Machine Protection Working Group

Minutes of the 40th meeting held on March 18th 2005

Present: J.C. Billy, E. Carlier, B. Dehning, R. Denz, R. Filippini, B. Goddard, G. Guaglio, V. Kain, D. Macina, V. Montabonnet, B. Puccio, R. Schmidt, R. Steinhagen, B. Todd, J. Uythoven, J. Wenninger, C. Zamantzas

Topics of this meeting:

- Dependability issues for the Beam Interlock System
  - interface between BIS and users
  - ideas for redundant VME crate powering
- Update on the machine protection review
- AOB:
  - shared power converters for TI8/CNGS extraction
  - Interlocking of screens
  - Interlocking of TEDs and TBSEs

Follow up to the 39th MPWG meeting:

- The use of fast valves has been rejected until this matter is further discussed (ACTION: J.C. Billy)
- The damage simulation for the Totem experiment should be presented during one of the coming meetings (ACTION: D. Macina)
- The proposed new modified mandate for the MPWG should be distributed for comments (ACTION: J. Wenninger)

Dependability issues for the Beam Interlock System (B. Todd)

note: The term 'dependability' covers safety, maintainability and reliability

- **B. Todd** presents some results of the Failure Modes, Effects and Critically Analysis (FMECA). The FMECA procedure (specified by the MIL-STD-1629 standard) consists of:
  1. breaking the system to be analysed into manageable sub-systems
  2. estimating the MTBF based on the used components of the sub-system. The MTBF estimate calculations are based on operational (maintenance) experiences and by the vendor or other parties supplied recorded lookup tables. Due to long term time dependent effects on the components, there are no other easy and reliable ways to test them experimentally.
  3. evaluating the effect of a single failing sub-system on the total system

  while reviewing possible failure scenarios (e.g. open/short circuit etc.)
- The FMECA of the Beam interlock System user boxes (CIBU) is due to the large number of devices in the LHC (~150) of special importance for the total reliability/failure probability of the BIS-System. His analysis results yield:
  - Removal all or partial redundancy in the CIBU causes a drop to SIL1 or less.

- Two independent user beam permit inputs to the CIBU modules are imperative in order to guarantee a SIL3 reliability of the beam permit signal and may not be locally wired together. Users shouldn't wire together those input loops on their side either. However, the user may short the two permit loop circuits in his device and keep SIL3, if the user can guarantee a SIL3 reliability of his single signal. **B. Todd** points out, using only one input signal, it is unlikely that a user interface can provide a single permit signal for the CIBU that alone fulfils SIL3 requirements.
- The beam permit status due to lack of redundancy for this particular signal in the system cannot be tested before startup. It conforms only with SIL1. In case a safe beam permit status flag is required, more redundancy would need to be added. Another option is to use a redundant information, for example via the control system, to achieve the required safety. Presently the signal is used e.g. by the vacuum system to confirm a (SIL3) beam dump before actually closing the vacuum valves.
- Total failure per year estimates (based on the analysis of ~75% of the system):
  - total failures rate: 2-3 dropouts per year
  - 0-1 failure without impact on the system
  - 0-1 failure during mission causing a beam dump and requesting maintenance
  - 1-2 will fail only requesting maintenance after the end of the current mission
  - probability of a single blind input = 3*10^-2 per year
  - probability of a both inputs being blind = 2*10^-8 per year
  - 1-2 dumps per year will be caused due to failing power supplies of the VME crates housing the BI-Systems (failures rates confirmed with experience of the LEP experiments).

- Conclusions:
  - The transport of the beam permit signal from the CIBU to the BIC is **conform with SIL3** requirement.
  - Two independent inputs are needed in the CIBU to fulfill SIL3 requirement. *Can the users accommodate this? Is it required for all users?*
  - The estimated number of beam dumps per year is acceptable. In case the number of beam dumps due to failing VME power supplies should be reduced, B. Todd suggest to now prepare the option for redundant power supplies in the 16 BICs and to add PS (one per crate) once operation confirm their need.
    - Immediate upgrade costs: 4675 EUR/crate -> 5107 EUR/crate
    - total budget estimate (16 crates): present 75000 EUR -> 82000 EUR (+ 47000 EUR for additional power supplies)
    - An upgrade could be staged: the VME systems would be prepared for a later addition of power supplies. This preparation costs 432 EUR/crate.
    - *Are redundant 11U VME power supply required for other systems as well?*
  - Are there failure modes in the VME powering that could prevent correct operation, but not lead to an automatic beam dump?
  - The beam permit status signal conforms with SIL1 but is unsafe for protection. It was agreed on to keep the present design and to not use the beam permit status flag for safety critical purposes. *Is a SIL2 conform beam permit status required? Can the software interlock system used to capture inconsistent states?*
  - Failures should be categorised and logged during operation.

Update on the machine protection review (R. Schmidt et al)

- dates: 11th to 13th of April 2005
- Invited reviewers: Marc 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).
- R. Schmidt presents the structure and program of the review (see attachment):
  - main blocks:
    - Introduction
    - Beam interlocks and safe LHC parameters
    - Beam dumping system
    - Events leading to beam losses (catalogue of failures)
    - Equipment and beam monitoring connected to the beam interlock
    - System performance
  - The session 'Interlocking' will be switched 'Dumping the Beam'
  - otherwise accepted as is.
- Further information and an updated program can be found under:
  http://lhc-mp-review.web.cern.ch/lhc-mp-review/
- There won't be a separate public announcement but the review is open for everyone. Special bodies will be invited separately (as LTC, MPWG, InjWG, CollWG, ..)
- R. Schmidt asks the speakers to send the abstracts of their talks to coordinators.
- There will be a meeting (to be announced) to prepare and to coordinate the interfaces between the talks.

AOB (J. Wenninger)

- Shared power converters in TI8/CNGS extraction:
  - For the time being the circuits are mechanically switched. An electronic switching is foreseen for 2006.
  - The standard surveillance is based on MUGEF (power converter hardware control) but cannot detect switching errors.
  - Each transfer line as one DCCT for interlock purposes. There are the following options for to survey them:
    1. Surveillance of each DCCT with a reserved MUGEF
    2. Surveillance each DCCT with a fast current decay monitor. The voltage change is not sufficient alone but the absolute current has to be surveyed as well.
    3. Building of a 'low-tech' comparator with moderate precision to cross check with reference setting (preferred).
- Interlocking of screens:
  - The screens are safe for OUT and/or OTR positions.
  - A (maskable) hardware interlock is generated when thick alumina screen is inserted or screen is moving. *Note: command to move the screen is always given in the period of the SPS cycle without beam ("beam-out" segment).*

- Interlocking of TEDs and TBSEs:
  - Proposal of following permit signals, sufficient for protection the machine:
    1. 'TED-in' permit signal only true when TED is IN-BEAM, otherwise false (e.g. OUT, moving, intermediate...). This signal may masks interlocks from devices downstream of the TED.

2. 'TED-not-moving' permit signal only true if TED is IN-BEAM or OUT-BEAM, otherwise false. This signal may be used to inhibit beam upstream of the TED.

- J. Wenninger proposes to use software interlocks to capture inconsistent TED positions.

Next meeting 1. April:

- Summary of the workshop on beam generated heat deposition and quench levels
- Possible staging of the BLM system

R. Steinhagen, 24 march 2005