Report from the LHC Machine Protection Review
May 10th, 2005

J.Annala (FNAL), R.Bacher (DESY), R.Bailey (CERN), V.Dang (PSI), D.Forkel-Wirt (CERN), G.Ganetis (BNL), M.Harrison (BNL-Chair), M.Ross (SLAC), C.Sibley (SNS)

This report is the outcome of a review of the LHC Machine Protection System that took place at CERN during April 11-13th 2005. The charge to the Committee was embodied in a series of questions. The answers to these questions form the main body of this report. Some short comments on various items are also included.

Summary

The Committee found that the fundamental strategy adopted for the Machine Protection System (MPS) was sound and represented a reasonable extension from existing systems used on currently operating accelerators. The LHC design luminosity will require a stored beam energy of more than two orders of magnitude beyond that of present day machines and this fact has necessitated a more complex system using dynamic configuration within various machine states.

The configuration management task of handling this complexity in an operational environment was the Committee's highest concern; it poses the largest risk of significant machine damage. Ensuring the fidelity of the system at all times will prove a significant challenge. Possible scenarios involving the loss of the complete circulating beam appear remote but all seem to involve a few critical aspects of the dump kicker system in some way. We suggest consideration be given for back-up capabilities in these areas.

The front-end hardware and associated interface design were found to be quite mature. The Committee was less convinced by the software status. The application software will be a highly complex package and is in a much less well-developed state than the hardware at this time.

A comprehensive post mortem data acquisition capability after a beam dump is crucial in ensuring efficient operations. The Committee suggests that the various sub-system post mortem requirements should be defined centrally rather than determined *ad hoc* as seems to be happening at present.

The machine availability will probably be determined by component failure (power converters) during initial operations rather than erroneous status reported by the MPS system itself. The Committee feels that the main risk for beam operation appears to involve achieving design luminosity rather than merely operating with beam. A beam loss rejection rate of 10^{-4} required from the collimation system has not been achieved at any other facility. The safe beam concept (pilot pulses) and the comprehensive injection protection scheme are noteworthy aspects of the MPS design

Do you consider the overall strategy for the machine protection adequate ?

The Committee feels that the fundamental strategy is sound. The basic approach relies on: a failsafe link with redundancy, a safe beam logical state incorporating the systematic use of a pilot pulse, dynamically configurable machine states, a machine aperture defined by collimators, and a comprehensive series of inputs from the various machine sub-systems. We also found the measures adopted to address the special problems associated with injection to be well thought out.

The LHC machine protection system represents a reasonable extension of similar systems from the other existing facilities. The Committee notes that the 360MJ of stored energy at design luminosity is more than two orders of magnitude greater than current machines and results in correspondingly more complex machine protection requirements and implementations.

And what could be the main risks ?

The Committee considers that configuration control represents the main risk to compromising the operation of the machine protection system. The complex logic involved with the state changes associated with the beam intensity and energy affecting such factors as variable loss threshold levels, dynamic input masking, and other parts of the system allow for many potential error scenarios. The numerous input channels also provide many opportunities for mistakes.

Configuration control will be needed to cover essentially all aspects of the machine protection system. The hardware side of the system should be protected by a suitable configuration layer from clear labeling of MPS signal cables and equipment, to access control over the cabinets housing MPS hardware. During the installation and testing phase inputs will most likely be bypassed to perform subsystem tests until all components are in place for full system testing. These should be tracked and verified that bypasses are removed before a handover for beam commissioning.

At the hardware / software interface there will be many tables associated with the MPS: energy to power converter current set point, BLM limit tables, kicker settings, MPS masking tables, etc. The complexity will increase as new machine or beam modes are introduced. Many of these tables will be downloaded at initialization and changes will need to be made in controlled access areas. The MPS team mentioned the configurations would be verified after access to these areas which is a big step towards solid configuration control. Some of these tables could change frequently during commissioning. The tables can only be changed by system experts but will still need to be verified after changes by qualified personnel.

Configuration controls should cover all loadable software including FPGA code, PLC code, VME drivers and applications, and operator applications code. Strict version control should be used for all software modules. While the implications for damage are obvious for MPS mask tables and energy vs. power supply settings, bugs can be introduced by “enhancements” to software applications. Changes to device drivers and low-level applications should be tested and version controlled with a well-defined roll back mechanism during commissioning and operations. Upgrades to operating system software and commonly used application software libraries and services can have unpredictable side effects, such as a function call returning a different value in newer software releases. The exception handling of these systems calls might not have been predicted so thorough test suites need to be defined and implemented. As stated in the comments section, some level of software verification needs to be defined and implemented.

Client application software and configuration files should also be monitored for changes. (Client applications refer to software that changes hardware set points remotely as distinct from software that directly controls the hardware). For instance restore files could cause machine damage if invalid files are used to restore the machine for beam or machine setups not intended for a machine cycle. The post mortem configuration files and archive request files should also be controlled with some type of version control such as CVS. Inadvertent deletion of signals could cause an erroneous sense of security for system integrity. Alarm limits will be dependant on the beam intensity and will also need version controls.

In addition to risks involving the complexity of configuration control the Committee considered the worst-case scenario involving the possible loss of the complete circulating beam. While this eventuality appears highly remote the Committee notes that all scenarios of this type appear to involve the dump kicker system in some way. The worst scenario is a failure of the triggering system that could lead to beam in the LHC with nowhere to go. A simultaneous failure of two or more extraction kickers, extracting the beam with a wrong energy setting, or the spontaneous firing of a single kicker module will all lead to extensive damage. The Committee suggests that a backup system with wide operational tolerances should be investigated to minimize the impact of these failures.

Are there mechanisms for beam losses not being considered that could impact on the strategy ?

The reasons for beam loss at LHC are manifold. Most likely are hardware and software equipment failures, irregular beam parameters or obstacles in the beam aperture. Besides passive beam loss protection and active surveillance measures, beam loss monitoring is an important pillar of the LHC machine protection system. Localized beam loss detectors distributed along the accelerator components will be used in many respects either to protect accelerator equipment or to facilitate optimum beam steering. Based on recent experience at HERA the committee believes that fast beam current and magnet current monitoring could be suitable alternative techniques to further improve the equipment protection strategy at LHC.

According to the concept of beam cleaning, beam-tracking studies have been performed to understand various patterns of slow beam losses at the LHC aperture borders. The committee acknowledges that the most prominent locations of slow beam losses have been identified and discussed extensively. In addition, fast accidental losses should be studied to verify that the proposed distribution of loss monitors is capable to detect critical beam losses in time and with sufficient efficiency.

Long-term experience at the SPS demonstrates that the proposed ionization chambers are suitable, safe and reliable instruments capable to cover the huge dynamic detection range required. The flexible mounting scheme based on fixing straps will easily allow placing monitors even not yet assigned to a particular location according to the actual operational needs. However, the committee thinks that detectors based on alternative technologies should be considered in addition to increase the overall safety figure of the system. Irradiation experiments have verified that the front-end electronics will withstand the expected radiation doses while reliability tests simulating other ambient conditions have still to be done.

Are the interfaces between the different systems clearly specified ?

The hardware interface for the Beam Interlock Controller is of a robust and flexible design. The easy connection of maskable or non-maskable inputs to the system allows for any number of devices to participate in the Beam Interlock system. Additional controllers can be inserted into the link without difficulty to expand the system. Completed tests show that the system performs as expected.

The committee recognized that the software interface to the beam interlock system was not a subject of the review. However we believe that including the eventual software interface to any subsequent test or reviews would be valuable. LHC systems such as the BLMs and collimators have state dependent nominal conditions. These subsystems must therefore be notified in some way of the state of the LHC. They in turn communicate to the beam interlock system that they are configured properly for the state of the LHC in the form of a beam permit. This two-way communication between hardware systems is operationally complex and is worthy of the same degree of scrutiny as the hardware.

Are there other protection devices that should be considered ?

The Committee feels that while the postulated protection devices are suitably comprehensive there may be a role for back-up systems for the small number of critical systems that could cause " Doomsday Scenarios ". These are failures involving the full beam energy that could cause major machine damage resulting in extensive downtime. To avoid the availability issues associated with 'protection systems protecting the protection systems', these back-up systems would have loose tolerances resulting in operationally benign systems.

We note the widespread use of redundancy for the critical functions of the protections system. We suggest that the redundancy concept could be extended to encompass alternative hardware and software platforms (the diverse systems approach) in the most critical systems. For hardware one could use different topologies and components. For software using different programmers to develop code. For computers systems and PLCs using different platforms. Using a diversified design for the redundant system will greatly reduce the chances for a systematic design error. In a similar vein, a more formal software validation approach, such as that typically adopted for personnel protection systems, might be considered for the more critical system aspects. Both the dump triggers and energy tracking system are example of such critical systems.

The committee also recommends that a suitable professional engineering firm perform a detailed design review of the final design of the critical systems. This detailed engineering review should be at the circuit component level for hardware and line-by-line code level for software.

Are there other input channels to the Beam Interlock System that should be considered ?

The Committee believes that the machine protection inputs as presented are comprehensive.

We suggest that improving the response time from the power converters could be useful. If the MPS signal comes from the control logic rather than the output of a relay indicating the power converter has tripped the signal indicating the fault should allow the beam to be aborted before the power supply starts to ramp down. This is typically at the end of the internal interlock chain and would show a fault for internal, external interlocks or an off or disable command. This should be in parallel with the FCCM current monitor design in progress which should detect a fault like shorted coils in a warm magnet before losses are detected.

The Machine protection system designers should consider inputs from the control system. What should MPS do when remote computers are down? Software monitoring of the systems could shut down MPS if this is desirable. Likewise, what happens if the post mortem software is not running for some reason. Should the beam be aborted before an MPS hardware trip dumps the beam? Can multiple instances of the post mortem application or archiver be run on different servers for redundancy? Although the MPS system is designed to fail safe, post mortem diagnostics while systems are down could be lost.

Network failures may also require some form of protection system input. What happens in the case of a network storm caused by unpredictable events such as a reboot of a core switch? Local storage of data was discussed and is a good idea. Still, the remote computers could be unavailable for motion control, power supply control, etc.

Will the protection system have the required safety ?

The Committee thinks that as designed the machine protection system should provide the desired level of safety. Operational scenarios involving significant damage appear suitably improbable and have been commented on in other sections.

The Committee offers two caveats. The request from the accelerator physics section for an aperture kicker to measure dynamic aperture appears to present an unjustifiable risk. As described, this device would be capable of producing a single turn, 5σ, beam deflection at top energy. An uncontrolled firing of this device could cause serious consequences that the machine protection system would be unable ameliorate. If there is indeed a need to measure the dynamic aperture directly at high energies then the Committee suggests that a slower acting resonant device such as an A.C. dipole be considered instead. (The Committee notes that HERA has chosen not to use a full aperture kicker for similar reasons.)

The use of fast acting beam valves around the LHCb region also causes the Committee some trepidation. Although not capable of a single turn loss event, a fast acting loss by a device impinging on an otherwise well behaved circulating beam proved difficult for the Tevatron machine protection system to diagnose effectively. We suggest that the use of any fast vacuum valves in the LHC be subject to a suitable risk/benefit scrutiny.

Will the protection system allow for efficient operations (availability) ?

The MPS affects the availability of the LHC for in the following ways:

- Low availability of the MPS reduces the LHC's availability. If the MPS is not available, the LHC will not be allowed to operate.
- The reliability of the MPS with respect to unsafe conditions (to conditions requiring a beam dump) affects the safety and protection of the LHC. The MPS must reliably generate a dump request and the LHC beam dumping systems must function when demanded. As can be seen, the reliability of the MPS is the reliability of the beam dump requests combined with the reliability of the LHC beam dumping system to function when demanded. For increased safety, the MPS must have a low rate of "false negatives" (i.e. high rate of true positive); it must not allow beam when the LHC is unsafe.
- The reliability of the MPS with respect to safe conditions affects the availability of the LHC. For increased availability, the MPS must have a low rate of "false positives" (i.e. high rate of true negative); it must not request beam dumps when the LHC is safe.

Impact of various aspects of MPS reliability on LHC safety and LHC availability

Actual condition of LHC	**MPS reliability with respect to:**	**Impact on LHC safety**	**Impact on LHC availability**
LHC unsafe	“False negative” (Failure to generate beam request)	High rate of failure of dump requests reduces LHC safety.	not applicable
	Failure of the LHC Beam Dumping system on demand	High rate of failure of LBDS reduces LHC safety.	not applicable
LHC safe	“False positive” (False dumps, i.e. erroneous dump requests)	not applicable	High rate of false dumps reduces availability.

The Review Committee found that the main risk for LHC availability would not appear to be the MPS not allowing the machine to be run with beam as a result of false dumps. Instead, the main risk for LHC operations would appear to involve achieving design luminosity.

- Achieving design luminosity will require a beam loss rejection by the collimation system of 10E-4 in order to avoid quenches. The tolerances required to achieve this rejection level are tight and have not been demonstrated in any existing machine.
- It is less than obvious to the Committee that the ability of the collimator system to clean the beam to the required level, i.e. collimator efficiency, can be validated in an operational way.

The LHC staff presented a number of reliability calculations to aid in analysis of the LHC availability and safety. The Review Committee found these analyses helpful and strongly encourages their use to evaluate implementation options, as well as to validate the safety and availability goals for the LHC. Numerous sub-systems affect the safety and availability of the LHC. These analyses provide inputs to determining how to allocated fixed resources among these. In combination with design calculations and simulations, they also ensure that the performance requirements of the sub-systems are balanced.

As noted also by the presenters, component reliability data is an important limiting factor for these reliability calculations. In view of the lack of data pertinent to the operating conditions (environment, demand frequencies, duration of operation) of the LHC, the methods that were used to estimate component reliability are probably the best feasible approach. The Committee agrees that these estimates are more indicative of the relative reliability that can be expected of the different design options rather than predictions of actual reliability levels.

Looking forward, the test and validation period planned as a part of LHC commissioning may indeed provide some information relevant to system and component reliability. The information from this period should be used to the extent possible. The Committee would suggest additionally that a systematic data collection effort be considered as a part of LHC operation. The LHC is a large machine with many components used in relatively large numbers; systematically collected data would be valuable to the LHC and could also be useful for other machines at CERN. Both the routine testing program and the post-mortem data and analysis program are relevant in this regard.

Based on experience elsewhere what is most critical and where have been surprises

Power converters seem to have caused the most problems during the startup of other machines. With most high power components a period of infant mortality will be experienced. Only through extensive operation of the power converters before beam operations can failures be minimized. Some of the power converters problems can only become evident when the full system becomes operational.

All machine systems will benefit from adequate time in commissioning. During this commissioning phase there will be a high component failure rate and consequent down time due to repairs. This will cause schedule pressure. This is an inherently a risky time. Suitable care must be taken to avoid 'shortcuts' and responsibilities must be well defined to avoid problems.

It is prudent to note that every machine has had at least one event that would have been catastrophic had it involved LHC stored beam energy. In machines where the beam energy can only cause a magnet quench there have been several such events. There seems to be no obvious single root cause. Each failure was unique and depended on the particular hardware and software design. Some examples of failures that have occurred in other machines are:

- Failure in the abort trigger.
- Spontaneous trigger of abort module without triggering other abort modules in the beam dump system either at all or not fast enough.
- Energy tracking did not work; abort modules capacitors were not at the correct voltage.
- Beam loss system did not trigger the abort system by either hardware or software failure. In addition some machines allow the beam loss system to be disabled by operations.

The Committee believes that these kinds of failures have been potentially addressed in the LHC machine protection system.

Comments

In addition to the safe beam concept the Committee believes that a low intensity validation cycle for a 'warm start' scenario will also prove necessary (a semi-safe beam ?). Certain operations such as collimator alignment will prove difficult with purely a pilot pulse.

The basic operation concept of the machine protection system requires comprehensive post mortem data acquisition and analysis as well as automatic mandatory self-tests to ensure and re-qualify the anticipated safety level of the system. Those functions require tight coordination between the machine protection and the overall accelerator control system. Technical post-mortem procedures have to be designed, implemented and tested and practicable operational sequences have to be specified and executed. Post mortem requirements on the sub-systems need to be centrally determined rather than defined *ad hoc*. Based on the presentations the committee was not able to review the software interfaces and software methods involved in any detail. The Committee is concerned that the remaining time until the first beam tests might be insufficient to implement all relevant applications and services.

The apertures associated with the extraction septa in the dump line are not large and these septa are at risk of beam related damage in many of the 'dirty' beam dump scenarios. The Committee recommends that the acquisition of additional spares (or components thereof) of these devices be considered to avoid the significant downtime in the event of damage to more than one of these elements.

We note the widespread use of redundancy for the critical functions of the protections system. We suggest that the redundancy concept could be extended to encompass alternative hardware and software platforms (the diverse systems approach) in the most critical systems. In a similar vein, a more formal software validation approach, such as that adopted for personnel protection systems, might be considered for the more critical system aspects.

The DCCT sub-system used to measure circulating beam current was described as having a 100ms response time to meaningful beam losses. If this device is to be used as an input to the machine protection system then a faster response is desirable.

The Committee thought that the concepts associated with the determination and distribution of the safe beam parameters were vague.