RELIABILITY ISSUES ON THE LHC BEAM DUMPING SYSTEM

R. Filippini, E. Carlier, B. Goddard, J. Uythoven, CERN, Geneva, Switzerland

Abstract

The Beam Dumping System of the Large Hadron Collider, presently under construction at CERN, must function with utmost reliability to protect the personnel, minimize the risk of severe damage to the machine and avoid undue impact to the environment. The dumping action must be synchronized with the particle free gap and the field of the extraction and dilution elements must be well adjusted to the beam energy. The measures taken to arrive at a reliable and safe system will be described, like the adoption of fault tolerant design principles and other safety related features as comprehensive monitoring, diagnostics and protection facilities. These issues will be discussed in the general framework of the IEC standard recommendations for safety critical systems. Some examples related to the most critical functions will be included.

INTRODUCTION

The LHC [1] Beam Dumping System (LBDS) [2] must always be ready to remove the beams either at the end of a run or in case of anomalies concerning the beam or LHC equipment. It comprises in turn, per ring, 15 horizontally deflecting extraction kicker magnets MKD (the kick gets enhanced by the superconducting quadrupole Q4), 15 vertically deflecting septum magnets MSD, and 10 dilution kicker magnets MKB, followed by several hundred metres of transfer line before the beam reaches the dump TDE.

The requirements for a reliable and loss-free extraction at any beam energy impose tight functional specifications. With regard to the important damage that may occur to the LHC in case of failure, special features such as redundancy, surveillance and post mortem facilities have been included in the system design.

Redundancy is used for the MKD triggering system, which is doubled in the trigger generation and distribution, and for the MKD system in general where the loss of one kicker module out of 15 is tolerable. On-line surveillance detects failures in the magnet power converters, over-pressure and over-temperature in the TDE and erratic triggers of the MKD. Any unsafe condition generates a dump request thus preventing further degradation of the situation. Post mortem facilities perform extended diagnostics after any beam dump to get confirmation on the system's healthy state before the next LHC fill. Passive protection devices are located upstream of the MSD and the Q4 to reduce the consequence of the MKD firing asynchronously with the beam abort gap.

Reliability and safety issues, like those concerning the introduction of the above mentioned measures, are addressed in the IEC61508 standard [3]. It provides a general framework to quantify the safety of a given system, using a risk classification and the notion of SIL (Safety Integrity Levels). In general there is a trade-off to be found between cost and the acceptable risk.

After an analysis of serious possible failure scenarios and system unavailability [4], one failure over 100 years of operation is found to be acceptable for the LBDS. Following the IEC61508 standard a SIL3 corresponding to a failure rate between 10^{-8}/h and 10^{-7}/h is recommended for the critical sub-systems. Among these, the complete failure of the MKDs is deemed catastrophic in terms of downtime and repair cost. The measures taken to obtain a safe system are illustrated in the next example, together with the influence they may have on the LHC operational cycle.

ANALYSIS OF THE MKD SYSTEM

Figure 1 shows a block diagram of the MKD system. Each MKD consists of a magnet and its pulse generator. Each generator is charged according to information delivered by the beam energy meter (BEM), triggered by two power triggers, and continuously monitored by the beam energy tracking system (BET). The generator consists of two identical branches (A and B), each branch including three independently powered circuits with separate capacitor and switch, one for the current pulse (primary) and the others for the overshoot compensation (OS1, OS2). Once the trigger is generated, the capacitors discharge through the switches thus producing the synchronized and energy tuned magnet pulse.

Failure Modes and Coverage

The system is protected against powering and triggering failures as well as erratic triggers by a re-triggering system [5]. Failures of the triggering and the re-triggering system or the BEM are not included in the present analysis.

The loss of one of the 15 MKDs can be due to a magnet failure, an internal triggering failure or an internal powering failure. The internal *triggering failure* is a missed trigger or a switch failure and is covered by redundancy of power triggers, which drive both the generator branches, and by switch redundancy. This permits a capacitor to discharge indifferently through one of the two switches (OS1 and OS2 discharge via the same switch) where it is connect to.

The internal *powering failure* (conservative definition) is the failure of the capacitor in at least one powering circuit (6 per generator) or the failure of at least one power supply (3 per generator). Any powering failures are caught by the surveillance system and the operation is aborted (fail safe mode).

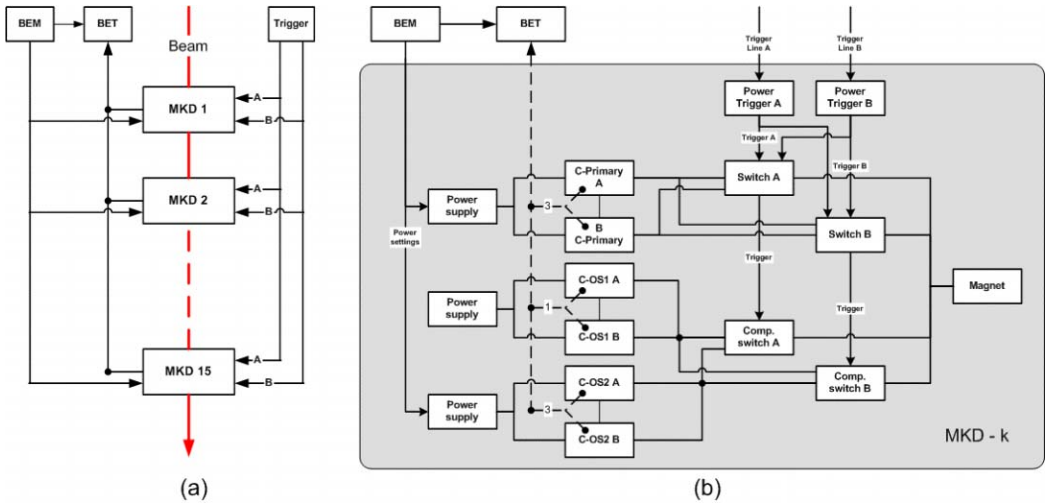

Figure 1: Global MKD system (a) and functional block diagram of a MKD (b).

The surveillance consists of many data acquisition channels going to the BET where they are compared with the BEM signal [5]. A *channel* is the series of a voltage divider, an ADC converter, a transmission and a reception unit. There are 3 channels for the primary capacitors, 3 for the OS2 capacitors and one shared by the two OS1 capacitors, namely 7 channels per MKD, 105 in total. As no voting at the BET is foreseen, then 6 + 3 monitored components plus 7 channels per MKD results in 135 + 105 independent failure processes, which can be at the origin of an internal dump request.

After a pulse, the post mortem checks the current of all the magnets deducing information on the status of each generator. This operation takes a few seconds and if the result is OK, the system will again allow injection in the LHC.

System Modelling and Analysis

The system description can be arranged into a compact four states model (Figure 2): X0) the MKD system is available, X1) the MKD system is available and BET failed, X2) the MKD system has failed safe and X3) the MKD system has failed unsafe. Four transitions drive the states changes: T01) failure of the BET, T02) internal dump request, T03) internal triggering failure or magnet failure and T13) any system failure mode. The expressions of transition rates are deduced from the failure modes description.

At time t the system can be found in one of the four states. Safety is the probability S(t) that the system is 1) in the state X0 or X1 and the operation has been regularly concluded or 2) in X2 and the operation has been aborted.

Calculations were made under the following assumptions:

(A1). The channels going to the BET are identical and fail always safe (dump request).

(A2). Failure rates of components are assumed constant (Table 1).

(A3). The LHC operation duration (the mission) is 10h.

(A4). After the post mortem the system is restored to its initial conditions.

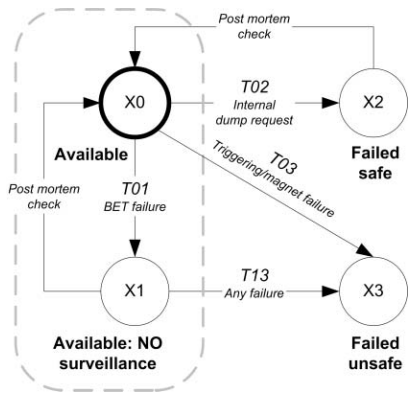

Figure 2: MKD state transition diagram.

The system analysis requires the solution of a not time-homogeneous Markov chain [6] with initial state probability vector $P\{\underline{x}(0)\}=[1,0,0,0]$. The probability to fail unsafe 1–S(t) is almost 1×10^{-8} per mission of 10h or 4.2×10^{-6} per year (assuming 200 days of 400 missions). This means a failure rate of 10^{-9}/h, hence largely SIL3. It is important to remark that: 1) without post mortem the probability to fail unsafe would be 0.8×10^{-3} per year, 2) without redundancy in the MKD generators it would be 4×10^{-3} per year and 3) without surveillance would be 5.4×10^{-3} per year (Figure 3).

The achieved risk reduction is traded off with the number of internal dump requests (i.e. mission aborts) per year, which is a binomially distributed random variable. Two curves, respectively for the failure rate settings (1) and (2) of Table 1, are shown in Figure 4. One order of magnitude more in the capacitors failure rate generates 6 instead of 2 mission aborts (average values), while safety remains almost the same.

The contribution of the channels should be a small percentage of the total. In the analysed cases, the channels

bring almost 0.5 mission aborts per year, per MKD (25% the total for the (1) setting), which is acceptable.

This example demonstrates the importance of dimensioning surveillance with respect to the required risk reduction that could lead to an unacceptable number of mission aborts, depending on the reliability of the monitored components.

Table 1: Assumed components failure rates

Components	**Failure rates/h**
Primary and compensation capacitors	$1x10^{-6}$ (1), $1x10^{-5}$(2)
Power triggers, primary and compensation switches	$1x10^{-5}$
Power supplies	$1x10^{-5}$
Magnet	$1x10^{-6}$
Channels	$1x10^{-6}$
BET	$1x10^{-8}$

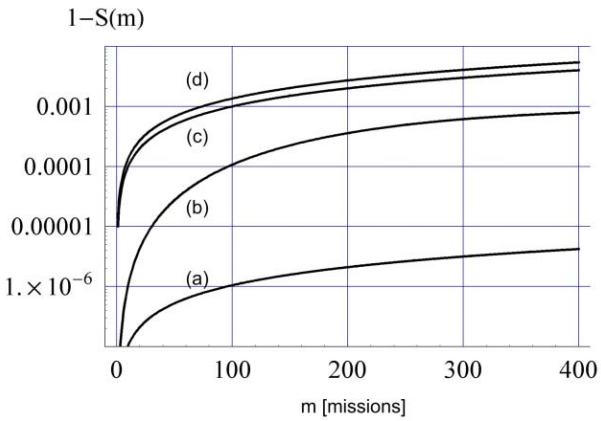

Figure 3: Probability of MKD system failure over one year of LHC operations (setting (1), Table 1): default case (a), no post mortem (b), no generator redundancy (c), no surveillance (d).

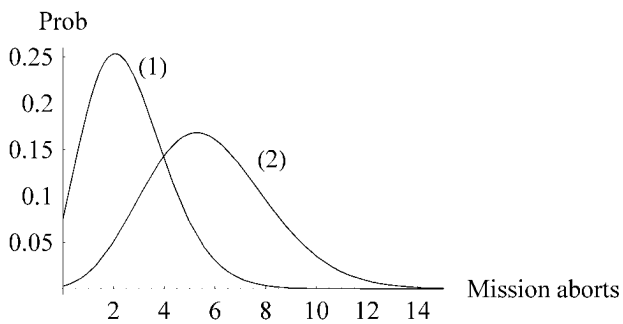

Figure 4: Distribution of mission aborts over one year. (1) and (2) refer to failure rates of Table 1.

CONCLUSIONS

This study illustrates that it is possible, through the introduction of safety measures and fault tolerant design, to obtain a safe MKD system, corresponding to SIL3, without penalizing its availability for physics runs. Redundancy and surveillance reduce the probability of system failure during an LHC operation. Similar results are expected for the other LBDS or LHC systems adopting analogous high protection measures. Finding the balance between risk reduction and machine availability, here related to the percentage of mission aborts, is a major issue for the machine protection system in general [7].

Comprehensive post mortem analysis helps to ensure that the LBDS is healthy before the next machine fill. In terms of reliability studies this last assumption implies that the system never ages, which is obviously untrue. For example, components wearing due to the fast and intense discharge, though difficult to foresee, could become a critical factor for MKD reliability and might necessitate periodic maintenance as additional safety measure. The benefit of this is currently being studied in more detail.

ACKNOWLEDGEMENTS

The authors would like to thank the colleagues of the AB-BT and the machine protection working group.

REFERENCES

[1] P. Lebrun, “Industrial Technology for Unprecedented Energy and Luminosity: the Large Hadron Collider”, EPAC04, Lucerne, July 2004.

[2] B. Goddard, M. Gyr, J. Uythoven, R. Veness, W. Weterings, “LHC Beam Dumping System: Extraction Channel Layout and Acceptance”, PAC03, Portland, May 2003.

[3] International Electrotechnical Commission, “Functional Safety of Electrical-Electronic-Programmable Electronic Safety Related Systems” IEC 61508 International standard, Geneva, 1998.

[4] J. Uythoven, R. Filippini, B. Goddard, V. Kain, R. Schmidt, J. Wenninger, “Possible Causes and Consequences of Serious Failures of the LHC Machine Protection System”, EPAC04, Lucerne, July 2004.

[5] E. Carlier, et al. “Design Aspects Related to the Reliability of the Control Architecture of the LHC Beam Dump Kicker System” ICALEPS’03, Gyeongju, October 2003.

[6] K.S. Trivedi, “Probability and Statistics with Reliability Queuing and Computer Science Applications”, Prentice-Hall, New York 1982, p. 360-362.

[7] R. Schmidt, J. Wenninger, “Machine Protection Issues and Strategies for the LHC”, EPAC04, Lucerne, July 2004.