RELIABILITY ANALYSIS OF THE LHC MACHINE PROTECTION SYSTEM: TERMINOLOGY AND METHODOLOGY

S. Wagner, Laboratory for Safety Analysis, ETH Zurich, Zurich, Switzerland
R. Schmidt, J. Wenninger, CERN, Geneva, Switzerland

Abstract

The LHC Machine Protection System (MPS) ensures machine safety by performing a beam dump (or inhibiting beam injection) in case of non-nominal machine conditions, thus preventing machine damage. The trade-off between machine safety and beam availability is one of the main issues related to the LHC MPS. For a global analysis of the entire MPS, a generic methodology is being developed. In order to keep the related model and simulations traceable, a terminology frame is being compiled which clarifies and specifies the basic terms and their interrelations. This paper provides the most relevant terminology. Furthermore, it presents latest features included in the model.

INTRODUCTION

The trade-off analysis of the MPS involves basic terms like *safety*, *reliability* and *availability*. Besides, it must take into account common design principles such as *redundancy*, *fault tolerance*, *fail-safe* and *self-monitoring*. These terms and in particular their interrelations easily cause confusion, while for the traceability of the analysis a consistent understanding of the underlying terminology is essential. The first part of the paper therefore specifies the most relevant terms and their interrelations.

The methodology has already been introduced [1], discussing its initial model, which includes almost 5000 MPS components being modelled as individual objects, and the simulations based on Monte Carlo method. The development of the methodology since has been focusing on further model adaptation to the real MPS specifications. The adapted model allows addressing the impact of masking components on machine safety, which is presented with a case study in the second part of the paper.

TERMINOLOGY

The presented frame bases upon standard definitions. Although it is specified to the LHC MPS and its analysis, it is adaptable to any kind of accelerator.

General

From a reliability analysis point of view, it is helpful to divide the LHC systems into three functional groups, which are hereafter referred to as *machine*, *detectors* and *MPS*. The machine includes all LHC components and systems that represent the basic equipment needed for the LHC function, i.e. providing colliding beams. The beams are regarded as part of the machine. The detectors cover the equipment for gathering data tracing the collision of the beams. The MPS spans the components and systems that, while not being directly involved in the machine function, ensure machine safety. *Machine safety* implies machine operation under nominal conditions. In case of non-nominal conditions, the MPS performs a dump (*emergency dump*), i.e. the extraction of the beams from the LHC ring into so-called dump blocks, which absorb the beams. Without MPS intervention, non-nominal operation conditions lead to machine damage.

This paper focuses on machine and MPS, the detectors are not within the scope. However, their inclusion to the frame is straightforward.

MPS Reliability, Machine Safety and Beam Availability

Reliability refers to the ability 'to perform a required function under given conditions for a given time interval' [2]. For the MPS, the required function is the performing of emergency dumps in case of non-nominal conditions, the related time interval starting at beam injection. With regard to that function, the MPS can fail in two ways, 1) missing an emergency dump or 2) performing a dump at nominal conditions (*false dump*). While both affect beam availability, only the former involves compromised machine safety thus leading to machine damage.

Availability refers to the ability 'to be in a state to perform a required function (…) at a given instant of time (…)' [2], depending on the combined aspects of reliability and maintenance. Following [3], an available system finds itself in an up-state as opposed to a down-state. *Beam availability* in the context of this paper relates to the presence of colliding beams.

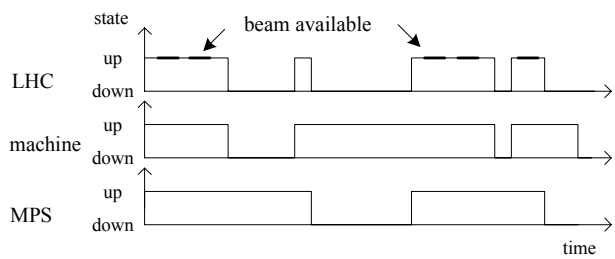

Figure 1: Dependence of beam availability on machine and MPS availability

Figure 1 illustrates the dependence of the beam availability (as part of the overall LHC availability) on the availability of the machine and MPS. Their up-state corresponds to their finding themselves at a point of the nominal operational cycle. Downtime names the time beyond nominal cycles, i.e. where operation is interrupted due to repair or other measures to restore nominal operation conditions. The downtime of the machine and MPS sums up to the overall LHC downtime. Following

this scheme, an availability of 100% is achieved by one nominal cycle following another. This ideal case also defines the denominator for beam availability as the sum of LHC uptime with beams available. By contrast, the total time is useful as denominator for comparison of different nominal cycles of an accelerator or of the performances of different accelerators of the same kind.

It is to be noted that the presented scheme does not cover machine safety. The up-states only relate to operation. Machine safety depends on the condition of the MPS during operation. It is compromised by MPS components that are in a blind state.

Machine Operation

A nominal machine operation cycle is illustrated in Figure 2 [4]. A cycle (and mission) starts with the injection of two pre-accelerated beams to the machine. During the following phase, the field of the dipole magnets is ramped up, leading to top particle energy. At top energy, the beams collide and the detectors take data. After this *physics* phase, which lasts for about 10 hours, the mission is ended by a scheduled dump (*end-of-mission dump*). The magnets are ramped down and the machine is prepared for a new cycle. While *cycle* names the time period between two injections, *mission* covers the time between injection and beam dump, i.e. the time where there are beams in the machine. The analysis assumes a nominal cycle of 12 hours.

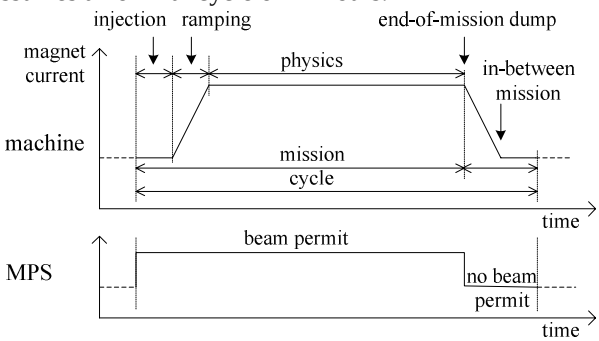

Figure 2: Nominal operation cycle of machine and MPS, ‘physics’ corresponds to ‘beam available’ in Figure 1

In case of non-nominal beam or machine equipment conditions, a mission is ended early by an emergency dump performed by the MPS. Non-nominal conditions entail the risk of machine damage or downtime. While damage, besides costs for repair always includes downtime, downtime does not necessarily imply damage.

One of the most common non-nominal machine conditions is the quench of a superconducting magnet. *Quench* refers to the unwanted local transition from superconducting to normal conducting, which without intervention of the MPS leads to damage to the magnet. The replacement of the damaged magnet takes about one month of downtime. If damage is prevented through the intervention of the MPS, the cooling of the related magnet down to nominal range still results in a downtime of 1-8 hours. Besides, each quench implicates a wearout. Quenches therefore should be avoided.

MPS Operation

The presence of beams in the machine conditions MPS *beam permit* status, indicating that it is ready and no non-nominal machine conditions are detected. In case of a nominal machine and MPS cycle (Fig. 2), beam permit is granted for beam injection and maintained until the end-of-mission dump is triggered in the control room, which involves the withdrawal of the MPS beam permit leading to the dump. After successful testing and diagnostics, beam permit is provided for the next cycle to begin.

Failures in the MPS can be grouped into three main categories, 1) undetected failures that leave a component in an inoperable state (*blind failures*), 2) failures that generate a dump request signal and 3) failures that generate a warning.

Blind failures (leaving the component in a *blind* state) compromise machine safety. On the MPS component level, they prevent the treatment and transmission of an incoming dump request signal. On the global system level, the concurrence of non-nominal machine conditions and blind MPS components can result in a missed emergency dump. The MPS design features a wide range of redundancy to avoid this scenario. *Redundancy* is defined as the existence of more technical means than necessary for the required function [5] and is one of the design principles rendering a system *fault tolerant*, i.e. able to continue functioning (‘service’) despite a (‘hardware or a software’) failure [6].

Failures generating dump request signals base upon the *fail-safe* principle. Following that principle, such failures trigger a dump (*false dump*), thus passing the machine into a safe state [7]. The generation of the related dump request signals emerges either directly from inherent fail-safe design or indirectly from extra *self-monitoring* features. Monitoring means activity intended to observe the actual state of a component (‘item’), usually carried out during operation (‘in the operating state’) [2], in order to detect failures. These failures and the related beam dumps compromise beam availability.

The third category includes failures that, unlike the failures leading to false dumps, are considered as not critical with regard to the MPS functionality and machine safety respectively. Their detection leads to a warning, as a hint for the maintenance measures after a beam dump. Failed components are detected after a dump by diagnostics and testing. The time for their repair may contribute to LHC downtime (if it cannot be done in the shadow of other repair or in-between-mission activities).

METHODOLOGY

Based on the initial model [1], adaptations have been made with regard to the system demand (reflecting the beam loss pattern) and the ionisation chamber (IC) state diagram. These adaptations underlie the case study on the impact of masking ICs on machine safety. The key model assumptions [1], in particular the independence of failures (excluding internally and externally induced common cause failures) still apply.

System Demand

The adapted system demand differs from the initial model in the following parameters:

- covering the entire LHC
- involving ICs of up to ten magnets at the same time
- IC weighting according to its position at the magnet
- Mean Time To Failure ($MTTF^{beamLoss}$) of 33 hours

The $MTTF^{beamLoss}$ value bases upon experience with HERA at DESY [8], while the weighting of ICs approximates the expected beam loss pattern in the LHC magnets [Dehning, pers. comm.].

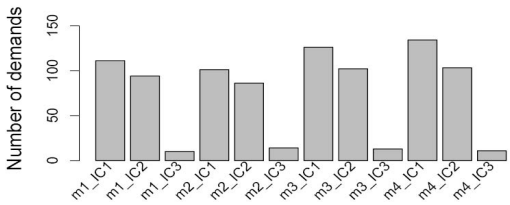

Figure 3: Demand pattern on the ICs of four magnets

Figure 3 illustrates the resulting demand pattern in the simulations, on the basis of four magnets with three ICs each (one beam). It shows the frequency of ICs involved in system demand, with a weighting on the first and second IC (downstream).

Case Study on Masking ICs

The masking of components or parts of the MPS is a measure to reduce the number of early ended missions in case of numerous false dumps. Masking is included to the model by adding a new state (*masked* state) to the component state diagrams [1]. It corresponds to the blind state except for being set at the start of each mission simulation instead of upon a failure.

Figure 4 shows the results of simulating 100,000 missions with two-thirds of the ICs being masked, namely of each magnet the second and third IC for each beam.

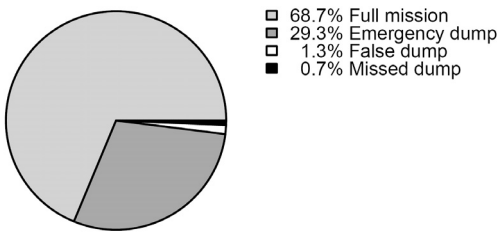

Figure 4: Fraction of early ended missions (due to emergency and false dumps) and missed dumps

In total, 68,750 missions are completed, representing an estimated LHC reliability of 68.7 % (relative to a 12-hour cycle) [3]. Reliability is restrained by 30,590 early ended missions, of which 29,263 as a result of emergency dump and 1327 or 1.3% due to false dump. Machine safety is compromised by 660 missed dumps. They are all due to masked or blind ICs, thus representing missed emergency dumps. The missed dumps are underlain by 128,942 missed dump requests, which are defined by a dump request meeting a blind component [1]. By contrast, a corresponding simulation without masking shows no missed dump and only two missed dump requests in components. The model feature allows figuring out optimal masking modes, which don't compromise safety.

CONCLUSIONS

The paper presents the terminological frame underlying the reliability analysis of the MPS. The frame specifies the most relevant terms and their interrelations, thus contributing to the traceability of the related methodology. The new model feature of masking components is presented with a case study on the impact of masking two-thirds of the ICs on machine safety. Its results have been illustrated and discussed and have again shown the feasibility and potential of the methodology. The inclusion of both machine reliability (represented by a weighted demand pattern) and MPS reliability (defined by failures generating dump requests and by blind failures) makes up for the major advantage of the methodology. The masking feature provides a means for comparing different system configurations with respect to the balancing of machine safety and beam availability.

The further development of the methodology includes common cause failures (e.g. wrong beam energy signal), whose implementation is similar to the masking feature. The expansion of the model to the Beam Dumping System is currently being worked on, as well as a rare event approach.

REFERENCES

[1] Wagner, S., et al. (2008), "Balancing Safety and Availability for an Electronic Protection System", in European Safety and Reliability Conference 2008 (ESREL 2008), Valencia, Spain (accepted)

[2] EN13306 (2001), "Begriffe der Instandhaltung", Beuth: Berlin

[3] EN61703 (2002), „Mathematische Ausdrücke für Begriffe der Funktionsfähigkeit, Verfügbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft", Beuth: Berlin

[4] Schmidt, R., et al. (2006), „Protection of the CERN Large Hadron Collider", New Journal of Physics 8, 290. 31p.

[5] VDI4001 (1986), "Begriffsbestimmungen zum Gebrauch des VDI-Handbuches Technische Zuverlässigkeit", Blatt 2, VDI: Düsseldorf

[6] TCSC (2008), IEEE Technical Committee on Scalable Computing, http://www.ieeetcsc.org

[7] Birolini, A. (2007), "Reliability Engineering Theory and Practice", 5th ed., Springer: Berlin Heidelberg New York

[8] Wittenburg, K. (2004), "Beam Loss & Machine Protection, 33rd ICFA Advanced Beam Dynamics Workshop on High Intensity & High Brightness Hadron Beams, Bensheim, Germany