ARCHITECTURE OF THE MACHINE PROTECTION SYSTEM

K. H. Meß[1], R. Schmidt, CERN, Geneva, Switzerland

Abstract

The protection of the LHC accelerator has to work under all circumstances, with and without beam. Several sub-systems, such as beam dump systems, beam loss monitors, magnet protection, and powering systems etc. are combined coherently with some dedicated hardware as "glue" to form the machine protection system. The structure, some aspects of the hardware, and in particular the interfaces to the other systems are described.

1 INTRODUCTION

The LHC is a complex accelerator operating close to the limits, both as far as beam energy and beam densities are concerned. Major faults in the complex equipment will result in long repair times. To optimise the operational efficiency of the accelerator, accidents should be avoided and interruptions should be rare and limited to short time. Hence a system is needed that prevents damage to the magnets, the cables and the power-leads, minimises damage due to irradiation caused by beam losses, and provides the necessary tools to implement a consistent and congruent error and fault tracing, throughout the machine.

Machine protection is not an objective in itself; it is a mean to maximise operational availability by minimising time for interventions and to avoid expensive repair of equipment and irreparable damage. The proposal, presented here, is based on work done for the Tevatron, HERA_p, RIHC and the string tests at CERN [1,2,3,4]. As an evolution of the ideas presented at the Chamonix_X workshop [5] it has been discussed since with numerous colleagues from SL-BI, SL-BT, SL-PC, LHC-ICP, and ST-AA. It has been presented to the DEWG, IWG, and the AIWG working groups as well as to the SL-TC, the TCC, the MAC, and at other occasions.

The interlock and access system for personal safety does in principle not depend on the machine protection system. The two systems are, however, related.

2 THE CHALLENGE

Both, the stored magnetic energy and the energy stored in the beams are unprecedented. Moreover, both systems are coupled. Obviously, faults in the magnet system will in general often result in a beam loss, which in turn may induce quenches. The machine protection system has, however, be made to accept that at times the magnets will be powered, without beam in the machine. The opposite case is not possible.

At nominal operating current, predominately the dipole magnets store a large amount of energy. The LHC magnets are powered separately in each of the eight sectors in order to reduce the energy stored in a particular electrical circuit. Still, the energy in each sector of the LHC amounts to 1.29 GJ, sufficient to heat up and melt 1900 kg of copper [6].

During operation without beam, the large energy stored in the magnets presents the main risk. Various reasons can lead to an uncontrolled energy release. Magnets, superconducting bus bars, current leads, or cryogenic infrastructure could in such a case be destroyed. In case of a failure the magnetic energy has to be extracted. Due to the large inductance a response time in the order of 10 ms to abort the power is acceptable for most elements (such as all superconducting magnets).

Each beam stores energy of up to 0.35 GJ, equivalent to the energy for warming up and melting 515 kg of copper. A sophisticated collimating system protects the magnets from beam losses.

If the operation of the machine becomes unsafe and beam loss has already been observed by the beam loss monitors, or is imminent due to equipment failure, the beams have to be dumped as soon as possible, in order to prevent radiation damage, quenches, and downtime. However, due to the size of the LHC at least 110μs are required on average to request a beam dump.

The large number of vital components will be a major challenge. More than 8000 superconducting magnets, including about 2000 large dipole and quadrupole magnets, and 6000 corrector magnets, are powered in about 1800 circuits. Several thousand electronic channels may, in case of failure, force a beam dump. To limit the number of superfluous aborts below one per fortnight, the mean time between failure (MTBF) must exceed 100 years for each channel!

The machine downtime depends on the type of faults and their frequency. It could be between two hours and several weeks for one incident. Major accidents may include the partial destruction of a magnet. To warm up the neighbourhood, the repair, and the cool down will require some weeks. Should no spare magnets be available, the repair may last many months.

---

[1] On leave of absence from DESY, Hamburg, Germany

3 ARCHITECTURE OF THE MACHINE PROTECTION SYSTEM

3.1 General aspects

Some general requirements have to be considered for the machine protection system:

- Protect the machine: In case of fault the necessary steps shall be taken to dump the beam and to discharge the energy stored in the magnets in a safe way.
- Protect the beam: The system shall not generate unnecessary beam dumps.
- Provide the evidence: The system shall help to identify the initial fault, in case of beam dump or power failure.
- Improve the operation: The status of the system must be transparent to the operator at all times.
- Enable tests: Almost all functions must be remotely testable.

This can be achieved by:

- Hardwired abort links protect the equipment (Hard Abort).
- Soft aborts, possibly via computer links, improve the operation efficiency; they may be disabled or may fail.
- The number of channels that may provoke an abort will be minimised.
- The same structure across different sub-systems in the abort chain will be used.
- All inputs can be simulated or bridged. However, in such a case “permits” are also simulated and not passed to destinations outside of the system.

3.2 General Architecture

The architecture of the machine protection system is derived from the structure of the LHC and from operational requirements. It consists of a distributed, globally acting Beam Interlock System that informs the Beam Dump System if any unsafe situation is detected, and of locally acting, distributed, Power Interlock Systems. They cause a safe discharge of the energy stored in the magnet system in case of a quench, or other failures. Interfaces between the Power Interlock Systems and the Beam Interlock System ensure the dumping of the beams, if necessary. A Post Mortem System described elsewhere [7] records data from various systems to understand the cause of a fault leading to a beam dump or power abort.

3.3 Architecture of the Power Interlock

The eight sectors in the LHC consist (Version 6.2) of 44 continuous, largely independent cryostats [8], and some warm magnets. Powering of one electrical circuit is always limited to one of those cryostats or half-insertions

The powering system for each electrical circuit includes power converters, (warm) cables from power converters to the current feedthroughs, the current feedthroughs, superconducting bus bars for the current distribution, and finally the superconducting magnets.

In case of a fault in one of the cryostats the energy of some or of all electrical circuits in this cryostat has to be discharged. Each cryostat will have a local Power Interlock System. Hence, any cryostat can be powered irrespective of other cryostats. An example of the architecture between IP1 and IP8 is given in Fig.1

LHC contains 36 short cryostats requiring one Power Permit Controller (PPC) each, preferentially located close

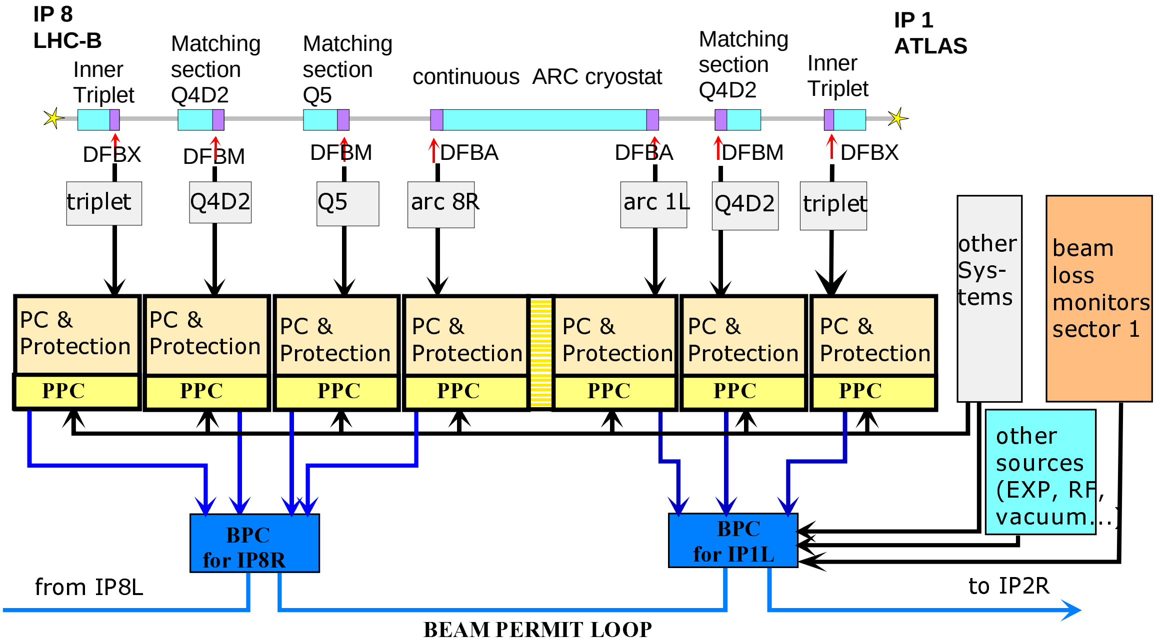

Fig. 1. Power and Beam Protection System between IP1 and IP8

to the power converters. Warm magnets on either side of an interaction point (IP) are treated as if they form an additional “continuous cryostat”.

The eight long arc cryostats span the major part of a sector and are electrically fed from both sides. The energy extraction systems for the MQ magnets are in the even points. The MB magnets are discharged at both ends of the arc cryostat. Hence the long arc cryostats need Power Permit Controllers (PPC) on both sides and a communication link in between. The quench detection for main magnets in the arc cryostats comprises about 200 units distributed along the arc.

About 100 power converters installed in the tunnel power the orbit correctors in one sector.

In total, almost 60 Power Permit Controllers (PPC) are required. They will also be connected to the controls network and the timing system.

3.3 Architecture of the Beam Interlock

There will be one Beam Interlock System for the LHC. Right and left from each IP one Beam Permit Controller (BPC) will be installed (see Fig.1). These controllers are connected to two fast, optical links (Beam Permit Loops) running at 10MHz (see Fig 2). The two links distinguish between beam I and II. When a link is broken, the corresponding beam is extracted into the beam dump by the Beam Dump System. In addition, a computer connection to the BPC for monitoring, testing and post mortem analysis is required.

Note that Beam Permission is a necessary but not sufficient condition for beam injection. In order to inject beam, additional conditions have to be met.

Power Permit Controllers report their state to a BPC in the vicinity.

3.5 Inventory of the Machine Protection System

The Machine Protection System consists of:

- 16 Beam Permit Controller BPC,
- global fast links between the BPC and the Beam Dump System,
- a set of 52 (v. 6.2) Power Permit Controller (PPC) for the cryostats,
- some PPC for the warm magnets
- and a computer network connection to each controller.

In addition the Machine Protection System makes use of features provided by the Quench Protection System and Power Control System:

- a set of 8 arc links to collect the quench messages (Quench Loop),
- a set of 8 arc links to fire heaters (Heater Activation Link),
- and field-busses, joining the controls for quench detectors and heater power supplies and the power converters in the arc.

Some details about the Beam Interlock System (BPC and links) and the Power Interlock System (PPC and links) are described below. More information will be presented in a forthcoming report [9].

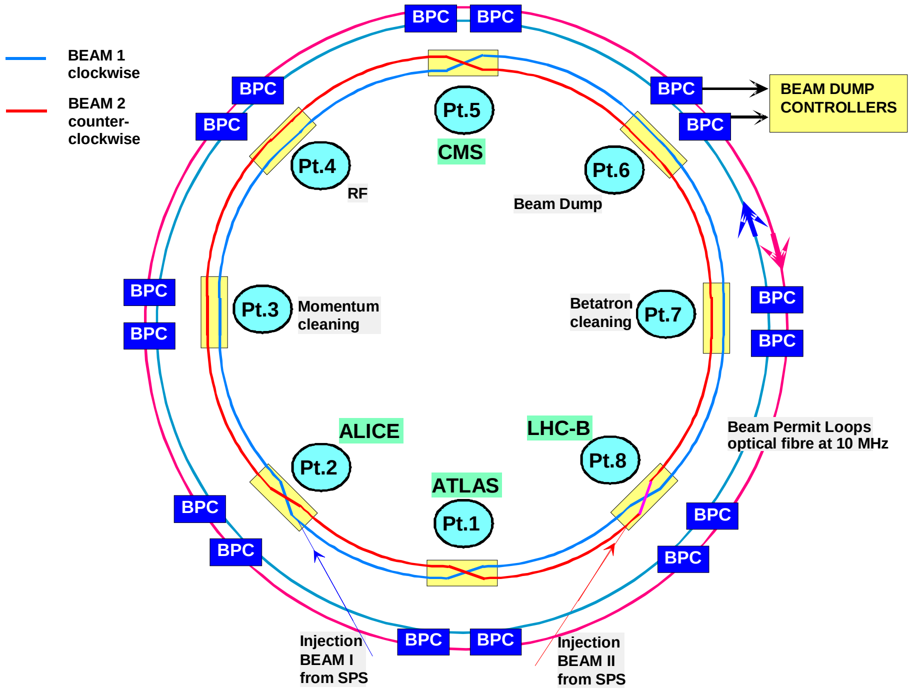

Figure 2. General layout of the Beam Interlock System

4 COMPONENTS OF THE POWER INTERLOCK SYSTEM

A Power Permit Controller monitors the powering status of one cryostat. Depending on the cryostat, it monitors the elements in a few electrical circuits for short cryostats, and of some ten electrical circuits in the long arc cryostat. Therefore a modular design is proposed. Similar controllers will monitor the powering of all warm magnets in one half-insertion.

An electrical circuit is connected to the PPC through a dedicated channel, identifying the type of the electrical circuit. With respect to the magnet protection, the circuits are divided into two classes:

- Main magnets: Circuits that include magnets with large stored energy. A quench is likely to affect other magnets and electrical circuits. Therefore all magnets in the cryostat will be de-excited (Cryostat Power Abort).
- Other magnets: Circuits that do not include magnets with large stored energy. Normally, a quench of an element in such circuit is contained in that element.

With respect to the impact of a magnet fault to the beams a different distinction has to be applied. Depending on the state of the accelerator, some electrical circuits may not be vital ("critical") for machine operation. It would be inappropriate to dump the beams, if such a circuit quits functioning. Hence, some circuits are "critical", i.e. required for beam operation under all circumstances, and some are only sometimes required. Switches set this classification.

4.1 Quench of a main magnet

The electrical circuit to be monitored defines the input and output signals for a given channel. For example a main magnet circuit will have a Quench Loop.

In case of a quench, the loop is opened by the quench detector. Since a main magnet quench will cause a Cryostat Power Abort, the discharge switches extract the energy from the main circuits in this cryostat. In addition the corresponding power converters are switched off by raising the Power Converter FAST ABORT signal and by removing the corresponding Power Converter PERMIT (constant current outputs). All other circuits of the cryostat are discharged by the PC controller or by a Discharge Switch Trigger command.

The power converter informs the PPC of a fault by dropping the PC OK signal. If the fault requires a fast discharge, the PPC sends in addition a DISCHARGE REQUEST to the PPC (by interrupting a current loop) that activates the discharge switch for this circuit.

In the unlikely and worst case that a discharge switch fails to open after a request (Switch Open Fault), a number of selected heaters will have to be fired by the PPC using the Heater Activation Link.

For the triplet cryostats, the heaters of the MQX magnets are fired in case of a discharge request, since there is no system to extract the energy and the time constants for slow ramp down are too large.

In all cases both signals to the BPC (ALL CIRCUITS OK and CRITICAL CIRCUITS OK) will be switched off.

4.2 Quench of a low energy magnet

Circuits that have little energy stored require only a Quench Loop, a PC OK link, a PC PERMIT link, and a PC ABORT link. If one of the quench detectors for the circuit indicates a quench, it breaks the Quench Loop. The controller switches the power converter off (PC PERMIT, PC ABORT). If the circuit has an extraction resistor, the energy is extracted.

In case of a power converter fault, a signal is transmitted to the controller in order to record the failure.

It is not required to discharge magnets powered in other electrical circuits. In all cases the ALL CIRCUITS OK signal to the BPC is switched off. Internal readable jumper settings determine, whether the electrical circuit in question is considered "critical". If this is the case, also the CRITICAL CIRCUITS OK signal is switched off.

4.3 Interfaces to other systems

In general, the PPC has per electrical circuit the following signals/links:

- one Quench Loop ,
- one PC OK input,
- one power permission link (output),
- one PC Fast Abort link (output),
- one PC Slow Abort link (output),
- one Current Low input (I< I_access).

The PPC of the long arc cryostat requires one additional I/O section for the three main magnet circuits with:

- one Quench Loop connecting the PPCs on both sides with all quench detectors for main electrical circuits, and the discharge switches,
- three PC OK inputs,
- three PC PERMIT outputs,
- three PC Fast Abort outputs,
- three PC Slow Abort outputs,
- three Current Low signals (input),
- three NO DISCHARGE requests (input),
- three Discharge Switch Open Fault (input),
- three DISCHARGE TRIGGER links. (The second MB discharge switch is operated by the second PPC.)

All electronics of the Power Interlock System is connected to the control system. Status and memory is readable at any time.

The computer connection to the control system is established via the VME bus, a suitable processor board and VME. It might be considered to employ a local display unit and a keyboard for debugging.

Electronics that is directly connected to the Power Interlock System, like quench detectors, must be connected to the control system, either via Ethernet alone or via fieldbus and Ethernet.

5 COMPONENTS OF BEAM INTERLOCK SYSTEM

The Beam Permit Controller (BPC) combines the messages from different sources to interrupt the 10 MHz pulse trains in the optical fibres of the Beam Permit Loop (BPL) in case of a fault condition. The absence of a pulse train will be interpreted as BEAM DUMP command for the corresponding beam.

The 10 MHz trains are produced in one BPC only (IP6L, set by a jumper). The setting of the jumper (master/slave) is visible at the front panel and readable from the computer.

Name	Conditional[2]
RF system	Yes
Loss monitors I	Yes
Loss monitors II	Yes
Beam excursion	Yes
arc cryostat, All Circuits OK	Yes
triplet cryostat, All Circuits OK	Yes
Q3 cryostat, All Circuits OK	Yes
Q4 cryostat, All Circuits OK	Yes
Q5 cryostat, All Circuits OK	Yes
Q6 cryostat, All Circuits OK	Yes
Q4D2 cryostat, All Circuits OK	Yes
4 spares	Yes
Experiment OK	No
Loss monitors at collimators	No
Collimators	No
Access system OK	No
Extraction system OK	No
Beam Injection Permit	No
Vacuum valves OK	No
spare	No
arc, Critical Circuits OK	No
triplet, Critical Circuits OK	No
Q3, Critical Circuits OK	No
Q4, Critical Circuits OK	No
Q5, Critical Circuits OK	No
Q6, Critical Circuits OK	No
Q4D2, Critical Circuits OK	No
Warm magnets	No

Table 2. Input signals to the Beam Permit Controller

There will be three types of inputs to the BPC. The BPL input will be used to feed the BPL output, unless one of the unconditional inputs indicates a fault condition or one of the conditional inputs does so, provided it is not masked.

All input states and the output state are continuously sampled and stored into a memory as well as displayed life on the front panel.

The control system sets the masks, senses the memory state (frozen or life) and performs the readout. The fail-safe and reliable inputs are described below

Each Power Permit Controller provides two signals to the BPC:

- A fault in one of the main magnets, such as dipole or quadrupole magnet, would always cause a total beam loss. After such fault the signal CRITICAL CIRCUITS OK would disappear, and both beams would be dumped.
- A fault in a corrector magnet, such as a spool piece magnet or orbit dipole corrector, might cause a beam loss. After such fault the signal ALL CIRCUITS OK will disappear. This may imply a beam dump, depending on the machine status.

In case of circulating beams, the breakdown of the BEAM DUMP SYSTEM presents a major hazard. The beams must be dumped, as long as the system is still capable to do so. The signal is unconditional.

Inputs from the LHC experiments are foreseen. The details have still to be discussed.

If the RF system does not work correctly, the beam will debunch. It will not be possible to dump the beam properly without unacceptable beam losses. A signal from the RF system is therefore required to dump the beam if a debunching is to be anticipated or if the feedback is going to fail.

There will be beam loss monitors distributed around the ring, with a set of monitors close to each quadrupole, as well as monitors close to the collimators for beam cleaning. The signature of a beam loss that should request a BEAM DUMP remains to be established.

The input to the Beam Interlock System would be via one of the BPC close to the insertion. It needs to be understood if a link from the alcoves to the BPC is required. Alternatively, the beam loss monitor system might be subdivided into eight sections. In this case one input per octant or sector might be used.

The access system for the protection of people needs to follow the legal requirements. It needs to be completely separate from the Machine Protection System. However, there is an interface between the state of the access system and the actions to be taken by the Machine Protection System. The Machine Protection System will automatically request a beam extraction in case of an access violation. For safety reasons, a separate link from the access system to the BEAM DUMP SYSTEM is required.

There will be some elements to prevent the accidental injection and circulation of a beam, such as valves in the beam tubes, collimators and some magnets in the transfer

---

[2] Preliminary assignment

line. Such systems are activated if ACCESS to the tunnel or the galleries should be given, or if there is an ACCESS VIOLATION. Considering valves or collimators, an injection can not be allowed unless they are out of the beam.

Two Beam Permit Loops run around the entire accelerator. The signals need to be transmitted as fast as possible to the BEAM DUMP SYSTEMS. The number of access points to the link is limited to 16. Hence, a transmission using optical fibres seems appropriate. The state of these loops is available for local distribution.

All electronics of the Beam Interlock System is connected to the control system. The computer connection to the control system is established via the VME bus, a suitable processor board and Ethernet. It might be considered to employ a local display unit and a keyboard for debugging. All electronic connected to the computer link has to have a post mortem memory to record all essential signals. The computer link can also provide the machine status and the timing information, as well as operator commands.

6 ACKNOWLEDGEMENTS

The authors thank all colleagues that contributed to the discussions and the LHC management for the support.

REFERENCES

[1] Robert Flora, FNAL, private communication

[2] R. Bacher et al., The HERA Quench Protection System: A Status Report, EPAC ’96, Sitges, 1996, Institute of Physics Publishing, Bristol, p2264ff

[3] C. R. Conkling, RHIC Beam Permit and Quench Detection Communication System, PAC ’97, Vancouver, IEEE, p2496ff

[4] F. Brodry et al., The Interlock System for String 2: Power enable and abort, LHC-XMS-ES-00001.00, January 2000

[5] R. Schmidt, Diagnostics and Protection of LHC equipment, CHAMONIX_X, CERN-SL-2000-007 DI, p203ff

[6] Werkstoff Handbuch, Nichteisenmetalle III, H.Stendel (ed.), VDI-Verlag Düsseldorf 1960

[7] R. Lauckner, What data is required to understand failures during LHC operation, this workshop, session 8

[8] LHCLSD1_0001 through LHCLSD8_0008, version AB, optics 6.2

[9] K. H. Mess and R. Schmidt, to be published