RELIABILITY ASSESSMENT OF THE LHC MACHINE PROTECTION SYSTEM

R. Filippini, B. Dehning, G. Guaglio, F. Rodriguez-Mateos, R. Schmidt, B. Todd, J. Uythoven, A. Vergara-Fernandez, M. Zerlauth, CERN, Geneva, Switzerland

Abstract

A large number of complex systems will be involved in ensuring a safe operation of the CERN Large Hadron Collider, such as beam dumping and collimation, beam loss and position monitors, quench protection, powering interlock and beam interlock system. The latter will monitor the status of all other systems and trigger the beam abort if necessary. While the overall system is expected to provide an extremely high level of protection, none of the involved components should unduly impede machine operation by creating physically unfounded dump requests or beam inhibit signals. This paper investigates the resulting trade-off between safety and availability and provides quantitative results for the most critical protection elements.

MACHINE PROTECTION AND DEPENDABILITY CONCERNS

The Machine Protection System (MPS) [1,2] guarantees safe conditions in the LHC by: 1) checking the status of the equipment before every new fill and 2) preventing damage to the machine by safely stopping operation once the beam is circulating, either at the end of a fill or after a failure. In all cases the beams must be extracted into the dump blocks, the only elements that can stand the LHC beams without being damaged.

Safety is the main concern for the MPS. The system must be available on request, resulting in a correct execution of the beam dump. If a failure in the MPS is detected it must still be possible to dump the beam safely (false beam dumps). In case the MPS is not available to dump the beam serious damages are expected [3]. For this reason the overall system failure rate is required to be in the range [10^{-8}/h, 10^{-7}/h] in agreement with the SIL3 (Safety Integrity Level) specification [4].

The system architecture includes all safety related systems surveying beam conditions (beam losses, beam position, etc) and the status of critical equipment (super conducting magnets, power converters) in the LHC. These systems send dump requests to the Beam Interlocking System (BIS) that are transmitted for execution to the Beam Dumping Systems (LBDS). The control room and other non-safety related systems in the LHC may also issue dump requests but these are not part of the MPS core architecture.

This paper considers a simplified MPS architecture including the BIS, with 16 Beam Interlock Controllers (BIC), two LBDS (one per ring) plus three interlocked systems: the Beam Loss Monitors (BLM) including 3500 monitors plus electronics, the Quench Protection System (QPS) including 4000 channels and the Powering Interlock Controllers (PIC), 36 in total. More details on each system may be found in [1]. Figures of safety and unavailability due to false dumps will be given for one year of operation under different operational scenarios.

MPS MODELLING ASPECTS

The system is studied in two steps. Firstly, safety and unavailability due to false dumps have been evaluated for each system of the simplified MPS, passing through the definition of the functional architecture, Failure Modes, Effects and Criticality Analysis (FMECA) [5] and reliability prediction at component level. This has been the most time-consuming part of the study because for all system components the failure modes needed to be defined and therefore classified with respect to the consequences, including the means to prevent them. Failure rates were deduced from literature [6] or experience (historical CERN databases), in both cases adopting conservative criteria (e.g. overestimating the component stress factors).

As second step, results obtained for the individual systems have been arranged into the simplified MPS model with the source of dump requests and their frequency. The sources of dump request have been classified as: 1) planned dump requests from the control room, 2) fast beam losses (<10ms), 3) slow beam losses (>10ms) and 4) others. False dumps have been assumed safe and for this reason they do not enter the list. All failures have been assumed leading to beam losses (directly or indirectly) that are perfectly covered by the BLM and QPS (slow beam losses).

The studied MPS model is shown in Figure 1. With the exception of the BIC and the LBDS, which are always demanded, the other MPS systems may be demanded or not depending on the source of the dump request. In addition, it is possible that more systems act in parallel, resulting in cross-redundancy for the dump request generation.

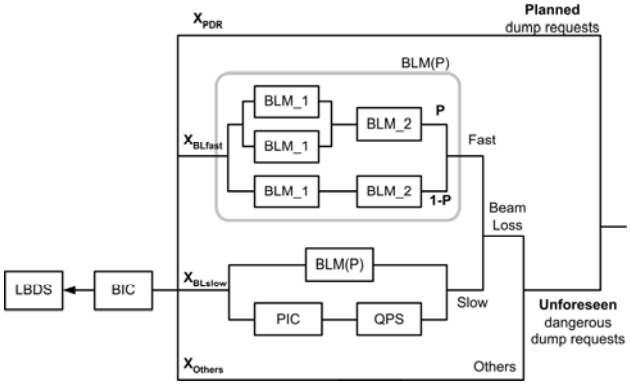

Figure 1: Simplified MPS model.

The BLM system consists of detectors with their front-end electronics (BLM_1), several of which are connected to the same VME crate (BLM_2) (see Figure 1). Possible cross-redundancy exists within the BLMs; this is represented with the probability P that two monitors are detecting the same beam loss, as shown in Figure 1. More redundancy within the BLMs is still possible but not taken into consideration. Possible cross-redundancy exists also between the BLM and the QPS (in series with the PIC) for slow beam losses, which are also detected as magnet quenches. In this study it is assumed that for other dump requests the only MPS systems involved are the BIC and the LBDS.

Each branch contributes to the total unsafety by the weight of the respective fraction of dump requests. The unavailability due to false dumps is the sum of the contribution of each system and does not depend neither on the given apportionment nor on cross-redundancy.

Design facilities like redundancy, on-line surveillance and off-line diagnostics are essential for keeping the system safe. Benefits are illustrated in the following example (see Figure 2). A system is assumed to have a constant failure rate of 10^{-3}/h. If one identical system is placed in parallel the failure rate is reduced. A further improvement is obtained by adding surveillance, which may cover system failures (here assumed 90%) and generates operation aborts (failsafe). Diagnostics, performed every 10 hours, recovers the system to an "as good as new" state resulting in a further benefit for the failure rate that, in the end, is reduced by 3 orders of magnitude. As drawback, this leads to a more complex system with higher costs and increased unavailability (operation aborts). This example shows the importance of addressing the trade-off problem between benefits and drawbacks that exists for many systems in the MPS.

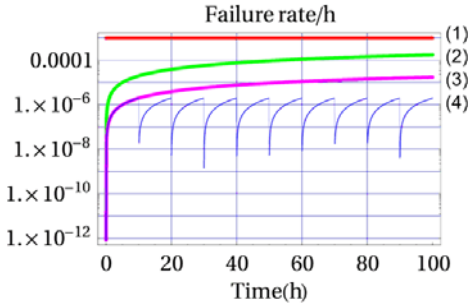

Figure 2: Comparison of designs for safety and consequences on failure rate: one system with constant failure rate (1), two systems in parallel (2) plus surveillance (3) and diagnostics (4).

MPS ANALYSIS

For the analysis of the simplified MPS the following assumptions are made:

(A1). The operational scenario consists of 200 days of operation, 400 machine fills (10h each) followed by 2 hours without beam.

(A2). The diagnostics recover the LBDS, the BIC and the BLM (all electronics) "as good as new" before every fill. The QPS and the PIC are "as good as new" at periodic monthly inspection or after a power abort.

(A3). Dump requests are apportioned in 60% planned beam aborts, 15% fast beam losses, 15% slow beam losses and 10% other sources.

(A4). Cross-redundancy within the BLM is not included (P = 0).

The 2 hours without the beam, between the fills (A1), include time for diagnostics, system rearming and possible downtime repairs.

Results for the individual systems and the complete MPS are shown in Table 1. The probability that the MPS is not available on request (unsafety) is 2.3×10^{-4} per year. This corresponds to an equivalent failure rate per hour of 0.58×10^{-7} which is SIL3. The number of expected false dumps is 41 per year on average (+/-6), about 10% of the total machine fills.

Table 1: Results for the assumed dump requests apportionment (unsafety and std. dev. do not sum up).

System	Unsafety / year	False dumps/y	
		Average	Std. D.
LBDS [7]	1.8×10^{-7}(2x)	3.4(2x)	+/-1.8
BIC [9]	1.4×10^{-8}	0.5	+/-0.5
BLM [10]	1.44×10^{-3} (BLM_1)	17	+/-4.0
	0.06×10^{-3} (BLM_2)		
PIC [11]	0.5×10^{-3}	1.5	+/-1.2
QPS [8]	0.4×10^{-3}	15.8	+/-3.9
Overall results			
MPS	2.3×10^{-4}	41.6	+/-6.2

Sensitivity analyses

The calculated safety is sensitive to the dump requests apportionment, cross-redundancy and other parameters.

If a different dump requests apportionment is assumed, namely 40% planned, 25% fast beam loss, 25% slow beam losses and 10% others, then the unsafety per year becomes 3.8×10^{-4}, now at the limit of SIL3, with fast beam losses being the largest contribution as shown in Figure 3.

It is important to remark that no cross-redundancy was assumed so far within the BLMs (A4). If this assumption is relaxed, then the unsafety decreases with the parameter P and drops to 9.7×10^{-6} per year in case of 100% redundancy (P=1), which is SIL4 for the default dump requests apportionment (see Figure 4).

Unsafety is also sensitive to diagnostics. As an example, for the LBDS [7] the unsafety increases from 1.4×10^{-7} to 5.4×10^{-5} per year if diagnostics (post mortem after every beam dump) is not performed. The safety of the LBDS also depends on the operation length. For example, keeping the same total operation time of 4000 hours per year, the LBDS is less safe (1.7×10^{-7}) for 320 longer missions of 12.5 hours each than for 500 short missions of 8 hours each (1.1×10^{-7}).

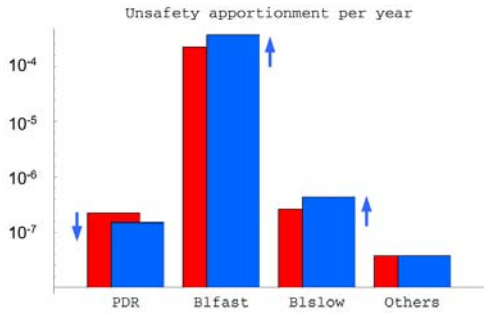

Figure 3: Sensitivity to dump requests apportionment: red bar (60,15,15,10) %, blue bar (40,25,25,10) %.

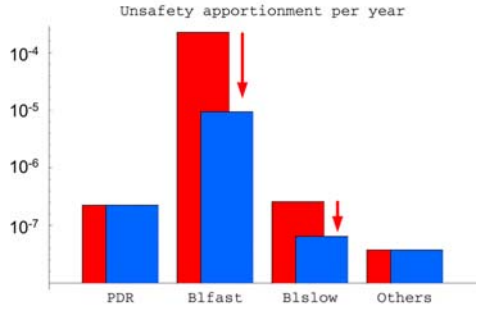

Figure 4: Sensitivity to cross-redundancy within the BLM: red bar (no redundancy, P=0), blue bar (100% redundancy, P=1)

The number of false dumps is not sensitive to the above parameters. They depend on the complexity of the MPS and the surveillance. Within all systems of the MPS, the power converters (PC) are the main source of false dumps. If these are made redundant, for instance by putting two power converters in parallel, a strong reduction is expected as demonstrated for the QPS with the false dumps halved from 16 to 8 per year [8].

CONCLUSIONS

The presented study on the MPS has demonstrated that the safety of the system strongly depends on the source of the beam dump request and the ability to cover it possibly with more systems acting in parallel (cross-redundancy). For the analysed scenario, unsafety ranges between SIL4 (Mean Time To Failure = 47K years) and SIL3 (MTTF = 2K years) depending on the assumed cross-redundancy. These figures are reached generating an estimated average of about 40 false dumps per year (+/- 6), which corresponds to 10% of the machine fills.

Sensitivity analysis shows that fast beam losses are the major concern for safety and that power converters for MPS electronics are the principal cause of false beam dumps. Results were based on a conservative method of calculation that was adopted throughout the different stages of the study, from the failure rate prediction to the building of the MPS model. This leads to an underestimate of the MPS safety as well as an overestimate of its unavailability. It is also important to note that the studied model refers to a simplified MPS with assumed perfect coverage of BLMs and QPS. Some parts still need a more complete analysis and other systems like Beam Current Transformer, Beam Position Monitors, Collimators etc, presently not included in the MPS, may add cross-redundancy in the dump request. Other systems external to the MPS can reduce significantly the overall machine availability.

The presented model can be progressively updated including other features relevant for the reliability assessment of the machine protection of the LHC, like the integrity of the checking and rearming procedures. A study apart can be done looking at the trade-off between safety and unavailability in order to find a balance between the two quantities. For the latter issue especially, it is important that analogous studies will be addressed across all contributing LHC systems.

ACKNOWLEDGEMENTS

The paper is the result of fruitful discussions over several months within the Machine Protection Reliability Working Group.

REFERENCES

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

[2] J. Wenninger, R. Schmidt, “Protection Against Accidental Beam Losses at the LHC”, Particle Accelerators Conference PAC 2005, 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] Failure Mode/Mechanism Distributions, FMD-97, Reliability Analysis Center RAC, Rome (NY, USA), 1997.

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

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

[8] A. Vergara-Fernandez, F. Rodriguez-Mateos, R. Denz, “Reliability Analysis for the Quench Detection in the LHC Machine”, 8th European Particle Accelerator Conference EPAC 2002, Paris, France, 3-7 July 2004.

[9] B. Todd, private communication.

[10] G. Guaglio, private communication.

[11] M. Zerlauth, private communication.