Machine Protection Working Group

Minutes of the 11th meeting held on March 8th 2002

Present: F. Balda, J.C. Billy, F. Bordry, E. Carlier, E. Ciapala, B. Dehning, R. Denz, E. Gschwendtner, B. Jeanneret, G. Mugnai, B. Puccio, R. Schmidt, A. Vergara, J. Wenninger

Excused : F. Bordry, B. Camanzi

Main topics of this meeting:

- Reliability assessment of the SPS access system (F. Balda)
- Report from the Accelerator Reliability Workshop (A. Vergara)
- Abort gap monitor (B. Dehning)
- AOB :
  - Cable requests (R. Schmidt)
  - LHC filling patterns (J. Wenninger)

Reliability assessment of the SPS access system (F. Balda)

F. Balda presented his reliability study of one SPS access system safety function. The aim of the exercise was to use the new RAMS software and to perform a risk analysis of the system now that the SPS falls under INB regulation. The analysis concerns one key safety function : send an inhibit to the SPS machine equipment involved in personnel protection when a door is forced in ECX5. Two redundant interlock signals from the door are sent over a local and a central PLC to the master PLC in the control room. The veto signal is then send back to the equipment, again over 2 PLCs. The goal of the study was to learn more about availability, SIL and risk assessment. The analysis was made in conformity with the IEC 61508 norm. The first step consisted in collecting the data on all the components involved in the function. Secondly the Fault Tree was build, and finally an Event Tree analysis (together with a Fault Tree Linking) was made. The mission time of the system was assumed to be 9 months, the system being "as good as new" after the maintenance during a shutdown period. The only inspection during the mission time is a check of the local PLC CPUs every 10 minutes. Other components (including the central and master PLCs) are not checked. The likelihood of breaking through a door is roughly once per year, i.e. 'probable' (according to the *Frequency Table* approved by the Access Interlock Working Group). Since there are 15 access points in the SPS, the probability to force the door at ECX5 is 1/15 per year, which is considered to be 'occasional'. The consequences range from a high radiation dose to death within hours or days if the beam is lost in the vicinity. The later consequence is considered to be 'catastrophic'.

The result of the analysis shows that the availability of the system for this function is 93% at the end of the Mission Time, corresponding to SIL1 according to IEC 61508. In other words, if one forces this door, there is a 7% chance that the system does not react and that no inhibition signal is sent to the concerned EIS-beam. Note that this number is valid at the end of the Mission Time. After 3 months, for instance, the probability is less than 2.5%. This probability must be 2 orders of magnitude lower to be classified as SIL3. Such an improvement can be achieved for instance by reducing all components' unavailability by about a factor 100 without changing the architecture. The risk class of this function is II, i.e. 'tolerable risk', according to the Risk Matrix approved by the AIWG. For the SPS access system as a whole, i.e. considering all access points and assuming that the architecture is the same, the risk class would be I, i.e. 'intolerable risk'.

An "important analysis" was performed to find out the most critical components. To improve the system, a first possibility is to simply duplicate it. This improves the availability to 99.5%, corresponding to SIL2 and Risk Class II ('tolerable'). Obviously this is an expensive solution for a moderate improvement. A second option is to work only on critical components. By doubling a number of relays, checking all PLC CPUs and junction boxes, improving the maintenance and doubling the PLC Output modules, it is possible to obtain an availability of 99.93% corresponding to SIL3 and Risk Class III ('acceptable'). This is clearly better and much cheaper.

F. Balda's conclusion is :

- Although it is well designed and supposed to be fail-safe, the SPS access system has a 7% chance of failure on demand at the end of its 9 month Mission Time.
- The importance analysis is crucial to improve the systems.
- The analysis should be done systematically for all functions of the SPS access system and for critical LHC systems.
- The RAMS software performs well.

In the discussion **F. Balda** explained that this work took him approximately 2-3 months, essentially to find the suitable data and the build the architecture of the system.

Report from the Accelerator Reliability Workshop (A. Vergara)

A workshop on accelerator reliability took place between February 4th and 6th 2002 in Grenoble. **R. Schmidt** was supposed to make a presentation on the LHC, but since he could not attend the workshop, **A. Vergara** kindly agreed to give the presentation. In the meeting **A. Vergara** gave a summary on the main topics of the workshop. With the exception of LHC, only smaller accelerators were represented. The workshop focused on accelerator and sub-component reliability as well as some general issues. Among the accelerator sub-components, powering and RF are generally viewed as being the most critical systems in terms of reliability and downtime. For many accelerators the focus of the 60's and 70's to achieve mainly higher energies and currents has now shifted towards high reliability. An often debated question concerns the design of a reliable accelerator : should it be very safe but rigid or more flexible at the risk of a reduced reliability ? Reliability in operation was a very important part of the workshop, and many machines presented data on availability and on their weakest parts (powering, RF, water cooling). Schemes to improve the reliability include product assurance and a well organized and supervised preventive maintenance, using EDH-type system to control and track access and repair.

During the discussion **G. Mugnai** and **J. Wenninger** mentioned that at LEP the super-conducting low-beta quadrupoles quenched frequenctly during the last 3 years of LEP operation. **R. Schmidt** proposed to have a presentation on this topic in one of the next meetings.

Abort gap monitor (B. Dehning)

A list of requirements for the abort gap monitor was presented by **B. Dehning**. The key parameters and requirements are :

- The time interval to monitor is 3 μs long.
- The energy ranges from 450 GeV to 7 TeV.
- The synchronization signal for the gap monitor should be derived from the signal generated by the RF system and used by the dump system, to ensure optimum reliability.
- The sensitivity of the monitor must still be studied. It depends on the amount of beam deposition that is acceptable for the collimation system and for the TCDQ (the absorber block which must protect the Q4 quadrupole in IR6 in case of asynchronous dumps) when a beam with (partially) filled abort gap is dumped. A rough preliminary estimate places the sensitivity in the range of 10^9 protons. More precise evaluations are required.
- The update time of the measurements should be approximately 10 ms (possibly even more), a number that came out of the discussion. **B. Dehning** suggested 1 turn, but that does not seem necessary since the time constants to fill the gap are quite long. **E. Ciapala** mentioned that **E. Chapochnikova** has estimated the time to fill the gap when the RF is off to ~ 7 seconds at injection and ~ 20 seconds at top energy (see LHC Note 281, not yet published). Similar time estimates were also given by **O. Bruning**. Furthermore, when the gap is filled during a bad injection, there is no need to obtain this information one turn later.
- Maximum intensity range is $120 \times 1.7 \times 10^{11}$ (gap completely filled with ultimate intensity bunches).
- The accuracy should be ~ 10%.
- The MTBF should be 20 years.
- The monitor must be 100% available during machine operation.

B. Jeanneret commented that an injection into the abort gap should be a rare event and that the normal BCT could be used to determine more precisely the currents in the gap in case of an incident. It is therefore not required to measure up to the highest possible intensity, an opinion shared with other people in the room. Candidates for such monitor considered by the SL-BI group are a BCT and photon counting. **E. Ciapala** said that another instrument could be based on a detection of the 400 MHz structure of the beam in the gap. Some studies of such a device in the SPS have been proposed. The possibility of cleaning the abort gap with the transverse damper as it has been proposed some time ago was mentioned. **B. Jeanneret** raised the question of the longitudinal lifetime in the LHC, which should be evaluated to obtain an estimate for the abort gap population.

It is proposed that that requirements for the monitor would be further discussed in the MPWG. The final specification for such monitor would be done in collaboration with the BI-SPEC team, and therefore the colleagues of BI-SPEC should be kept informed.

Actions and topics for future meetings :

- Abort gap cleaning with the damper (**SL-HRF**).
- Status and intensities intercepted by the TCDQ (**SL-BT, B. Goddard**).
- Evaluation of longitudinal losses (**SL-HRF**).
- Evaluation of possible instrumentation for the abort gap intensity monitoring (**SL-BI**).

AOB

R. Schmidt recalled that in about one weeks time every cable in the LHC tunnel should be announced. And if the cable is not known precisely, one should at least give an estimate in order to reserve space. **B. Puccio** and **R. Schmidt** are going through the groups to sort out the number and type of cables for the interlocks.

J. Wenninger informed the WG members that during a discussion on SPS-LHC synchronization (in the framework of SPS interlocks), a possible solution to the problem of beam injection into the abort gap was found, see also the presentation of **E. Carlier** at the previous MPWG meeting. Protection of the abort gap by gating off the injection kicker becomes much simpler if the filling pattern is changed such that the last SPS extraction consists of 4 PS batches. The present filling pattern, see the figure below, is :

334 ⊕ 334 ⊕ 334 ⊕ 333 ⊕ abort_gap

where '3(4)' represents 3(4) PS batches. The proposed filling pattern is :

334 ⊕ 334 ⊕ 334 ⊕ abort_gap ⊕ 333

A movement of the abort gap position has consequences on the collision schedule and on parasitic beam-beam effects. **W. Herr** (**SL-AP**) pointed out that the symmetry around IR1 and IR5 is a very important constraint. This symmetry is maintained with the proposed scheme, but further detailed studies are required. **P. Collier** remarked that with ions, the filling scheme would be again different, so some flexibility is required. It is also possible that the proton filling scheme is modified. **J. Wenninger** will follow up this point

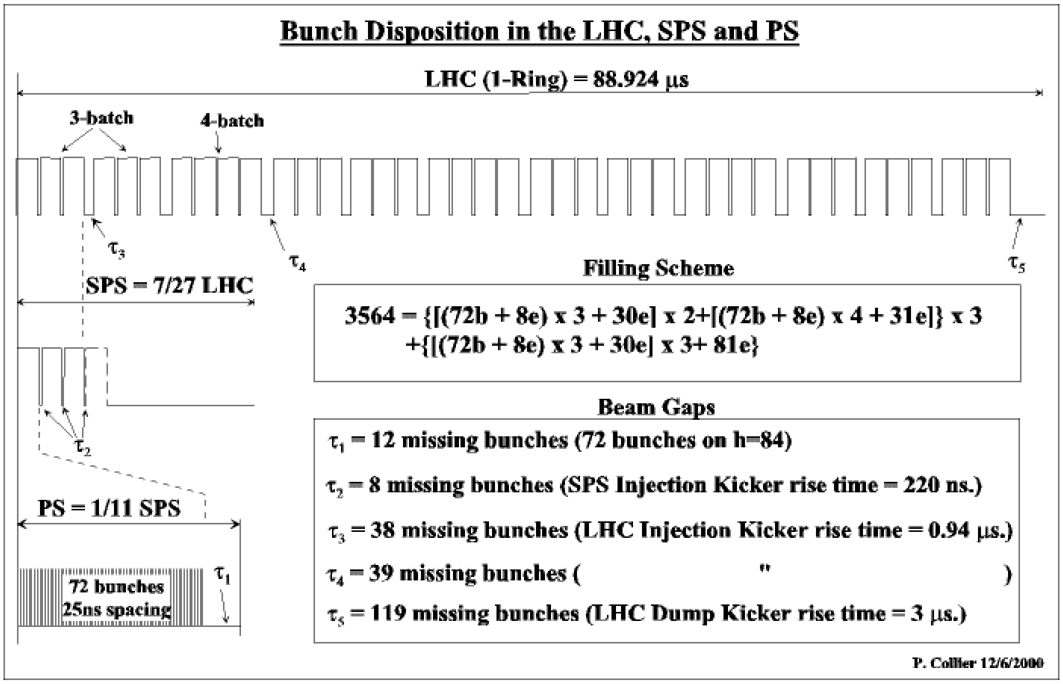

Figure : the present nominal filling pattern for proton operation.