RELIABILITY ANALYSIS OF THE LHC BEAM DUMPING SYSTEM

R. Filippini, E.Carlier, L. Ducimetière, B.Goddard, J.Uythoven, CERN, Geneva, Switzerland

Abstract

The design of the Beam Dumping System of the Large Hadron Collider at CERN is aimed at ensuring a safe beam extraction and deposition under all circumstances. The system includes redundancy and continuous surveillance for most of its parts. Extensive diagnostics after each beam dumping action will be performed to reduce the risk of a faulty operation upon the subsequent dump trigger. Calculations of the system's safety and availability are presented for the beam dumping kickers and septa magnets.

THE LHC BEAM DUMPING SYSTEM

The LHC Beam Dumping System (LBDS) [1] must be able to remove both beams upon request and deposit them safely onto the absorber blocks. It comprises, per ring, 15 horizontally deflecting extraction kicker magnets MKD, after which the deflection is enhanced by the superconducting quadrupole Q4, 15 vertically deflecting septum magnets MSD and 10 dilution kicker magnets MKB, followed by a lever arm of several hundred meters of vacuum tube before the beam reaches the dump absorber block TDE (Figure 1).

Most failures can be tolerated or their consequences be mitigated by passive protection systems. Some "beyond design" failures may lead to catastrophic consequences [2]. In particular, failures in the MKD or MSD are most often critical for safety. Failures in the MKB are less critical though the complete unavailability may destroy the dump block with long downtime for repair or replacement. For these reasons, the overall LBDS must comply with at least SIL3, in agreement with the general requirements on safety related systems [3].

Fault tolerance (redundancy) and on-line surveillance reduce the likelihood of non-acceptable failures [4]. For instance, a proper beam dump extraction can still be performed with 14 out of 15 MKD magnets. All MKD generators consist of two identical parallel branches, each with a solid-state switch, which permit to stand a switching failure in one branch [5]. The capacitor voltage settings are tuned to the beam energy and are continuously monitored by the Beam Energy Tracking System (BETS) that generates a dump request if an error is detected. Any erratic trigger in an MKD generator is caught by the re-triggering system that re-distributes them to the other generators. The MSD has no redundancy but continuous surveillance. The BETS surveys the septa power converter output current and the Fast Magnet Change Current Monitors (FMCCM) discovers fast magnet current changes. Two out of 10 operational MKB magnets are still acceptable for the beam dilution. Their generators are surveyed by the BETS as well.

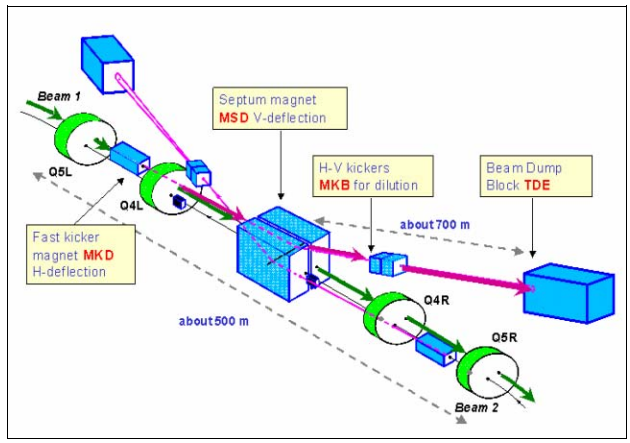

Figure 1: Schematic Layout of the LHC Beam Dumping System

The complete failure of the trigger system is largely prevented by using two trigger systems acting in parallel plus the re-triggering line and multiple paths for the signal distribution to the MKD and MKB systems.

Other failures, not critical for safety, are covered by on-line surveillance and lead to dump requests, like the loss of synchronization with the beam abort gap (tolerated by passive protection) or general power faults in most of the electronics. In addition to redundancy and surveillance, extensive post mortem diagnostics permits to discover hidden faults and to recover the system to an "as good as new" state before the next fill.

LBDS MODELLING

With respect to previous work [6], mainly focused on the MKD system, this study extends the analysis to the MSD and the MKB systems, including their power converters, the triggering and re-triggering systems, plus surveillance and diagnostics facilities. For this LBDS core architecture the safety is calculated over one year of operation together with the expected number of operation aborts originating from the LBDS (false beam dumps) that represent the system's unavailability. Some considerations on the existing trade-off between safety and unavailability will also be addressed.

The system architecture has been decomposed into functional blocks. For each of these blocks, Failure Modes, Effects and Criticality Analysis (FMECA [7]) has been performed at component level. Every failure mode has been assigned a failure rate as deduced from experience or literature [8] except for few parts of the LBDS still under development for which failure rates were assumed, using conservative estimates.

The above information has been arranged into a state transition diagram that represents the fault-driven system behaviour over one year of LHC operation (see Figure 2).

0-7803-8859-3/05/$20.00

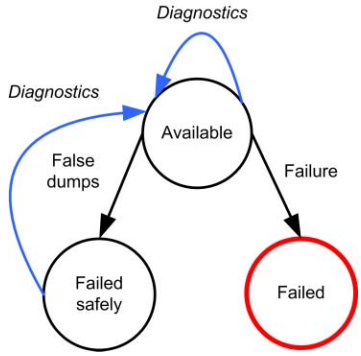

Figure 2: State transition diagram: "false dumps" and "failure" are enabled during operation, "diagnostics" is enabled during checks.

When operating, the system can be found in three states: 1) available (the initial state), 2) failed safely or 3) failed. Failures drive state changes only when operating: silent failures and other undetected failures make the system unavailable, leading to the failed state, while detected failures generate false dumps.

After each beam operation, a check is performed and the system is diagnosed and recovered to the available state with the exception of the failed state that corresponds to a full stop of the LHC operations.

LBDS ANALYSIS

Dependability attributes [9] are defined for the model given in Figure 2. Safety is the probability that the system is available upon dump request or has failed safely. Unavailability is the probability to have generated a false dump during a beam operation and it is given in terms of number of false dumps per year. The system is analysed under the following assumptions.

(A1). The operational scenario is one year of LHC operation with 400 fills of 10 hours each, followed by 2 hours without beam.
(A2). Failure rates are assumed to be constant.
(A3). The system can fail only when operating and, if failed, it cannot be recovered.
(A4). Checks are regeneration points ("as good as new") for the system failure process.

Assumption A4 permits to analyse the system failure process within single identical beam operations. Concerning A2, failure rates have been assumed for the BETS and the FMCCM, as the systems are still under development. For the other systems the applied numbers are the results of an extensive FMECA analysis and reliability prediction at component level.

The results for unsafety and false dumps over one year of operations are summarised in Table 1. The calculated unsafety for the LBDS is 1.8×10^{-7} per year, which is the sum of the independent contributions of the MKD, the MSD and the MKB. This corresponds to an equivalent failure rate of 4.5×10^{-10} per hour, therefore largely SIL3.

Table 1: Results for unsafety and false dumps per year.

System	Unsafety/year	False dumps/year	
		Synchronous	Asynchronous
MKD	1.4×10^{-7}	1.9	0.7
MSD	0.4×10^{-7}	0.1	-
MKB	6.5×10^{-10}	0.7	-
LBDS	**1.8×10^{-7}**	**2.7**	**0.7**

There will be 3.4 false dumps per year (+/- 1.8) of which 2.7 are synchronous and 0.7 asynchronous. They are apportioned in 2.6 from the MKD (triggering system included), 0.7 from the MKB and 0.1 from the MSD.

The power converter failures within the different systems are expected to cause 2.5 false dumps per year, by far the main source of unavailability, according to experience. It is important to remark that these results do not include the possible false alarms generated by the surveillance system (BETS).

Sensitivity analyses

Safety is sensitive to redundancy, surveillance and diagnostics. Without 14 out of 15 redundancy the MKD unsafety would increase to 0.01 per year. Analogously, a trigger system without redundant architecture would increase its contribution to unsafety from the negligible 5.5×10^{-10} to 4.7×10^{-4} per year.

Removing surveillance has a dramatic effect on safety. For example, without the BETS the powering faults would remain undetected and the unsafety per year would increase to 0.031 for the MKD, 0.016 for the MSD and 0.002 for the MKB (see Figure 3). The removal of the re-triggering system would drastically increase the unsafety to 0.3 per year.

Diagnostics is complementary to surveillance and effective for all systems that have a redundant architecture. For the MKD system the failure rate is assumed to start again at zero due to the diagnostics that is performed after every beam dump (see Figure 4). Without that, the failure rate would increase over the operations, resulting in 5.4×10^{-5} unsafety per year.

The system safety depends also on the operational scenario. Sensitivity to the operation length is evaluated for the MKD only. Keeping the same total operating time, the MKD is safer (1.1×10^{-7}) for 500 shorter operations of 8 h than for 320 longer operations of 12.5 h (1.7×10^{-7}).

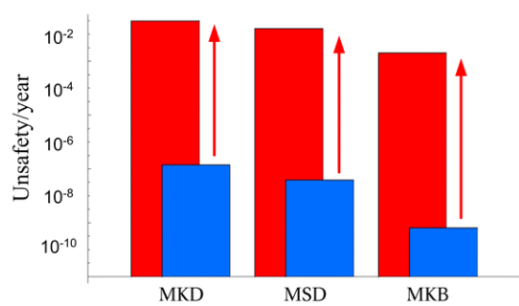

Figure 3: Unsafety per year due to MKD, MSD and MKB, with (blue bar) or without surveillance (red bar).

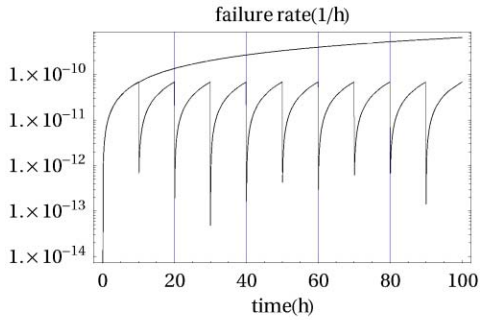

Figure 4: Diagnostics for the MKD performed every 10h (bottom) or not performed (top). Only operational time is shown.

Trading-off safety and unavailability

Redundancy and surveillance make the system safer but more complex, which affects the expected number of false dumps and therefore the machine unavailability. Even though availability is not an a-priority goal in the LBDS design, it could be useful to consider strategies capable of keeping it as high as possible, compatibly with the safety requirements (trade-off).

In the presently foreseen system, every detected failure leads to a dump request, which makes the number of false dumps sensitive to the components failure rate. For example, by increasing the failure rate of the power converters by one order of magnitude the number of expected false dumps will be doubled. This is still acceptable for the system safety but undesirable for the LHC availability as many other systems may disrupt the operational cycle for identical safety reasons [10].

Masking the false dump requests of power converters in the MKD and MKB power triggers (40 in total) results in 2.1 false dumps less with a negligible increase of unsafety that moves from 1.8×10^{-7} to 1.9×10^{-7} per year. This strategy is feasible due to the massive redundancy used in those systems. The remaining 1.3 false dumps are harder to eliminate or unavoidable. They include the MSD (0.1) the triggering system (0.1), the MKD and MKB powering (0.4) and the erratic triggers caught by the re-triggering system (0.7).

CONCLUSIONS

The presented work reports on safety and unavailability for the core architecture of the LBDS including the MKD, the MKB and the MSD considering their powering, triggering and re-triggering systems as well as surveillance and diagnostics. The overall calculated unsafety is 1.8×10^{-7} per year (400 machine fills), which complies with SIL4 [1×10^{-9}/h, 1×10^{-8}/h]. For the unavailability, 6.8 (+/-2.6) false dumps (5.4 synchronous and 1.4 asynchronous) per year are expected for the two LBDS.

The analysis has demonstrated the importance of redundancy, surveillance and diagnostics for achieving the required safety level. If one of these facilities is removed the safety goal cannot be reached anymore. The trade-off between safety and unavailability has been addressed and a possible solution for a reduction of the number of false dumps has been illustrated.

It is important to remark that these results are provisional for the parts of the system still under development and in particular for the BETS and the FMCCM a certain additional contribution to the given unavailability number is expected.

The results will be validated during a reliability run planned for 2007 before the start of LHC beam operation. The foreseen three months period should be sufficient to obtain significant statistics on partial system failures and system availability.

ACKNOWLEDGEMENTS

The authors would like to thank Gene Vossenberg for the many fruitful discussions.

REFERENCES

[1] "The LHC Design Report: Vol. I, The LHC Main Ring", CERN-2004-003, Geneva 2004.

[2] J. Uythoven, R. Filippini, B. Goddard, M. Gyr, V. Kain, R. Schmidt, J. Wenninger, "Possible Causes and Consequences of Serious Failures of the LHC Machine Protection System", 9th European Particle Accelerator Conference, EPAC 2004, Lucerne, Switzerland, 5-9 July 2004.

[3] International Electrotechnical Commission IEC, "Functional Safety of Electrical-Electronic-Programmable Electronic Safety Related Systems" IEC 61508 International standard, Geneva, 1998.

[4] E. Carlier, A. Antoine, P. Bobbio, G. Gräwer, A. Marchand, J. Uythoven, H. Verhagen, "Design Aspects related to the Reliability of the Control Architecture of the LHC Beam Dump Kicker Systems", 9th International Conference on Accelerator and Large Experimental Physics Control Systems, ICALEPCS 2003, Gyeongju, Korea, 13 -17 October 2003.

[5] J. Bonthond, J.H. Dieperink, L. Ducimetière, U. Jansson, E.B. Vossenberg, "Dual Branch High Voltage Pulse Generator for the Beam Extraction of the Large Hadron Collider" 25th International Power Modulator Symposium, Hollywood, California, June 2002.

[6] R. Filippini, E. Carlier, B. Goddard, J. Uythoven, "Reliability Issues on the LHC Beam Dumping System", 9th European Particle Accelerator Conference EPAC04, Lucerne, Switzerland, 5-9 July 2004.

[7] Failure Mode/Mechanism Distributions, FMD-97, Reliability Analysis Center RAC, Rome (NY, USA), 1997.

[8] MIL-HDBK-217F, "Reliability Prediction of Electronic Equipment", Department of Defence, Washington D.C. USA, 1993.

[9] J. C. Laprie ed., "Dependability: Basic Concepts and Terminology", Springer-Verlag, Wien, 1992.

[10] R. Filippini, B. Dehning, G. Guaglio, F. Rodriguez-Mateos, R. Schmidt, B. Todd, J. Uythoven, A. Vergara Fernandez, M. Zerlauth, "Reliability Assessment of the LHC Machine Protection System", Particle Accelerator Conference PAC05, Knoxville, USA, 16-20 May 2005.

