Reliability of Beam Loss Monitors System for the Large Hadron Collider

G. Guaglio, B. Dehning, C. Santoni

Reliability of Beam Loss Monitors System for the Large Hadron Collider

G. Guaglio[*+], B. Dehning[*], C. Santoni[+]

[*]*CERN, CH-1211 Genève 23 (Switzerland)*
[+]*UNIVERSITE BLAISE PASCAL, 34 avenue Carnot BP 185, 63006 Clermont-Ferrand FRANCE*

Abstract. The employment of superconducting magnets, in the high energies colliders, opens challenging failure scenarios and brings new criticalities for the whole system protection. For the LHC beam loss protection system, the failure rate and the availability requirements have been evaluated using the Safety Integrity Level (SIL) approach. A downtime cost evaluation is used as input for the SIL approach. The most critical systems, which contribute to the final SIL value, are the dump system, the interlock system, the beam loss monitors system and the energy monitor system. The Beam Loss Monitors System (BLMS) is critical for short and intense particles losses, while at medium and higher loss time it is assisted by other systems, such as the quench protection system and the cryogenic system. For BLMS, hardware and software have been evaluated in detail. The reliability input figures have been collected using historical data from the SPS, using temperature and radiation damage experimental data as well as using standard databases. All the data has been processed by a reliability software (Isograph). The analysis ranges from the components data to the system configuration.

INTRODUCTION

The Large Hadron Collider (LHC) is the next CERN particle accelerator that will try to penetrate further into the matter structure, accelerating protons up to 7 TeV. The innovative characteristic is the wide scale use of superconducting magnets to reach fields closed to 9 Tesla so as to bend the high energy particles beam. The superconducting technology involves different challenges, mainly addressed to generate and maintain the magnets in the superconductive state. One of the critical applications is the Machine Protection System, which intends to avoid machine damages caused by the heating following a beam loss.

In this work we will introduce the general LHC approach to prevent these events with the utilization of different systems. Later we will focus on the Beam Loss Monitors System, analyzing the design aspects and the dependability figures.

SIL APPROACH

In this paragraph we will discuss the possibility to use the Safety Integrity Levels (SIL) approach for the machine protection purpose. In fact, strictly speaking, the standard IEC 61508 [1] is used as guideline for the personal safety and not for the

TABLE 1. Category table used for LHC consequences definition.

Category	Injury to personnel		Damage to equipment	
	Criteria	N. fatalities (indicative)	CHF Loss	Downtime
Catastro-phic	Events capable of resulting in multiple fatalities	≥1	$> 5*10^7$	> 6 months
Major	Events capable of resulting in a fatality	0.1 (or 1 over 10 accidents)	$10^6 – 5*10^7$	20 days to 6 months
Severe	Events which may lead to serious, but not fatal, injury	0.01 (or 1 over 100 accidents)	$10^5 – 10^6$	3 to 20 days
Minor	Events which may lead to minor injuries	0.001 (or 1 over 1000 accidents)	$0 – 10^5$	< 3 days

machine protection. In any case, it gives general figures and hints that could wisely used to protect machine rather than people.

The aim of the SIL is to suggest failure rate figures to face a risk occurrence. In the following we will define the risk concept and we describe the procedure used to extract the reliability figures for the system.

RISKS FOR LHC BEAM LOSSES

Generally speaking, we can define the risk associate to an event as a product of the probability that this event will happen multiplied by a general cost of that consequence, which is "how often we pay something".

The SIL standard simply gives a way to estimate and to fix that probability to minimize the risk to pay a cost.

In fact, the probability P is strongly connected to the system designed to minimize the risk of the outcome: its range runs from the event frequency F, when there is no protection system, down to a level defined by the system functionality.

In the following we will extract from the SIL standard the figures for a safe operation (the system works when it has to work) and for an efficient one (the system does not work when it does not have to work).

The two main failures that can occur are Magnet Destruction and False Dump: we will have a Magnet Destruction (MaDe) if there is a dangerous loss and the beam is not extracted. This eventuality could cause a down time of around 30 days to substitute the 250 kCHF superconductive magnet with a spare one. Currently, only 16 spare main quadrupole magnets are foreseen.

A False Dump (FaDu) generation occurs when the system generates a false alarm, followed by a dump, even if there were no dangers for the superconductive magnets. This generates on average almost 3 hours of downtime to return to the previous beam status.

TABLE 2. Frequency table used for LHC risk definition.

Category	Description	Frequency (per year)
Frequent	Events which are very likely to occur	> 1
Probable	Events that are likely to occur	10^{-1} - 1
Occasional	Events which are possible and expected to occur	$10^{-2} – 10^{-1}$
Remote	Events which are possible but not expected to occur	$10^{-3} – 10^{-2}$
Improbable	Events which are unlikely to occur	$10^{-4} – 10^{-3}$
Negligible	Events which are extremely unlikely to occur	$< 10^{-4}$

TABLE 3. Failure rate (SIL) and Risk table used for LHC risk evaluation. See text for details.

Event Likelihood	Consequence							
	Catastrophic		Major		Severe		Minor	
Frequent	SIL 4	I	SIL 3	I	SIL 3	I	SIL 2	II
Probable	SIL 3	I	SIL 3	I	SIL 3	II	SIL 2	III
Occasional	SIL 3	I	SIL 3	II	SIL 2	III	SIL 1	III
Remote	SIL 3	II	SIL 2	II	SIL 2	III	SIL 1	IV
Improbable	SIL 3	II	SIL 2	III	SIL 1	IV	SIL 1	IV
Negligible	SIL 2	III	SIL 1	IV	SIL 1	IV	SIL 1	IV

Inspirited by the IEC 61508-5 annex B [1], LHC expert judgment created the consequences table, the frequency table and the risk table (tables 1-3).

For our scenarios, we will have a major consequence for the MaDe occurrence, a minor (or less) for the FaDu, as shown in table 1.

The second step is to estimate the frequency of the event.

Due to the fact that there is no historical data on machines that are comparable for technology, size and luminosity, we have to estimate the order of magnitude of the event frequency. We can guess, on LEP experience, that we can expect probably more than 10 dangerous losses per years. What's more, due to the fact that every dump comports around 3 hours of downtime to come back to the original conditions, we hope to have less than 1000 dumps per year. Consequently, we try to face and event that we guess to have a frequency of 100/y.

To avoid the Magnet Destruction, we will develop a system that can generate some False Dumps per year, caused by its internal failures. As already said, every dump brings around 3 hours of no operational beam, consequently we will try to keep this number on the order of 30 per years (1 per week), so as not to seriously decrease the LHC luminosity time.

The frequency of both events is "Frequent", as show in table 2.

Now we have to decide which approach we want to follow. In the standard IEC 61508-5 Annex A and B, two possibilities are present: Functional Approach (FA) and Malfunction Approach (MA).

FA is based on the definition of the SIL levels and it requires that the system has to work with that failure rate to be considered safe, later it verifies that the risk is acceptable. MA defines first the acceptable risk and then tries to reduce it As Low As Reasonably Practicable.

In both philosophies, we have to define what the maximum tolerable risk for our events is. For MaDe we can say that, due to the fact LHC will work for 20 years and there will be 16 spares magnets, we tolerate a maximum of 0.8 MaDe per year. For FaDu, we have already said that we would prefer to stay around 30 FaDu per year so as not to deteriorate operational efficiency.

FA and MA give us the failure probability per hour, then we have to multiply that number by the operational hour per year to have the failure probability per years and finally, with the proper factors, we will have our failures per year. This should be

TABLE 4. Probability of a dangerous failure per hour.

SIL	Probability of a dangerous failure per hour
4	$10^{-9} < Pr < 10^{-8}$
3	$10^{-8} < Pr < 10^{-7}$
2	$10^{-7} < Pr < 10^{-6}$
1	$10^{-6} < Pr < 10^{-5}$

TABLE 5 Risk table with the definitions of the risk extrapolated from table 3**.**

RISK	DEFINITIONS
I	Intolerable
II	Tolerable if reduction is impracticable or cost is disproportionate
III	Tolerable if cost exceed improvement
IV	Negligible

less then the tolerated value. In other words

$$Failure_{MaDe}/_{h} \cdot 4000\, h/_{y} \cdot 100 \leq Tolerated_{MaDe}/_{y} \quad (1)$$

$$Failure_{FaDu}/_{h} \cdot 4000\, h/_{y} \leq Tolerated_{FaDu}/_{y} \quad (2)$$

In Eq (1), we multiply the probability to have a MaDe by the expected number of annual dangerous losses, because we will "throw the dice" 100 times in the years.

For simplicity, we will develop the FaDu concept in the FA and MA.

In the FA we have, from table 3, that a frequent-minor consequence has to reach SIL2 level, that means, from table 4, a failure probability less than 10^{-6}/h. So we have to design the system to have a failure rate, for the FaDu, which is less then this value. Substituting in Eq (2) the higher limits, we calculate 4 10^{-3} failures per years: probably we are too conservative if we compare it with the tolerated 30 failures per year. Table 3 is also useful to estimate what is the risk (roman number and table 5)if we don't reach the suggested SIL level with our system. Suppose we design a system with a failure probability of 10^{-4} for FaDu. With equation 2 we calculate an error Frequency of 4 10^{-1} failures per years that, in table 2, is an "occasional" event. With table 3 we read that we have to face a III risk, which means that we are allowed to not improve the system only if the changing "costs" more than the improving.

In the MA we start assigning the tolerate FaDu per year and calculating the Failure figures: with 30 FaDu/y we have 7.5 10^{-3} failure per hours. Note that entering in table 3 with the 30 tolerated FaDu, a frequent-minor event, we have a II risk. That means (table 5) we have to reduce it if it is possible and the cost are not disproportionate; as it could be expected, due to the fact that 30 is our maximum tolerated value.

It has to be noted that table 3 is extracted by the suggestion of [1], but it could and should be adapted to the different situations with expert judgment, as well as table 1 and 2.

Following the same procedure for the MaDe, we obtain table 6. From this table we can see that there is a good agreement between the two approaches in the MaDe predictions, whereas for FaDu they are deeply different, probably because there is an overestimation of the gravity of the event (3 days of downtime is much greater than 3 hours) that brings the FA to be too conservative.

TABLE 6. FA and MA results for LHC machine protection. In **bold**, the input parameters

		Failure/h	Total/y
MaDe	FA	**10^{-7}**	0.04
	MA	2 10^{-6}	**0.8**
FaDu	FA	**10^{-6}**	4 10^{-3}
	MA	7.5 10^{-3}	**30**

LHC SYSTEM: MAIN ACTORS

In the LHC the safe philosophy will be: whenever there will be a dangerous proton loss, we extract the beam from the machine. The first line safety systems are: the Beam Loss Monitors System (BLMS), which detects the dangerous loss and inhibits a beam permit through the Beam Interlock System (BIS), so that the LHC Beam Dump System (LBDS) can extract the beams from the machine in a safe way. This extracts the beam in function of the beam energy signal given by the Beam Energy Meter (BEM). These 4 main systems are assisted by other second line systems that additionally protect the machine but with slower time constants: the first line system has to act for 100μs intense losses as well for 100s low losses, the second line systems react after 10 ms of time, so they cannot help for fast losses. Currently there are also ideas to extend the Beam Position Monitor and the lifetime system to protect the machine also for the fast losses, but they are still not well defined.

Nevertheless, several systems can generate dumps but not exclusively for the machine protection aim. From the operational systems to the safety ones we can have almost 20 systems that can request for a dump, as show in Fig 1.

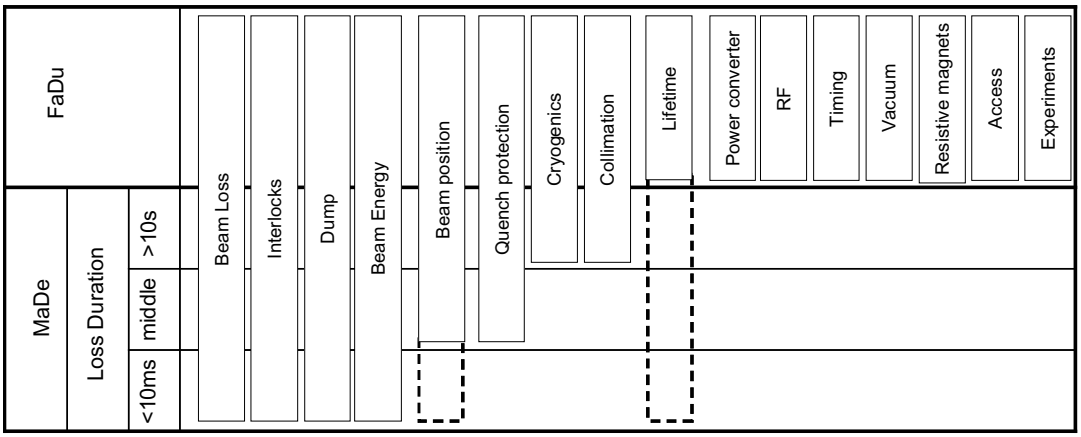

FIGURE 1. Main LHC systems connected to the Beam Interlock System and that can generate a dump and classification of the protective systems.

If we assume that the previously calculated failure rate has to be equally shared between the different systems, we should guarantee a failure rate, with MA, less than 6 10^{-8} for MaDe and less than 3.8 10^{-4} for FaDu. The equal distribution of the failure rate could be mainly unrealistic for the FaDu event, due to the fact that some of these systems, like Access, have historically really high reliability.

BLMS FOR MAGNET PROTECTION

As reported in [2] and calculated in [3], Beam loss Monitor System have to protect the superconducting quadrupoles against losses of different duration and intensity. The quadrupole locations have been chosen because they are expected to be more loss sensible due to the larger beam dimensions and the limits in physical aperture.

As show in Fig. 2, there is also a strong dependence with the energy and with the loss duration, that brings to a dynamics of 9 orders of magnitude. Note that the Fig.2

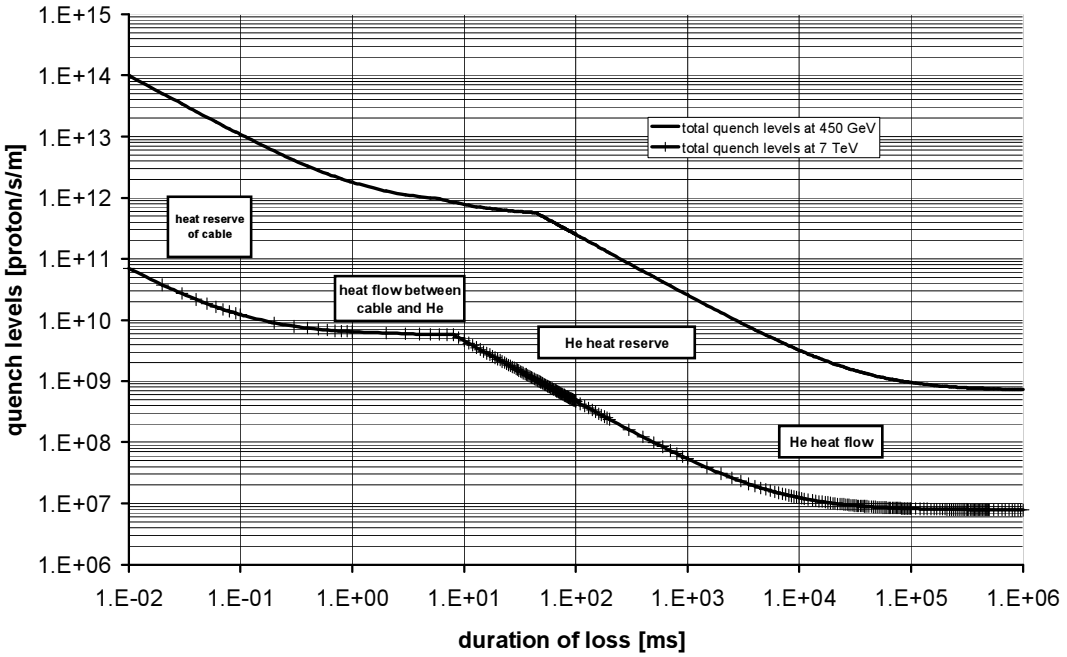

FIGURE 2. Calculated quench level for LHC dipole.

has been calculated for the dipole magnet. Better definition of the levels for the quadrupoles is still on going.

The BLMS is mainly constituted by Ionization Chambers (ICs) around the quadrupole magnets in the LHC tunnel. There will be 6 ICs per quadrupole, in different locations, to cover all the quadrupole, as calculated in [4].These chambers send a current, which ranges from 1 pA to 1 mA, to a Current to Frequency Converter which digitizes the current into pulses. These pulses are then counted by the digital part of the front end electronic. The digital part, hosted in a FPGA, multiplex 8 different channels and several status bits; it doubles the signal and sends it to the surface through 2 optical lines. At the surface the signals are checked and compared, to avoid transmission error, de-multiplexed and then compared with the threshold levels corresponding with the current beam energy. The measured signal, that arrives every 40 μs, is then averaged to compare it with the other threshold levels [5].

RELIABILITY DATA COLLECTION

The failure rates of the different components are calculated using the Military Handbook 217F [6]. The general inputs are: expected ambient temperature of 10°C into the tunnel and 30° at the surface, fixed ground environment (a factor of 2 in the failure rate) for the tunnel, benign ground for the surface (factor 0.5); the average time to substitute a failed unit is 1 hours. Then all the usual component failure rates are evaluated with the military standard. For unusual component we have evaluated the failure rate using historical data from similar components. For example, for the Ionization Chambers we have 140 LHC like chambers installed in SPS which have been operational for 30 years without changing in the chamber sensitivity. It is a

TABLE 7. Summary of the calculated failure rate.

Element	Failure rate λ [10^{-8} 1/h]			Inspection interval [h]	Notes
	Single	Not redundant	Redundant		
IC+cable+terminations	2.5	24		20	Experience SPS
Integrator	2.0			Continuous (40 μs)	Dose and fluence tested
Switch	8.7				
FPGA TX*	200	840	0.014		
Laser	510				
2 Optical connectors	20				
Optical fibre	20				
Photodiode	3.2				
FPGA RX*	70				

general procedure that the upper $\alpha \cdot 100\%$ confidence level of failure rate for a test of t_{tot} hours over N component and F fails after t_i hours is given by

$$comulative\_time = \sum_{i=1}^{F} t_i + (N - F) \cdot t_{tot} \tag{3}$$

$$\lambda = \frac{\chi^2(1-\alpha, 2 \cdot F)}{2 \cdot F \cdot comulative\_time} \tag{4}$$

Assuming F=0 in Eq (3) and F=1, i.e.: 1 failure just after the 30th year, for the Eq (4), we have for IC a failure rate of 2.5 10^{-8}/h. Table 7 summarize some significant figures. From the table we can see that the lasers are the weakest components: this is the reason why we have decided to double the optical line, with the improvements reported in the column "Redundant". The FPGA figures, here, are overestimated with the MIL standard, experimental data will substitute them. The power supply is not considered here, because there are actions on going for their final layout definition.
In the previous table is also reported the inspection interval, this could be continuous, (that means an on line measurement of the functionalities), every operational dump, (roughly every 20 hours), or every year, (IC gas is checked during every shout down with a radioactive source). A frequent inspection interval decreases the probability to find the system not ready when required and so decrease the Magnet Destruction probability.

ANALYSIS

The entire system has been studied with a commercial software (Isograph). A fault tree analysis has been performed, with particular attention to the unavailability of the system (the probability to find the system not ready to act), for the MaDe, and to the failure rate of the system for the FaDu generation. The unavailability of a single BLMS channel, without power supply, is 4.9 10^{-7}/h and it is given for the 55% by failure of the IC, mainly for the reason that it is the least checked component. The single channel failure rate, on the other hand, is around 2.4 10^{-7}/h, 70% given by the switch systems into the CFC. Considering that we have 3200 channels in the system, we have a failure rate of 7.7 10^{-4}. The FaDu number is quite close to the maximum accepted by the MA, after the LHC systems apportionment. In this way BLMS

generates, in 4000 operational hours per years, 3 false dumps. We are trying to reduce this number, which is in any case not so worrying, by improving the switch electronics. For the MaDe further considerations are required. The previously given figure is the unavailability (U_1) of a single channel. For the system, we have to consider the probability that the losses could be seen by just 1 or more channel. It is in fact common experience that a single dangerous loss could affect more than one location around the ring and so more than one channel that could detect the loss. So, if we define N_i to be the number of losses per year that occur in i locations and U_i to be the probability to have i unavailable channels, the system unavailability per year (U_s) is:

$$U_s = \sum U_i \cdot N_i \approx \sum U_1^i \cdot N_i \approx U_1 \cdot N_1 \qquad (5)$$

In fact, the probability that 2 channels (so distant to avoid common failure causes) fails at the same time is U_1 squared, and so on for more channels. In the last step of Eq (5) we neglected the term higher than U_1, due to the fact that U_1 is $<<1$. So the question now is: how many losses, of the 100 initially foreseen, are affecting just one channel? If we suppose that $N_1=100$, we will lose in 4000 hours 0.2 magnets, the maximum MaDe per years. If $N = N_1+N_2 = 5+95$ we will decrease U_s to the FA requirements. To estimate what the loss distribution along the rings is and their correlation, a beam dynamics simulation project is required and it has already been lunched.

CONCLUSIONS

The IEC 61508 standard has been used as a guideline to estimate the failure rate of the Beam Loss Monitor System. Either for the main function failure, the Magnet Destruction, or the system induced failure, False Dump, our current design is on the border of the tolerated risk; further analysis are required to better estimate the LHC loss distribution and correlation. Improved electronics is also in the process of being developed.

REFERENCES

1. *IEC 61508 International Standard*, First edition, 1998-12
2. Jeanneret J.B., Burkhardt H., "Measurement of the Beam Losses in the LHC Rings", *LHC Project Document*, LHC-BLM-ES-0001.00, 2003
3. Jeanneret J.B., Leroy D., Oberli L.,Trenkler T., "Quench Levels and Transient Beam Losses in LHC Magnets*", LHC Project report 44*, 1996
4. .Arauzo Garcia A., Dehning B., "Configuration of the Beam Loss Monitors for the LHC arcs", *LHC Project note 238*, 2000
5. Dehning B., Ferioli G., Friesenbichler W., Gschwendtner E. and Koopman J., "LHC Beam Loss Monitor System Design" in *Beam Instrumentation Workshop-2002*, edited by Gary A. Smith and Thomas Russo., AIP Conference Proceedings 648, New York: American Institute of Physics, 2002, pp. 229-236.
6. Military Handbook, "Reliability Prediction of Electronic Equipment", *MIL-HDBK-217F*, 1991