MPP meeting 4 March 2011

Original agenda:

```
- SMP 3v0 - Introduction (B. Todd).
- Hardware – Dependable Design (M. Kwiatkowski).
- Testing and Testers – The “V” Approach (S. Gabourin) + input from A. Garcia.
- Software – FESA, RBAC, MCS, GUI (I. Romera) + demonstration by M. Audrain.
- Status and Future Plans (I. Romera).
```

Present:

P.Alvarez (BE/CO), M.Audrain (TE/MPE), D.Belohrad (BE/BI), J.Blanco (TE/MPE), B.Dehning (BE/BI), M.Deile (PH/TOT), M.Ferro-Luzzi(PH/LBD), A.Garcia (TE/MPE), M.Guthoff (PH/CMX), R.Jacobsson (PH/LHCB), E.Nebot (BE/BI), P.Nouvel (TE/MPE), G.Papotti (BE/OP), C.Parkes (PH/LBD), B.Puccio (TE/MPE), I.Romera (TE/MPE), M.Sapinski (BE/BI), R.Schmidt (TE/MPE), J.Serrano (BE/CO), A.Siemko (TE/MPE), N.trofimov (TE/MPE), S.Wagner (TE/MPE), S.Wenig (PH/ATLAS), J.Wenninger (BE/OP), C.Zamantzas (BE/BI), M.Zerlauth (TE/MPE).

Minutes:

Special meeting of the MPP dedicated to the Safe Machine Parameters (SMP) system showing all the different aspects of the project from the conceptual ideas behind it to the realization, testing and software involved.

SMP 3v0 – Introduction (Benjamin Todd)

Ben presented the main concepts of the SMP system: fast, safe, reliable and available. He explained the two different ways used to transmit the generated flags and values, either through direct transmission (hardware link <ms delay) used for extraction interlocks or broadcast transmission through timing network for other users (example of protection system users are Beam interlock System, Collimation, Beam Loss Monitors amongst others). **David** asked how reliable the timing transmission is. **Ben** replied

that non critical systems can rely on software to extract the data but critical users must use dedicated timing receiver hardware in order to avoid any misinterpretation of the information.

Ben explained the different input flags and values received for both the SPS and LHC systems. He detailed how they are processed and later transmitted to the different clients. **Rüdiger** asked how the crosscheck of the energy value in the SMP LHC is implemented. **Ben** explained that for the moment it is done in software but it is foreseen to be implemented in hardware. **Jörg** remarked that, for the moment, the SIS reads the dipole current (LHC energy) from the eight different sectors and also the values from all BLM crates checking that all are coherent. If an inconsistency is detected a beam dump is triggered. **Jörg** commented that the Beam-1 and Beam-2 energy tracking systems are sending slightly different values of energy to the LHC SMP. They differ by around 1.5GeV due to the different field errors models used for the calculation, as the SMP uses a voting logic, it is possible to have steps of 1.5GeV in the energy value received by user systems. **Jörg** explained that the SIS also reads and sends beta* using the same principle. The SIS will be also connected to the LBDS to read information. **Jörg** also clarified that only authorised people (Rüdiger, Markus, Verena and himself) can modify critical parameters such as the Operator Probe Beam Limit.

Andrej asked how the Setup Beam Flag limit is to be switched from NORMAL to ION. **Ben** answered that it is done manually but the property is protected by RBAC (same access map as Operator Probe Beam Limit). **Rüdiger** commented that for the RELAXED and VERY RELAXED equations there is also a timeout (around 4h30m) that happens even with circulating beam. **Stefano** pointed that the timeout is a bit tight for collimation setup. **Markus** asked if it is possible to change the timeout. **Ben** explained that the timeout value is implemented in hardware in the VHDL critical part.

Ben stressed that Probe Beam Flag and the Setup Beam Flag are generated 1s before the extraction and the value is held during 2s after the extraction. In case that the timing event doesn't arrive then the extraction will be missed.

Ben introduced the CISX card as a dependable and flexible solution used in the SMP. It behaves as the CISR, CISGL, CISGS or CISA depending of the firmware (VHDL).

Hardware – Dependable Design (Maciej Kwiatkowski)

Maciej presented the design flow followed on the SMP project which is based on 5 main steps: specification, implementation, simulation, hardware testing and code reviews. He explained how based on the system requirements critical and non-critical parts are identified at the specification level. He said that he will focus only on the implementation of the critical parts. The specification is later formalized using predicate logic language and all critical functions are verified for completeness and consistency. Each function is implemented in VHDL and tested independently in software simulation and optionally using dedicated hardware tester. Finally, the system is assembled in the hierarchical design and tested in software simulation. Software simulation either of the function or of the system requires writing software test-benches which specify the simulation procedure by generating input stimulus and verifying the device model response. The simulation tool examines code coverage by checking if all the lines of code and all the branches were executed, all the expressions and conditions were verified. Full code coverage is the goal, to be sure that all functions work correctly. The final step of testing is the hardware tester for the complete system which is obligatory. In hardware testers embedded logic analyzers can be used, these are provided by FPGA vendors. Maciej said that the concept of the software simulation and hardware testing is similar but in both cases there are some advantages that make them complementary. Software simulation allows precise source code tracing and can verify code coverage on the other hand hardware testing works in real time and allows real distortions to be introduced. In summary Maciej reiterated the most important steps in the dependable PLD design which are formalization, splitting and minimizing critical functions, exhaustive code simulation and hardware testing.

Bernd asked how the procedure for HW testing is defined. **Maciej** answered that it is similar to the software simulation but using real hardware. The CISX card is re-programmed with a dedicated firmware often using embedded logic analyzer which monitors and records the data inside the FPGA that is lately retrieved via JTAG connection to a PC.

David asked why predicable language is used in between the specification and VHDL and why it is used when VHDL is predicable de facto. **Maciej, Ben and Markus** explained that predicable language is simpler than VHDL therefore it can be understood for non-expert people. It helps to find any mistake in the early stages of the design and using software tools allows the completeness of the specification to be checked. **Ben** stressed that predicate logic is one of many tools to help find issues, and that it has identified problems much earlier in the design cycle than previous projects. The use of such logic does not remove the need for testing.

David asked what happens when the power PC hangs and the system needs to be rebooted. **Ben** commented that the SMP follows the same approach as the BIS, in which all the cards are interconnected by private communication links and hence they don't depend on the PPC to work. In addition there is no connection from the cards to the VME System Reset pin, so the cards are not even aware that a reset is ongoing.

Bernd asked how the tests are defined. **Ben** explained that the software block tests are defined by the engineer that designed them. The system block tests are defined by **Amanda** based on the English specification. **Maciej** pointed out that the hardware testing phase is not only internal to the FPGA but sometimes additional hardware is used (other CISX, fiber attenuators…).

Testing and Testers – The "V" Approach (S. Gabourin) + input from A. Garcia.

Stephane presented the "V" approach followed in the SMP design. Two independent teams developed the SMP controller and the SMP tester according to the specification of the system. In this way the SMP controller is validated against the SMP tester and against specification. **Stephane** explained that the tester is composed of a LabVIEW program made by **Amanda** and a VME crate which sends and receives signals to and from the SMP controller. The tester checks the functionality of the SMP controller. It reads stimulus, which are needed to verify a certain functionality of the controller from an Excel file which contains all possible test combinations. It's possible to choose in this file which tests have to be done. The tester writes the output and a detailed description of the test results and steps in both Excel and text files. **Markus** asked how many different energy variations are tested. **Stephane** answered that for the case of the Probe beam flag three random intensities are tested for both input intensities A and B (then 9 combinations in total): one over the limit, one on the limit and one below the limit. The random intensities change on every test. No negative intensities are tested as the numbers are defined as 16-bits unsigned. **Bernd** asked whether all the boards are tested. **Stephane** confirmed that every board which is installed is subject to complete testing.

Software – FESA, RBAC, MCS, GUI (I. Romera) + demonstration by M. Audrain.

Ivan presented the FESA class that interfaces the SMP with the GUI and how it is configured. He explained how the different properties of the class are accessed and what roles (RBAC) are required. Finally he presented the concepts of operational checks performed in three stages: before, during and after operation (PreOp, DIAMON and Post-Mortem).

Ivan commented that there is no active communication between the database and the frontend. The database has a description of the different boards in the frontend that is used to configure the FESA class.

Jörg explained that there are some properties (Ex. SqueezingFactorLimits) that are protected by the Machine Critical Settings. Only Machine Protection Experts can provide the digital signature needed to modify the values although Operators can re-write existing values.

Maxime presented the two main parts of the SMP Graphical User Interface. The first part concerned the overview frame made for operators to monitor general parameters and set commands to the controllers. The second part described the detailed frame, allowing experts to easily diagnosis and monitor SMP hardware in detail.

Status and Future Plans (I. Romera)

Ivan presented the plans for the SMP project for the current year. He commented that during the first half of the year the documentation is to be completed, a study concerning the BCT intensity acquisition is to be launched and some minor issues in the monitoring and diagnostics are to be solved. For the second half of the year the Pre-Operation checks, DIAMON and Post-Mortem tools should pass from beta to release. The cross-check is to be implemented in hardware. And an in-house replacement is to be studies will be implemented for the substitution of the CTG-CTDLT and the CISV-CTDAD cards.

Ivan commented that the DIAMON tool monitors the infrastructure issues; it comes with basic agents but more specific tests can be implemented/customized (Ex: email or SMS notification). **Ivan** pointed that every second all the new data retrieved from the SMP cards is stored in the logging DB.

Siegfried asked how is possible to send fake data. **Ben** replied that according to the specification it is now possible to fake data but for commissioning purposes there is one card that does it. This card is store in his office. **Jörg** added that in case the energy is faked with beam in the machine the SIS will dump the beam. **Ben** also clarified that the fake data card has a fail-safe mechanism rendering it useless for operation.

Bruno commented that the experiments will have to be redundant for the Stable beam flag (2 flags). **Ben** said that there is no space for additional bits on the telegrams because all 32 available telegrams are full. **Richard** added that the experiments should retransmit what they receive back to the SMP as a kind of cross-check.

In closing **Ben** proposed a review of the BCT and its interface with the machine protection system. "The SMP is as safe as the information it gets". **Rüdiger** commented that an intensity measurement for the machine protection system does not necessarily need to be precise, but it must be very dependable.