WILL WE EVER GET THE GREEN LIGHT FOR BEAM OPERATION ?

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

Abstract

The primary task of the machine protection system is to prevent equipment damage. To guarantee the required system safety the subsystems have evolved in large and often complex systems. As a result the machine protection system could become a major cause of machine downtime by triggering too many false beam dumps or failing to allow a beam permit. The paper will present the major components of the machine protection system and the method used to calculate the dependability of the system. The results of a study of a subsystem are given, resulting in the estimated number of requested beam dumps which will not be correctly executed (safety) and the number of false beam dumps per year initiated by the subsystem (unavailability).

BEAM OPERATION AND DEPENDABILITY CONCERNS

Ideally, an LHC physics run is terminated when the operator pushes the beam dump button. This definition of an end of fill corresponds to the optimal exploitation of the machine. At the same time, requirements exist for fault-free and safe conditions during operation. The LHC Machine Protection System (MPS) [1] guarantees these attributes. It assures the execution of a proper beam dump if required (red light) and gives a beam permit signal when safe machine conditions are met (green light).

The beam permit signal generation is the result of heterogeneous information coming from the LHC safety critical equipment. The MPS boundaries are difficult to set as almost all equipment in the LHC is directly or indirectly interlocked to its architecture. A reasonable definition restricts the MPS to the systems that *actively* participate in the protection task. It consists of the systems that generate the interlock signals via their transducers, transmit those signals to the beam dumping system and execute the beam dump action.

The MPS can be suitably addressed by considering *availability*, which is "the probability the system performs the required function at a stated instant of time", and *safety*, which is "the probability to complete its task without any consequences regarding damage or loss of equipment". *Reliability*, which is "the probability the system is functioning for a stated period of time" is not the most suited attribute for the MPS. If reliability were used instead of safety then one would totally miss the fact that also a safe beam operation abort (no conditions for the green light) is acceptable. If reliability were used instead of availability one would miss the fact that a large part of the system can be recovered from failures (between two beam operations) without any consequence during beam operation. It is important to remark that availability and reliability are the same for those systems that are not repairable and always demanded at a beam dump request. The ensemble of safety, availability, reliability and other related terms is generally called *dependability* [2,3].

The following example can help to further clarify the definitions. An airplane is asked to be available at a certain time *t* for take-off (available = beam permit given when beam operation required, seen over several fills) and once it is in the air it is required to be reliable until its landing (reliability = beam permit given during a single LHC fill). Some failures, say one engine breaking down, can be safely handled for instance by landing at the nearest airport (false beam dump), but the airplane is unreliable because it did not arrive at the planned destination (no beam permit). The airplane is unsafe if it crashes (no or bad beam dump leading to damage).

In the MPS safety is reached with self-surveillance that catches internal failures (within the MPS) and generates beam dump requests. These dump requests are commonly called *false dumps* as the source is not the surveyed equipment but the MPS itself. False dumps affect availability while they improve safety so that it is likely that a safer MPS might have a lower availability.

Early concepts of MPS dependability mostly refer to the beam dumping system only, considering something like 1 failure per 100 years as an acceptable rate for safety [1, 4]. No estimates exist for the availability. The aim of this paper is to consider safety and availability of the whole MPS and to determine if an acceptable trade-off is reached or not.

THE SIMPLIFIED MACHINE PROTECTION SYSTEM

A simplified architecture of the MPS is shown in Fig. 1. This model is representative for the MPS functional architecture that essentially includes the dump request generation, the reception and the execution units arranged in series. Eight sectors of the LHC house almost identical

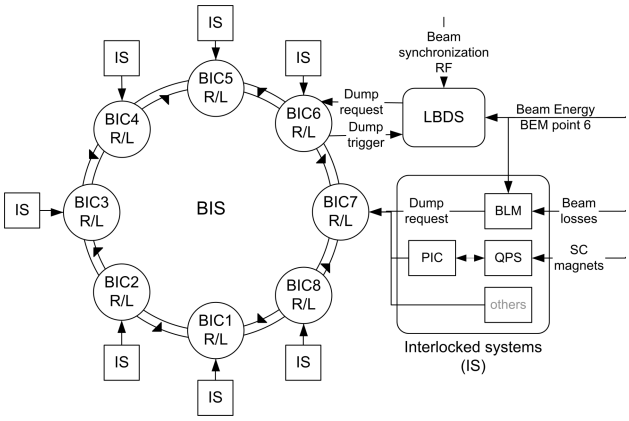

Figure 1: Simplified MPS.

protection equipment consisting of the Beam Loss Monitors (BLM), the Quench Protection System (QPS) and the Powering Interlock Controller (PIC), which are connected to the Beam Interlock Controllers right and left of each IP. Beam dump requests are transmitted from the local BIC to the LHC Beam Dumping System (LBDS) in sector 6. More details on the functioning of each system may be found in [1].

The dump request may come from the control room as the normal completion of the physics run, from the sector x following a detected beam anomaly or failure in the surveyed equipment, or a false dump. With the exception of the LBDS, which always needs to be operational, other systems need to be operational or not, depending on the source of dump request. The analysis of all possible combinations is beyond the aim of this paper. The MPS safety is calculated based on the following sub-systems: one BLM, one QPS, one PIC and one BIC, all these at sector x plus two LBDS necessary to dump the beams. The model accounts for the following sources of false beam dumps affecting availability: in total some 3500 BLMs (monitors) and 4000 quench detectors (QPS), 36 PICs, 16 BICs and 2 LBDS.

Assumptions for calculations

The operational scenario of one year of LHC operations with 400 fills of 10 hours each is assumed. Failure rates are assumed to be constant (at component level) and calculated in accordance to the Military Handbook 217F [5]. The system can fail only when operating and if failed it cannot be repaired so that the LHC is shut down for a long period.

Post mortem diagnostics and repair facilities are apportioned to the respective sub-systems as summarised in Table 1. The "as good as new" assumption implies the "regeneration" of the failure rate in the redundant systems of the MPS. The complete regeneration point is the yearly overhaul when also the BLMs are fully inspected. Partial regenerations exist using the post mortem diagnostics (before the new fill) and periodic inspections for the other sub-systems. This is demonstrated in Fig. 2 for one system with a failure rate of 10^{-7}/h in series with two parallel systems with a failure rate of 10^{-4}/h each. The regeneration points are every 10 hours (redundancy recovery) when the system is fully inspected and recovered to a "as good as new" state.

Table 1: Diagnostics effectiveness.

System	Partial	As good as new
LBDS, BIC	-	Every new fill
QPS, PIC	-	Power abort or monthly inspection
BLM	Every new fill	Yearly overhaul

EXAMPLE: LBDS ANALYSIS

As an example, the analysis of the LBDS, as a sub-system of the MPS, is presented in more detail. Each LBDS consists of 15 horizontally deflecting extraction kicker magnets MKD followed by the superconducting quadrupole Q4 (which enhances the MKD kick), 15 vertically deflecting septum magnets MSD and 10 dilution kicker magnets MKB followed by the absorber block TDE several 100 m further [1].

The dumping action must be synchronised with the particle free gap (triggering system) and the magnetic field adjusted to the beam energy (beam energy meter BEM and beam energy tracking system BETS) [6].

Failure rates and modes have been collected at the component level and then arranged into failures at sub-system and system level [7,8]. The overall system failure processes have been modelled with a state transition diagram including three states only: system available, failed unsafe or failed safe (see Fig. 3).

The system has failed unsafe only if failed silently or the surveillance missed the detection, leaving the fault undetected. In all other cases, the system, either available or failed safely, is considered safe. Results are shown in Fig. 4 and Fig. 5. After one year of operation, one LBDS has the probability of failing unsafe equal to 1.4×10^{-7} and produces 2.6 (+/-1.6) false dumps on average [8].

The analysis accounts for 15 MKD generators and magnets, the triggering and re-triggering systems, based on the MIL-HDBK reliability prediction, and the BEM and the BET, based on realistic assumptions. These systems represent the core of the LBDS architecture. The upstream elements in the dump line are not included in the present analysis.

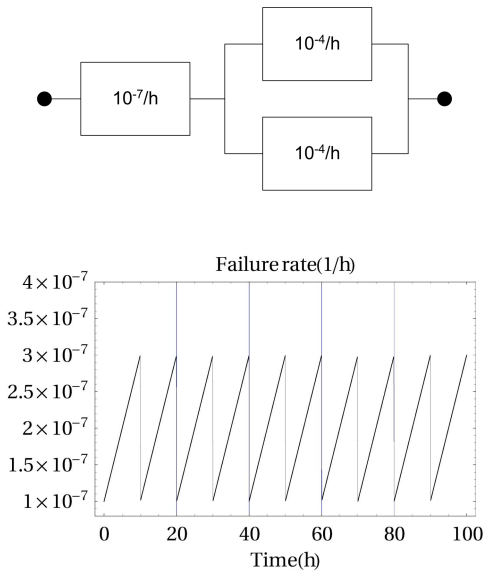

Figure 2: Example of diagnostics regenerating the failure rate in redundant systems.

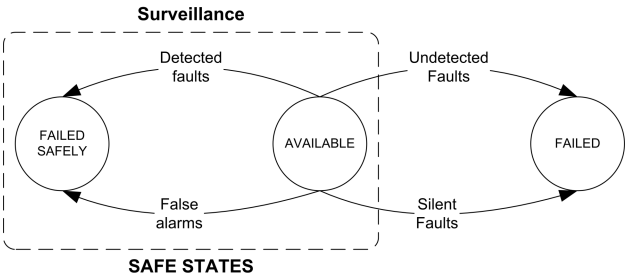

Figure 3: LBDS state transition diagram.

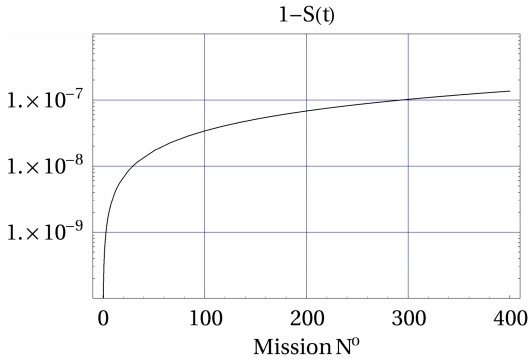

Figure 4: Unsafety of the LBDS per year.

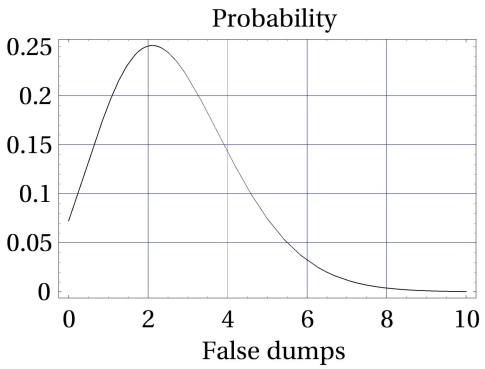

Figure 5: Distribution of false dumps generated in the LBDS for one year of operation.

The magnet coils, cables and connectors supplying the current to the magnets (from the pulse generator) are the safety bottlenecks of the LBDS system. This is explained by the lack of continuous surveillance of the MKD magnets. Availability bottlenecks are the power triggers (2 per MKD, 30 in total) with their power converters. Static redundancy (like double branch switches) and on-line surveillance explain the high safety figure, which also benefits from post mortem diagnostics as demonstrated in Fig. 6. The failure rate comes back to the initial value after the beam dump and successful post mortem while it would keep increasing in absence of diagnostics. This requires of course that the result of the post mortem is taken seriously and, if necessary, corrective action is immediately taken.

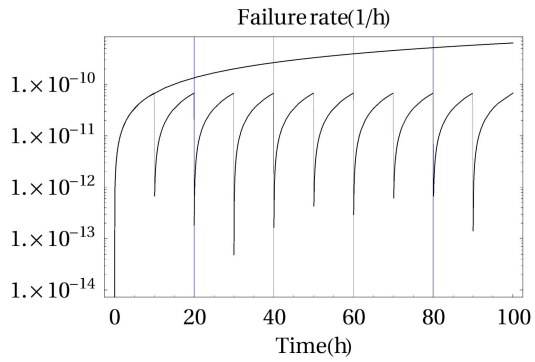

Figure 6: The effect of post mortem diagnostics for the LBDS: without (top) and with regeneration (bottom) for 10 missions.

MPS ANALYSIS

The attributes of interest are the probability that the overall MPS fails unsafe and the number of false dumps per year. Calculations have been done for each sub-system separately and then arranged into the general model.

Results for the simplified MPS

The results for the simplified MPS are shown in Table 2 [8 – 12]. The probability of failing unsafe is about 0.003 per year with 29 false dumps on average expected, which accounts for 7 % of the assumed 400 requested beam dumps. The probability of failing unsafe as a function of the numbers of years of LHC operation is shown in Fig. 7. The table shows that the BLM system has the highest unsafety number but it needs to be kept in mind that calculations are based on a punctual loss model, which is very conservative as a beam loss is likely to affect several monitors. If at least two monitors are concerned, then the probability to fail unsafe drops to 2.9×10^{-6} per year.

The complete MPS is required to be available at every dump request, which is a very conservative assumption. In almost all cases an unstable beam or hardware failures will be detected by several systems simultaneously and it is very likely that the most critical users enter two BICs (right/left) instead of one. If this is taken into account then safety contributions from the BIC and the other systems are expected to decrease.

It has to be kept in mind that the contribution from the powering system (power converters for VME crates, etc.) is likely to be overestimated. This might be especially true for the QPS. Here the contribution of the power converters accounts for half of the number of false dumps from the QPS (8.1 per year) [12]. If required by experience, a design solution, namely the insertion of redundant units, is possible.

The results may still change because of some sub-systems have still to be analysed and in the end safety might worsen. In particular for the BIC, where the analysis is presently not including the core electronics and the permit loops.

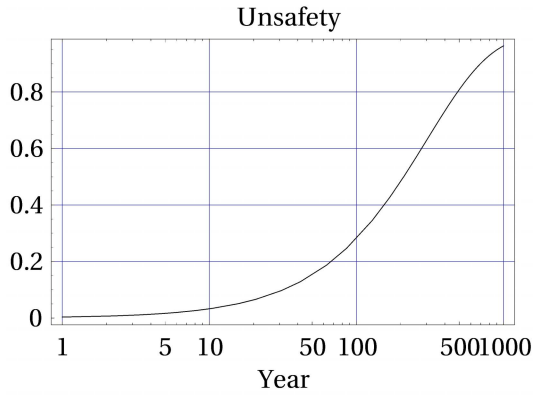

Figure 7: Probability of the MPS failing unsafe as a function of the number of years of LHC operation.

Safety and availability trade-off

The many interlocks within the MPS add safety to the beam operation but they are also a potential source of false dumps, therefore reducing the availability. The proper dimensioning of the MPS is a delicate apportionment of the two attributes to each sub-system, with safety remaining the primary goal.

The issue can be addressed for each system separately or treated as a whole. The safe beam flag [13] represents a solution for the latter approach. The safe beam flag implements a strategy for masking some MPS interlocks (flag on) during non-critical phases and activating them (flag off) in the critical ones. A gain in operational freedom is expected and also an increased system availability. However, reliable tracking of phase changes will be mandatory and the mechanism always has to fail safely.

CONCLUSIONS

The LHC Machine Protection System has a mean time to failure of 300 years. This means that over an assumed LHC lifetime of 20 years the probability of not failing unsafe is 0.93. For the availability, 29 (+/-12) false dumps per year (on average) are expected, which affects 7 % of the runs.

The overall system has an equivalent failure rate of 7.5×10^{-7} per hour, compatible with SIL2. This is higher than required for SIL3 [1×10^{-8}/h, 1×10^{-7}/h] as recommended in the IEC-61508 prescription for safety critical systems [14]. It is important to remark that results are still provisional and for safety rely on conservative assumptions both in the model (single source of beam dump request) and in the analysis based on the military handbook, which usually provides rather pessimistic figures. For the same reason, also the number of false dumps might be overestimated.

The model can be either refined or more specific analyses can be done, for instance looking at the sensitivity to the critical design parameters, like the post mortem diagnostics and surveillance with its fraction of false alarms.

The study needs to be completed with the inclusion of other systems interlocked to the MPS like the beam position monitors, the RF system, the collimation system and the general post mortem facilities. The systems outside the MPS, like the power converters of the magnets, are also expected to provide similar figures of availability, which can be arranged together in order to obtain the overall analysis of the LHC.

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] Hoyland, M. Rausand, "System Reliability Theory", p. 490, Wiley, 1994.

Table 2: MPS results.

System	Unsafety/year	False dumps/year Average	Std. Dev.	Analysis including	Not included
LBDS [8]	1.4×10^{-7} (2X)	2.6 (2X)	(+/-1.6)	(Re-)triggering system,MKD (MIL-217F) BET, BEM (assumptions)	MSD, Q4, MKB TDE
BIC [9]	0.7×10^{-3}	1.6	(+/-1.3)	User Boxes only (MIL-217F)	BIC core, VME and permit loops
BLM [10]	1.7×10^{-3}	4.8	(+/-2.1)	Focused loss on single monitor (MIL-217F, SPS data)	Design upgrades
PIC [11]	0.5×10^{-3}	1.5	(+/-1.2)	Complete system (MIL-217F)	PLC
QPS [12]	0.4×10^{-3}	15.8	(+/-3.9)	Complete system (MIL-217F)	
OVERALL RESULTS					
MPS	3.3×10^{-3}	28.9	(+/-11.7)		

[3] J. C. Laprie et al., "Dependability: Basic Concepts and Terminology", Springer-Verlag, 1992.
[4] J. Dieperink et al., "Design Aspects Related on the Reliability of the Beam Dump Kicker Systems", CERN-LHC project report 113, CERN, Geneva 1997.
[5] MIL-HDBK-217F, "Reliability Prediction of Electronic Equipment", Department of Defence, Washington D.C. USA, 1993.
[6] E. Carlier et al. "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.
[7] 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.
[8] R. Filippini, unpublished studies.
[9] B. Todd, private communications.
[10] G. Guaglio, private communications.
[11] M. Zerlauth, private communications.
[12] A. Vergara, "Reliability of the Quench Protection System for the LHC Superconducting Elements" CERN-Thesis 2004-019, Geneva, 2004.
[13] B. Puccio, "Proposal for the Transmission of Safe LHC Parameters", minutes of the Machine Protection Working Group meeting, CERN, September 2004.
[14] International Electrotechnical Commission IEC, "Functional Safety of Electrical-Electronic-Programmable Electronic Safety Related Systems" IEC 61508 International standard, Geneva, 1998.