229th Meeting of the Machine Protection Panel

LHC topics

July 15th, 2022, via Zoom

Participants:
C. Accettura (EN-MME), E. Blanco Vinuela (BE-ICS), A. Butterworth (SY-RF), R. Calaga (SY-RF), G. Daniluk (BE-CEM), S. Fargier (BE-CEM), B. Fernandez Adiego (BE-ICS), P. Fessia (ATS-DO), C. Hernalsteens (TE-MPE), A. Herty (BE-GM), D. Jacquet (BE-OP), A. Masi (BE-CEM), F. Moortgat (EP-CMG), D. Nisbet (SY-EPC), M. Noir (BE-GM), F. Nuiry (SY-STI), B. Petersen (EP-ADT), B. Schofield (BE-ICS), A. Siemko (TE--), P. Sollander (BE-ICS), E. Soria (BE-CEM), M. Sosin (BE-GM), M. Trzebinski (EP-UAT), J. Uythoven (TE-MPE), C. Wiesner (TE-MPE), D. Wollmann (TE-MPE).

The slides of all presentations can be found on the website of the Machine Protection Panel and on Indico (229th meeting).

Minutes and actions from the 226th (LHC topics)

The minutes from the last MPP meeting were not available at the time. Daniel recalled the actions and mentioned that the direct dump BLM test is on-going and that the DOROS BPM interlocks in IR7 are still masked in SIS.

Introduction to full remote alignment system and initial study of FRAS operation failure modes (Mateusz Sosin)

Mateusz first introduced the Full Remote Alignment System (FRAS). The main functionalities and impact analysis was started in September 2019 and summarized in FRAS functional specification (EDMS-2166298). The scope of the FRAS control system was defined in March 2022 (EDMS-2589302). The FRAS safety assessment and proposed compensatory measured (EDMS-2592013, EDMS-2727128) followed and include the study of the FRAS failure modes, the proposition of FRAS control system safety measures. It was presented at the RASWG. The following FRAS stakeholder meetings gathered feedbacks and comments on the proposed safety measured. A complete failure mode analysis was performed and will be presented today.

The main aspects of the risk assessment and protection layers are summarized in EDMS-2727128 (see next presentation).

The FRAS will be implemented between Q1 and Q5 of the HL insertions in points 1 and 5. The components of the new layout are classified in three categories: the remotely aligned components (Q1, Q2A, Q2B, Q3, CP, D1, TAXN, TCTs, D2, CCs, TCMB, Q4 and Q5), the components that are never realigned after the initial alignment and the components aligned during YETS, LS and which are “FRAS compatible”.

The FRAS will allow to align rigidly and remotely all FRAS components from Q1 to Q5 on both sides of the IP within a range of +/- 2.5 mm. Also, each component will be allowed to move independently within the stroke of the corresponding bellows. The FRAS will provide an important reduction of the radiation dose taken by surveyors, a reduction in the mechanical misalignment, allowing to decrease the required correctors strength and a gain in aperture. The FRAS will be used during the TS as a machine requalification will be required after each movement. Small machine movements (order of 100 μm) could be allowed without requalification during the operation of a pilot beam. The target absolute position of the components reaches an accuracy of 0.15 mm and the relative position of neighboring components will be within 10 μm.

The FRAS LSS components will be equipped with reference sensors (Wire Position Sensor (WPS) (radial and vertical position regarding a wire), Hydrostatic Levelling Sensor (HLS) (vertical position and roll of component, using equipotential water surface as reference), inclinometer (roll for the IT, TAXN, collimators, CCs and TCLM) and longitudinal and UPS gallery long range monitoring. Each component is also equipped with motorized adapters, for the remote adjustment of its position.

The FRAS motion control system and its software are studied as a generic solution to cope with the requirements of the different WPs responsible for the components to be included in the FRAS.

Two technologies of micrometric sensors will be used, with capacitive technology (WPS sensors and inclinometers) and with frequency scanning interferometry technology (HLS sensors, inclinometers and distance measurements). The real time data acquisition will use FESA. A SCADA and DB interface will be provided via WIN CC OA. Only passive components will be located in high radiation areas. In addition, the jacks' motorized adapters position will be measured with resolvers (in absolute). Multiple sensors and technologies are used, providing redundancy of systems and measurement data.

Mateusz then discussed the motorized adapters and the main assumptions for their operation. The speed of the different axes will be limited by the measurement time of the protection layers with a maximum speed at 20 μm/s. There is no constraint on the displacement time on all the degrees of freedom. The maximum displacement in a single step is 0.5 mm. Before executing a motion command, its step size will be validated with regards to the bellows' deformation capabilities.

It was commented that the inclusion of a second WPS wire between Q1 and D1 is not currently in the baseline. Daniel asked if there is a specific challenge regarding the integration of the second wire. Paolo replied that it is a big challenge and that it is part of the design of the cryogenic line.

The sensor cables of the WPS sensors cannot be connected to the collimators HYPERTAC patch panels as the cables are calibrated together with the sensors and electronics.

Introduction to FRAS operation scenarios and outcome of the Failure Mode and Effect Analysis (FMEA)

Four main operation scenarios are considered:

- *Remote alignment* mode (no beam) where FRAS can perform the alignment (no personnel in the tunnel)
- *Maintenance* (no beam and personnel close to the machine) where FRAS can perform the alignment with only expert personnel presence allowed in the tunnel
- *Pilot beam* where FRAS can perform small alignment in order of 100 μm displacements. Only on special request from OP.
- *High-intensity beams*: where FRAS cannot perform any alignments and where motion is disabled.

The main consequence risk for personnel if present if the ODH hazard due to helium leakage. FRAS experts would be considered differently regarding that risk.

The following failure modes have been identified for FRAS (see EDMS-2727128):

1. Exceeding the bellow limits (for vertical, horizontal and rotational displacements) causing damage of interconnection bellows
2. FRAS power cut (FRAS unpowered)
3. Magnet drop due to the mechanical issue with the jack
4. Component position change due to quench
5. Any displacement of FRAS with high-intensity beams.

The main consequences of these failure modes for the LHC machine are the damage of the interconnecting bellows and the damage of components when high-intensity beam is circulating in the machine.

Daniel commented that the triplet areas are usually not accessible when there is helium in the triplets, how does this work for the FRAS experts? Mateusz replied that one needs to have the "cryo lockout" permit. The same rule will be followed in the case of FRAS access.

Daniel asked what would happen to the readings of the resolver measurements in case of FRAS power cut. Mateusz replied that the resolvers are integrated in a way to provide absolute position reading.

The bellows are considered as components most sensitive to alignment activities as they might be damaged if their limits are violated. If such a failure occurs, it will be catastrophic (loss of vacuum and helium spill) and the repair of a bellow collapse might cause several months of machine stop. The bellows are assumed to not be extensively deformed during their lifetime and their deformations must be followed-up and interlocked if limits are reached. This is one of the main functions of the FRAS. The safety analysis on bellow damage found that mechanical stops or limit switches within the jacks are insufficient to mitigate the risk of bellow damage. The tracking of the position of the components extremity is required and the precision of the tracking system must be below 100 μm. Solution of three redundant protection layers, based on different technologies of sensors are proposed as generic safety solution. (see next presentation).

In case of interest to add additional (non-generic) protection features, proposed by an equipment owner, such an option could be integrated to FRAS as a nonstandard interlock.

The HL-LHC components can be damaged if not properly aligned when a high-intensity beam is circulating. The strategy is to disable the FRAS motor while having high-intensity beams

and to check before injection the beam that the HL-LHC components are properly aligned. A mechanical key located in the CCC will disable the FRAS motors while high-intensity beam is injected and at the same time will send a signal to the BIS to dump the beam if the FRAS motors are not disabled. An interlock signal produced by FRAS to inhibit the injection of high-intensity beam into the LHC when misalignment between components is above limits.

Jan commented that this could be rephrased to state clearly that the default situation has unpowered motors. In case they are powered, a beam interlock would be generated, which can only be masked with safe beam. Mateusz confirmed that this is the foreseen baseline configuration anyway.

Daniel asked about the bellow protection mechanism calculating the position of the components using redundant sensors, and if it is foreseen to provide hardware experts with a visualization of the state of each below. Mateusz replied that this capability is foreseen. In addition, all calculated positions and below deformation results will be logged in NXCALS.

FRAS risk analysis and risk mitigation using protection layers according to the IEC61511 standard (Borja Fernandez Adiego)

Borja summarized the context of the risk analysis by re-iterating that the main risk concerns the bellow breakage and component damage due to excessive displacement between two components. The analysis follows the IEC-61511 standard. The standard provides very strict requirements to design a safety instrumented system in terms of SIL level, certified safety devices etc. For the FRAS design, this path was not followed but the alternative provided by the standard is followed, using multiple layers of protection to manage the risk mitigation.

The objective is to design and develop a protection system that meets the necessary risk reduction - both for personnel and for machine protection.

All the risks related to component displacement are analyzed. Including displacements induced by the FRAS but also by other causes (quenches, ground motion, etc.). The FMEA is available in EDMS-2727128, including the analysis of personnel and machine risks. Several failure modes were identified, having two main effects for the machine protection: bellow breakage (potentially up to 1 year of delay for the LHC) and component damage (potentially more than 1 year of delay for the LHC).

The potential causes are:

1. Software or communication error on FRAS control system
2. Controls hardware failure on the FRAS control system
3. Wrong operator/expert command
4. Mechanical problem on the jack support
5. Quench
6. Ground motion
7. Power failure

Borja recalled the major elements of the FMEA and the severity / probability risk reduction requirements. The focus for machine protection is to focus on the risk prevention (reducing the risk by reducing the probability of occurrence, without reducing the severity by additional protections). The frequency of major failures (e.g. bellow breakage) can be estimated from

historic data of similar systems, using reliability predictions or based on the IEC 61511-3 guidelines. The analysis follows the LHC risk matrices (EDMS-2647876). The strategy used for risk reduction by mean of frequency reduction uses multiple redundant layers.

Taking these elements in consideration, the frequency of occurrence of the above-mentioned root causes has been estimated. It was considered that in the case of bellow damage, the starting point for the risk frequency is of 3 damages every 10 years. The target frequency, based on the severity of the risk, is 1 damage every 100 years. The risk reduction factor is ~ 100. A safety system with multiple layers must be designed to achieve that goal.

A similar analysis for the risk of component damage leads to a risk reduction factor (RRF) of a factor 10. The same analysis without considering the BLMs as a safety layer leads to a RRF of a factor 100.

A RRF of 100 can be achieved using 2 independent protection layers (or using a SIL2 safety instrumented system). Due to some technical and economical challenges, the recommendation is not to develop a safety instrumented system (SIL). Some of these challenges include the sensor technology and the software requirements, including the usage of a Full Variability Language.

The final proposal is to use protection layers following the IEC 615111-3 Annex C guidelines.

A protection layer consists of a grouping of equipment and administrative controls that function together with other protection layers to control or mitigate the risk. A protection layer reduces the identified risk by at least a factor of 10 and has the important characteristics: specificity, independence, dependability, and auditability.

Protection layers to protect from bellow breakage

The first layer is provided by the resolver technology able to stop the motor immediately. The same function is also provided by capacitive sensors. In addition, FSI sensors are also able to stop the motor relays. Depending on the component and the exact failure mode, this provides a RRF from 100 (SIL2) to 1000 (SIL3). For each protection layer a detailed reliability model has been built.

Protection layers to protect component damage

The FRAS motor key cuts the power to the FRAS motors. If the motor is powered, an interlock is triggered on the ring BIS. In addition, the components limits using the sensors could also send a signal to the SIS. Also, it would send a signal to the injection BIS.

Conclusion

The necessary risk reduction is bigger for machine protection than for personnel protection according to the risk analysis. The proposed protection levels reduce the risk for both cases.

The risk graph and the estimations of the consequences and initial cause frequencies from the risk matrix must be validated.

According to the current failure frequency estimations. We need 2 PLs for bellow protection (3 are provided in many components configurations). One extra PL must be provided for component protection. The FRAS key to avoid a misalignment provoked by the FRAS with an interlock to the ring BIS and a SIS and injection BIS interlock if a misalignment is detected.

In addition, potential common cause of failures between the different layers must be analyzed.

The possibility of replacing the FEC by a PLC for the PL1 (capacitive sensors) is being explored.

Discussion

Alessandro commented on the FESA and FEC for the resolvers and added that the basic safety functions (crosscheck of motor vs. resolver position, resolver diagnostics) are performed at the FPGA level. Mateusz added that the FEC is foreseen be used to the below deformation computation, basing on the sensor (resolver) information. The below deformation is then communicated from FEC to FPGA to perform the interlock function.

Mateusz commented also that each part of the system will be equipped with diagnostics capabilities, which is another layer of protection.

Daniel commented on the component damage protection with the FRAS key and referred to Jorg's comment on implementing a global position (like the orbit) and a tolerance for the whole chain of components. The interlocking would then be done with respect to the tolerance. Jan commented that the interlocking is done by the survey monitoring interlocking to the SIS and to the injection BIS.

Alessandro recalled the comment from Jan about triggering an interlock (possibly maskable) in any case when the motors are powered. This would provide an additional layer on top of the interlock key system and can easily be implemented in the low-level controls of the jacks. This will require a CIBU on each IP side of IP1 and 5. Daniel commented that this should indeed be implemented.

Jan added that Alessandro's proposal will require further BIS channels. Mateusz commented that specifications at that level of detail will follow.

Jan clarified that there will be an additional redundancy, in the sense that the interlock key will be connected to another CIBU compared to the "FRAS motor powering interlock" which will have an input in the CIBUs in IR1 and IR5.

Action: Prepare detailed specifications for the interlocks, including the FRAS interlock key and the newly discussed "FRAS powering interlock" to a maskable input of the CIBUs in IR1 and 5 (FRAS team, MPP).

A discussion followed about the need to integrate these new requirements and coordinate with the hardware teams for integrate within a short timescale.

Action: By the end of the year inputs for potential additional interlocks or hardware stops for the protections of components in the FRAS must be provided by the relevant teams and collected for the FRAS specifications (François-Xavier Nuiry (WP5)).

Enrique mentioned the possibility to increase the diversity of technologies by replacing the FEC by a PLC (and the additional WFIP/Profinet passerelle) and asked inputs from the MPP on the topic. Jan replied that this is certainly a good idea as it could remove common cause issues. Daniel added that this should be pursued if a first feasibility and reliability study is positive.
Daniel summarized that the MPP does not require the PLC option but strongly encourage that it is studied and possibly implemented.

Daniel concluded that the MPP endorses the proposed functional specifications, with the discussed changes to add a BIC interlock on the motor powering in IR1 and 5 and a SIS/Injection BIC interlock based on limits for the alignment of the whole chain of components. Following these changes, the MPP propose that the functional specifications of the FRAS protection layers and risk analysis (EDMS-2727128) are distributed for engineering check.

AOB

AFP

Maciej asked how long the high-mu part of the 600b fill will last. Daniel and Jan replied that the MPP ask that the high-mu part of the fill should last for 4 hours minimum.

Summary of actions

The actions from the meeting are:

- FRAS risk analysis and risk mitigation using protection layers according to the IEC61511 standard
    1. Prepare detailed specifications for the interlocks, including the FRAS key in CCR and the newly discussed “FRAS powering interlock” to a maskable input of the CIBUs in IR1 and 5 (FRAS team, MPP).
    2. By the end of the year inputs for potential additional interlocks or hardware stops for the protections of components in the FRAS must be provided by the relevant teams and collected for the FRAS specifications (François-Xavier Nury (WP5)).