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.

Contents

1 Scope

This audit is supposed to verify the design, implementation, and pre-series of the Beam Interlock System (BIS). It should cover fundamental design decisions and documentation, PCB schematics and layouts, VHDL programming, mechanics, as well as the interfaces to other systems, mainly the BIS users and the LHC Beam Dump System. As such it should verify whether the requirements for the BIS are adequately defined, and if the current implementation matches those requirements.

Particular focus should be put on the safety relevant aspects, i.e. the verification whether the BIS allows for a safe and efficient operation of the LHC, 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. permitting beams, when it should not).

However, this audit does not cover control aspects and system software running on the PowerPC nor does it treat methods for remote diagnostics.

2 General Comments

The auditors are convinced that the fundamental implementation of the BIS is sound and properly executed. The system as such makes a mature and solid impression. The requirements have been adequately defined, and the present implementation fulfils completely the requirements.

The design has taken into account the reliability requirements as a constraint. High reliability and availability was consequently implemented by a fully redundant BEAM_PERMIT loop. Which such an implementation, the BIS can reach a Safety Integrated

Level (SIL) 4. However, in order to keep the reliability of the system high, functional testing on a regular basis is vital. The respective procedures, not presented within the review, should be carefully elaborated and implemented.

Having gone thoroughly through all PCB schematics, through the VHDL code, and through all documentation, several areas for improvements have been found. Errors in the PCB design have been corrected immediately during the discussions with the relevant experts. Other mistakes have been directly communicated to the corresponding experts. However, in case of the VHDL code, we recommend a more detailed analysis of what has been provided.

3 Recommendations by the Auditors

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 BIS team.

Major points and issues are marked in bold.

3.1 Documentation

The BIS team has provided a quite complete set of documentation, including drawing for PCB schematics, PCB layout and VHDL code. All documentation is stored on EDMS. Additional documents have evaluated the Bit-Error-Rate of the optical link, the resistance under high electromagnetic noise, or provided an exceptionally detailed FMECA (Failure Mode, Effects and Criticality Analysis).

1. However, most of the documents are not completely consistent and more recent documentation is lacking on EDMS but stored elsewhere. Also, PDF-versions of the PCB schematics, and pictures of all boards are favorable.

   A consistent set of up-to-date and finalized documents should be provided.

2. Furthermore, one of the main actors is a PhD student who is finishing his thesis soon. Thus, some kind of transition can be expected in the near future, which will lead to a loss of expertise. Unfortunately, this transition is coming during a very critical phase of the BIS production.

   It has to be made sure that all information relevant for the project is properly retrieved.

3. Finally, a lot of design aspects haven't been finally settled (e.g. future usage of the ELED, extension of the RS422 by means of an optical fibre link; see also Section 3.2.3 below).

   A full listing of all pending design aspects should be provided.

3.2 Electronics & PCB Layouts

The schematics for the PCBs and the PCBs themselves have been designed and produced with a lot of skill and care. A huge effort went into studies on electromagnetic compatibility, bit-error-rates, and the analysis of failure modes, effects and criticality (FMECA).

3.2.1 Electrical Design

4. The frequencies of the optical loops (8.000 and 8.192 MHz, respectively) have been chosen such that they are no harmonics of the beam cycling frequency. However,

8.000 MHz is a sub-harmonic. Furthermore, 8.192 MHz is very close to it, which makes it more difficult to detect crosstalk between both loops.

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

Both frequencies can be easily derived from 40 MHz quartz at the expense of a jitter of +/-12.5ns with a non-integer-divider.

5. Extra power filters to 230V mains should be added in order to protect the system against power spikes. This improved e.g. the availability of some sensitive systems at DESY to a high degree.
6. Erroneous oscillation of a user system or a malfunction of the CIBU or CIBM might create a continuous signal with a frequency above 300 kHz. This signal fed into the matrix produces a constant BEAM_PERMIT signal due to the filter software.
7. In the optical receiver electronics (CIBO), the functioning of the two time constants (one high pass filter after the optical receiver, one after the differential amplifier) and the Schmitt trigger threshold should be well understood and — if necessary — adapted in order to obtain the desired functionality.

3.2.2 Choice of Components

8. Since 5×20mm fuses do not have the capability to cut AC high short circuit currents, it must be ensured that the maximum short circuit current of the AC network is below the short circuit capability of the CIBU.
9. A ceramic capacitor reliability is

   - given by dielectric material choice (e.g. X7R is a good choice);
   - inversely proportional to C×V (where "C" denotes the capacitance and "V" the applied voltage) for a given size;
   - proportional to the thickness of the layers inside chip;
   - inversely proportional to the number of layers (i.e. a high C×V in low size chips requires high number of layers);
   - influenced by the electrode material: For example, silver is the best material, while nickel is not as good (e.g. under high humidity it is more likely to corrode). However, nickel electrodes are likely used in high C×V chips, since silver electrodes are not compatible with so thin layers (i.e. there are migration problems inside too thin layers);
   - depending on the fabrication process (i.e. wet or dry).

   The use of the current 10µF 10V 1206 X5R capacitors in the CIBO should be checked in detail if they match the high required reliability. In case these capacitors are to be kept, each capacitor should pass 1.5 times the nominal voltage at maximum temperature for at least 168 hours.

10. The bidirectional transil suppressor with reference "SMBJ15CA" from Fairchild was used for the QPS electronics and on LHC power converters but found to be of bad quality. The current manufacturer is now Vishay.
11. Some PI filters use ceramic capacitors and SMD inductors. The BIS team is asked to verify that no high-frequency over-shoots arrive at startup. Also they are asked to check the power supply decoupling of the opto-transmitter and the receiver.

12. The redundant power supplies are decoupled from each other by the usage of Schottky diodes. However, it was not clear if these diodes are covered in the FMEC analysis.

3.2.3 The Optical Link

13. During the live presentation, the BIS encountered a severe denial-of-service due to spurious signals on the optical fiber link.

    In order to keep 50% duty cycle, the signal on the optical loop is inverted on each CIBM. Thus, every second ELED emits while the BEAM_PERMIT is false. It turned out that the spurious signals were due to the ELED driver which amplified power supply ripples on the "high" state after the signal inversion. This signal was transmitted by the ELED, and amplified and shaped by the PIN diode receiver circuit.

    A solution should be found to avoid this behavior.

14. The availability of the "old-fashioned" ELED seems to present a potential problem.

    Alternatives should be investigated.

15. For the hardwired SPS and LHC interlock signals used by the operators in the CCC, the CIBU will be installed at a distance exceeding the RS422 maximum distance. The BIS team is currently discussing two options:

    - an interface using optical transmission for the signals to be exchanged between the CIBU and the BIC [2]; or
    - an additional BIC crate with CIBM boards near the CCC being part of the optical link loop.

    A consistent and safe solution should be found for mitigation. However, for the sake of simplicity, the auditors prefer the later option.

    Any solution should be reviewed and integrated in the FMEC analysis.

3.2.4 Electrical Testing & Commissioning

16. 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. These electrical tests are easily possible using standard automatic cable testers.

    Additional, electrical tests of all PCBs should be conducted.

17. Currently power soak tests are conducted for about one hour.

    The test duration should be justified and adjusted.

    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. Both tests might improve detecting faulty components and boards.

3.2.5 Electromagnetic Compatibility (EMC)

18. The system itself has been tested successfully with respect to EMC [1].

Additionally a "Walkie-Talkie"-type or RF susceptibility test should be conducted.

19. The BIS depends highly on proper electrical grounding. It has to be verified that the grounding of the VME crates, the chassis and the racks is properly made and does not spoil the efforts being put in the grounding inside the BIS itself.

    The conductivity of the unit's enclosure and the earth connection of the rack should be tested after installation.

20. It has to be made sure that all cables including those installed by the TS/EL group use 360 degree shielding on the BURNDY type connectors.

21. The Xilinx chip on the BIS Manager Board (CIBM) and the matrix implemented therein will block once the external clock is missing. For example, the local oscillator might fail due to external power glitches. Thus, the Xilinx chip might fail blind.

    Failure modes and corresponding mitigations for the local oscillator should be checked.

    A small series of gates (i.e. a basic ring oscillator) implemented in the Xilinx chip might provide mitigation.

3.3 VHDL Coding

The VHDL software can, in particular, affect the reliability of the BIS system through the design and programming of the matrices in the CIBM. 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.

22. Quite a substantial number of questions came up during reviewing the VHDL code.

    For example, if a CIBM board is not properly initialized, the BEAM_PERMIT signal might be permitted permanently. Also, a reset line stuck to its active state will drive the permit output permanently to an "active" state. Another example refers to the anti-glitch circuit, which, unfortunately, couples some signals to others: Instead of using several 1-bit comparators, an n-bit comparator is used, such that glitches (or even normal transitions) on one signal are taken into account for the deglitching of another signal. These are just some examples of issues that should be carefully checked by a team of logic designers in a dedicated review.

    Since the CIBM is undergoing a hardware revision, it is proposed to hold a VHDL code review when the final CIBM design is ready.

    This code review should include all boards considered critical, and in particular the CIBM and the CIBU.

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

3.4 Mechanics & Installation

The electronic boards are installed at several locations around the accelerator. Each installation uses standard CERN infrastructure and equipment, e.g. standard LHC racks, standard VME crates, and being connected with standard 230V plugs. However, the stringed requirements for the BIS on safety, reliability and availability impact also on these components.

3.4.1 Mechanics

24. The BIS uses standard IEC 230V plugs for electrical equipments. Appropriate measures should be taken to avoid the connector being disconnected accidentally e.g. fixing them with screws or using small locks.
25. A labelling / key system for its individual slots should be added to the VME crates to avoid mixing modules e.g. during maintenance.

3.4.2 Cabling

26. The BIS is currently not using the latest procedure for cable assembly, which improves manufacturing time by quite a lot (see section “Recommended Procedure Variation”). The latest revision can be found at [3].

3.4.3 Radiation & Magnetic Fields

27. The BIS, and especially the CIBUs, has never been specified to be radiation tolerant (as many other LHC components). Due to the use of not hardened switch mode power supplies it will fail (safely) probably already at moderate radiation levels. This is, apparently, not an issue now, but must be taken into account in case LHC approaches its design luminosity.

    The radiation tolerance of the CIBUs should be defined, verified, and communicated to the BIS users.

    The persons responsible for the BIS users must be made aware of the situation concerning radiation tolerance.
28. Some components on the CIBU might not resist high magnetic fields, e.g. the power supplies or the relays used to toggle between user and test inputs. Upper magnetic compatibility limits should be defined and the system tested accordingly.

3.5 Interfaces with other Systems

The BIS is depending on quite a long list of user systems providing signals to permit or dump the beam. Also, it highly depends on the proper functioning of the LHC Beam Dump System (LDBS). However, the complete system for LHC safety is only as good as its weakest element.

Since a substantial amount of effort has been put in the high reliability and availability of the BIS, justifications are needed to show that the user systems and, in particular, the LBDS do not bring this effort to nothing. In particular, the USER_PERMIT signal must be transmitted with a comparable reliability and availability.

3.5.1 The LHC Beam Dump System (LBDS)

29. The LBDS, especially the kicker magnet system, is essential for the safety of the LHC. However, although the BIS has been audited and its reliability has been proven to be SIL4, a formal study and audit of the reliability of the kicker magnets of the LBDS and the corresponding trigger mechanism using BIS signals is missing.

Therefore, a similar audit as this BIS audit should be conducted for the LBDS kicker magnets and their trigger mechanism.

30. Furthermore, the detector of the optical beam permit loop is *not* part of the BIS, but part of the LBDS. Thus, exceptional care has to be put on its integration and functional testing. The extensive FMEC analysis performed for the BIS must be extended to contain at least this detector.

3.5.2 The BIS User Systems

31. The LHC safety relies largely on a small set of monitoring and control systems, i.e. the Beam Lifetime Monitors, the Beam Loss Monitors (for the accelerator and inside the LHC experiments), the Fast Magnet Current Change Monitor, the Powering Interlock System, and the Transverse Feedback System. However, a detailed study of the individual dependencies and their relative importance is missing.

    An analysis of the dependencies with regard to LHC safety and of an audit of the major ones should be conducted.

32. Procedures are mandatory to guarantee that the BIS user systems obey standard safety rules (e.g. that they handle redundancy through-out their system and do not duplicate single signals for the purpose of the BIS). A lack of these standard safety rules will lead to points of single failure.

    Awareness discussions & training on safety might be useful to propagate the stringent needs for the BIS.

33. The BIS has been tested successfully with respect to EMC [1] (see point 18). Additional “Walkie-Talkie”-type or RF susceptibility test have been suggested by this audit.

    The same type of tests should also be conducted on the (critical) BIS user systems.

34. The PowerPC allows feeding a so-called SOFTWARE_PERMIT into the BIS logic. However, software signals per se and the EMC resistance of the PowerPC [1] in particular call in question, if the SOFTWARE_PERMIT can sustain the high level of reliability and availability of the overall BIS.

    Alternative solutions of the SOFTWARE_PERMIT should be evaluated.

35. Special “Good-As-New”-tests are envisaged to guarantee the proper cabling of the BIS users, and to verify the proper functioning of the BIS. In particular, the internal tests, e.g. to proof detailed safety features, are non-trivial. Care must be taken not to provoke unstable states because of an elaborated test procedure. The respective test procedures should be carefully elaborated and implemented together with the persons responsible for the BIS user systems. Regular “toggle on/off”-tests prior to injection with cross-checks against a central database might be able to find errors in the BEAM_PERMIT-signal chain, false cabling, and wrong “inhibit”-switch settings. These tests should also cover cases of sabotage or simple vandalism.

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

3.5.3 Safe Beam Mode

36. A SAFE_BEAM_FLAG allows masking half of the user inputs to the BIC, i.e. those which are less critical when e.g. running a low energy, low intensity beam. The BIS interface boards provide connectors for both types of user inputs (critical and non-critical ones). However, no hardware-based protection mechanism prevents the accidental (or intentional) exchange of the cables for both types (e.g. accidentally swapping cables).

    The implications of such misbehavior should be studied and documented.

37. No documentation has been provided for the implementation of the SAFE_BEAM_FLAG and the corresponding “Safe LHC Beam Receiver” (SLBR) board. Since user signals might be masked using this mechanism, the SLBR and the SAFE_BEAM_FLAG have to be at least SIL2 or the SAFE_BEAM-mode might be entered accidentally (or intentionally) when the beam is *not* safe.

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

38. The SAFE_BEAM_FLAG is distributed by the SMP (Safe Machine Parameters system) based on the GMT (General Machine Timing). Thus, the distribution itself is outside the control of the BIS.

    The distribution of the SAFE_BEAM_FLAG should be consistent with points 36 and 37 above.

3.6 Other Issues

39. According to the SPS operators, the BIS history buffer provides valuable information for the commissioning and running of the SPS, and is expected also to provide LHC information with the same level of importance. Thus, the design of the BIS with respect to buffer overflows and loss of data should be reviewed.

40. The short BEAM_PERMIT states at injection and extraction should be displayed with some kind of “persistency” on the supervision system such that operators could clearly observe the BEAM_PERMIT signals being produced.

4 References

[1] B. Todd, “Signal Integrity and Electro-Magnetic Compatibility of the Beam Interlock System”, EDMS #762174

[2] A Dinius, B. Puccio, B. Todd, “Optical Extension of User Interface Connection to the Beam Interlock System”, EDMS #762135

[3] Y. Thurel, “Assembly Procedure”, EDMS #527992