Machine Protection Working Group

Minutes of the 52nd meeting, held 25th November 2005

Present: R. Schmidt, J. Wenninger, V. Kain, B. Goddard, M. Zerlauth, J. Uythoven, R. Steinhagen, B. Puccio, B. Todd, R. Lauckner, B. Dehning, A. Butterworth, M. Lamont, E. Carlier, H. Schmickler, V. Montabonnet.

Meeting Agenda:

- Machine Protection Software Issues for MAC [RS]
- Management of Critical Settings – MCS [VK]
- RF Frequency Interlocking [AB]

The following items from the original agenda have been postponed to the following MPWG Meeting:

- *Inputs to the LHC Beam Dumping System [EC]*
- *Direct IR6 Beam Dump Trigger [BG]*

R. Schmidt began the meeting by introducing the topic of Software Issues in the Machine Protection System that has been requested for discussion by the Machine Advisory Committee.

Machine Protection Software Issues for MAC [RS]

R. Schmidt made a presentation introducing the proposed topics that are to be discussed in the upcoming MAC, where Software Issues in the Machine Protection System are to be considered. **R. Schmidt** began by describing the overall layout of the LHC Machine Protection System, and by introducing the four main scenarios in which Software is involved in the MPS: Management of Critical Settings, Software Interlocks, Sequencing and Post Mortem.

It was noted that software is not needed for the core MPS processes of detecting a fault with the machine and requesting a beam dump, these actions are implemented in hardware, with fast deterministic responses. **B. Goddard** noted that the hardware implemented is redundant in many cases. **R. Schmidt** continued by saying that some systems use Critical Settings to determine Interlock levels, in these cases an incorrect setting could compromise Machine Protection. The Post Mortem processes are also to be implemented in software, these are vital for the protection of the LHC, as Post Mortem information is used to determine the correct action of the MPS, ensuring systems have operated correctly without loss of safety. **R. Schmidt** then briefly described the Software Interlocks, allowing more complex combinations of events to force a beam dump, and allowing rapid implementation new Interlocks. It was noted that Software Interlocks are not to be elaborated upon in the MAC.

R. Schmidt expanded the role of software during the *Filling Phase* of the LHC operation. Where many Critical Settings are to be managed to correctly determine interlock levels, software processes are needed to give a Beam Extraction Permit signal, and the chain of events needed to successfully transfer a beam from SPS to LHC will be controlled by a software sequencer. Other software implementations needed during the *Filling Phase* include: Shot-by-Shot logging / Post Mortem and the use of Software Interlocks to perform the slow monitoring of parameters.

R. Schmidt then described software influence during the *Circulating Beam Phase* of operation, emphasising the application of Critical Settings within the chain.

R. Schmidt expanded the idea of settings by describing *Operational versus Critical Settings*, using an example of the kicker septum strength control. These magnets track the energy of the LHC Beam, providing a stronger magnetic field when the beam has more energy, in the case of the Septum and Q4 magnets the Operational Setting is the strength of the kick, which can be trimmed remotely, the Critical Setting is the absolute Maximum and Minimum value that the strength of the kick should be, being set in hardware. Online monitoring using a hardware system of the actual Septum strength versus the desired strength is to be used, invoking a beam dump when the read Operational Setting exceeds the limits set by the Critical Setting. Software is needed to manage and verify these Settings.

R. Schmidt continued the discussion of *Operational versus Critical Settings* by describing the Beam Loss Monitors. During machine operation Beam Loss Monitors compare the measured beam losses to Operational Settings and request a beam dump if excessive losses are detected. The Critical Settings again serve as a safety net, providing absolute Maximum values of the beam losses. If losses are detected that exceed Critical Settings, then a beam dump request is issued, regardless of the Operational Setting. **B. Dehning** remarked that the current implementation of the BLMS is somewhat different, having a single threshold, that can only be changed by a connection to the BLMS in situ. **Various Members** questioned the flexibility of this, as thresholds may need to be changed remotely. **B. Dehning** added that it should not be forgotten that around 10 sub-sets of BLM settings exist; there is no generic BLM setting that can be applied to all.

R. Schmidt then introduced the concept of *Dynamic and Static Critical Settings*. Static Critical Settings are ones that do not change during a mission, an example of this would be an input to the Beam Interlock System, as regardless of machine state, the topology remains the same, meaning the Critical Settings will not be changed. Dynamic Critical Settings are ones that do vary during a mission, an example of this would be the kicker septum strength, or Beam Loss Monitor threshold as previously described.

R. Schmidt continued to describe LHC Configurations, describing both *Static and Dynamic Configuration Parameters*. A Static Configuration Parameter is a value that is constant for the whole of one LHC mission, an example would whether ions or protons were being accelerated. Dynamic Configuration Parameters are those that could change during a single LHC Mission, such as the machine state, or current machine energy.

M. Lamont questioned the terminology employed throughout, as it creates confusion when compared to terminology already existing, **R. Schmidt** agreed, saying terminology needed to be agreed upon and ratified.

Action: Agree on a terminology [RS, ML, VK, BG et al]

R. Schmidt continued, describing the way in which *Critical Settings map to Configuration Parameters*, some Critical Settings are completely independent of LHC Configuration Parameters, such as Beam Interlock System channel enabling, some Critical Settings change when Static Configuration Parameters change such as the safe beam thresholds for proton and ion acceleration.

Other Settings change when Dynamic Configuration Parameters change, such as the BLM thresholds with respect to the beam energy. **R. Schmidt** emphasised that Settings must not be allowed to change in an uncontrolled way, noting that effort has been made to make Settings fixed in hardware, and difficult to change. At the very least, Settings need to be verified once they have been applied to ensure they are correct.

Management of Critical Settings – MCS [VK]

V. Kain made a presentation describing the required implementation and scope of a software for the Management of Critical Settings. **V. Kain** began by providing some background to the MCS; The LHC Machine Protection System requires Settings to be applied to determine whether the machine is in a safe or dangerous state, as described in the previous part by **R. Schmidt**. The MCS System is to provide a means of managing these Settings in a safe and efficient manner, ensuring the protection of the LHC is not compromised by poor or abusive application of Critical Settings.

V. Kain explained that it should be made impossible to bypass the MCS for the application of Critical Settings and that a detailed log should be stored of who changed what setting and when, implying that the database used to hold the critical settings should have the same security, possibly by implementing public-private key authentication. This would secure not only the modification of values in the database, but their safe transmission from MCS to Front-End.

The access to Critical Settings should be limited to the relevant system experts, implementing a signature chain for the approval or denial of modification to the Critical Settings. **V. Kain** continued to describe the functionality of the MCS: It will

- Store Critical Settings
- Allow the modification of Critical Settings by the relevant person/s
- Apply the Critical Settings to the Front End hardware
- Verify that the application of the Critical Settings was successful
- Generate a software interlock if this is in error

In the cases where the Critical Setting varies as a function (of energy of beta-star or time etc.) the MCS will verify that the function being implemented by the front end is the same as that described by the MCS. The MCS Configuration Settings will be modified very infrequently, for example, during Machine Hardware Commissioning, for the fine adjustment of values. At the beginning of every mission it is expected that the MCS will download and verify all the Critical Settings of the machine relevant to the specific physics run being prepared. **J. Wenninger** remarked that this implies a persistence of the Critical Settings at the Front End level.

V. Kain continued to describe a possible implementation of the Software Interlock System, whereby it continually compares values read from the Machine Protection System with values in the MCS System – if any are inconsistent a Software Interlock could be issued. **V. Kain** then described a non-exhaustive list of Systems known to need an MCS: Movable Protection Devices and Beam Cleaning Collimators, Warm Magnet ROCS Surveillance, SPS Extraction Septa Girder Position, Some Kicker

Magnets, Beam Instrumentation, RF and the LBDS XPOC. **B. Puccio** noted that similarities exist between the SIS and MCS, and questioned who would be responsible for its implementation.

RF Frequency Interlocking [AB]

A. Butterworth made a presentation describing an implementation of an RF frequency interlock. The need for this interlock emerges from the machine aperture limitation of the extraction channel; this limits the error in beam energy due to the error in RF Frequency to +/- 0.2%. The nominal frequency of the RF is 400.8 MHz, a change in energy of +/-0.2% corresponds to a change in RF Frequency of just +/-259Hz.

Measuring the RF to a high precision requires a relatively long integration window, **A. Butterworth** showed results of a preliminary study, where detection would take $1/20^{th}$ of a second. Beam reaction time is determined by synchrotron frequency, which in the LHC varies from 61.8 down to 21.4 Hz from injection to top energy. This yields a beam response time of just $1/120^{th}$ of a second. This implies that the RF Frequency interlock cannot react quickly enough to catch sudden shifts.

A. Butterworth finished by describing a simple topology that could be implemented to realise the RF Interlock, by using an SLP receiver together with a COTS frequency counter, this could be realised relatively quickly. However, currently no manpower exists to implement a safer or more sophisticated design.

R. Schmidt said that the proposed solution is acceptable for LHC start up, if it's deemed necessary, efforts could be made to upgrade this device after the first 6-8 months of machine operation in 2007, when more manpower will be available, and by considering realistic failure cases for RF Frequency change (slow change, sudden jump) to further evaluate the required reaction time.

AOB

none

Next Meeting
Friday 16th December 2005 at 10:00 in room 864-1-C02

BT