ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TU2BC002

# PROTECTION LAYER DESIGN FOR THE HIGH LUMINOSITY LHC FULL REMOTE ALIGNMENT SYSTEM

B. Fernández*, A. Germinario, E. Blanco, M. Sosin, H. Mainaud
CERN, Geneva, Switzerland

*Abstract*

The Full Remote Alignment System (FRAS) is a complex measurement, alignment and control system designed to remotely align components of the Large Hadron Collider (LHC) following its High Luminosity upgrade. The purpose of FRAS is to guarantee optimal alignment of the strong focusing magnets and associated components near the experimental interaction points, while at the same time limiting the radiation dose to which surveyors in the LHC tunnel are subjected.

A failure in the FRAS control system, or an operator mistake, could provoke a non desired displacement of a component that could lead to damage of neighbouring equipment. Such an incident would incur a considerable repair cost both in terms of money and time.

To mitigate this possibility, an exhaustive risk analysis of FRAS has been performed, with the design of protection layers according to the IEC 61511 standard proposed.

This paper presents the different functional safety techniques applied to FRAS, reports on the current project status, and introduces the future activities to complete the safety life cycle.

## INTRODUCTION

The High-Luminosity Large Hadron Collider (HL-LHC) [2] is an ambitious project to upgrade the LHC and increase its discovery potential. During the next long shutdown, between 2026 and 2028, many LHC components will be upgraded and some completely new systems will be deployed. These upgrades aim to improve the overall LHC performance and increase the total number of particle collisions produced by a factor of 10.

One of the new systems that will be deployed during this long shutdown is the Full Remote Alignment System (FRAS) [1]. FRAS will allow to remotely align components in both sides of the Interaction Points (IP) 1 and 5 of the LHC. The reduction in the mechanical components misalignment will decrease the required orbit corrector strengths, improving the accelerator performance and will allow to reduce the radiation doses for surveyors working in the tunnel.

However, these benefits come with a risk. An excessive misalignment of more than ±2.5 mm in the vertical and horizontal axes or 1 mrad in the rotational axis between two LHC components could damage the interconnecting bellows. This would provoke a downtime of the LHC between several months and one year for reparations. In addition, there are many potential failures that can cause this bellow damage as FRAS is a complex control system with many hardware and software components and operator interactions.

To mitigate the risk to an acceptable level, two primary actions have been undertaken. Initially, a comprehensive risk analysis and assessment were conducted to identify the combinations of failures resulting in a possible bellow damage and ascertain the required risk reduction measures. Secondly, a number of protection layers were designed in alignment with functional safety standards, aiming to bring the risk down to tolerable level.

The paper is structured as follows: Section  describes the FRAS controls architecture. Section  shows the risk analysis and assessment methods that have been applied. Section  presents the design and analysis of the protection layers. And finally some conclusions and future work are outlined.

## FRAS

Remote alignment of the LHC components (e.g. collimators, quadrupoles, dipoles, etc.) requires to equip them with high precision sensors that allow to determine the 3D position of each component and to compute their necessary displacement for an optimal alignment. The FRAS will enable remote positioning of 68 accelerator components, whose are installed across two Long Straight Sections (LSS), spanning a distance of 400 meters each. For such a big and complex installation, whose main role is to monitor and displace accelerator components, often weighing tenths of tons, the primary focus is ensuring its safe operation. This can be achieved thanks to a network of over 450 micrometric sensors, and a set of controllers and stepper motors that constitute the FRAS control system. Figure 1 depicts the controls architecture the FRAS.

This schematic shows 2 of the 17 LHC components controlled by the FRAS on each side of the IP. In this case, both components are equipped with Wire Positioning Sensors (WPS) based on a capacitive technology and 2 types of inclinometers, one based on Frequency Scanning Interferometry (FSI) and the other on capacitive technologies [1]. FRAS can also read the position of the 5 motorized actuators that are in charge of moving the jacks or Universal Adjustment Platform (UAP) that supports FRAS components. This is done by reading the resolvers that provide an absolute position of the motorized actuator assembly.

The control layer of FRAS is comprised of a combination of Commercial Off-The-Shelf (COTS) and in-house hardware devices that read each sensor, compute the 3D position of each component and provide the optimal movement commands to be transmitted to the stepper motors. Some of the COTS devices are the so-called FECs (Front End

* borja.fernandez.adiego@cern.ch

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TU2BC002



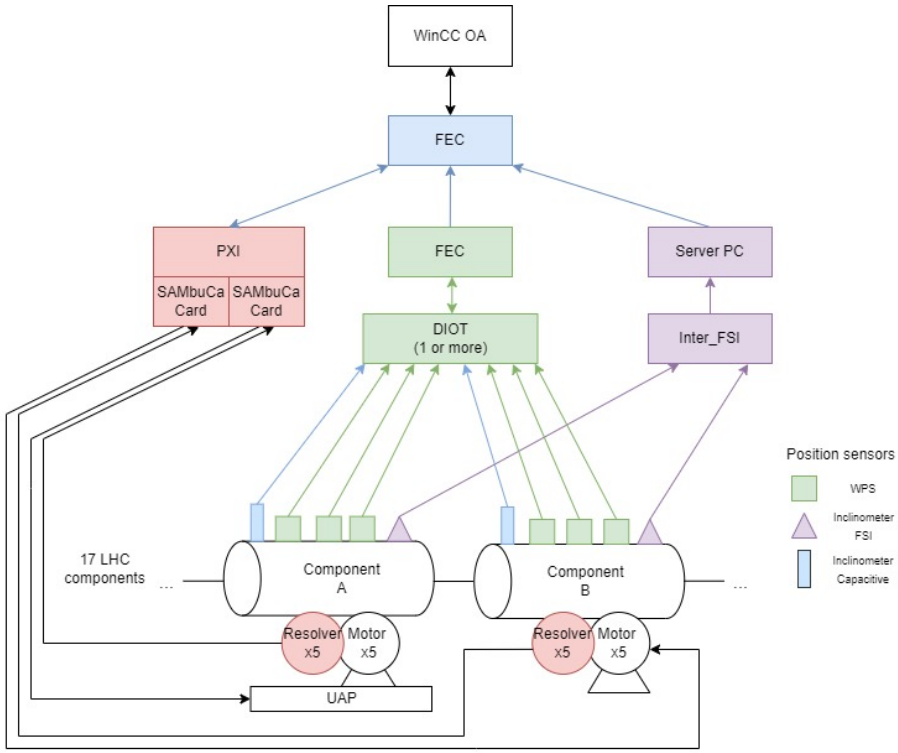


Figure 1: Simplified FRAS controls architecture for one Interaction Point side.

Computers) from Siemens and industrial PXI-e controllers provided by industrial partners under CERN specifications. The in-house designed hardware include (1) the Sensors Acquisition and Motion Control system (SAMbuCa) [3], (2) the Distributed IO Tier (DIOT) [4] and (3) Frequency Scanning Interferometry (FSI) systems [5]. In terms of software, the control devices execute C++ programs generated by the CERN FESA (Front End Software Architecture) controls framework [6].

At the supervision layer, the system deploys the Siemens WinCC OA SCADA (Supervisory control and data acquisition) [7] and the CERN UNICOS (UNified Industrial Control System) framework [8] providing the human machine interface for the experts monitoring and operation as well as the long-term archiving and alarm capabilities.

## HAZARD AND RISK ASSESSMENT

The initial safety-related task for this project involved conducting a high-level risk analysis using the FMEA (Failure Mode and Effect Analysis) methodology. In this analysis, the impact of various failure modes to the CERN personnel, the environment and the LHC machine (economic and reputation impact) was analysed. The analysis covered the different components that can be aligned by FRAS and the different operational phases of the LHC (e.g. maintenance, pilot beam or high intensity beam phases). It considered a wide range of potential causes that could lead to misalignment, such as earthquakes, operator errors, magnet quenching, or failures in the FRAS system.

The findings from the FMEA indicate that the personnel safety risk is linked to the potential oxygen deficiency hazard (ODH) within the tunnel, which could result from a minor helium spill caused by an excessive displacement. Since the LHC tunnel has already sufficient protection measures in place to protect the personnel in the tunnel from ODH (e.g. escape routes and ODH masks), the risk to the personnel is small. Results also show that there is no environmental impact related to this risk. However, the most critical consequence would be damaging the LHC, in particular damaging the interconnecting bellows between the LHC components. Indeed, this scenario would entail a downtime of the LHC lasting up to one year, and currently, there are no protective measures in place to mitigate this outcome.

Regarding the causes, the analysis shows that the biggest contributor to this risk (i.e. the cause with the higher failure frequency estimation) would be a failure in the FRAS control system (a wrong command sent to the motors or a motor failure itself. For this reason, FRAS has been thoroughly analysed.

It is well-known that risk is the combination of the likelihood of an event and the severity of harming humans, the environment or an economical impact to the company or organization. In general, risk can be defined as:

$$Risk = Likelihood \times Severity$$

This means that to reduce a risk to a tolerable level, one can reduce the likelihood of the dangerous event or the severity of its consequences. In this specific situation, it's important to note that the severity cannot be mitigated. If the limits of relative displacement are exceeded, there are no safeguards in place to prevent bellow damage and the resulting machine downtime. Then, the only strategy to reduce the

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TU2BC002

Table 1: Example of the Component Failures Analysis

| Component | Failure Mode | Effect | Frequency estimation | Justification (failure/year) | Beta estimation | Justification |
|---|---|---|---|---|---|---|
| Resolvers | Hardware issues | Wrong measure | 0.006 | 550 resolvers, 25 failures in 8y | 15 % | IEC61508-6 Annex D |
| | Radiation | Wrong measure | 0 | no failure records | 20 % | IEC61508-6 Annex D |
| | Electric shortage | Wrong measure | 0.0006 | 128 resolvers, 1 failure in 15y | 80 % | Same power supply |
| Stepper motor | Wearing out | Wrong movement? | 0.002 | 650 motors, 10 failures in 8y | 10 % | IEC61508-6 Annex D |

risk to a tolerable level is to reduce the likelihood or probability of occurrence. To this end, three different methodologies have been applied:

1. Another FMEA to identify the individual failure modes of each of the FRAS components and estimate their failure frequencies.
2. A Fault Tree Analysis (FTA) to identify which combination of component failures may lead to the risk of damaging the bellow. FRAS is by design a highly redundant system and in most cases, a single component failure will not lead to this risk.
3. The LHC risk matrix to identify the necessary risk reduction to bring the risk to the tolerable level.

### *Component Failure Analysis*

The purpose of this analysis is to identify the maximum number of dangerous undetected failures for each FRAS component. In order to identify the failure modes of the individual component, a FMEA has been applied as shown in Table 1. This table illustrates an example of two FRAS components, the motor resolvers and the stepper motors. In the case of the resolvers, 3 failure modes were identified and for each failure mode a failure frequency was assigned with the information provided by the equipment groups based on operational experience. In the case of the motors, only one main failure mode was identified and again the failure frequency was assigned with the information provided based on operation experience. In addition, the common cause failure factors were assigned to each failure mode, based on operational experience and the guidelines from the IEC 61508 standard [9].

The complete table contains failure modes caused by hardware and software failures and also by operator mistakes. The failure frequency estimations have mainly been calculated based on operational experience in the LHC. When data was not available, conservative assumptions based on the guidelines of the functional safety standards have been applied. In the case the FRAS operators, the estimation was performed using the Human Error Assessment & Reduction Technique (HEART) method [10], a widely validated method across critical industries like the marine and aerospace industries [11].

### *System Failure Analysis*

Once the failure modes of each FRAS component have been identified, a FTA allows to identify the combination of failures that may lead to the risk of damaging the bellows. The FTA contains the combinations of hardware, software and human failures, identified in the FRAS components FMEA, that may lead to a risk. It was developed using the commercial tool *Isograph reliability workbench* [12].

Figure 2 displays a limited subset of these combinations that have been identified and analysed. For example, any dangerous undetected hardware or software failure in the high level FEC ("UPPER_FEC") could lead to bellow damage. However when analysing the "actuation path", if the SAMbuCa card hardware fails, the PXI should fail at the same time to have a dangerous undetected situation for this risk.

The results of the FTA show a total frequency of failure for the bellow damage risk of $\lambda_1$ = 8.393E-5 $h^{-1}$ = 0.735 $y^{-1}$ = 7.35 failures per 10 years. They also show which FRAS components are more critical for the analysed risk. The results reveal that due to the high redundancy in the FRAS controls architecture, hardware failures are not really critical, the single point of failure are mainly software flaws. The information derived from the FTA holds paramount significance for three key reasons:

- Together with the next method (the LHC risk matrix), it allows to determine the necessary risk reduction to reach the tolerable risk level.
- It helps to identify the critical components that have a higher contribution for this risk.
- It evaluates if the reduction measures are focused on the most critical failures.

### *Risk Matrix*

Once the combinations of failures that may lead to the risk are identified and their failures frequencies are calculated, it is necessary to asses if this risk is acceptable for CERN.

For such assessment, CERN has developed the so called *Data-Driven Risk Matrices for CERN's Accelerators* [13]. Table 2 displays the LHC risk matrix, which facilitates the assessment of whether the risk, computed by combining the resulting failure frequencies from the Fault Tree Analysis (FTA) and the estimated severity, falls within the *Unacceptable* region (highlighted in red). It also provides insight into the amount of risk reduction required to transition the failure frequency into the *Acceptable* region (highlighted in green).

In this case, the calculated failure frequency is $\lambda_1 = 0.735y^{-1}$ and the failure frequency target for stopping the LHC between 1 month and 1 year is $0.01y^{-1}$. Since there are 4 FRAS systems (one per IP side). Therefore the failure frequency target for each FRAS system is at least $\lambda_2 = 0.01y^{-1} \div 4 = 0.00250y^{-1}$. This means that the Risk Reduction Factor (RRF) is:

$$RRF = \frac{\lambda_1}{\lambda_2} = \frac{0.735}{0.00250} = 294$$

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TU2BC002



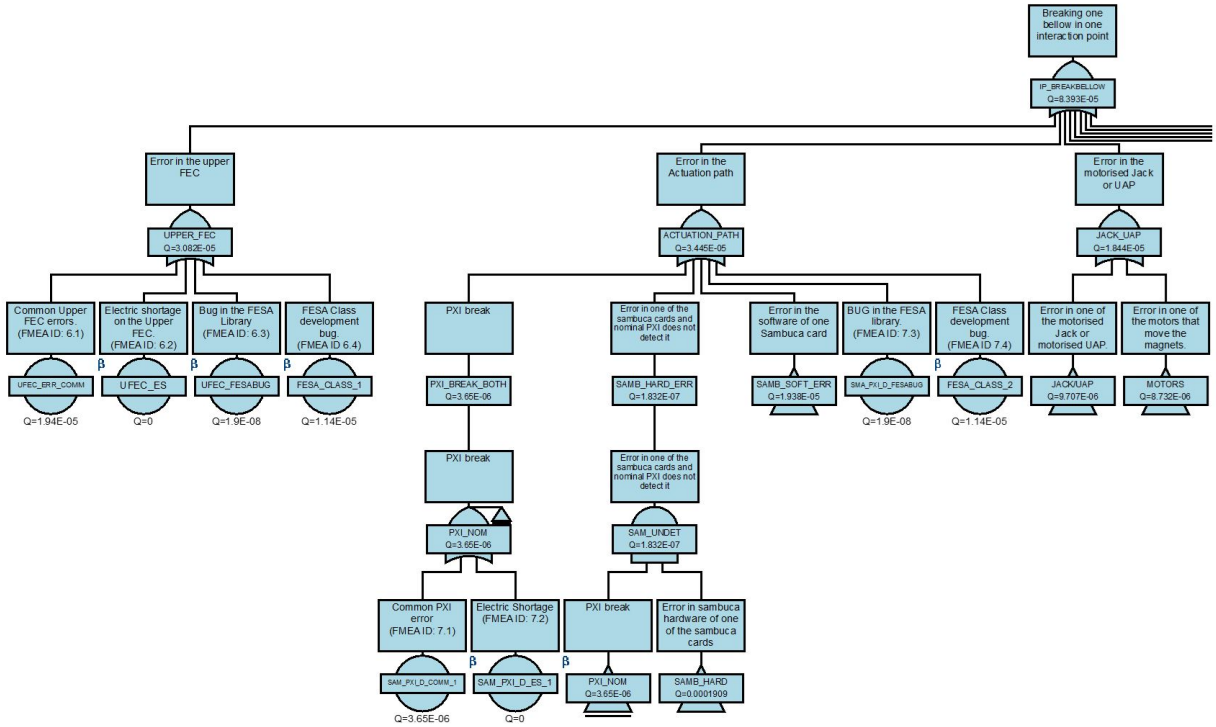


Figure 2: Isograph partial FTA for the FRAS control system.

Table 2: LHC Risk Matrix from Ref. [13]

| | 1m - 20m | 20m - 1h | 1h - 3h | 3h - 6h | 6h - 12h | 12h - 24h | 24h - 2d | 2d - 1w | 1w - 1M | 1M - 1Y | 1Y - 10Y |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1/H | U | U | U | U | U | U | U | U | U | U | U |
| 1/Shift | U | U | U | U | U | U | U | U | U | U | U |
| 1/Day | A | U | U | U | U | U | U | U | U | U | U |
| 1/Week | A | A | A | A | U | U | U | U | U | U | U |
| 1/Month | A | A | A | A | A | A | U | U | U | U | U |
| 1/Year | A | A | A | A | A | A | A | A | U | U | U |
| 1/10Years | A | A | A | A | A | A | A | A | A | U | U |
| 1/100Years | A | A | A | A | A | A | A | A | A | A | U |
| 1/1000Years | A | A | A | A | A | A | A | A | A | A | A |

It is necessary to reduce the risk either by re-designing the system reducing $\lambda_1$ or by adding an automatic system that can cope with this risk reduction.

According to the IEC 61511 standard [14], there are two main paths to achieve the necessary risk reduction calculated during the risk assessment:

1. Design a Safety Instrumented System (SIS) that meets the RRF. This is described in the Clauses 10 to 13 (phases 3 and 4) of the safety life-cycle, shown in Fig. 3. Each of the Safety Instrumented Functions (SIF) of the SIS must be compliant with a series of strict requirements in the design, the development and during the validation process. These requirements depend on the the associated Safety Integrity Level (SIL) for each SIF, which quantifies how critical the risk is. The concept of SIL is directly linked with the RRF as shown in Table 3 for *Low Demand* risks. Since the RRF is 294, it means that to reach the tolerable risk level, we should design an independent SIS from the initiating events with a SIL2 SIF.
2. The IEC 61511 standard gives an alternative path, the Clause 9. It offers guidelines for designing and developing "alternative risk reduction methods" when it is not feasible to create a Safety Instrumented System (SIS).

Table 3: Relationship Between SIL and RRF

| *SIL* | *RRF* |
|---|---|
| 4 | 10000 to 100000 |
| 3 | 1000 to 10000 |
| 2 | 100 to 1000 |
| 1 | 10 to 100 |

In this project, the second option was chosen for the following technical considerations:

- It is not possible to add new sensors or controllers independent from the FRAS control systems devices. The limited space in the LHC components and control racks, together with the extra cost of new equipment make the first option not viable.
- To the best of our knowledge, there are currently no certified position sensors available that simultaneously

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TU2BC002

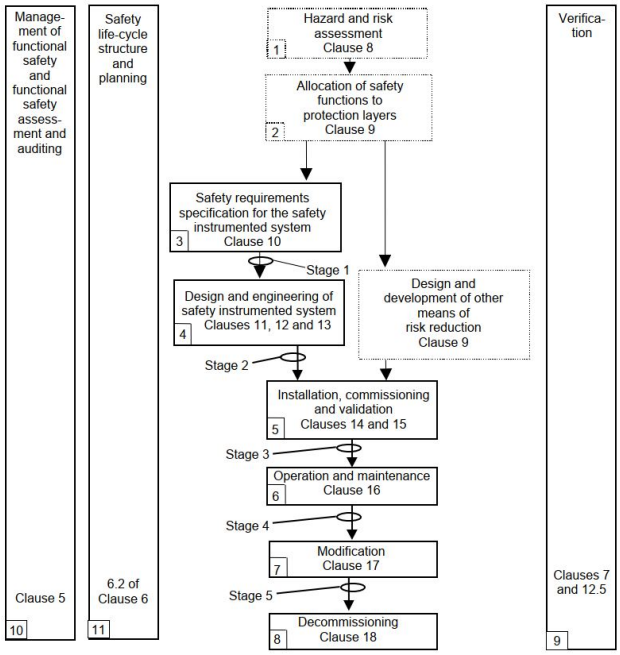


Figure 3: IEC 61511 safety life-cycle.

meet the SIL2 requirements, the necessary precision standards, and possess radiation tolerance.

- To program the necessary logic of the SIF, it would be necessary to use *Full Variability Languages* (FVL) instead of *Low Variability Languages* (LVL). Consequently, the application program requirements should adhere to the IEC 61508 standard, which would lead to higher costs for the design, development, and validation of the software component.

Due to these considerations, it was decided to apply other means of risk reduction. In particular, independent layers of protection were designed, following the requirement of the IEC 61511 Clause 9.

## LAYERS OF PROTECTION DESIGN

Figure 4 shows the typical protection layers and risk reduction means from the IEC 61511-1 Clause 9.

This Clause also describes the requirements on the Basic Process Control System (BPCS) as a Protection Layer (PL). When the PL is not designed to meet the SIL requirements, The risk reduction claimed for a BPCS protection layer shall be $\leq 10$. In addition, the BPCS PL should respect certain rules (text extracted from the IEC 61511 Clause 9):

- no more than one BPCS protection layer shall be claimed for the same sequence of event leading to the hazardous events when the BPCS is the initiating source for the demand on the protection layer; or
- no more than two BPCS protection layers shall be claimed for the same sequence of events leading to the hazardous event when the BPCS is not the initiating source of the demand.

The standard also gives the requirements to prevent common cause, common mode and dependant failures. The assessment to prove that these categories of failures have

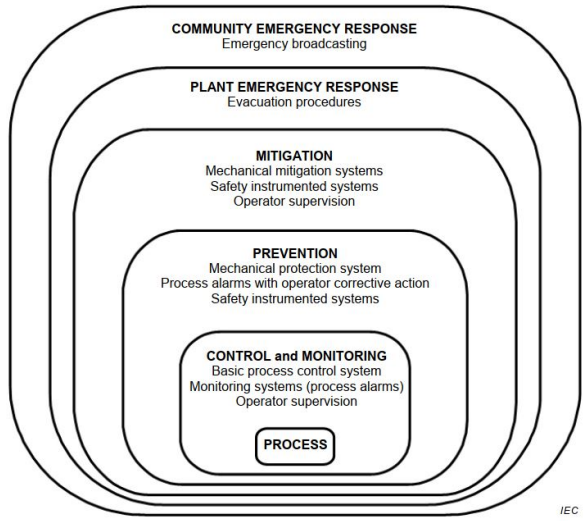


Figure 4: Typical protection layers and risk reduction means from the IEC 61511 - Clause 9.

been adequately addressed should encompass the following aspects (text extracted from the IEC 61511 Clause 9):

- independence between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS.

Respecting all of these criteria, three BPCS PLs have been designed and analysed using the LOPA (Layers of Protection Analysis) method. The three PLs are integrated in the FRAS controls as show in Fig. 5. The new hardware added to FRAS is highlighted compared with Fig. 1. Only 3 safety relays have been added, no new sensors or controllers.

The required functionality of the PLs is to continuously monitor the position of two adjacent components using only one of the sensor technologies, compute the relative displacement and stop the motors if the safety threshold is reached. For example, PL1 uses the capacity sensors of both components, reads the sensor values through the *DIOT*, computes the engineering values, calculates the relative displacement in the *FEC* and if requested, sends the signal to stop the motors via the safety relay.

As can be seen, many hardware and software components are shared between FRAS and the PLs. Consequently, in the LOPA analysis, it is essential to demonstrate that the initiating failure event is entirely independent of a PL in order to claim some risk reduction.

### *Layer of Protection Analysis*

The effectiveness of each PL must be analysed for each combination of failures identified in the FTA. Moreover, to bring risk reduction, every PL must meet the requirements listed before.

Table 4 shows the LOPA method applied to the FRAS PLs. The table shows three columns with three of the several initiating events that may lead to damage the bellow. These events correspond with the combination of failures identified

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TU2BC002

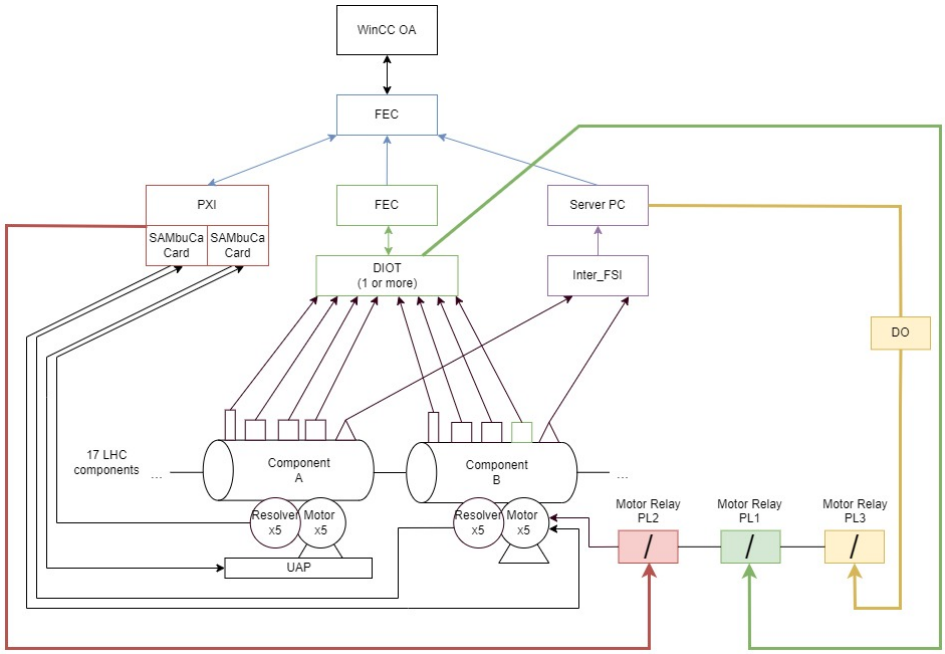


Figure 5: Protection Layers (PLs) design for each Interaction Point side.

in the FTA. For each PL, an analysis is conducted to determine whether it can provide protection against each initiating event. Additionally, the assessment includes an evaluation of the PL's complete independence from the hardware and software components that may be potentially involved in the same sequence of events. If it is the case, a risk reduction of 10 is assigned to each PL.

Due to technical constrains, there is a *common cause of failure* between the three PLs. They all use the same control software framework (FESA). For that reason, when two PLs could contribute to reduce the risk coming from the same sequence of events, only one PL is considered in terms of risk reduction. In general, only one PL is claimed (RRF of 10) for one initiating event.

It is worth noting that the FRAS will not operate continuously throughout the entire duration of LHC operations. Instead, it will only be active during technical stops and specific periods within the year. The presence of risk not being continuous is factored into the assessment, and this is reflected in the "operation time" row of Table 4.

The failure frequencies taking into account the PLs and the operation time are calculated and compared with the failure frequency target. As shown in the last row of Table 4, the residual risk is positive, meaning that after considering the PLs risk reduction and a reduced operation time, the risk is now in the tolerable region of Table 2.

Table 4: Layers of Protection Analysis (LOPA) for the Risk of Damaging One Bellow in One IP Side of the LHC

| | | **Initiating cause 1** | **Initiating cause 2** | **Initiating cause 3** | ... |
|---|---|---|---|---|---|
| | | **Upper FEC** | **Error in actuation PXI - SAMbuCA** | **Error in actuation jack, UAP and motors** | ... |
| | Event Frequency (1/h) | 3.08E-05 | 3.45E-05 | 1.84E-05 | ... |
| | Event Frequency (1/y) | 0.27 | 0.30 | 0.161534 | ... |
| **Protection and mitigation layers - RRF** | PL1 | | 10 | | ... |
| | PL2 | 10 | | | ... |
| | PL3 | | | 10 | ... |
| **Operation time (days) - RRF** | 11 days | 33.1818 | 33.1818 | 33.1818 | ... |
| **Cumulative** | Intermediate event frequency (1/y) | 0.000814 | 0.000909 | 0.00048682 | ... |
| | Weight over the overall frequency (%) | 33.61 % | 37.57 % | 20.11 % | ... |
| | Total mitigated event frequency (1/y) | | 0.00242 | | ... |
| | Tolerable event frequency - LHC (1/y) | | 0.01 | | |
| | Tolerable event frequency - IP side (1/y) | | 0.00250 | | |
| | Residual risk | | 0.00007922 | | |

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TU2BC002

## CONCLUSION

This paper presents the functional safety activities applied to FRAS, a complex remote alignment system for the HL-LHC. A malfunction in the FRAS control system has the potential to damage the LHC interconnecting bellows, incurring significant financial and time-related costs for CERN.

These activities, following the guidelines of the IEC 61511 functional safety standard, can be summarized in four main phases: (1) identification and analysis of the FRAS component failures based on an FMEA, (2) identification and analysis of the FRAS system failures based on a FTA, (3) determination of the necessary risk reduction to reach tolerable risk level using the LHC risk matrix and (4) design and analysis of the protection layers based on the LOPA method.

This enables the application of a quantitative approach to assess the risk and meet the required risk reduction according to CERN's safety standards. These methods can also be applied to any other complex system where a system failure might pose significant risks to human safety, the environment, or the reputation of an organization or company.

The technical design of the FRAS protection layers is already underway. As part of future work and given that the analysis indicates that the most critical undetected failures would come from the FRAS control software, various techniques, including testing, formal verification [15] and runtime monitoring [16] are under evaluation to mitigate potential software flaws within the FRAS system.

## REFERENCES

[1] P. Biedrawa *et al.*, "Full remote alignment system for the High-Luminosity Large Hadron Collider HL-LHC", CERN, Geneva, Switzerland, CERN-BE-2023-007, 2022, http://cds.cern.ch/record/2849056

[2] HL-LHC, https://home.web.cern.ch/science/accelerators/high-luminosity-lhc

[3] SambuCa, https://ohwr.org/project/sambuca/wikis/home

[4] DIOT, https://ohwr.org/project/diot/wikis/home

[5] M. Sosin, "Frequency sweeping interferometry for robust and reliable distance measurements in harsh accelerator environment", in *Proc. SPIE 11102, Appl. Opt. Metrol. III*, vol. 11102, San Diego, California, USA, 2019, pp. 145–161. doi:10.1117/12.2529157

[6] M. Arruat, "Front-End Software Architecture", in *Proc. ICALEPCS'07*, Oak Ridge, TN, USA, Oct. 2007, pp. 310–312, paper WOPA04.

[7] Siemens WinCC OA SCADA, https://www.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-oa.html

[8] UNICOS, https://unicos.web.cern.ch

[9] "Functional safety of electrical/electronic/programmable electronic safety-related systems", International Electrotechnical Commission, CERN, CH, IEC 61508:2010, 2010, https://webstore.iec.ch/publication/5515

[10] E. Fowler, "Critical evaluation of quantitative human error estimation methods in light of different incident causation models and Hollnagel's research on performance variability", Bachelor thesis, University of Aberdeen, Aberdeen, Scotland, 2018.

[11] T. F. Alexander, "Human Error Assessment and Reduction Technique (HEART) and Human Factor Analysis and Classification System (HFACS)", in *Int. Assoc. Classif. Space Syst. Conf. 2017*, Toulouse, France, Oct. 2017.

[12] Isograph reliability workbench, https://www.isograph.com/software/reliability-workbench

[13] T. Cartier-Michaud *et al.*, "Data-Driven Risk Matrices for CERN's Accelerators", in *Proc. IPAC'21*, Campinas, Brazil, May 2021, pp. 2260–2263. doi:10.18429/JACoW-IPAC2021-TUPAB325

[14] "Functional safety - Safety instrumented systems for the process industry sector", International Electrotechnical Commission, CERN, CH, IEC 61511:2016, 2016, https://webstore.iec.ch/publication/24241

[15] R. Monteiro *et al.*, "Model checking C++ programs", *Software Testing, Verification and Reliability*, vol. 32, no. 1, Sep. 2021. doi:10.1002/stvr.1793

[16] I. Perez *et al.*, "Copilot 3", NASA, Geneva, Switzerland, Rep. NASA/TM–2020–220587, Apr. 2020, https://ntrs.nasa.gov/citations/20200003164