, mainly the Beam Interlock System (BIS) and the Direct Current Current Transformers (DCCT) used for energy tracking, and the RF system.

Particular focus should be put on the safety relevant aspects of the LBDS kicker and trigger system design, i.e. the verification whether the LBDS allows for a safe and reliable dumping of the LHC beams, and whether it provides a sufficiently high reliability and availability. The audit should reveal also single points of failures and failure modes leading to blind faults (i.e. failing to dump beams when demanded).

Furthermore, this audit does not cover accelerator hardware like the kicker magnet design, the septa design, the magnet system used for beam dilution nor passive protective devices (beam diluters) and the beam absorber block. It also does not cover beam-related aspects like the synchronization with the beam abort gap or the correct aperture of the beam when being dumped. Finally, high-level control aspects and system software running on the PowerPC are covered only as far as needed for reviewing the "As-Good-As-New"-approach.

4 General Impression

The auditors are convinced that the fundamental implementation of the LBDS (as defined by the scope of Chapter 3) is sound and properly executed. The system as such makes a mature and solid impression. The requirements for the safety-critical functions, especially for a safe and reliable execution of the beam dump, but also for a high availability of the system itself have been adequately defined and the present implementation fulfils a very large part these requirements. High reliability and availability was consequently implemented by a fully redundant signal chain from the BIS to the LBDS kicker magnets.

A thorough analysis of failure modes, effects and criticality (FMECA) [1] has shown that the current design of the LBDS can reach a Safety Integrated Level (SIL) 4 and better. However, the analysis and the subsequent LBDS design were based on two crucial assumptions:

- The "As-Good-As-New"-tests (XPOC and IPOC) must be *very reliable in detecting* that something failed, and
- Failures during operation *must happen at random.* Simultaneous failures of e.g. two independent boards in different locations, which are seemingly unconnected, have not been taken into account.

The auditors agree that the XPOC and IPOC tests and their connections to the connection to the Injection Inhibit are critical and must be able to cover most if not all of the failure modes. However, **neither the XPOC nor the IPOC currently seem to be fully mature.** Areas of concern have been listed in Section 5.1.2. Although the inherent LBDS hardware does not show evidence for potentially correlated failure modes, **the auditors are concerned about external "common mode" influences** in particular due to Single Event Effects (SEEs; see Section 5.2.2.).

As a side remark, the review itself has been well prepared by the LBDS team. A summary of the LBDS team on their actions should be given in 6 months time.

5 Recommendations by the Auditors

Having reviewed carefully the basic design principles and functionalities, and having gone thoroughly through PCB schematics, through the VHDL and PLC code, and through available documentation, several areas for improvements have been identified.

This chapter lists all recommendations the auditors consider important enough to be mentioned. Quite some more comments have been directly made during the audit and in dedicated discussions with the LBDS team. Errors in the PCB design and VHDL code have been corrected immediately during these discussions. Other issues have been directly communicated to the corresponding experts.

Major points and issues are marked in bold.

5.1 General Design and Functionality

The design of the LBDS requires a couple of basic design decisions. In particular, the width of the beam abort gap put stringent boundaries on the LBDS timing, and subsequently on the choice of hardware and its implementation. Furthermore, the LBDS is embedded into the overall LHC controls which, thus, require interfaces to other systems like the BIS or the RF system. A thorough FMECA [1] was very important in validating the design choice of the LBDS.

5.1.1 Major Design Aspects

1. The most important input to the LBDS is the BEAM_PERMIT signal from the Beam Interlock System (BIS). The BIS is responsible for transmitting beam dump requests from numerous systems to the LBDS. The BIS achieves a high level of safety (SIL 4) as confirmed by a recent review [2]. In 2006, one of the BIS review conclusions triggered a redesign of the initially weak "CIBO" optical component. This initially weak design, combined with a poorly installed optical transmission links resulted in a denial of service of the Beam Interlock Controller history buffers during some trials in 2006 [3]. Following the BIS review an improved CIBO design was realized, and the corresponding specification describing the interface between the BIS and LBDS was revised [4].

   The interfaces between the BIS and the LBDS are crucial for the overall safety chain. Thus, these 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. The LBDS must be properly locked on the beam revolution frequency. This frequency is distributed by the RF system in point 4, but means are lacking which ensure that the LBDS is locked onto the proper revolution frequency and that the edge is absolutely fixed (i.e. a locked receiver must not necessarily be locked onto something proper). In fact it turned out that swapping beam 1 and beam 2 signals on the RF side is easily possible.

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[1]. This might also require actions from experts of the RF system.

3. An impressive effort has been put by the LBDS team into ensuring the correct timing for the critical trigger path. Unfortunately, the reaction times of the high-voltage switches deployed for triggering the kicker magnets have shown a dependency on the necessary kicker energy (which, in turn, is proportional to the beam energy). This introduced an additional delay which is compensated by modulating the kicker voltage through additional look-up-tables in the LBDS PLC controlling the kick energy. However, this significantly increases the complexity of the PLC code.

    Alternatives to compensate this additional delay should be discussed.

4. The first experience of the LBDS has shown a slight, but constant degradation of the kicker magnet switches, presently studies by the experts.

    A deeper study must be conducted to understand this behaviour and alternative solutions must be elaborated.

5. The time window for triggering the kicker magnets and raising the magnet fields is rather tight, provides no slack, and, thus, does not allow for a potential future needs (e.g. due to wear-out of the cables or degradation of the electronics). Especially together with the two aforementioned implementation issues, this tight time window providing no contingency is worrying to the auditors.

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

6. In order to achieve a very high availability, the LBDS is employing full redundancy in the trigger signal chain and the beam energy measurement starting from the BIS and dipoles, respectively, and ending at the kicker magnets. However, incidents elsewhere (e.g. at the Detector Safety System) have shown, that even accidentally swapped cables can completely spoil this redundancy and, thus, the availability.

    Therefore, the redundancy and its correct and complete separation must be verified. Means to ensure that external cables can not be swapped must be applied. Furthermore, the consequences of the non-redundant signal paths on the PTM and TFOT boards on the overall availability must be reviewed.

7. The LBDS is monitoring the state of primary and UPS alimentation and is able to dump the beam in case of power failures. However, in case of a simultaneous failure of both sources the LBDS depends fully on internal power contingencies and latencies of local power supplies and capacitors.

    Adequate tests should be conducted to confirm that the system remains being capable of dumping the beam in case of simultaneous main and UPS power failures.

---

[1] The auditors acknowledge the fact that much effort has been put on protecting the dump gap by an inherent mechanism of the LBDS itself. However, it would be more elegant and proper if the RF could guarantee that they transmit the actual orbit pulse locked at a constant phase with respect to the dump gap via an interlock.

5.1.2 Testing, Rearming, Resetting & "As-Good-As-New"

8. Special "As-Good-As-New"-tests are envisaged to verify the proper functioning of the LBDS and to guarantee the proper cabling with the external users (i.e. BIS and RF). However, being very crucial for the proper functioning of the LBDS, such internal tests are non-trivial.

    The respective procedures, still lacking in detail, should be carefully elaborated and implemented together with the persons responsible for the RF and BIS systems. Regular "toggle on/off"-tests prior to injection with cross-checks against a central database might be able to find errors in the data chain, false cabling, and wrong "inhibit"-switch settings. However, these tests should also take into account cases of sabotage or simple vandalism.

9. Special and automated connectivity test procedures must be deployed in order to detect bad or faulty cable connections.

10. Additional procedures must be established for maintenance and inspection in order to detect degradation of the LBDS hardware, esp. of the kicker magnets.

11. Additional procedures have to be put in place for the restart of the LBDS after a beam-dump and after shut-down periods. In particular it must be defined and documented when "dry dumps" and "safe beam dumps" are needed, and how this is enforced.

12. Finally, an assessment must be conducted on how far the "safe beam dump"-tests resembles operation with full beam, which failure modes this test is able to covers, and which failures can not be detected by the "safe beam dump"-test.

5.1.3 Failure Mode Error and Criticality Analysis

13. A detailed Failure Mode Error and Criticality Analysis (FMECA) has validated the basic design of the LBDS and the choices and extent of redundancy [1].

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

14. The FMECA has identified the magnets, their switches, and the power converters account for about 99.5% of the un-safety, while the trigger electronics covers the remaining 0.5%.

    Since the focus of this review was on the trigger electronics, an independent review of the magnet components should be organised.

15. The FMECA has used the Military Handbooks and failure modes methods and is, thus, only as strong as the original information. Generally the FIT rates do not seem either too optimistic or too pessimistic; they fall largely in line with the studies carried out for the Beam Interlock System [5].

    A sensitivity analysis should be conducted to estimate if the sources (Military Handbook and the methods) are directly applicable and realistic to power systems. For example, the value of 103 FIT for power converter failure (λps) was obtained from the corresponding manufacturer.

16. In addition to the previous point, relative failure rates are much more meaningful that absolute ones. A comparison of the estimated values and values derived by

accelerated testing of specific components (components identified by the aforementioned sensitivity analysis) should be made.

17. It is equally vital that failures are tracked in order to ensure that the assumptions made in the FMECA thesis hold. Therefore, a "reliability database" should be set up in order to track failures and to accumulate "real life" statistics. This can be done in collaboration with other groups concerned (e.g. BIS, BLM, QPS).

18. Furthermore, it is crucial that failures which could potentially undermine the safety are fully understood. Procedures must be put in place to verify, after a failure, that no safety aspect has been compromised at a design level (see also Section 5.1.2).

19. Following from the FMECA results, 0.23 false dumps per year are produced on average by the trigger electronics. However, it is not clear in how far bit error rates of all the fibre links have been included in this estimation. Eventually, the Manchester decoder can be made more robust by oversampling.

5.2 Environmental Aspects

Most of the LBDS hardware has been installed in the service galleries UA63 and UA67 with direct cable ducts to the kicker magnets. The service galleries are shared with many other systems and a manifold of signal cables are routed through the galleries.

5.2.1 Electromagnetic Compatibility (EMC)

20. All high voltage coax cables to the kicker magnets (eight per magnet and 15 magnets per beam) pass right below a manifold of other signal cables used by other systems.

   During the planned EMC testing period, it is strongly recommended to verify the impact of triggering the kicker magnets onto these crossing signal lines with respect to cross-talk and EMC. Eventually, additional shielding measures must be deployed.

21. Vice versa, the LBDS signal lines might be susceptible to EMC from other systems. Such cross-talk might create false beam-dump requests.

   All external cables (from one crate to another, e.g. via the re-trigger lines) should be tested with burst tests to identify EMC potential susceptibility.

5.2.2 Radiation

22. Radiation-tolerance has not been considered in the design of the LBDS and its electronics does not cope with radiation higher than the average flux at sea-level due to e.g. cosmics[2]. However, observations during the CNGS experiment [7] have shown that the exposure of some hardware components, esp. PLCs, was higher that initially anticipated and lead to a drop-out of these components.

   In case of the LBDS, some electronics is located in line with the large (90 cm diameter) cable ducts guiding the power cables to the kicker magnets in the accelerator. This direct line-of-sight might create Single Event Effects (SEEs; i.e. single event upsets or latch-ups) in the CMOS or FPGA hardware, the VHDL and

---

[2] According to [6], even at sea-level the Xilinx Spartan 31000 is much more probable to be affected by SEUs than statistically failing due to normal wear-out. The expected FIT at sea level is around 60 for configuration buts and 110 for the BlockRAM for a fully charged FPGA. The real FIT scales linearly with the configuration and memory load.

PLC code, or in the look-up tables used for beam energy determination and kicker strength settings. In addition to immediate upsets neutron radiation may cause long term effects ("aging"). The Fast High Current Thyristors switch wafers are also known to be sensitive to irradiation.

Thus, it is recommended to quantify what risks, if any, are posed to the LBDS by radiation effects. The risks of SEEs and "aging" on the LBDS hardware must be understood and critical locations and components must be identified.

Correcting mitigations must be implemented. Separate measurement devices and additional protections, i.e. shielding, must be deployed or improved if needed. Other, longer term, measures could include installation of radiation-resistant components or displacing critical racks.

23. In particular, it is recommended that:

    Simulations are advanced to determine the expected flux in UA63 and UA67;

24. **A list of potentially susceptible LBDS components is created (e.g. all CMOS devices on the critical signal path);**

25. **An SEE expert coordinates irradiation experiments to identify failure modes and cross-sections of these components;**

26. **A Xilinx FAE is contacted in order to quantify the risks of FPGA mal-function with the given flux;**

27. **An updated FMECA model is created, plotting safety versus flux to show the boundaries of the system operation.**

    These studies should include factors to determine the likelihood of combined failures within a 10 hour exposure window, which quantifies the risk for a normal operational sequence. With view on the workload involved with this, an expert study a few components on the critical path should be able to give an indication of the impact of the radiation.

5.3 Electronics

The LBDS electronics consists of three branches with different functionality:

- The VME-based hardware trigger electronics receives the beam dump signal from the BIS, the direct Beam Loss Monitors or the LHC Access Safety System, synchronizes the signal with the beam abort gap, and distributes this signal reliably to the kicker magnet high-voltage generators. It mainly consists of the Trigger Synchronization Unit (TSU), Trigger Fan-out unit (TFO), the Power Trigger Unit (PTU) as well as the Re-trigger Delay unit (RTD). Particular care has been invested into proper delay lines and correct timing between those elements.

- The VME-based BETS measures the beam energy and calculates the kicker magnet reference strengths (Beam Energy Measurement (BEM) cards), surveys the charging voltages of all magnet generators (Beam Energy Interlock (BEI) cards), and dumps the beam in case of abnormal deviations (Beam Energy Controller (BEC) cards).

- Finally, the whole system is supervised by a safety PLC ("State Control & Surveillance System" (SCSS)) which is also responsible for adjusting the kicker strength to the corresponding beam energies taking the energy reference from the BETS. The PLC is

using the Siemens S7 family, partially employing failsafe modules and PROFIsafe communication.

5.3.1 PCBs and Choice of Components

28. Quite a substantial number of PCBs use components close to their rated limits. This might compromise safety. For example, some tantalum capacitors rated 16V are used at 12V nominal operation voltage. Usually this value drops if the temperature at the cap is hot (i.e. rating is down at 12V at 125°C).

    It is recommended to use components with higher margins like a 25V rating.

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.**

30. In order to detect faulty components and boards, additional power soak tests should be conducted.

31. In addition, an accelerated thermal aging test of one system might be conducted as well, in order to check that the computed lifetime is not completely wrong.

32. Careful functional testing is essential. Even electronics manufacturers with good reputation produce faulty equipment. Therefore, electrical testing is preferable to visual inspection and, if properly implemented, even faster. Errors on that level are very cumbersome to find once a unit is fully assembled.

    Electrical tests of all PCBs should be conducted. These are easily possible using standard automatic cable testers.

33. Some schematics deviate from the real PCB implementation which might lead for confusion if PCBs have to be reproduced. Design schematics should always be kept up-to-date.

34. Furthermore, it appears that the DTACK signal on the TSU card may not adhere to the complete VME specification [8]. Rule 6.21 "Drivers and Loading Rules for Open-Collector Lines" states for the correct implementation of these signals: "If a VMEbus board drives the lines BR[0..3], BBSY, IRQ[7..1], DTACK, BERR, SYSFAIL, SYSRESET, ACFAIL, IACK then its drivers must meet the following specifications: IOL>48 mA, VOL<0.6V at IOL=48mA".

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

35. In general designing FPGA power supplies is quite complex. Particular care has to be taken to ensure that the most effective decoupling is used so that the design will function correctly in all cases. Note that the FPGA power consumption is directly linked to the VHDL code which is running. Some code may consume substantially more than others (primarily depending on resource usage and clock speed).

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

    Reference [9] might provide a guideline (Its principles hold for any particular FPGA design, including the S31000; esp. page 13pp and Figure 8. This also documents procedures to check on potential supply issues). Once the VHDL code has been

finalized, "Xpower" (ISE Accessory) or "Xilinx Power Estimator" (XPE) can be used to get an overview of more detailed consumption [10].

36. Finally, studies on frequent FLASH memory read/write cycles have shown them to be error prone [11]. In particular Single-Level-Cells should have no more than 1,000,000 read cycles per block; Multi-Level-Cells no more than 100,000 cycles. Both are about one order of magnitude higher than the PROGRAM-ERASE cycle-limit of the devices. The LBDS is reading back data about once per millisecond. Thus, in just a few hours errors may occur.

    The expected rate of errors in the FLASH ROMs used in the LBDS have to be verified with regard to these studies. If applicable, the use of EEPROMs instead of FLASH RAM (as e.g. done in the Safe Machine Parameters project) is strongly recommended.

5.3.2 VHDL Code

37. The LBDS' TSDS and BETS cards are extensively using FPGAs running VHDL code. This firmware can, in particular, affect the reliability of the LBDS system through the design and programming of the look-up-tables in the TSU and in the BETS. Generally, a commonly agreed body of knowledge for safe digital design exists, which includes concepts such as systematic synchronization of all asynchronous inputs before using them anywhere, making sure unreachable states in state machines are properly handled, etc.

    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.

38. Quite a substantial number of questions came up during reviewing the VHDL code. The VHDL code is following a synchronous reset strategy, which is very good. However, in some designs the remaining few asynchronous resets should also be modified into synchronous resets.

39. The "When others" clause is extensively used to make state machines safer, but at least left out on the BEC.

40. Furthermore, it is very important to clock in asynchronous signals by three consecutive flip-flops (at least) using the system clock before propagating them further. However, in the TSU FPGA this has been omitted and the revolution clock is fanned out to a number of blocks before being synchronized. This can give problems with metastability and, subsequently, incoherent states in the different blocks.

41. With the decision of including the TF ROM inside the FPGA in the BEM, a change in the contents of that ROM will imply a whole re-run of the FPGA's synthesis, place & route, etc.[3].

    Extensive tests must be performed every time a re-design of the FPGA VHDL code is conducted. This must include re-assessments if the VHDL compiler changes or is upgraded. A robust framework and simulation test bench must be put in place to assure that any upgrades are regression tested.

42. Proper documentation of the VHDL code inside a software repository like CVS is recommended.

---

[3] Unless partial re-design software is used.

5.3.3 Programmable Logic Controller (PLC) Code

43. The PLC code has been written by a several programmers in STL and SCL and has grown rather complex. The current code is a mixture of being finally deployed and programs for test purposes.

    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.

44. Appropriate commentary statements, currently widely missing, should be inserted into the different programs.

45. The operational blocks (OBs) 80, 81, 82, 83, 84, 85, 86, 121, 122 have been deployed which is very good since this avoids stopping the PLC is case of internal failure. However, appropriate programs should be added in order to transmit failures to the supervisory control system.

46. Proper version management of the PLC code inside a software repository like CVS is recommended. AB/CO is currently preparing guidelines for this. Methods must be put in place to ensure that the right code is loaded in the right PLC.

47. A high-level document describing the code, all programs and the data blocks, should be produced prior to the aforementioned peer-review.

6 References

[1] R. Filippini, "Dependability analysis of a safety critical system: the LHC beam dumping system at CERN", CERN, 2006, CERN-THESIS-2006-054

[2] S. Lüders et al. "The Beam Interlock System (BIS) — Report on the audit held on September 18th-25th 2006", CERN, 2006

[3] B. Todd, " Beam Interlock System – FMECA", CERN, 2006, CERN EDMS 762129, https://edms.cern.ch/document/762129/;
B. Todd, CERN, private communication, 2008

[4] B. Todd, "Beam Interlock System - Beam Permit Loop Frequency Detection Parameters", CERN, 2008, CERN EDMS 882596, https://edms.cern.ch/document/882596/;
B. Todd, "Beam Interlock System - Beam Permit Loop Study", CERN, 2007, CERN EDMS 762158, https://edms.cern.ch/document/762158/

[5] B. Todd, "A Beam Interlock System for CERN High Energy Accelerators", CERN, 2007, CERN-THESIS-2007-019

[6] J. Le Mauff, Xilinx Military/Aero Sales Development, private communication, 2008

[7] T. Wijnands et al., "Radiation Tolerance Assurance of the LHC baseline machine", CERN, 2007, http://ab-div.web.cern.ch/ab-div/Meetings/ltc/2007/ltc_2007-17c.pdf;
E. Gschwendtner et al., "CNGS Run 2007: Radiation Issues", CERN, 2007, http://indico.cern.ch/getFile.py/access?contribId=20&resId=1&materialId=0&confId=20366

[8] VITA, "The American National Standard for VME 64, ANSI/VITA 1 - 1994", 1994, p. 225, Section 6.4.2.5, Rule 6.21

[9] M. Alexander, "Power Distribution System (PDS) Design: Using Bypass/Decoupling Capacitors", Xilinx, 2005, Xilinx XAPP 62, http://www.xilinx.com/support/documentation/application_notes/xapp623.pdf

[10] Xilinx, "Xilinx Power Estimator", 2007, http://www.xilinx.com/ise/power_tools/license_spartan3.htm

[11] J. Cooke, "Flash Memory Technology Direction", Micron Technology Inc., 2007, http://download.microsoft.com/download/d/f/6/df6accd5-4bf2-4984-8285-f4f23b7b1f37/WinHEC2007_Micron_NAND_FlashMemory.doc