RELIABILITY ANALYSIS OF THE LHC BEAM DUMPING SYSTEM TAKING INTO ACCOUNT THE OPERATIONAL EXPERIENCE DURING LHC RUN 1

R. Filippini[#], Filippini Consulting, Italy
E. Carlier, N. Magnin, J. Uythoven, CERN, Geneva, Switzerland

Abstract

The LHC beam dumping system operated reliably during the Run 1 period of the LHC (2009 – 2013). A number of internal failures of the beam dumping system occurred that, because of built-in safety features, resulted in a safe removal of the particle beams from the machine, so called “internal beam dumps”. These failures have been appointed to the different failure modes and are compared to the predictions made by the reliability model established before the start of LHC operation. A statistically significant difference between model and failure data would identify those beam dumping system components that may have unduly impacted on the LHC availability and safety or might have been out of the scope of the initial model. An updated model of the beam dumping system reliability is presented, taking into account the experimental data presented and the system changes to be made during the LHC shutdown 2013 – 2014.

INTRODUCTION

The LHC Beam Dumping System (LBDS) is the final element of the LHC Machine Protection System (MPS) [1]. Its function is to dump the beam safely onto the beam dump block, at any dump request issued by the MPS or self-triggered by the LBDS itself. In the present study, the LBDS is partitioned into three functions: actuation, control and surveillance. The actuation includes the extraction kickers (MKD), the septa magnets (MSD) and the dilution kickers (MKB) all with their power converters. Control includes the Trigger Synchronization and Distribution System (TSDS) and the Beam Energy Tracking System (BETS). Surveillance is about monitoring of internal processes and component’s state, and it also implements internal failsafe mechanisms. The LBDS also depends on auxiliary systems such as post-mortem and diagnostics and the vacuum system, and it receives the dump request signal from the Beam Interlocking System (BIS).

The analysis of the expected safety and availability of the LBDS was performed in 2003 – 2006 [2]. It returned a SIL4 figure of safety and a number of 8 ± 2 internal beam dumps per year, for both beams. MKD and MKB systems were found to be the most critical components for safety, with a contribution of 80% and were at the origin of 82% of the false dumps. These results were obtained by probabilistic failure models and, at that time, were not supported by any operational evidence. LHC operation from 2010 to2012 has given a rich record of operational data of the LBDS. In total, 139 failure events were recorded over that period of which 90 originated in the LBDS. Figure 1 shows the time series per month of the failure events in the LBDS over the three years. The trend is irregular, characterized by peaks. The most evident discontinuities are found in correspondence with a machine restart, after a technical or Christmas stop. Globally, a decreasing failure rate can be observed, which means that the LBDS, after an infant mortality period, is moving to a steady state situation.

The study of these failure events made it possible to update the reliability models, recalculate and validate the failure rates, estimate the availability and the safety, and finally draw a list of recommendations to the designers. This paper presents a summary of the published results of these statistical analyses [3].

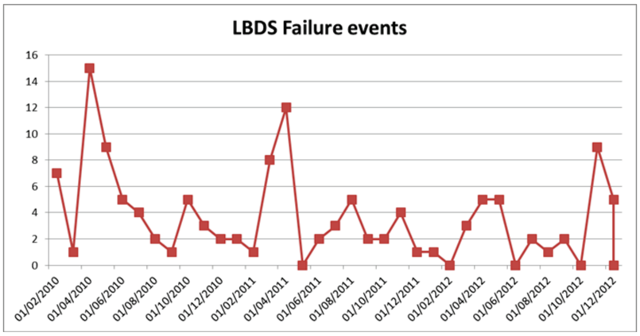

Figure 1: Time series of failure events recorded for the LBDS in 2010-2012.

FAILURE ANALYSIS

All failure events and technical interventions were systematically recorded in the LBDS technical and operational log books. Their identification was time consuming and their interpretation often needed the help of system experts. At the conclusion of this phase, data were arranged in a datasheet in which every failure event was classified with: 1) time stamp, 2) physical location of the fault (i.e. function, system, sub-system and component), 3) type of intervention, length and the repair action, and 4) identifier of the failure mode as clarified in the reliability analysis of 2006 [2].

[#] rob.filippini@tiscali.it

The next phase consisted of calculating the Time-To Failure of every component from the recorded failure data (TTF_{Data}) and comparing them with the TTF from the study of 2006. Depending on the agreement of the two figures, the reliability prediction models have been adjusted, by adding for example a failure on demand contribution, a common cause failure (CCF) mechanisms or an over-stress factor to the failure rates. Additional statistical hypothesis tests (H. test) were performed to further check whether observations agreed with predictions. Only if all tests failed, after any possible adjustment, the failure mode was declared as non-validated. In total 29 different failure modes in the LBDS were identified during the years 2010, 2011 and 2012. 19 of these were confirmed by observation of which 6 asked for adjustments of the respective reliability prediction model (3 are probabilities on demand and 3 CCF models). From the other 10 failure modes, 7 of these are new, 2 of which were not included in the reliability model and 5 were out of scope because the State Control and Surveillance System (SCSS) was not in the scope of the 2006 analysis. 2 failure modes were removed from the statistics, since ascribed to commissioning errors, and 1 failure mode was not validated, resulting in a failure rate much higher than expected and beyond any reasonable justification.

A sample of the results of the analysis is shown in Table 1 for the actuation system of the LBDS. The failure modes are associated with the identifier of the previous reliability analysis, the number of components that potentially suffered from that failure mode and 4 columns that account for the statistical validation process. The underscored text per row is the value taken as result of the validation process.

In addition to the recorded failure modes, about 70 failure modes in a total of 90 were also expected to occur, but did not occur during 2010-2012. All of them successfully passed the hypothesis test, with the only exception of the failure of the power supply of the Power Trigger Module [3].

AVAILABILITY

The LBDS is designed with failsafe mechanisms that prevent the development of failures and stop the operation by triggering an internal beam dump request when errors in the system are detected. The number of internal beam dump requests of the two LBDS was estimated at 8 ± 2 [2]. This estimate was obtained for an operation time split into two phases: 1) post mortem and arming phases, which were also assumed to be the regeneration point for the failure process (i.e. "as good as new"), and 2) the LHC machine fills. In this study, a more precise partition of operation phases was done. The new phases are post mortem and diagnostics, LBDS arming, beam setup, beam in (BI) and stable beam (SB). In order to compare results, only internal dumps that occurred during phases BI and SB are considered. Moreover, some internal beam dumps that were triggered by the same failure event, and separated by a short time interval, are counted only once. This is the case for example of the failure of the power supply in the Power Trigger Unit of the MKD in 2010, which was not completely resolved by diagnostics and generated another internal beam dump. One of these two events would not have occurred if the fault had been correctly diagnosed, as assumed in the original reliability model. The availability figures after the applied corrections are:

- 2010: 14 internal beam dumps;
- 2011: 10 internal beam dumps;
- 2012: 5 internal beam dumps.

Overall, the 29 internal beam dumps are in good agreement with the 2006 predictions (24 ± 6), in particular for years 2011 and 2012. The trend is decreasing, which is a good sign too. The higher contribution for 2010 is caused from the poor quality of some components. They did not meet technical specifications and were later replaced.

Table 1: Recorded Failure Statistics for the LBDS Actuation Components

#	*Failure mode*	*Model*	*Population*	*TTF (years)*			
				Raw	Corrected	Rel. pred.	H. test
1	MKD HV power supply breakdown	PSP1	30	3*30/7 = 12.8	β model	150	
2	MKD PTU HV PS	HV	60	3*60/10 = 9	1-count 26	16	TRUE
3	MKD Compensation PS breakdown	PSOS1	30	3*30/6 = 15	1-count 18	113	FALSE
4	PTC tracking error	PTC, PTC3	80	3*80/2 = 120	1-count 240	103	TRUE
5	MKD Power switch degradation	SP2	60	3*60/3 = 60	P_D model	633	n.a.
6	MKD PTC card failure	PTC1-3	80	3*80/1 = 240	-	1140	n.a.
7	MKB Power switch degradation	SW2	20	3*20/6 = 10	P_D model	633	n.a.
8	MKB HV power supply breakdown	PSH	20	3*20/1 = 60	-	152	TRUE
9	MKB HV power supply degradation	Not in the model	20	3*20/3 = 20	1-count 60	114	TRUE
10	MKD PTC power supply	PTC	80	3*80/1 = 240	-	114	TRUE
11	MKB Magnet sparking	Not in the model	20	3*20/1 = 60	-	-	n.a.
12	MKD Peltier cooling element	Not in the model	30	3*30/4 = 22.5	Removed	-	n.a.

SAFETY

No safety critical failure scenario was recorded; actually none was expected from the initial analysis of the LBDS. This is a necessary condition for the LBDS to meet SIL3 at least (i.e. failure rate < 1E10-7/h), nonetheless it is not sufficient. In order to find a sufficient condition for safety, a novel approach for inferring safety from operational data is devised. This section provides the background of the analysis with the most important results. More details and insights can be found in [3].

The LBDS is designed to tolerate faults up to a certain extent, i.e. don't generate an internal beam dump, although some internal condition is not fully ok. The essential requirement is that the system should never operate under a single point of failure conditions.

Actually redundancy makes it possible for the LBDS to work with even larger margins of safety for certain component's faults. The calculation of how much these margins were reduced at the time of a beam dump is the objective of this analysis. A metric of safety distance in the state space of the LBDS is defined, starting from the definition of a nominal set-point for the LBDS, a characterization of the state space around it and the state transitions at failures. The state space is split into different regions which correspond to a safety margin, starting from the nominal region, with the system in an "as good as new" state, to the border region with zero safety margins, in which the LBDS operates at a single point of failure condition. A safety estimator, i.e. the **safety gauge,** is conceived to infer the residual safety margins of the LBDS at the time the system was demanded to dump the beam. The possibility of building this safety gauge relies on the assumptions that every failure event in the LBDS turns into a detectable state transition.

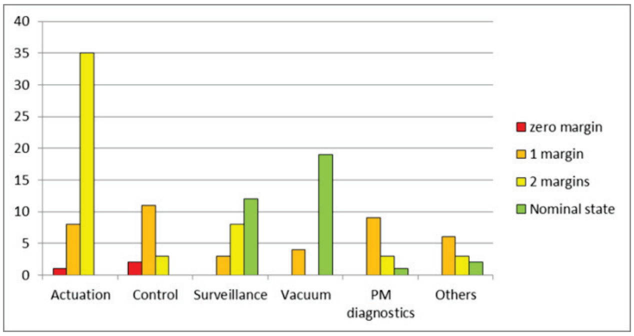

Figure 2: Safety margins versus LBDS functions.

The inference analysis of safety is applied to the failure events recorded in 2010, 2011 and 2012. 44 in a total of 139 failure events in the LBDS and external systems triggered an internal beam dump, while the others either remained silent or they did not occur in operation. Figure 2 shows the distribution of the 139 failure events per function, and apportioned to 4 safety regions: nominal ("as good as new"), 2 margins left, 1 margin left and zero margin.

Only three events occurred at zero safety margin, 2 of which in the control systems, resulting in the detected failure of the trigger and synchronisation units and one in the actuation, with the failure of two power converters [3]. All other failure events at a beam dump occurred with sufficient safety margins for the LBDS. Figure 3 shows the average values of the safety margin for the three functions of the LBDS. The safety gauges point at numbers from 1 to 5, which correspond to the safety margin left (+1) quantified at the time of a beam dump. On average, all LBDS functions (and the LBDS as whole) have at least 2 safety margins. Controls are the components with fewer margins (2.13 on average), whilst surveillance with a value of 3.39 turns to be the most protected. Further elaboration of these results made it possible to infer a SIL3 for the LBDS. This is the sufficient condition that was sought.. A positive trend of the safety margins over the years for the three functions was also discovered. Among other interesting findings, the new failure modes resulted as the biggest contributors [3, 4].

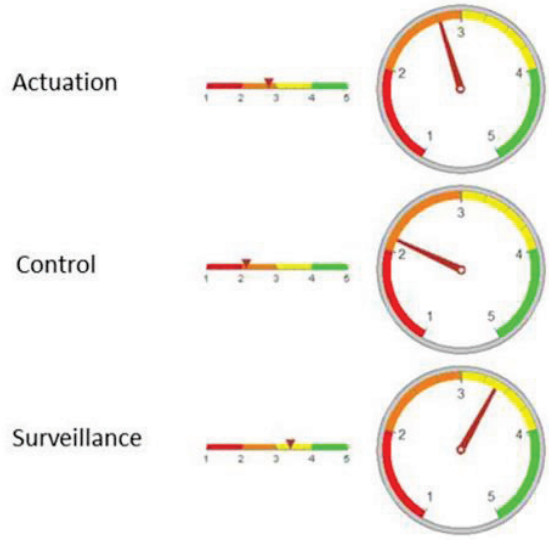

Figure 3: The LBDS safety gauge.

CONCLUSIONS

A large amount of data concerning failure events in the LHC Beam Dumping System was collected during LHC operation from the years 2010-2012 [3]. These data were used for the validation of the predictions from the safety and reliability analyses performed in 2003-2006 [2]. 139 failure events were recorded and apportioned to 29 failure modes, of which 19 were predicted in 2006, the updated failure rates have been included in the reliability model. In terms of safety, the LBDS meets SIL3. This is a more conservative value with respect to the initial 2006 prediction, essentially because of the contribution of new failure modes. The number of internal beam dumps (29) is in good agreement with the prediction (24). All statistics, including availability and safety, show a positive trend, which attests an improvement in operation with LHC. A series of recommendations were made to the designers [3, 4]. With respect to failure reporting, the quality has to be improved in order to facilitate the automatic retrieval of information. A design review is envisaged in the control function, which is the most safety significant component, with the implementation of the surveillance function in a separated board. Improvements are foreseen in the diagnostics procedures, which were not always able to recover the component to an "as good as new" state.

REFERENCES

[1] R. Schmidt and al., "Protection of the CERN Large Hadron Collider", New J. Phys. 8 290 (2006).

[2] R. Filippini, "Dependability Analysis of a Safety Critical System: the LHC Beam Dumping System at CERN", CERN-THESIS-2006-054 - Pisa University, 2006.

[3] R. Filippini, J. Uythoven, "Review of the LBDS Safety and Reliability Analysis in the Light of the Operational Experience during the Period 2010-2012", CERN-ATS-Note-2013-042 TECH.

[4] R. Filippini, J. Uythoven, "Reliability Analysis of the Trigger Synchronisation and Distribution System of the LHC Beam Dumping System", CERN-ATS-Note-2013-043-TECH.

ISBN 978-3-95450-139-7