UPDATE AND SUMMARY OF THE DEPENDABILITY ASSESSMENT OF THE LHC BEAM DUMPING SYSTEM

R. Filippini*, J. Uythoven, CERN, Geneva, Switzerland

Abstract

The LHC Beam Dumping System (LBDS) must be able to remove the high intensity beams from the LHC accelerator on demand, at any moment during the operation. As the consequences of a major failure can be very severe, stringent safety requirements were imposed on the design. The final results of an in-depth dependability analysis of the LBDS are summarised, assuming one year of operation and different operational scenarios. The trade-off between safety and availability is discussed, along with the benefit from built-in features like redundancy, on-line surveillance and post-mortem diagnostics.

INTRODUCTION

The LHC Beam Dumping System [1] consists per LHC beam of 15 horizontally deflecting kickers magnets MKD, the Q4 quadrupole that enhances the horizontal deflection, 15 vertically deflecting septum magnets MSD and 10 dilution magnets MKB, followed by several hundred meters of beam transfer line before the extracted beam reaches the dump absorber block TDE, see Figure 1.

During the LHC operation, the system is waiting for a dump request from the beam interlocking system, which is part of the LHC Machine Protection System [2]. Once the dump request is received, a trigger pulse, synchronised within the beam free gap of 3 μs, is distributed to the MKD and MKB generators and the beam is extracted into the dump transfer line. At the instant of the dump request it is important that all kicker pulse generators and power converters of the LBDS are tuned at settings proportional to the beam energy. The beam energy is derived by the Beam Energy Measurement System (BEMS) from several LHC main dipole power converters. The power settings are continuously surveyed by the Beam Energy Tracking System (BETS) and in case of detected errors, the operation is aborted according to a failsafe strategy. The resulting beam dump is called a ”false dump”. False dumps are also generated in case of loss of synchronisation with the beam free gap and detected failures in the power converters. A Re-Triggering System (RTS) contributes to a further increase of safety by covering potential erratic triggers in the MKD system. After each beam dump, an extensive post mortem diagnostics is performed.

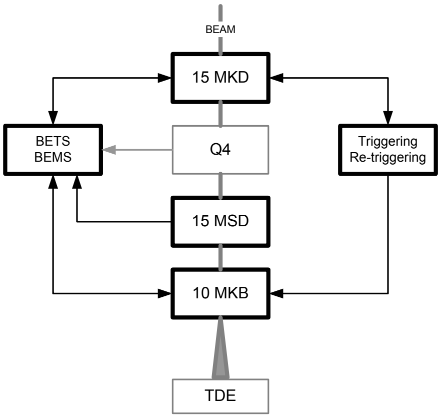

Figure 1: LBDS functional blocks.

Most malfunctioning of the LBDS does not lead to beam losses or leads to beam losses that can be tolerated as their consequences are mitigated by protective elements in front of the Q4 and the MSD magnets. Some ”beyond design” failures have been identified which may lead to the loss of the entire beam with catastrophic consequences [3]. The LBDS is classified as a safety critical system. It is an important component of the LHC Machine Protection System for which a safety level of SIL3 [4] is required, corresponding to a failure rate in the range $10^{-8} - 10^{-7}$/h. The aim of this study is to verify whether the LBDS stays within this safety requirement at an acceptable detriment to availability.

THE MODELING FRAMEWORK

Failure Modes Effects and Criticality Analysis (FMECA) and reliability prediction have been performed for the LBDS [5, 6]. Some 2100 failure modes have been classified at component level and arranged into 21 system failure modes with their hazard function [7]. This information enters a state transition diagram representing the failure processes at system level.

The state of the system is described by six states $\{$X0, X1, X2, X3, X4, X5$\}$ that account for the system being available $\{$X0, X1, X2, X3$\}$, the system failed safely $\{$X4$\}$ and the system failed unsafely $\{$X5$\}$, see Figure 2. The available states represent the system with respect to the status of the BETS and re-triggering system RTS. During the LHC operation, transitions drive state changes from the available states either to the state X4 or to X5. The model of Figure 2 is a Markov chain. The state vector X is given a probability distribution **p**(t)=$[p_0(t), p_1(t), p_2(t), p_3(t), p_4(t), p_5(t)]$, which is calculated by the Kolgomorov’s equation [7]:

$$\frac{d}{dt}\mathbf{p}(t) = \mathbf{p}(t)\mathbf{Q}(t) \qquad (1)$$

[*] Presently at the Interdepartmental Research Center E. Piaggio, University of Pisa, Italy.

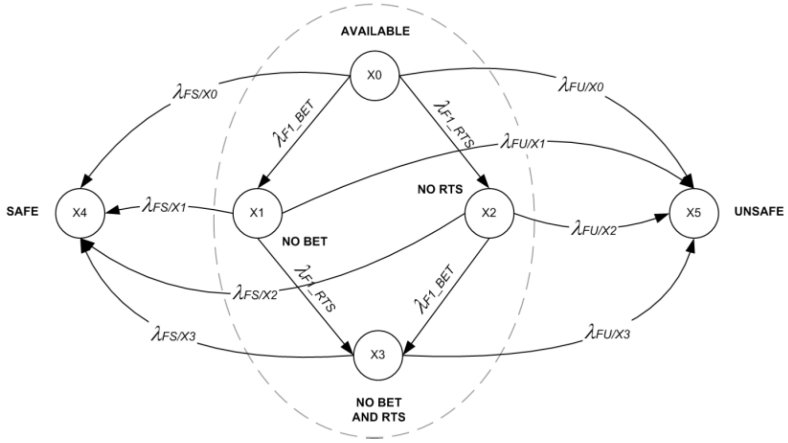

Figure 2: The state transition diagram of the LBDS failure processes.

where **Q**(t) is the 6×6 transition rates matrix. After the beam has been dumped, the system enters the check phase in which it cannot fail. The states $\{$X1, X2, X3, X4$\}$ are all recovered to X0, while X5 is absorbing and is not recovered. The system is 'as good as new' only if the matrix **Q**(t) of the transition rates goes back to its initial value. In this case, the checks are regeneration points for the stochastic process.

ANALYSIS

The dependability attributes of interest for the LBDS, safety and availability, are also defined by the Markov chain of Figure 2. The system is unsafe if it moves into X5. The system is safe but unavailable if it moves into X4. The unavailability is given in term of number of false dumps generated. The system is analysed over one year (200 days) of LHC operation, for three different operational scenarios.

Operational scenario 1 (OP1). 400 missions of 10 h each alternate with checks of 2 h, during which the system is recovered 'as good as new'. The analysis requires the solution of equation (1) for one mission time and the initial conditions **p**(0)=[1,0,0,0,0,0]. The formula of unsafety for one year of operation is:

$$U = 1 - [1 - p_5(10)]^{400} \qquad (2)$$

The number of false dumps is a binomially distributed random variable with parameter $p = p_4(10)$, average $400 \times p$ and standard deviation $\sqrt{[400(1-p)p]}$ [7].

Operational scenario 2 (OP2). Like OP1, with the exception that the system is regenerated only after false dumps (i.e. repair on demand instead of check at every beam dump), so that certain failures, masked by redundancy, may accumulate undetected. The analysis requires the solution of the Markov chain for each mission. The initial state probability distribution **p**(t) and the matrix **Q**(t) are updated on the basis of the results of the previous mission. Safety is the probability to be in X5 after 400 missions. Nothing changes for the calculation of the number of false dumps.

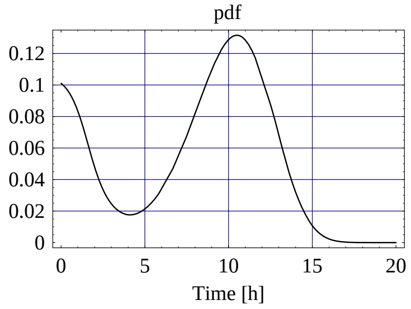

Figure 3: Planned and beam induced dump requests.

Operational scenario 3 (OP3). Like OP1, with the exception that the mission duration is a random variable. Three concurrent events are the regeneration points of the process: the false dumps, the planned dump requests and the beam induced dump requests. The planned dump request event is chosen Weibull distributed, with hazard rate $\lambda(t) = \alpha\lambda(\lambda t)^{\alpha-1}$. The beam induced dump request is chosen exponentially distributed with hazard rate $\lambda(t) = 0.001 + (t^3 + 10)^{-1}$ in order to model a higher rate in the early 2/3 hours of the injection phase when the beam is more unstable. The distribution of the dump request for the operational scenario 3 is shown in Figure 3. The analysis requires the solution of a Markov regenerative process [7].

The results for the three scenarios are summarised in Table 1. All analysed scenarios show similar results for the calculated safety and the number of false dumps, with the exception of OP2 that, because of partial regeneration at checks, results in a lower safety. The most realistic estimate is obtained for OP3: unsafety is 2.4×10^{-7}/year, i.e. largely SIL4 ($< 10^{-9}$/h), for 475 missions on average per

Table 1: Results for the three operational scenarios (av. stands for average).

Scenario	**Missions/y**	**T** [h]	**Unsafety/y**	**False D.**
OP1	400	10	2.418×10^{-7}	4.0
OP2	400	10	3.150×10^{-5}	4.0
OP3	475 (av.)	8.1 (av.)	2.401×10^{-7}	3.9

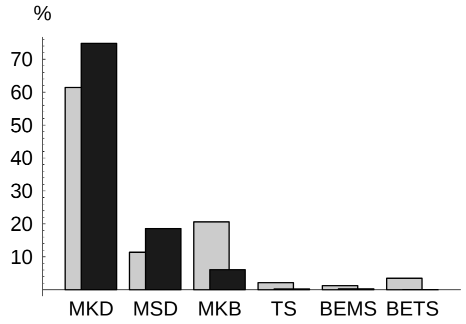

Figure 4: Apportionment (%) of unsafety (black bars) and false dumps (gray bars).

year, of which 110 are beam induced dump requests and 4 (±2) are false dumps.

The obtained results will be verified during the reliability run planned for the end of 2006. A test of three months on 30 MKD assemblies, 60 generator branches in total, allows to verify that the system is SIL3 at 95% confidence level if less than 6 failures of individual branches are observed.

The results have also been included in a simplified model of the LHC Machine Protection System (MPS), which also comprises the beam loss monitors, the quench protection system, the powering interlock controller and the beam interlock controller [2].

Criticality and Sensitivity Analyses

Safety and the number of false dumps have been apportioned to the LBDS components, for the operational scenario OP1, see Figure 4. The MKD is the most critical system contributing by 75% to unsafety and by 60% to the false dumps. A different apportionment for the false dumps ascribes 14% false beam dumps to detected energy tracking failures, 10% to the erratic triggers (i.e. 0.4 asynchronous dumps), 53% to others failures detected by internal surveillance and 25% of the false dumps per year to the false alarms in the surveillance electronics.

A sensitivity analysis makes it possible to investigate the trade-off between safety and availability with respect to the many design fault tolerance facilities: the dual branch generator of the MKD, the redundant triggering system (TS), the 14 out of 15 redundancy of the MKD, the BETS and the re-triggering system. The result of the analysis is shown in Table 2. Almost all cases demonstrate that such measures are either strictly necessary for reaching the desired level of safety or they add some extra-margin with a small contribution to the false dumps. The achieved trade-off can be sensitive to the failure rates of the components included in the redundant architecture and in the surveillance, like for example, the power triggers, the power converters and the beam energy data acquisition channels. In this sense, one order of magnitude more for the assumed component failure rates would almost double the number of expected false dumps, practically without any effect on safety.

Table 2: Safety and false dumps trade-off.

	Unsafety	**False D.**
Default	2.4×10^{-7} (> SIL4)	4.1
No dual branch	2.3×10^{-6} (SIL4)	3.0
No redundant TS.	4.7×10^{-4} (SIL2)	4.0
14/14 MKD	0.011 (SIL1)	3.9
No BETS	0.059 (< SIL1)	3.4
No RTS	0.32 (< SIL1)	4.1

CONCLUSIONS

The presented work summarises three years of study on the LBDS dependability and updates the provisional result, already presented in a previous publication [8], into the final figures for unsafety, 2.4×10^{-7}/year (largely SIL4), and the number of false dumps, 4 ±2 per year. The MKD system has proven to be the most critical component for safety and the main source of false dumps, which is logical as it is the most complex system in the LBDS. The analysis of the model has also demonstrated that a good balance between safety and availability (number of false dumps) is reached in the LBDS.

ACKNOWLEDGEMENTS

The authors thank B. Goddard and V. Mertens for the many fruitful discussions.

REFERENCES

[1] The LHC Design Report: “The LHC Main Ring”, Vol. 1, CERN, Geneva 2004.

[2] R. Filippini and others, “Reliability Assessment of the LHC Machine Protection System”, Particle Accelerator Conference, Knoxville, USA, 16-20 May 2005.

[3] 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.

[4] International Electro-technical Commission IEC, “Functional Safety of Electrical-Electronic-Programmable Electronic Safety Related Systems”, IEC 61508 International Standard, Geneva, 1998.

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

[6] Military Handbook 217F, “Reliability Prediction of Electronic Equipment”, Department of Defense, Washington D.C., 1993.

[7] A. Hoyland and M. Rausand, “System Reliability Theory: Models and Statistical methods”, Wiley, New York, 1994.

[8] R. Filippini, E. Carlier, L. Ducimetière, B. Goddard, J. Uythoven, “Reliability Analysis of the LHC Beam Dumping System”, Particle Accelerator Conference, Knoxville, USA, 16-20 May 2005.