Operation's point of view on handling Machine Protection issues

G. Papotti
CERN, Geneva, Switzerland

Abstract

LHC Machine Protection has worked extremely well in these first years of LHC operation, but in a few isolated cases issues presented themselves. Failures like design faults, software bugs or manual mistakes pointed out weaknesses in the protection mechanisms. This paper recalls a number of these issues, as experienced by operations, highlighting which follow-up actions were devised and identifying which actions might still be missing (e.g. new interlocks or new procedures).

INTRODUCTION

It is widely recognized that the LHC Machine Protection (MP) dependability has been excellent during operation in the years 2009–2013 [1] and only a few cases over the years can be defined as MP issues.

In MP issues, MP systems do not respond as foreseen and this could result in the machine being in an unsafe state. The exceptionality of these situations arises from them not having been thought of before, or them being a first occurrence, and is exacerbated by the fact that the next steps might be unclear and procedures might be missing. As a result, the actions to be taken are often left to the shift crew's experience, feeling or intuition. While in some occasions time to think might be available, in others it is imperative to act promptly.

After a short discussion on MP redundancy and combined system failures, in this paper we recall the main examples of these issues or failures and separate them into categories: failures that only experts can detect; failures that shift crews can detect, after beam dumps or with beam still in; dumps that could have been avoided. We also highlight measures that were put in place to solve them, or are possibly still missing (e.g. interlocks or procedures). Some open questions and conclusions close the paper. The failure examples discussed here are taken from the 2012 operational period, unless otherwise noted.

FAILURES AND REDUNDANCY

It is important to point out that the failure of a single system is generally not an issue as MP has abundant built-in redundancy. E.g. cases of "late" interlocks from magnet powering (i.e. through the Power Interlock Controller, PIC) were safely caught by the detection of beam losses by the Beam Loss Monitors (BLMs). This happened a few times over 2012, e.g.: for power converter faults in the inner triplet, for the LHCb dipole, for 60 A orbit correctors. More generally, the BLM and the Quench Protection Systems (QPS) are considered to be the "last line of defence" of MP as failures in other systems are eventually caught by beam losses or at the time of magnet quenches. Note also that the BLM system is redundant in itself, having three detectors per main quadrupole. Furthermore most failure cases will produce observable beam losses in several locations around the LHC ring.

Combined failures, instead, are a main worry. The typical example is an asynchronous beam dump happening while certain collimators are not in the desired position. In this case, that fortunately has not been experienced so far, the combined failures of the beam dump and of the collimation systems put the machine in an unsafe state and the protection of the hardware is not guaranteed, possibly resulting in magnet quenches or more important damage. As a general rule, if weaknesses are detected in one system, the beams should be immediately removed to allow for the necessary repairs before a second failure occurs which could expose the machine to serious damage. Unfortunately there are a few cases in which dumping might not be the best solution, namely when the dump could be dangerous in itself (e.g. impaired dump protection due to TCDQ with reduced efficiency or subject to overload, i.e. due to bad orbit at point 6 or too many particles in the abort gap).

FAILURES THAT ONLY EXPERTS CAN DETECT

Major events belong to this category, e.g. design faults and wrong reference settings in a MP system. In these cases the system expert detected the problem, often required the stop of beam operation to fix it, and decided when it was safe to restart. Little is in the hands of the operation shift crews as these faults could not have been detected by others than the experts themselves.

Examples are: the 12 V power supply failure that would have resulted in preventing the beam dump to fire; wrong settings defined for the transfer line collimators when shifting from SPS Q20 to Q26 optics and for ring collimators defined at the commissioning phase in the beginning of the year; the interrupted BLM High Voltage (HV) cable that would have prevented the BLMs from triggering the dump on heavy losses (2011, covered since by a Software Interlock).

FAILURES THAT SHIFT CREWS CAN DETECT, AFTER DUMP

Anomalous situations that led to the beam dump belong to this section. The shift crew might be able to identify them for example based on a careful analysis of the

Post Mortem data. E.g. during a physics fill, an internal trip of the Inner Triplet power converters (RTQX2.L2) was caught by beam losses due to a drift in orbit, while the PIC interlock came after the beam had already been dumped ($\approx$70 ms later). In this example one layer of MP redundancy was bypassed as the beam perceived the orbit perturbation caused by the Power Converter (PC) trip. The shift crew promptly informed the MP experts and the PC experts, and waited for their approval before resuming operations. The event was then followed up at the Machine Protection Panel and it was decided to reduce the over current protection thresholds of the PC [2].

A few other examples happened at injection energy: Injection Kicker (MKI) flashovers; lack of SPS-LHC synchronization due to the SPS being on local frequency or timing issues at the first Batch Compression, bunch Merging and Splitting (BCMS) tests (while SPS beam was extracted in TI2 the injection kicker MKI8 was pulsed). Already in 2010 it was pointed out that: "Beam dumps above injection are rigorously analyzed, we can do better at injection, avoiding repetitive trials without identifying the cause" [3].

For events that belong to this category (i.e. with the beam being dumped), the machine is in a safe state. However, the machine might have been in an unsafe state prior to the dump. Because of this, and in order to verify that the anomaly does not get repeated, the shift crews or often the system expert need to verify the correct behaviour of the systems and possibly take action to improve it.

Software tools can help the shift crew to spot these anomalous situations. Some of these checks are already included in the PM expert acknowledge (e.g. FMCM, PIC and BIC Internal Post Operational Checks (IPOCs)), but more checks can be added to the PM analysis frame: e.g. verification of collimation hierarchy, use of the power loss module to identify losses that are higher than normal.

FAILURES THAT SHIFT CREWS CAN DETECT, WITH BEAM STILL IN

In this case the system failure did not lead to a beam dump, resulting in a situation with the beam still in the machine but with at least one MP system that is impaired or partly impaired. At that point, it is up to the shift crew to judge and possibly decide to dump the beam manually if deemed necessary. In many occasions, after the first occurrence of such failure, an appropriate interlock was put in place so to increase protection. Examples are:

- during a physics fill, an RF feedback crate went down impairing the control of the whole RF line; taking into account that similar situations are interlocked and dump the beam to avoid putting excessive load on the collector, the shift crew dumped manually in agreement with the RF piquet; this event possibly highlighted a configuration to be added to the RF interlock connections to the Beam Interlock System (BIS);

- at a start of the energy ramp, all Beam Position Monitor (BPM) readings became unavailable, which meant no control or measurement on the beam orbit and no real-time corrections to it; the shift crew tried rebooting a few crates and then promptly dumped after realizing that the situation could not be recovered in a short time; such lack of BPM readings is now covered by a Software Interlock System (SIS);

- the tertiary collimators (TCTs) in point 2 did not respond to the timing event at the start of the collision beam process for a physics fill; consequently, at the end of the beam process, the orbit had changed but the collimators had the wrong centre (despite having the correct gap between the jaws); the state machine change to "Stable Beams" would have been prevented, but there is no interlock that dumps the beams automatically in such case (note that the LHC was not properly protected if an asynchronous beam dump had happened then); the suggested recipe in similar cases is to dump as soon as possible, as long as there is no strange orbit excursion in point 6; future improvements may come through the use of TCTs with integrated BPMs.

For failures in this category, the shift crew is faced with the choice of dumping manually or not: on the one hand there is cautiousness and MP, on the other hand there is operational efficiency (which gets degraded in case the situation could have been recovered by other means). In either case the support of both the machine and physics coordination would be appreciated. It is important, especially in the context of the restart after the first long shutdown, to define clear guidelines to alleviate the crews' choices during shifts.

It is also worth stressing that the time criticality of the manual dump changes from case to case: in the case of the RF collector heating for example the rapidity in the response is less important than in the case of missing BPM data during the ramp.

In fact, many interlocks are built on the experience from previously encountered situations and provide both a timely response and a coherent action across the shift crews. It should not be forgotten that at times, manual checks and dumps became the short term procedure: examples are the TCDQ not moving during a ramp in 2010 and the abort gap monitoring that was missing due to the BSRT mirror failure in 2012. The SIS provides the flexibility to add new interlocked conditions on very short notice and cover holes in the MP found once in the past (e.g. BLM HV verification missing interlock condition), software bugs (e.g. zeroed orbit feedback references during the squeeze), operational mistakes (e.g. incorrect settings on the main quadrupoles at injection in 2010).

Given these observations it is also unlikely that all failure scenarios have happened already. For this reason shift crews should be vigilant about unusual situations. Software

tools can be designed to help the crews, e.g. BLM "reference" readings per beam mode.

DUMPS THAT COULD HAVE BEEN AVOIDED

This category collects all the cases in which the machine safety was not in danger, but the impact was rather on machine efficiency as the beam was unnecessarily dumped. Some examples are: a beam dump due to orbit excursion while setting up $6\,\sigma$ Van der Meer scans in the 1.38 GeV/c run; a dump at the transition of the Setup Beam Flag (SBF) from true to false (intensity surpassed $5 \cdot 10^{11}$ppb) as a masked interlock from the collimators was active (the TCTs were at coarse settings for collisions at injection); the dumps from the interlocked BPMs in point 6 due to reflections or low intensity bunches, especially during the proton-lead runs in 2013.

Many of these dumps could have been avoided had the procedures been prepared more thoroughly. This is especially true for special runs and Machine Developments (MDs), in which the machine operates in a different regime for a short period of time, and at the transition from these special regimes back into physics operation.

The masking in the BIS is automatically not taken into account when the beam intensity is above the SBF threshold. In this sense, masks that are set, but should not be, impair efficiency more than safety. A task that clears all masks during the preparation for injection sequence (to be run in the shadow of the magnet rampdown) will mediate this problem.

Some masks in the SIS are also dependent on the SBF and some others are non-maskable, but there are also many for which more flexibility is allowed. Forgetting to set appropriate masks or interlock settings has sometimes impaired the efficiency for special runs and MDs (e.g. orbit references for 90 m optics runs), as most are tweaked around nominal physics operation. Forgetting to unmask at the end of the special runs, i.e. when going back to nominal physics operation, has an impact on safety.

One straightforward solution is the preparation of very thorough procedures for special runs and MDs, including detailed step-by-step plans, settings change list, masks list. This helps to achieve results and to improve efficiency. The preparation of the document itself even helps to avoid misunderstandings within the teams. The document can be circulated beforehand to the shift crews for information and helps to minimize surprises and the need to adapt the plans during machine time. The impact is also positive on the definition of responsibilities and the document can function as a checklist to remember all reversions to be carried out at the end of the special run. In this frame, the request for a written MP document for MDs of type C and D (which foresee changes to MP systems and non-negligible intensity beams) will be extended to require at least a detailed plan for all MDs, to be handed in a few weeks before the MD is scheduled to take place.

Successful examples of MD document preparation are the ones for the quench tests carried out in February 2013. These documents were handed in well in advance allowing proper discussion and comments by all the experts involved. Even then, the documents could have been even more thorough and include e.g. masking the SIS TCSG/TCDQ retraction interlock that has caused the unnecessary loss of a fill.

It is worth recalling that also settings for other MP systems should be verified regularly, e.g. interlocked BPMs in point 6, BLM Monitoring Factors (which is already carried out by the experts on a weekly basis).

MISCELLANEA

Interlocks that latch or are masked too often loose effectiveness. It is important to define clearly what is really critical and what is not, to avoid the risk of overlooking or ignoring what should not be. In this perspective, the philosophy of the Injection Quality Check (IQC) latches should be revised [4].

The beam dump external Post Operational Checks (LBDS XPOC, see also [5]) is divided into several individual modules, the results of which can fail independently. Only experts can reset the critical modules (e.g. concerning dump kicker waveforms or synchronization units), while shift crews can only reset non-critical modules (e.g. latches from filling pattern, missing intensity or BLM data). At present, latches on non-critical modules are abundant (also due to weaknesses in other systems), but this mainly affects efficiency, rather than safety.

Concerning dumps coming from magnet protection (i.e. QPS and MP3), the answer that the shift crew gets from the on-call service often sounds like: "I am not sure why the QPS triggered, but the magnet protection worked as it should have: so you can carry on with operation, and the analysis will follow offline". This is "safe" even though it does not satisfy the shift crew's curiosity. Finally, it has to be recalled that operation was always stopped when needed. One representative example, is the case of impaired redundancy which was revealed by the coexistence of a bad temperature sensor and a bad cabling of a QPS detection board. As a result a Distribution Feed Box (DFB) High Temperature Superconductor (HTS) was protected only by the other QPS board (which was correctly connected). With two redundant protection systems defunct out of three, no redundancy was left in the quench protection of the DFB HTS (2011).

OPEN QUESTIONS

As stated earlier, not all unforeseen failures have happened yet and some time should be invested in devising other procedures for possible failures, before they are actually needed on shift. For example it might be useful to develop further on the cases where it is better not to dump, e.g. in the unlikely case in which the orbit is out

of tolerance in point 6 or when the abort gap population is well above dump thresholds and keeps on increasing. A procedure is in place for high abort gap population [6], but it might be useful to include more details coming from the experience gained in 2012 (e.g. on transverse damper blow-up settings).

Another point concerns the confidence of the shift crews in executing the existing emergency procedures, it might be beneficial training them.

CONCLUSIONS

Machine Protection has worked remarkably well in these past few years of LHC operation and this success is the base for the success of the LHC. A catalogue of MP issues from 3 years of operation was presented though: cases of missing interlocks, design faults, weaknesses. The experience so far has helped to strengthen MP, but the long shutdown gives us the pause for thought to learn further from previous mistakes.

Shift crews can spot abnormal situations and act in case of need, but they should be assisted as often as possible with software and procedures so to align the decisions in stressful situations, and more importantly to shorten the decision time there where the human reaction time becomes too long for many beam-related failure scenarios.

ACKNOWLEDGEMENTS

The author would like to acknowledge the fruitful discussions with M. Albert, D. Jacquet, L. Ponce, D. Wollmann, J. Wenninger and M. Zerlauth that enriched the preparation of these proceedings.

REFERENCES

[1] B. Todd, A. Apollonio, S. Gunther, D. Wollmann, M. Zerlauth, “Machine Protection System Availability and Performance 2010-12”, these proceedings.

[2] I. Romera, Minutes of the 63rd Meeting of the Machine Protection Panel, 22 June 2012.

[3] M. Zerlauth, “Do we understand everything about MP system response?”, LHC Beam Operation Workshop, Evian 2010.

[4] D. Jacquet, “What we want”, LHC Beam Operation Workshop, Evian 2012.

[5] N. Magnin, “LBDS kickers”, these proceedings.

[6] E. Gianfelice-Wendt, B. Goddard, V. Kain, M. Meddahi, J. Uythoven, “Procedures for abort gap cleaning at full energy”, EDMS Id 1204352.