RAS Working Group meeting 28.10.2021

Participants: A. Apollonio, P. Bell, M. Bernardini, M. Blaszkiewicz, M. Brucoli, T. Cartier-Michaud, M. Chiotelli, G. Daniluk, L. Felsberger, B. Fernandez Adiego, G. Iadarola, P. Jurcso, M. Kalinowski, I. Lopez, N. Magnin, E. Mahner, C. Obermair, S. Ramberger, J. Uythoven, V. Schramm, B. Todd, N. Trikoupis, W. Viganò, F. Waldhauser

The slides are available on Indico:

https://indico.cern.ch/event/1089769/

A. Apollonio welcomed the audience to the 2nd new-format RASWG meeting. He presented the minutes of the last meeting and introduced today's speaker. There were no questions nor comments about the previous meeting and minutes.

HL-LHC Energy Extraction Systems Reliability Study - Speaker: Milosz Robert Blaszkiewicz

M. Blaszkiewicz presented the reliability study of the new HL-LHC Energy Extraction (EE) systems. The purpose of the EE systems is to extract the stored energy of the superconducting magnet circuits through dedicated EE resistors to protect the HL-LHC against quench-induced damage. Energy Extraction is triggered by a fast power abort request sent by the Quench Protection System and the Powering Interlock Controller. For the new HL-LHC system a new switching technology is introduced using vacuum switches (see Slide 4). The aim of the study has been to 1) establish the system reliability requirements, 2) develop a system reliability model and to 3) evaluate the system's compliance with the derived reliability target.

In brief, the main aspect of the design of the HL-LHC EE systems is the implementation of full redundancy both on the higher system level through duplication of entire hardware modules (Cassette 1 and 2), and on the lower levels for instance by multiplying the diodes and thyristors on the component level, see slide 9. M. Blaszkiewicz outlined that there is no single point of failure in the system, the duplication starts at the input of the high-level control chassis at the signal from the Quench Detection System. The design also implements a variety of monitoring capabilities and has followed a fail-safe approach. For example, a hardware link has been added between the FPGAs of the redundant cassettes, enabling them to identify potential fault states of one or the other FPGA and to perform actions. Other monitoring is performed in two ways: in an active way to detect potential failures and act immediately, as well as passively by processing the Post-Mortem information and behaviour. An example of the fail-safe approach is the ability of the system to react to a sudden loss of the powering, using redundant sources and a power switch, see slide 9. In the case of a failure in the supplies, the system uses charge stored in local capacitors to open the vacuum interrupter and perform an energy extraction.

Slide 19: J. Uythoven asked whether the “Mean Time To Energy Extraction” (i.e. the mean time between consecutive demands for the system to be activated upon detection of a quench) applies to a single system or to all of the around 80 systems. M. Blaszkiewicz replied that the plots present the data for a single system. J. Uythoven said that a Mean Time To EE may in reality be well beyond one year for some magnets and that it would make sense to extend these simulations to a Mean Time To EE of 3 years. A. Apollonio replied that depending on the circuit and the operating conditions of the machine, the system can receive a fast power abort much more frequently than once every 3 years, especially during hardware commissioning. For the inspection interval of 1 year, the probability of failure of the simulated blue data decreases thanks to periodic inspection. A similar behaviour can be expected for an inspection interval of 3 years, so A. Apollonio agreed that the simulation could be extended to account for this effect. The main takeaway from this graph is that even with a 3 years inspection period the reliability targets are met.

Slide 14: M. Blaszkiewicz pointed out that the spring of the vacuum interrupter has been considered as fail-safe, which is the reason its failure rate has not been modelled in the main presented results. Other potential non-safe failure modes of the spring have been extensively discussed. A conservative analysis based on the assumption that the spring would not be fail-safe was also carried out, but was left in the spare slides for documentation.

Questions and Discussion after the Presentation:

W. Viganò asked about the indicated rack temperature of 45°C (slide 9), while it seems that the MIL-HDBK-217F calculation has been performed with 25°C (slide 11). M. Blaszkiewicz replied that the 45°C are the absolute maximum for operational conditions, while 25°C has been used for non-operating conditions. In fact, the indication of 25°C on slide 11 is to be updated.

W. Viganò asked why the MIL-HDBK-217F has been used to which M. Blaszkiewicz replied that the approach taken was of hybrid nature, based on the failure rate sources available for the different components. A. Apollonio added that it is related to the course the study took. It started as a block level analysis, after which the granularity was increased, which partly led to this hybrid model. He also pointed out that it is never easy to find reliability data for the various components, but a conservative approach has always been used. Finally, the system is to be properly tested for the final proof.

W. Viganò pointed out that the data sheet reliability data may not include stress conditions and asked how this is handled. A. Apollonio explained that the data found in data sheets is in some case the best source of information. It is at least a good starting point, to be then confirmed with dedicated tests.

W. Viganò asked whether production testing has been considered. He especially pointed out the problem of common cause failures for using the same components in a redundant configuration. It is possible to have a blind failure of redundant components failing at the same time. In the future such failures can be considered. A. Apollonio replied that this is an excellent intro to the next RASWG presentation about production of electronic systems. Common cause failures due to similar defects during production were not considered in the analysis.

W. Viganò asked if it is possible to use the outcome of the study to organise the piquet service and maintenance at CERN. He asked if the repair times can be estimated and if this can be used to organise the teams. A. Apollonio replied that indeed a practical outcome of the study is the definition of inspection intervals. J. Uythoven added that the system should be tested every year and that the estimations on slide 19 should be extended up to 3 years. This data can enable us to optimise the inspection or maintenance strategy.

B. Todd asked how the system behaves if either of the vacuum interrupters opens. M. Blaszkiewicz replied that this could be studied in the future and that the current study only focussed on the vacuum interrupter failing to open when it is needed.

B. Todd asked how many times the vacuum interrupters open by accident. A. Apollonio explained that this can happen for the LHC EE, but that for this new vacuum technology this data is not yet available.

B. Todd asked how the system is turned on and whether there could be an inconsistency for a short moment in time regarding the vacuum interrupters? Follow up: This should be checked with the expert.

B. Todd asked about potential mechanical wear out of the vacuum interrupters. M. Blaszkiewicz explained that this was not an issue, as the number of activations was much smaller than the specified number of activations. J. Uythoven wondered whether the “use profile” was compatible with manufacturer numbers, if the interrupters are not used in the same time scales as the manufacturer calculated. For example, they are activated once a year, and the manufacturer is expecting it to be at a different rate.

B. Todd pointed out that the FPGA failure rate is not only composed of random failures in time accounting for the hardware, but also characterised by the configuration. Another metric may be needed to estimate the combined failure rate.

B. Todd asked about the failure modes and failure rate of a resistor bank. M. Blaszkiewicz replied that the resistor banks are not included in the model. A. Apollonio added that it’s generally difficult to get good failure data when interfacing with system experts. He points out that in such applications resistors generally don’t fail. B. Todd raised the point of what happens when the resistors fail by changing their resistance values, which on smaller resistors is a recorded failure mode. He also points out that for the EE resistors an operation of several decades is to be considered.

J. Uythoven added to that the point of the vacuum switches potentially failing. They usually switch at a rather high rate. A. Apollonio replied that the vacuum switches were tested for 20k cycles which covers the number of switching cycles foreseen for their lifetime. Discussing with B. Todd, J. Uythoven also pointed out that from an operational point of view and in terms of repeatability, it is better to open and close the switches every now and then, rather than relying on them switching after a long inactive period. B. Todd agreed.