Summary of the review on LHC machine protection – 11th-13th April 2005

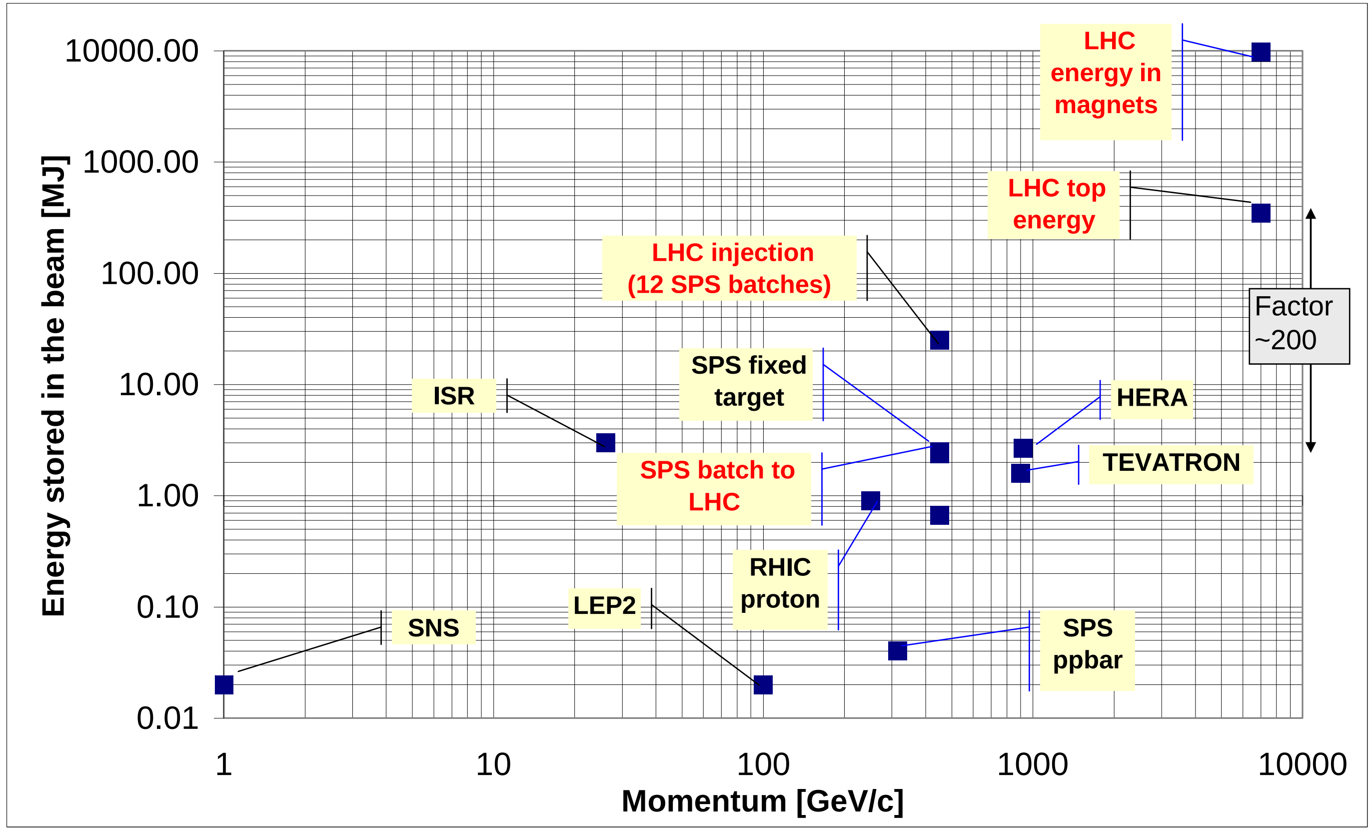
M.Harrison

with 'annotations' from R. Schmidt / J.Wenninger

Review committee

- Marc Ross (SLAC)
- Vinh Dang (PSI)
- Mike Harrison (BNL) – chairman
- George Ganetis (BNL)
- Jerry Annala (FNAL)
- Reinhard Bacher (DESY)
- Coles Sibley (SNS)
- Roger Bailey (CERN/AB)
- Doris Forkel-Wirth (CERN/SC)

Introduction



- The problem is obvious:
  - Magnetic field increase only a factor of 2
  - Energy increase only a factor of 7
  - Stored energy increase > 2 orders of magnitude (damage/quench)

General

- The Committee wishes to commend the speakers for the presentations. A great deal of hard work has obviously gone into the planning, design and in some cases realisation of the various sub-systems.
- The Committee thinks that the front-end system design for both the machine protection system and the associated sub-systems are quite mature.
- Knowledgeable personnel
- TI-8 tests proved useful (in more than one way)
- Radiation tolerance testing in the SPS beamline & PSI

Do you consider the overall strategy for the machine protection adequate ? And what could be the main risks ?

- The Committee feels that the fundamental strategy is sound:
  - Failsafe/redundancy
  - Pilot beam
  - Safe-beam concept
  - Injection protection well done
  - Aperture defined by collimators
  - Mask-able states
  - Comprehensive in the use of the various sub-systems
- The system represents a reasonable extension of existing systems

Do you consider the overall strategy for the machine protection adequate ? And what could be the main risks ?

- **The Committee feels that configuration control represents the main risk of machine damage**
  - Highly complex
  - Many elements
  - Mode changes
  - Software logic/release control

The systems involved in MP come with loads of settings, thresholds… and this is already a problem for the transfer lines (at the limit in 2004). We need some solutions for the SPS in 2006 (CNGS).

We are aware of this…

- **All Doomsday scenarios (350 MJ) appear to involve the dump kickers in one way or another**

All scenarios involve an incorrect dump kick (E-tracking,…) or a missing trigger (not necessarily a dump kicker problem !).

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

- **While the Committee can imagine other beam loss scenarios we do not feel that the overall strategy would be changed in any significant way**

From J.Annala we learned about very fast quenches (~ms) that are/were a problem at the Tevatron where the quench protection system is used for beam loss monitoring (BLMs are all masked out).

For slow quenches we are sure that the quench detection + powering interlock systems can dump the beam before anything happens to the beam, but such very fast quenches could be an issue for the LHC. We will look into this issue…

It also means :

- We need FAST BLMs (reaction time ~ turn) right from the start of the LHC.
- Our strategy with redundant interlock systems (BLMs, BPMs, BCTs…) is very important to cover the failure phase space.

Are the interfaces between the different systems clearly specified ?

- The hardware interfacing to the Beam Interlock Controller is well defined in most cases. Likewise the majority of the input signals are determined. The Committee notes the system is trivially capable of expansion (reduction !).
- We feel that the software interfaces are less well determined
  - BIC, BLM & Beam Dump control/interface software
  - Post mortem data
  - State control

We are aware of that…

Are there other protection devices that should be considered ?

- **We feel that while the postulated protection devices are suitably comprehensive there may be a role for diversified independent back-up systems for the beam dump triggers and energy tracking (Doomsday scenarios). The backup systems would be expected to have much wider operational tolerances.**
  - Possibly hire some professional outfit to look at this

We are looking at such options:

- energy tracking of the dump systems
- a special BLM channel (monitor @ TCDQ) that triggers the dump directly (and not over the interlock system).

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

- Nothing Obvious
  - Faster response from the Power Converters ?
  - Control system inputs ?
  - Network failures ?

We have triggered AB/PO on the issue of the PC interlock speed of ~ 50ms due to a 'slow' relay.

Each BIC has a software interlock channel that may be used by the control system.

So far we do not think that a network failure should trigger a dump, but it may be worthwhile to test such a failure with some beam. Effect of a network failure depends on duration, state of the LHC, systems affected…

Will the protection system have the required safety ?

- As designed it should. Two caveats:
  - The Committee strongly queries the utility of a device such as the aperture kicker given the potential risk inherent in it's operation.

    We know that this is a candidate for doomsday scenarios. It will require very sophisticated interlocking… and sufficient resources to implement the interlocking – no short-cuts HERE !

  - In a similar vein the use of fast vacuum valves is also something that needs to be carefully justified.

    It seems the fast valves can do more harm than good. Their utility is being reviewed.

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

- The main risk would appear to involve not achieving suitable luminosity rather than not being able to run the machine with beam
  - Achieving design luminosity will require a beam loss rejection of 10E-4 to avoid quenches. This requires tight tolerances and has not been demonstrated in any existing machine.
  - It is less than obvious to the Committee that the collimator efficiency can be validated in an operational way.

This is a collimation, not a MP issue…

- Reliability calculations provide a mechanism to determine the optimal strategy to allocate fixed resources among the various sub-systems.

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

- Power supplies gave the worst problems in the initial stages at all machines.

- Every machine has had at least one event that would have been catastrophic with LHC beam. There is no obvious single root cause. We believe that these failures have all been potentially addressed in one way or another in the LHC machine protection system.

- Commission of necessity involves a large amount of equipment failure/repair and associated downtime. It is an inherently risky time. Additional care must be taken to avoid 'shortcuts'. Responsibilities must be well defined.

Lot's of common (beam operation) sense !!

Comments

- Validation cycle for a 'warm' start - semi safe beam state
  - Reproduceability ?
- Post mortems are crucial to the machine operation. Data gathering and archival functions need definition for subsequent analysis and re-qualification.
- Formal qualification for the MPS system software ?
- Diverse systems for critical functions
- Define 'failsafe' in operational terms

Comments

- Spares for the dump septum
- Distribution of the safe beam parameters slightly vague

  System is in the design phase

- SPPS dump integrity (personal protection stopper)
- DC beam measurement was too slow (~100 ms)

  This is clear for us too! We must make another iteration with BDI.

Conclusions (R. Schmidt / J. Wenninger)

Our conclusions of the review:

- We had no surprises !
- We received many useful and detailed comments.
  - evaluation in the MPWG and elsewhere.
  - first analysis on 29th April in the MPWG.
- We are waiting for the written report.
  - we will come back to LTC with actions, recommendations…