Machine Protection Working Group

Minutes of the 49th meeting held on September 30th 2005

Present: R. Assmann, V. Baggiolini, A. Butterworth, E. Carlier, B. Dehning, R. Denz, R. Fillipini, R. Giachino, B. Goddard, G. Guaglio, C. Ilgner, V. Kain, J. Lewis, D. Macina, V. Montabonnet, B. Puccio, R. Schmidt, R. Steinhagen, J. Uythoven, J. Wenninger, J. Wozniak.

Topics of this meeting:

- Software Interlocking and Control Room Buttons
- Generation and Transmission of Safe Beam Parameters
- Timing System and Interlocks: What happens if Timing stops?
- Management of Critical Settings (postponed)
- AOB

Software Interlocking and Control Room Buttons (J. Wenninger)
J. Wenninger describes the features (and specifics) of the SPS Software Interlock System (SSIS) and presents some requirements for the new Software Interlock System (SIS) scheme that shall replace the legacy SSIS. Depending on its implementation, the system could be used as the future LHC Software Interlock System (SIS) (see slides for details).
The SIS's purpose is to handle more complex and less critical client beam dump requests that cannot directly (or that are not required to) be implemented in hardware. In contrast to sequencers, that performs checks only before any major state change (injection, ramp, squeeze, collision...), the SIS continuously monitors the beam and machine parameters in order to anticipate failures and to give early alarms. The SIS is complementary to and implements similar functionality as the (hardware based) Beam Interlock System (BIS).

In his presentation, **J. Wenninger** focuses on the SPS Software Interlock System that should be replaced in 2006. If carefully designed, the same system would fit the (in comparison to the SPS) less complex LHC usage.
The present SSIS is in use since 1995. In the style of the present SPS SIS, the future (S) SIS will be split into two functional parts: the 'Interlock Generation' and the 'Interlock Core'. The 'Interlock Generation' polls and receives information from the equipment systems and timing system and sends software interlock requests to the 'Interlock Core'. In addition, the 'Interlock Core' receives interlocks from other external users. The requests are transmitted through the technical network using a standard communication protocol. The 'Interlock' core relays these requests and is directly connected to the hardware BIS and the timing system.
Though, in the strict sense, the present SSIS and future SIS are not fail-safe or real-time systems, the expected delays will typically be in the range of a few seconds. **R. Assmann** questions whether 'second-scale' latencies are acceptable for a SIS.
J. Wenninger emphasises that the SIS is meant to captures less critical, slow and more

complex failures. Critical failures are in the scope of the deterministic and much faster hardware based BIS.
Presently the SPS Software 'Interlock Core' comprises a specialised dedicated hardware to interface with the PS, the emergency dump and four (physical) control room switches. Apart from the SSIS only a few other systems (e.g. the vacuum system) link directly to the SPS Emergency Beam Dump. In addition, the SSIS hardware is connected to four physical console switches that stop all beams in the SPS and further injections. As a default, a watchdog in the core hardware will dump the beam automatically if not reset by the software core within about 100 ms. Though this verifies the continuous function of the SSIS software core, it does not guarantee that all clients connected through the network are alive as well. The SSIS can be bypassed by a hardware switch. However, this rather drastic measure is only used only during checkouts at the beginning of the annual startup of the SPS. Normally masking of interlocks is the preferred choice.
Other users interface to this core using the 'SL_EQUIP' software communication library, a predecessor of CMW. The interlock are organised into logical channels that are associated to SPS 'Hadron' or 'MD' beam mode. The interlocks are in addition filtered based on the SPS mode (e.g. 'no beam', 'beam to TED XX', 'beam to target ...') and may be masked by the operators if required. Independent of their masking, interlocks always generate automatically alarms that are kept until the cause for the interlock is solved. Depending on the masking state the alarm message is modified. The list of presently by the the SSIS interlocked channels is found in the appendix.

Presently, the SSIS core hardware module sends two signals, specifying the 'Hadron' and 'MD' SPS beam operation, through a dedicated hardware link back to the PS. These signals are used to inhibit beams from the PS. Due to legacy software issues (use of SL_EQUIP), the use of only two signals for the SPS mode and the 'mode' concept itself, the future SPS operation is limited by the present SSIS and needs to be re-engineered. It is foreseen that the new future SIS should be ready for the CNGS commissioning in May 2006. The system will be developed by **V. Baggiolini** and **J. Wozniak** with input on requirements from **J. Wenninger**.
In order to overcome the limitation of only two signals to the PS for inhibiting SPS injections, a new output channel grouping scheme was evolved in cooperation with CO/HT. The future scheme will in contrast to 'beams' be based on 'geographical zones' (TT40, T41...) using the MTG in order to better exploit the SPS injector chain. The same grouping scheme will be used to connect the SIS directly to the BIC of the corresponding zones.
Since the present SSIS link between SPS and PS allows only two binary signals, the question was raised whether a new dedicated special hardware link should be developed or whether a software link would suffice. At least for the SPS startup in 2006, the SIS will be based on a software based link. Future more permanent solutions have to be evaluated.

In the CCC there will be the following physical switches/buttons for each island (CPS, SPS and LHC) directly connected to the BIS in addition to the software generated interlock requests:

- ‘dump/stop all beam’, connected DIRECTLY to one SPS ring BIC.
- ‘inhibit LSS4 extraction’, connected DIRECTLY to TT40 BIC.
- ‘inhibit LSS6 extraction’, connected DIRECTLY to TT60 BIC.

- One button per beam, connected to the MTG to stop the corresponding beam in the CPS : ALL (?), FT, CNGS, LHC, MD...

For the LHC the following switches are foreseen:

- 'dump beam1', connected DIRECTLY to one LHC ring BIC.
- 'dump beam2', connected DIRECTLY to one LHC ring BIC.
- 'inhibit injection beam2', connected DIRECTLY to injection BIC IR8.
- 'inhibit injection beam1', connected DIRECTLY to injection BIC IR2.

The question was raised followed by a lively discussion, whether it would be preferable to always dump both beams as a default in case of problems. **R. Schmidt** remarks, that it is not yet clear whether in case one beam has to be dumped [or further new injection be inhibited] that the other beam has to be necessarily dumped [/inhibited] as well. The possibility to dump beams individually should be available and be further evaluated.
J.Wenninger points out that these switches/buttons are not safety critical but implement a comfortable and visually secure method to inhibit e.g. further injections.
It was generally agreed that there should be one additional button to dump both beams and it was recommended that this button should be in reach of each console.
Action: B. Puccio
As mentioned above, the present SSIS implements the possibility to bypass all software interlocks.
J.Wenninger inquires whether a ("less drastic") version of the above mentioned physical bypass switch should be reimplemented for the SIS.
J. Wenninger stresses though at the present stage it is early to define a final software architecture of the SIS, one should keep in mind that the system should be designed with users being able to send software interlocks to the system.
There are the following open issues, related to the question how the 'maskability' of signals should be defined and the question how to deal with potential partial data and communication loss and how to establish certain margins.
In order to finalise the architecture of the future SIS a list of potential software interlocks and requirements needs to be established. **ACTION: J.Wenninger, V. Baggiolini, J. Lewis**.

Further it was mentioned that the beam quality checks prior to a LHC injection are not yet sufficiently defined.
ACTION: Injection Working Group.

Generation and Transmission of Safe Beam Parameters (B. Puccio)
In his presentation (see slides), **B. Puccio** gives an update on the transmission of the Safe LHC Parameters (SLP) and its technical realisation. The SLP system transmits information on the LHC energy, 'safe beam' flags, 'beam presence' flag and LHC beam modes to various end users (beam loss monitors, injection kickers, LHC beam interlock system, ...).
It is foreseen to use the general machine timing system as a SLP carrier since it covers the whole LHC and fulfils most of the requirements (e.g. SIL2). The system will transmit the SLP information at a rate of 10 Hz (to be confirmed), which is more than the 1 Hz required. An exception is the 'beam presence' flag (2 bits) that will be distributed at 1 kHz.

According to the present architecture, a Safe Beam Parameter Generator (SBP-Generator) will receive information on the beam energy and beam intensities and evaluates the 'safe beam' and 'beam presence' flags. The two flags are forwarded to the General Timing Generator (CTG) and encoded, among the beam energy and intensity itself, into timing telegrams that are transmitted to the various end users using the timing network. The SBP-Generator receives the same telegrams as a closed loop input, compares the information and may emit an interlock signal in case of inconsistencies between send and received signals, hence intercepting certain global timing system failures.
The SLP will be received by the Safe Beam Parameters Receiver boards that will very similar as the standard timing receivers but with slightly different FPGA programming including a watchdog: In case the required SLP information is not received within a given time or transmission errors, the SLP are set to a fail-safe state in the card. In addition the card will generate an alarm that will be transmitted to the control room for monitoring purposes.
The SBP generation process will be implemented in a dedicated FPGA based hardware. Including the watchdog functionality of the receivers, the expected safety integrity level should be SIL2. The final SIL level including the timing system is presently being verified.
D. Macina asks whether the experiments may use the same receiver cards with the modified programming as well? **R. Schmidt** affirms the request and points out that the users should be aware of the card's default state in case timing is not available.
It was proposed to perform additional cross-checks, for example through the software interlock system, between the energy transmitted through the CTR cards and the software system.

Timing System and Interlocks: What happens if Timing stops? (R. Schmidt)
R. Schmidt contacted several equipments groups and presents preliminary results of his survey on whether and which equipment would be affected by a failure of the timing system and whether this could lead to a fast beam loss. A summary on specific system groups that would be affected can be found in the slides.
The consequence of a timing failure depends on the operation phase of the machine: injection, ramp, squeeze and colliding beams. Without timing it is clear that neither injection nor changes of the machine and equipment state would be possible. Due to dependence on the timing system, it would be impossible to measure or adjust any given machine parameters for the period the timing would be unavailable. As a consequence the feedback loops would halt. All equipment systems have in common that they would suffer diagnostics in case of failures, due to the missing 'post mortem' trigger distribution.
However, the machine protection and its safety do not depend on the timing system!

Though an analysis of the possible effects is important, **J. Lewis** points out that the failure of the timing system is considered to be very rare and by design should by less than once per year.
If required, the SLP system would be able to detect a general timing distribution error and may trigger a hardware beam dump request. The criticality depends on the timescale the unavailability. **Q. King** (e-mail) hence proposes to introduce a 'grace period' of for

instance one minute in order to grant for example the power converter front-end computer the possibility to reboot during operation.
R. Assmann proposes to dump the beam as a default in any case of a timing failure.
R. Schmidt remarks that it is not self-evident that a loss of for example one single timing card would necessarily cause a fast beam loss and that it has to be further evaluated under which condition a timing system failure should yield in a beam dump request.

Further discussion are required. A responsible person is needed to follow up this issue.
ACTION: R. Schmidt

Management of Critical Settings (V. Kain)
Postponed to one of the following MPWG meeting. See slides for more info.

AOB
Preliminary future agendas:

Friday 14th October 2005
- Interlocks from experiments (DM / JW)

Friday 28th October 2005
- Report from the SubWG on Reliability (RF / JU)
-
- Handshake between PIC and QPS for powering electrical circuits – software interlocks (RD, MZ)

Friday 11th November 2005
- Commissioning – next discussion
- RF Frequency interlocking (AB / BG / EC)
- Interlocks and signals from BCT (DB)
- Cryogenics and powering / beam abort (LS)

Friday 25th November 2005
- Ions and protection (JJ et al)
- Closed orbit and protection (RSt)

Other topics:
- BLM – recent experience and results from HERA (BD et al.)
- Beam Dumping System and Injection interlock

LHC action / topic lists
- Interlock reference and tolerances / CO group - LSA project ?
- Extraction septum stability / Inj WG
- Software interlock system / J. Wenninger, R. Giachino , LSA project
- Fast valves
- BTV screens : how do we protect / interlock them SPS + LHC ?
- Interface to the experiments. TOTEM. LHCb VELO..
- Double failures :
  - TDI position & inj. kicker error.
  - Beam dump & TCDQ

SPS actions / topic lists

- SPS beam position interlocks / J. Wenninger
- SPS beam interlock system renovation (partial) for 2006, interlock team, E.Carlier
- SPS safe beam flags

APPENDIX:

List of presently implemented interlock channels in the SPS Software Interlock System (SSIS):

- Main Power Supplies error
- STOPPER MOVING
- DUMP INTLK DISABLED
- RADIATION BB4/5 or TI8/TT41
- Operator request
- Switching AUXPS / ROCS reload
- MD PODH in 4 should be off
- GEF'S EXT.N RELOAD
- W.Extr. (or N.Extr.) Bumper in bad state
- HIGH ENERGY STORAGE
- HIGH INTENSITY ON NORTH TARGET
- EDF CRITICAL PERIOD
- WOBBLE FAULT NORTH
- Injection Interlock Disabled
- EA UNSAFE
- SETTING UP SEM OFFSET TABLE
- SPS VACUUM INTLK. CHAIN BROKEN
- HIGH INTENSITY/HALO ON WEST TARGET
- W ZS in bad state
- MBBT 6202 OUT OF TOLERANCE
- QBM in 6 ON - should be off
- Beam loss ring
- NZS in bad state
- TED TT40
- TED TI8
- TBSE TT41
- TBSE 80243 in bad state or position fault
- WOBSU N/alarm system communication problems
- EXTRACTION INHIBIT CHANNEL DISABLED
- BI-BTV RING or BI-BTV TRANSFER could be IN
- Extraction Sextupole OFF
- ZS GIRDERS in beam
- SCHOTTKY PU in beam
- TIDV water fault.
- TED First Turn in beam
- TED TT60 or TED TT20 in bad state
- ACCESS CHAIN broken
- BHZ 377 in bad state
- COLLIMATORS 1 in bad position or COLLIMATORS STEP 4 in beam
- COLLIMAT & SCRAP 5 in bad position
- SCRAPER 5 ENABLED
- TT10 MAGNETS in bad state
- West MST/MSE or North MST/MSE in bad state
- TT60 MAGNET or TT20 MAGNET in bad state
- P0 Line TAX closed or P0 Line BEND error
- EAST BUMPERS in bad state
- COLDEX LSS4
- MDVW in 5 in bad state
- STOPPER TT20 or STOPPER north IN with TED OUT
- East EXT. GIRDER LSS4 in beam
- MBSG 410 OUT OF TOLERANCE
- TT40 MAGNETS or TT41 MAGNETS or TI8 MAGNETS IN BAD STATE
- EAST MSE IN BAD STATE
- TT40 TOO LOW (or TOO HIGH) INTENSITY
- VACUUM PLATES IN 5 IN BEAM
- MDHW / QSE in 5 in bad state
- MKE MAGNETS LSS4 OVER-TEMP
- 1 or 2 TBSE in with TED TT40 out