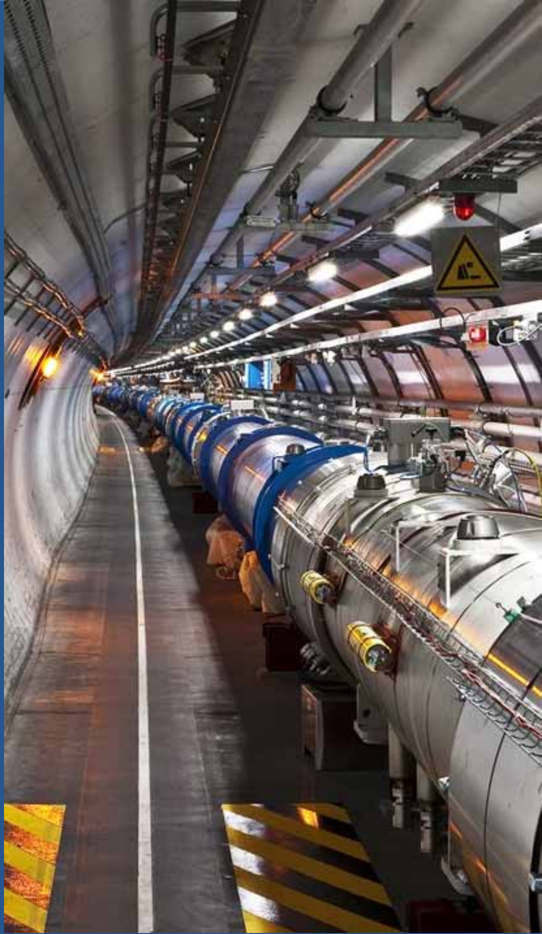
Protection Layers Design for the High Luminosity LHC Full Remote Alignment System

TU2BCO02, Functional Safety/Protection Systems/Cyber Security
October 2023

Enrique Blanco
Borja Fernández
Andrea Germinario
Mateusz Sosin
Helene Mainaud

ICALEPCS CAPE TOWN SOUTH AFRICA 2023



Outline

1. Introduction to FRAS (Full remote alignment system)

2. **Overview** of the functional safety methodology
   1. *Process hazards and risk assessment*
   2. *Designed system*
   3. *Reached risk level demonstration*

3. Conclusions and future work

HL-LHC and FRAS

The Large Hadron Collider (LHC) is the CERN’s largest accelerator

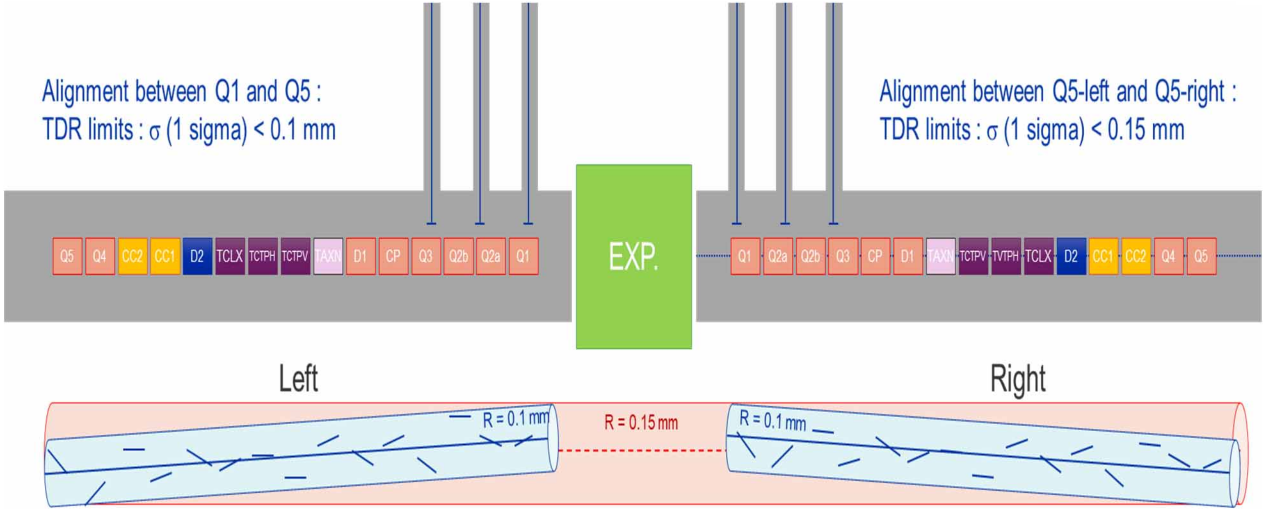
- 27 km, collision energy of 13.6 TeV and will run <u>until 2040</u>
- Nearly 1.2 km of key components will be exchanged during Long Shutdown 3 (2026-2028) to increase the **luminosity* by a factor 10** (Performance of the LHC)
  - Crab cavities
  - Bending and focusing magnets
  - Collimators
  - Superconducting links
- Very stringent **alignment requirements** in a radioactive environment.

FRAS (Full Remote Alignment System)

Luminosity: The number of particles per unit area per time, multiplied by the opacity of the target (its impenetrability) to electromagnetic radiation

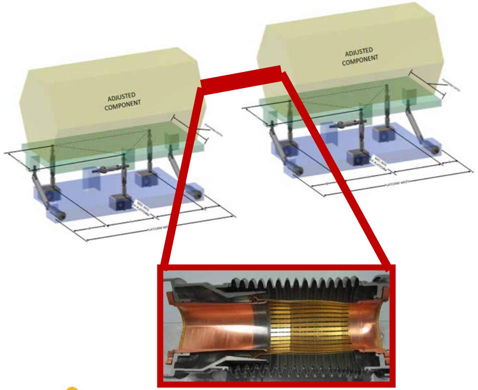
FRAS (requirements)

- 2 LSS (Long Straight Section) to align (400 meters each)
- **68 components** to align remotely



Constraints:

- **± 2.5 mm** vertical and horizontal axis
- **1 mrad** in the rotational axis between 2 components



Exceeding the limits could imply up to **1 year of stop** of the LHC

FRAS controls architecture

Supervision layer

- SCADA system
  (Siemens WinCC OA with CERN UNICOS framework)

Control layer

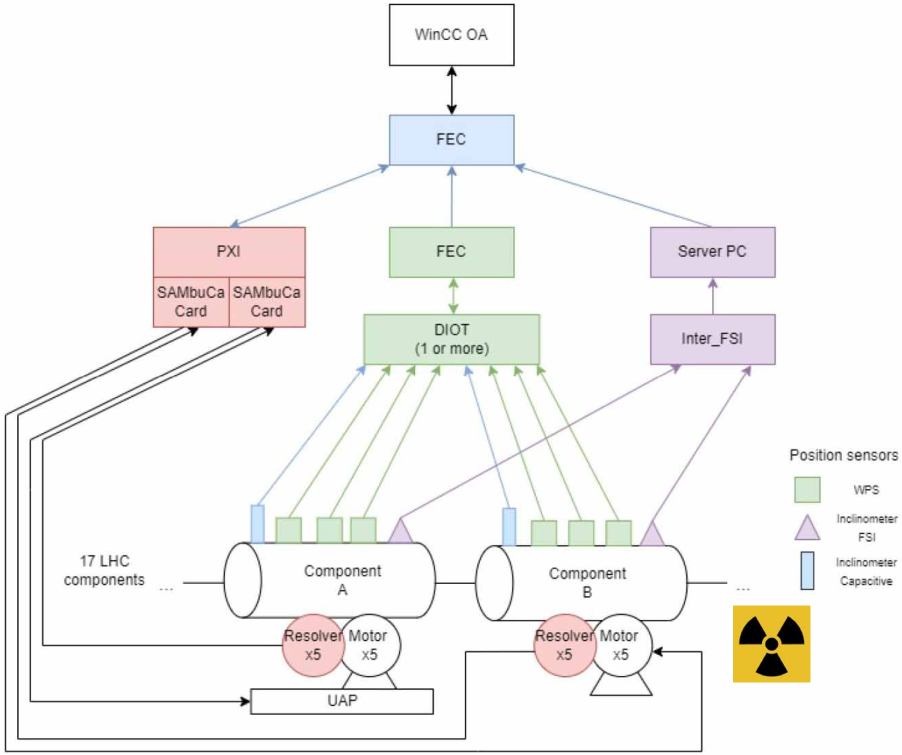
- Commercial controllers: FEC, PXI, ServerPC

(Top FEC implementing the feedback control and 3D pos)

- CERN FESA framework for the control software

Field layer

- 3 different technologies for measuring the component position (450 micrometric sensors + motion controllers + stepping motors)
- Electronics developed at CERN*



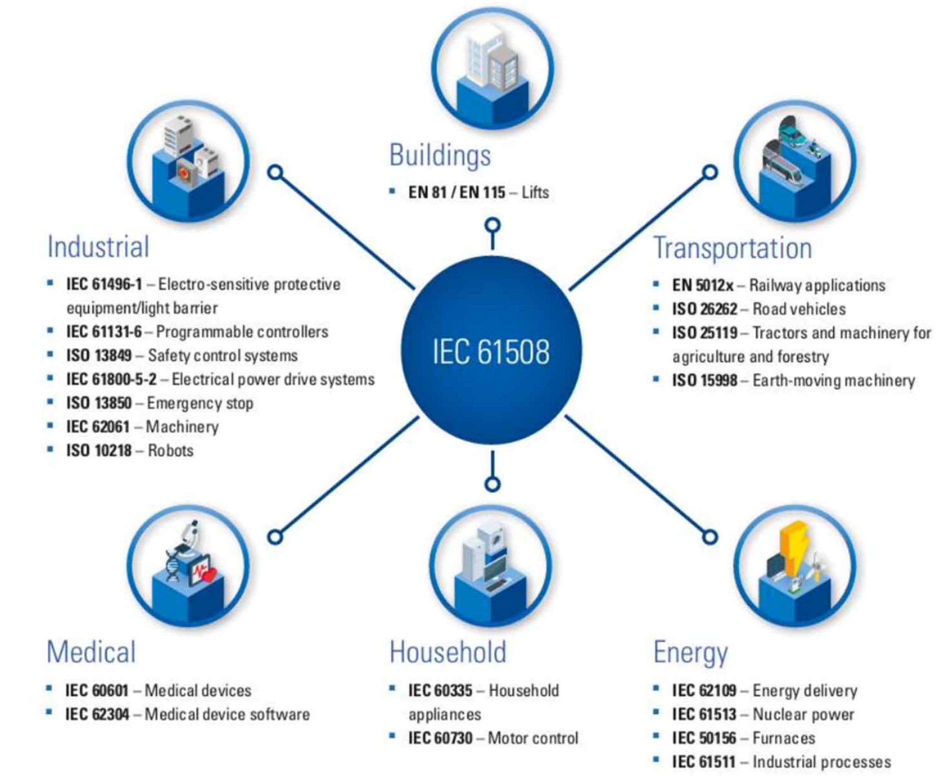
*TH2BCO04 SAMbuCa: High-Precision Motion Control and Acquisition System

Which is the risk introduced by FRAS?

Risk for the people, the environment and the installations (financial loss)

Functional Safety standards employed:

- IEC 61508
- **IEC 61511** (specific for the process industry)



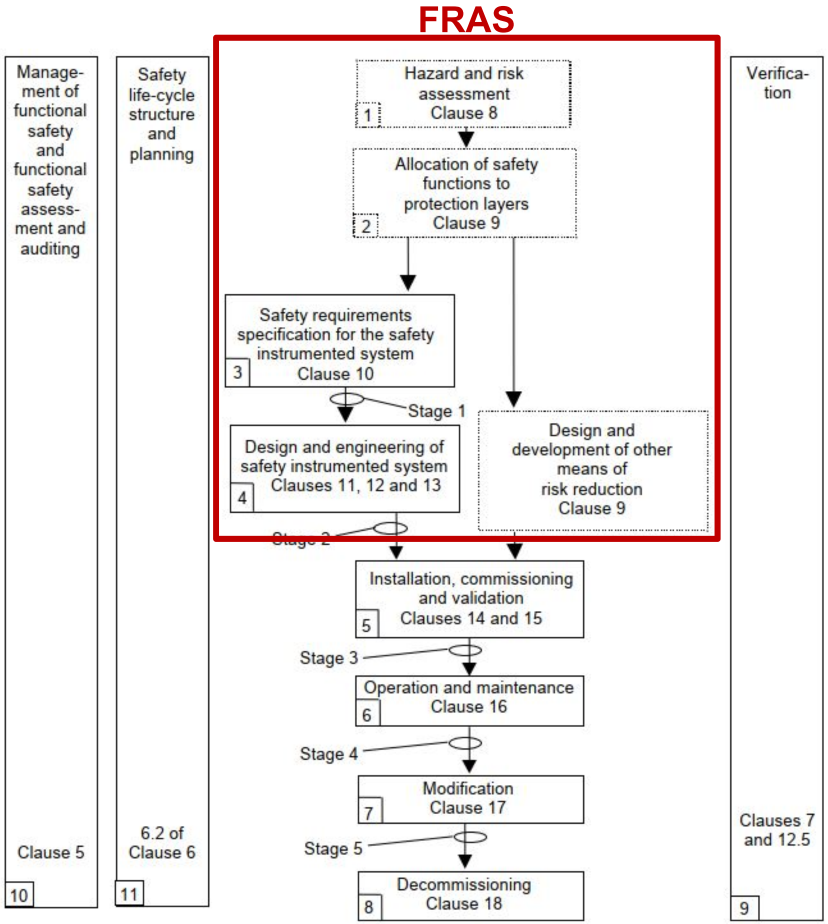
Functional Safety
*"**Systems** that lead to the **freedom from unacceptable risk** … by the proper implementation of one or more **automatic protection functions** (often called safety functions)." from TÜV SÜD*

Functional Safety – IEC 61511

- **Safety Life Cycle** followed
  1. **Risk** analysis and **assessment**
  2. Design and engineering of the safety system
  3. Commissioning, operation and maintenance
  4. Planning, **management** and verification

- Functional safety activities
  1. **High level FMEA**
     - **Cause: Failure of the FRAS control system**
     - **Effect: Damage the interconnecting bellows (Up to 1 year of stop of the LHC)**

- Probability calculation and needed risk reduction
  1. **Components failures analysis** based on a FMEA
  2. **System failures analysis** based on a FTA (Fault Tree Analysis)
  3. **Risk reduction calculation** based on a risk matrix



FMEA

Failure Modes and Effects Analysis

Identify the individual failure modes of each of the FRAS components and estimate their failure frequencies

For safety analysis, only **dangerous undetected failures** are considered

Source of information:

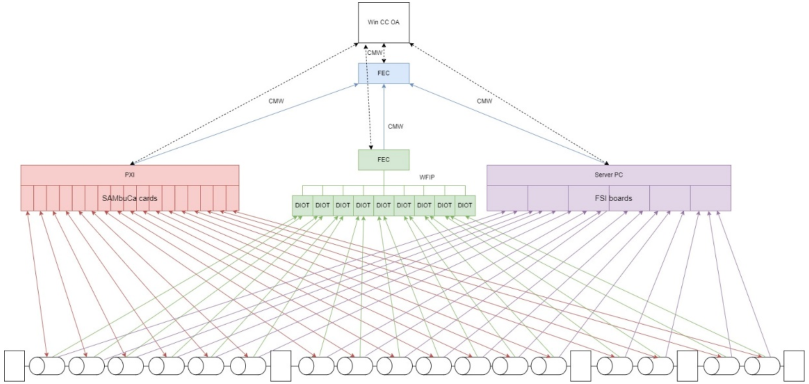
1. *Failure records*
2. *Reliability studies*
3. *Standard recommendations*

Subsystem		Failure mode	Failure mode	Effects of the failure mode	Frequency estimation (failure/year)	Remarks / Justifications	Beta value estimation (Common Cause of Failure)	Remarks / Justifications
Id	Notes	In Short	Description					
4	Stepper Motor							
4.1		(1) Motor breaks (2) Typical Stepper Motor wearing out (3) Stepper motor exaggerated movement	(1) Statistical death of a component during nominal operation. (2) Typical Stepping Motor Wearing out that may lead to imprecision in movement. (Two steps instead of one, etc..) (3) Exaggerated movement of the motor, can be originated by an uncontrolled voltage applied	Imprecise movement, may move the magnet out-of-range	0.002	Feedback from BE-CEM. Operational data of ~650 stepper motors in the LHC. 10 failures over 8 years of operation.	10%	IEC61508 - 6 Annex D - D.5
5	DIOT / InterFSI							
5.1		(1) Hardware failure (2) Short Circuit (3) Communication Error with sensor or with FEC	(1) Statistical failure of a component during nominal operation. (2) Short Circuit of the component. (3) Communication Error between the component and the sensor(s) below or the FEC above.	No Value / Wrong Value interpreted from sensors and/or sent to the lower_FEC.	0.1	According to IEC61508, proof test intervals 5 years, PFD=0.26 (data coming from BE-CEM)	0	Null because the DIOT and InterFSI are independent
5.2		Radiation	Radiation affect the value of measurement	No Value / Wrong Value interpreted from sensors and/or sent to the lower_FEC.	0.01	Feedback by BE-GM.	5%	IEC61508 - 6 Annex D - D.5 and assuming the power source is the same between different components on the same layer. (See the hierarchy in model files)
5.3		Electric Shortage	An electric shortage at the sensor level could make them send a null value or a wrong one.	No Value / Wrong Value interpreted from sensors and/or sent to the lower_FEC.	0	They are detected, so they are not 'undetected dangerous failures'	80%	IEC61508 - 6 Annex D - D.5 and assuming the power source is the same between different components on the same layer. (See the hierarchy in model files)

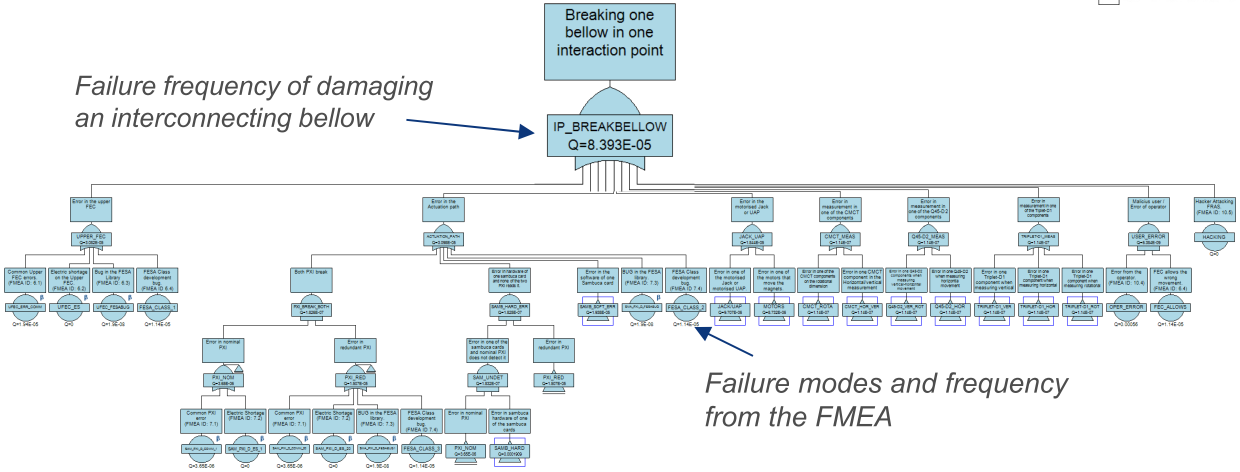
FTA for FRAS control system

Fault Tree Analysis

A <u>quantitative</u> risk analysis method that identify combinations of conditions and component failures which will lead to a single adverse effect.



Failure frequency of damaging an interconnecting bellow



Failure modes and frequency from the FMEA

Isograph reliability workbench
https://www.isograph.com/software/reliability-workbench/

Outcome:

λ_1 = 8.393E-5 h^{-1} = 0.735 y^{-1} = **7.35 failures per 10 years** according to the collected data

Identified **critical** paths: Top FEC and actuation path

It is possible to damage a bellow 0.735 times per year

Is this risk acceptable?

Machine protection:
Based on the experience of the MPE group (CERN EDMS2647876)

LHC risk matrix

Identify the necessary **risk reduction** to bring the risk to a tolerable level

(compatible with the ALARP method from IEC 61511-3 Annex K)

Up to 1 year LHC stop

*Failure mode consequence (**severity**)*

*Failure mode **frequency***

	[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

λ_1 0.735 times per year

λ_2

Risk reduction factor

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

1000 > RRF > 100

IEC 61511 Safety Life Cycle

SIL	PFD_{avg}	PFH_{avg}	*RRF*
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$	10000 to 100000
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$	1000 to 10000
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$	100 to 1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$	10 to 100

RRF=294

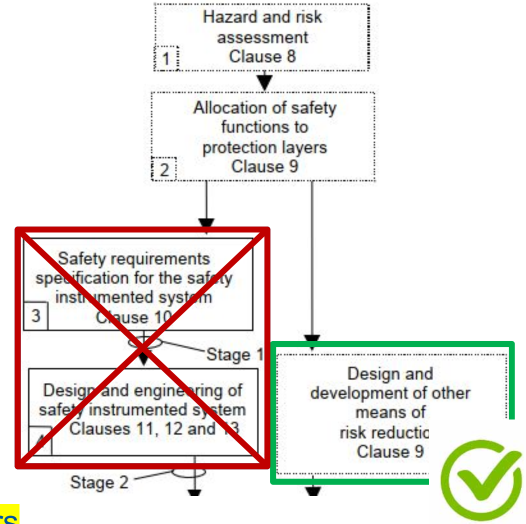
Consequence: A **SIS with a SIL2 Safety Instrumented Function (SIF)** independent of FRAS *(Clause 11,12,13)*

Safety Instrumented System (SIS) requirements:

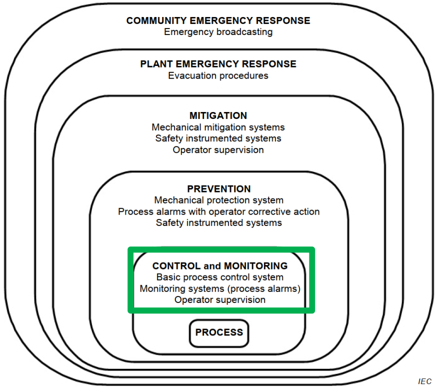
- SIL **certified hardware** components
- **Architectural** constrains
- **Software** design, development and validation
- …

Extremely difficult to engineer:

- Certified radtol sensors and actuators
- No new controllers (software FVL)
- Introduction of new hardware



Multiple **protection layers**

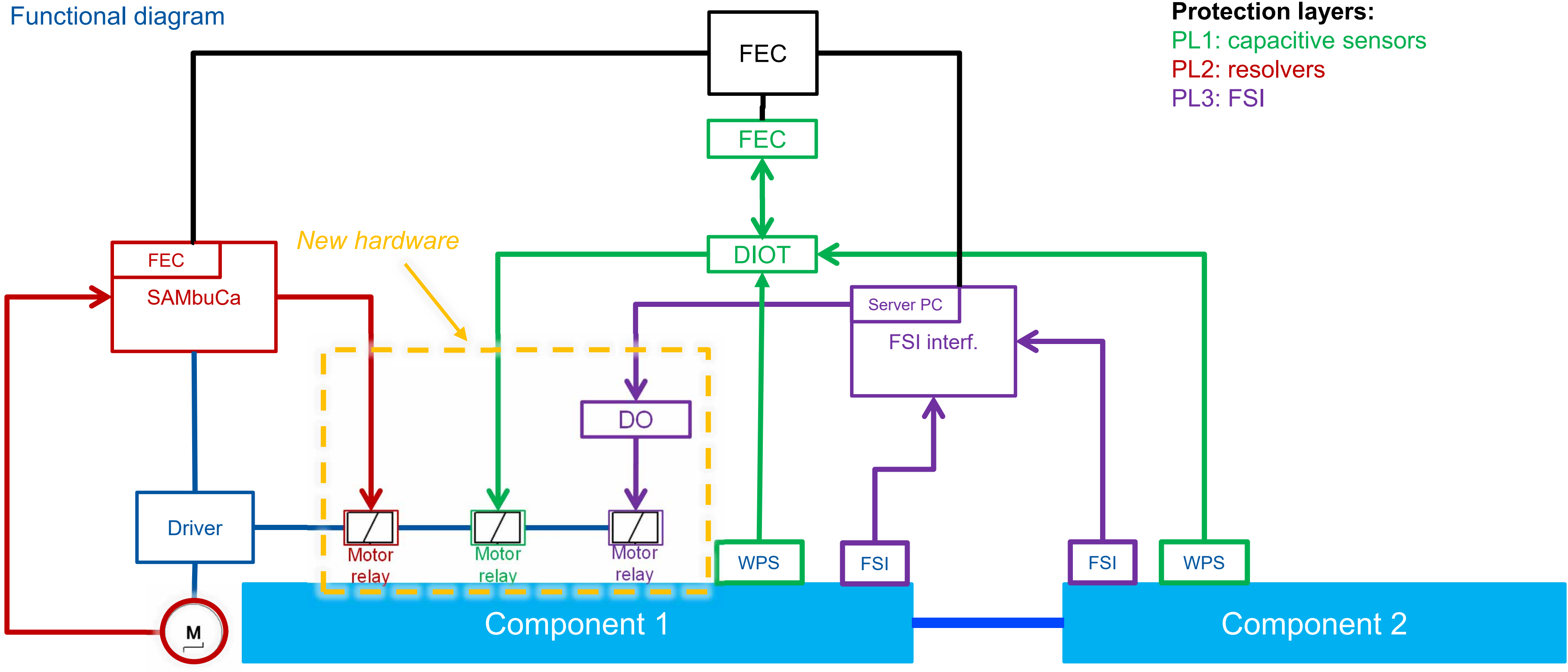


- The risk reduction claimed for a BPCS protection shall be ≤ 10
- Only a maximum of 10 risk reduction claim for all PLs protecting from a specific initiating event
- Avoid common cause/mode on the protection layers
- Dependable and auditable
- Assess: Independence / Diversity / Physical separation

Technical (and economical) limitations
(e.g. SIL certified radiation tolerant position sensors)

Protection layers proposal

Functional diagram



Protection layers:
PL1: capacitive sensors
PL2: resolvers
PL3: FSI

Demonstration: LOPA

Is the solution properly dealing with the hazards and the expected reliability?

- Sharing equipment: a failure of the control system may compromise the safety. Essential to demonstrate that the initiating failure event is entirely independent of a PL in order to claim some risk reduction

- LOPA (Layer Of Protection Analysis) is a methodology allowing the assessment of the designed system taking into account:
  - Hazard scenarios and consequences
  - Frequencies of all causes
  - Safeguards for prevention/mitigation of the consequences

LOPA

Initiating events and frequency from the FTA

Protection Layers Conditional modifiers

No claim for independent and diversity for the PLs

Target from CERN LHC risk matrix

Impact Event		Initiating Cause 1	Initiating Cause 2	Initiating Cause 3	Initiating Cause 4		Initiating Cause 5		Initiating Cause 6			Initiating Cause 7	Initiating Cause 8
					Error measurement one CMCT component		Error measurement one Q45-D2 component		Error measurement one Triplet-D1 component				
IP side Break Bellow		Upper FEC	Error in actuation path PXI - SAMbuCa	Error in actuation path Jack / UAP and motors	Rotational	Horizontal-Vertical	Vertical-Rotational	Horizontal	Vertical	Horizontal	Rotational	Malicius user / Error of operator	Hacker attack
	Event Frequency (1/h)	3.08E-05	3.45E-05	1.84E-05	1.14E-07	1.14E-07	1.14E-07	1.14E-07	1.14E-07	1.14E-07	1.14E-07	6.38E-09	0.00E+00
	Event Frequency (1/y)	0.27	0.30	0.161534	0.00099864	0.00099864	0.0009986	0.0009986	0.0009986	0.0009986	0.0009986	0.0000559	0.0000000
Protection and mitigation layers	PL1	10	10	10								10	
	PL2												
	PL3												
Operation Time	365	1	1	1	1	1	1	1	1	1	1	1	1
Procedures / Alarms													
Cybersecurity: TN + RBAC												0	100
Physical Limit Switches		0	0	0	0	0	0	0	0	0	0	0	0
Cumulative		10	10	10	1	1	1	1	1	1	1	10	100
	Intermediate event frequency	0.026998	0.030178	0.01615344	0.0009986	0.0009986	0.00099864	0.00099864	0.00099864	0.00099864	0.00099864	0.00000559	0.00000000
	Weight over the overall frequency	33.61%	37.57%	20.11%	1.24%	1.24%	1.24%	1.24%	1.24%	1.24%	1.24%	0.01%	0.00%
	Total mitigated event frequency						0.08033						
	Tolerable Event Frequency - LHC						0.01000						
	Tolerable Event Frequency - IP side						0.00250						
	Tolerable Event Frequency - Bellow						0.000119048						
	Residual Risk						-0.07782603						

LOPA

Area Occupancy:
Operation time

Impact Event		Initiating Cause 1	Initiating Cause 2	Initiating Cause 3	Initiating Cause 4		Initiating Cause 5		Initiating Cause 6			Initiating Cause 7	Initiating Cause 8
					Error measurement one CMCT component		Error measurement one Q45-D2 component		Error measurement one Triplet-D1 component				
IP side Break Bellow		Upper FEC	Error in actuation path PXI - SAMbuCa	Error in actuation path Jack / UAP and motors	Rotational	Horizontal-Vertical	Vertical-Rotational	Horizontal	Vertical	Horizontal	Rotational	Malicius user / Error of operator	Hacker attack
	Event Frequency (1/h)	3.08E-05	3.45E-05	1.84E-05	1.14E-07	1.14E-07	1.14E-07	1.14E-07	1.14E-07	1.14E-07	1.14E-07	6.38E-09	0.00E+00
	Event Frequency (1/y)	0.27	0.30	0.161534	0.00099864	0.00099864	0.0009986	0.0009986	0.0009986	0.0009986	0.0009986	0.0000559	0.0000000
Protection and mitigation layers	PL1	10	10	10								10	
	PL2												
	PL3												
Operation Time	11	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818
Procedures / Alarms													
Cybersecurity: TN + RBAC												0	100
Physical Limit Switches		0	0	0	0	0	0	0	0	0		0	0
Cumulative		331.8181818	331.8181818	331.8181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	33.18181818	331.8181818	3318.181818
	Intermediate event frequency	0.000814	0.000909	0.00048682	0.0000301	0.0000301	0.00003010	0.00003010	0.00003010	0.00003010	0.00003010	0.00000017	0.00000000
	Weight over the overall frequency	33.61%	37.57%	20.11%	1.24%	1.24%	1.24%	1.24%	1.24%	1.24%	1.24%	0.01%	0.00%
	Total mitigated event frequency	0.00242											
	Tolerable Event Frequency - LHC	0.01000											
	Tolerable Event Frequency - IP side	0.00250											
	Tolerable Event Frequency - Bellow	0.000119048											
	Residual Risk	0.00007922											

Conclusions and future work

- Critical system: a **failure of FRAS can provoke a downtime of the LHC up to 1 year**
- To bring this risk to the acceptable risk level:

FMEA top-down	FMEA	FTA	Risk matrix	Design of PLs	LOPA
High level	Component level	System level	CERN specific	IEC 61511	Demonstration

- Alternative solution to a SIS (Safety Instrumented system)
- Reliability information is obtained by operational experience at CERN, with many (conservative) assumptions.

- According to the data handled, the **tolerable risk** is accomplished if the alignment activity remains within **less than 11 full days** per year (area occupancy)

- The analysis showed that **the most critical failures may come from the actuation path and concretely by <u>software</u> flaws** (due to the high hardware redundancy)

- **Future work: (Software)**

Specification

Formal specification
Model-based engineering

Source code

Code synthesis (generation)
Formal verification (model checking)
Compositional verification

Executable

Testing
Runtime verification

Acknowledgements

CERN Beams department

- ICS (Industrial Controls Systems)
- CEM (Controls Electronics & Mechatronics)
- GM (Geodetic Metrology)

www.cern.ch

CAPE TOWN SOUTH AFRICA ICALEPCS 2023

Enrique Blanco Viñuela
Enrique.Blanco@cern.ch
Automation engineer, PhD in systems and process engineering
Head of the Control Systems Engineering section
Industrial Controls System group in the beams department at CERN