FRAS

Risk analysis and Protection Layers proposal according with the IEC 61511 standard

Borja Fernández Adiego **(BE-ICS)**

Mateusz Sosin **(BE-GM)**

Contains joint work of several members of the

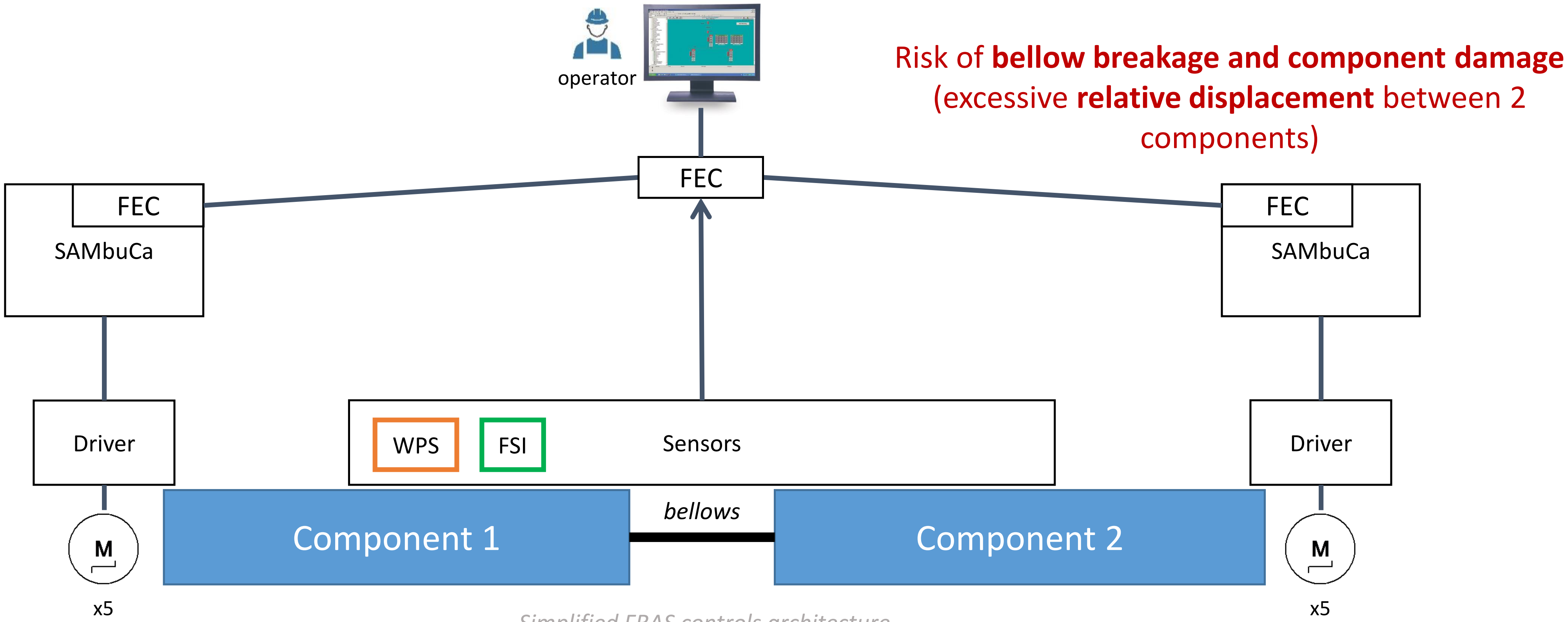
***BE-CEM**, BE-GM and BE-ICS groups*

Contents

Context and objectives

Context - FRAS

- The HL-LHC Full Remote Alignment System
- https://indico.cern.ch/event/806637/contributions/3487466/attachments/1925359/3186588/FRAS_MG.pdf

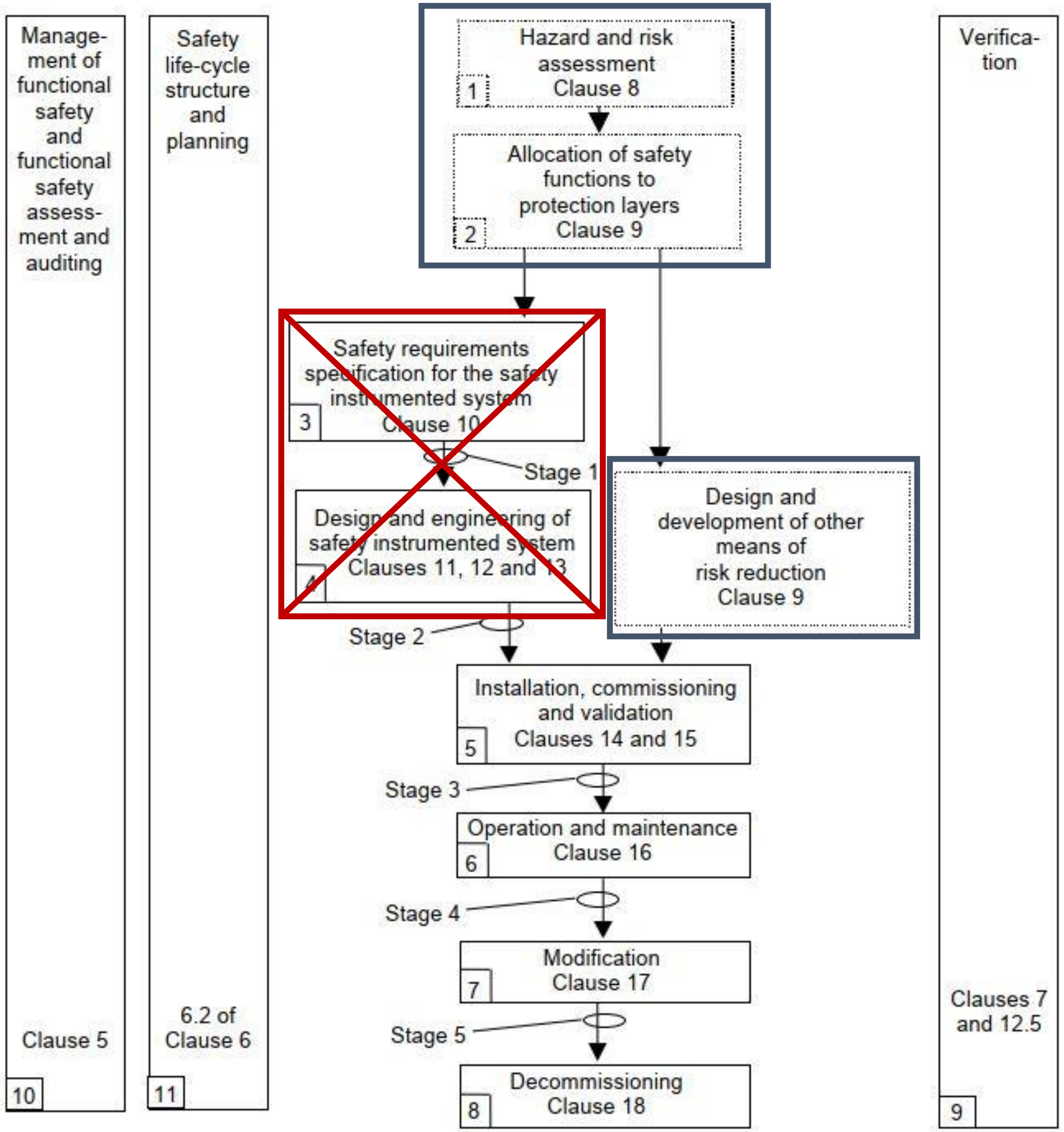


Simplified FRAS controls architecture

Context – IEC 61511 Safety Life Cycle

Safety Instrumented System requirements

- SIL
- Certified devices
- Architectural constrains
- Software requirements
- …



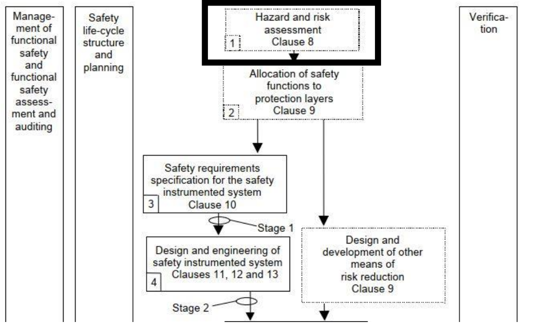
Protection Layers requirements

Objectives

1. Design and develop a **protection system** that meets the **necessary risk reduction** (both for personnel and **machine protection**)

2. Get recommendations and the **approval** of the **Machine Protection Panel (MPP)** https://edms.cern.ch/document/2727128/1

Hazard identification



Summary from the hazard identification

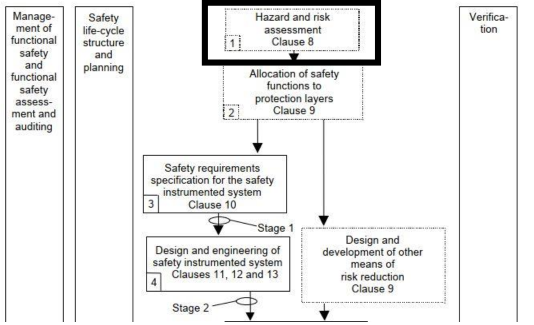
- **Scope:** analysis of any risk related to component **displacement**
  - **Displacement provoked by FRAS**
  - **Any other displacement** (provoked by a quench, any other ground motion, etc.)

- Risk analysis based on the **FMEA** (Failure Mode and Effect Analysis) https://edms.cern.ch/document/2727128/1

- Includes the analysis of **personnel** and **machine** risks

- **4 “FRAS-LHC scenarios”** have been analyzed:
  1. “remote alignment”: Alignment is allowed, NO beam and NO personnel in the tunnel
  2. “maintenance”: Alignment is allowed, NO beam and personnel in the tunnel
  3. “pilot beam”: Alignment is allowed, low intensity beam is injected and no personnel in the tunnel
  4. “high intensity beam”: Alignment is NOT allowed, high intensity beam and no personnel in the tunnel

Summary from the hazard identification



- Several failure modes were identified (≈ 10)

- 2 main **effects for machine protection:**
  1. Bellow breakage (potentially up to 1 year of delay for the LHC)
  2. Component damage (potentially more than 1 year of delay for the LHC)

- 1 **effect for personnel**
  1. 1 fatality by helium intoxication (or by impact with a component)

- The potential **causes** are:
  1. **Software or communication** error on "FRAS control system" (FEC, Sambuca, etc.)
  2. **Controls hardware** failure on the "FRAS control system" (motor, FEC, Sambuca driver, etc.)
  3. **Wrong operator/expert** command ("depending of the operational mode")
  4. Mechanical problem on the **jack support**
  5. **Quench**
  6. Ground motion
  7. **Power Failure**

Failure provoked by the FRAS control system

Failure provoked by other external systems

Summary from the hazard identification – machine protection

	Subsystem	Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard
REMOTE ALIGNMENT MODE (NO BEAM)					
1	All components (magnets, masks and collimators)	vertical displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command	
		horizontal displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command	
		rotational displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command	
		Components position out of alignment limits	(2) Component damage (in the next injection)	(3) Wrong operator command	(1) Operator procedure (validation of the component's alignment) (2) Detection of machine missalignment during pilot beam validations? (3) BLM interlock (Beam dump) during the PILOT beam mode if missalignment
		Realigment in the WRONG direction when a PL has been triggered	(1) Bellow damage	(3) Wrong operator command	
		Unpowered control system	No damage - motors movements would stop inmediately	(7) Power failure	
2	Only magnets and TAXN	Magnet drop due to mechanical problem on the jack	(1) bellow damage (2) Component damage	(4) Lossing of vertical support of the jack	(4) Operator procedure (motors and magnets shifts compared during the alignment process) (5) Load cells installed to control vertical contact between adapter and jack RAM. Alarm raised when the support load reaches the threshold (1) Operator procedure (validation of the component's alignment)

Failure mode provoked by the FRAS control system

Failure mode provoked by operator or other external systems

Summary from the hazard identification – machine protection

	Subsystem	Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard
HIGH INTENSITY BEAM					
1	Only magnets and TAXN	Magnet drop due to mechanical problem on the jack	(1) bellow damage (2) Component damage	(4) Lossing of vertical support within the jack	(4) Operator procedure (motors and magnets shifts compared during the alignment process) (5) Load cells installed to control vertical contact between adapter and jack RAM. Alarm raised when the support load reaches the threshold (1) Operator procedure (validation of the component's alignment)
2	Only magnets	Rapid component position change (~ 100um) caused by quench	(4) Component position drift (~100um) with beam (no component damage expected with small drift)	(5) Quench	(7) FRAS motors will be unpowered (6) QPS will detect the quench and dump the beam
3	magnets, masks and collimators	Component position out of alignment limits	(2) Component damage	(6) Ground motion bigger than alignment limits	(7) FRAS motors will be unpowered (3) BLM interlock if missalignment too big (BEAM DUMP)
		ANY displacement by FRAS	(1) Bellow damage (3) Component damage	(3) Wrong operator command (accidental turn ON the FRAS CCC KEY which power the motors while high intensity beam)	
		Unpowered control system	No damage - motors movements would stop inmediately	(7) Power failure	(7) FRAS motors will be unpowered

Failure mode provoked by a mechanical problem

Failure mode provoked by a quench or any other ground motion

Failure mode provoked by an operator mistake

Failure mode provoked by an external system

Summary from the hazard identification

Failure mode	LHC-FRAS scenarios	Machine consequences	Personnel consequences	Causes
V (vertical) – bellow limits R (rotational) – bellow limits H (horizontal) – bellow limits	Remote alignment Maintenance Pilot beam **High intensity beam*	Bellow damage	Asphyxia by helium	Software or communication error or Controls hardware failure or Wrong operator command
ANY component displacement – beam limits	**Remote alignment* **Maintenance* *Pilot beam High intensity beam	Component damage	-	Mechanical problem on the jack or ground motion or movement of the FRAS motors
Unpowered control system	Remote alignment Maintenance Pilot beam	-	-	Power failure
Rapid component position change	High intensity beam	-	-	Quench

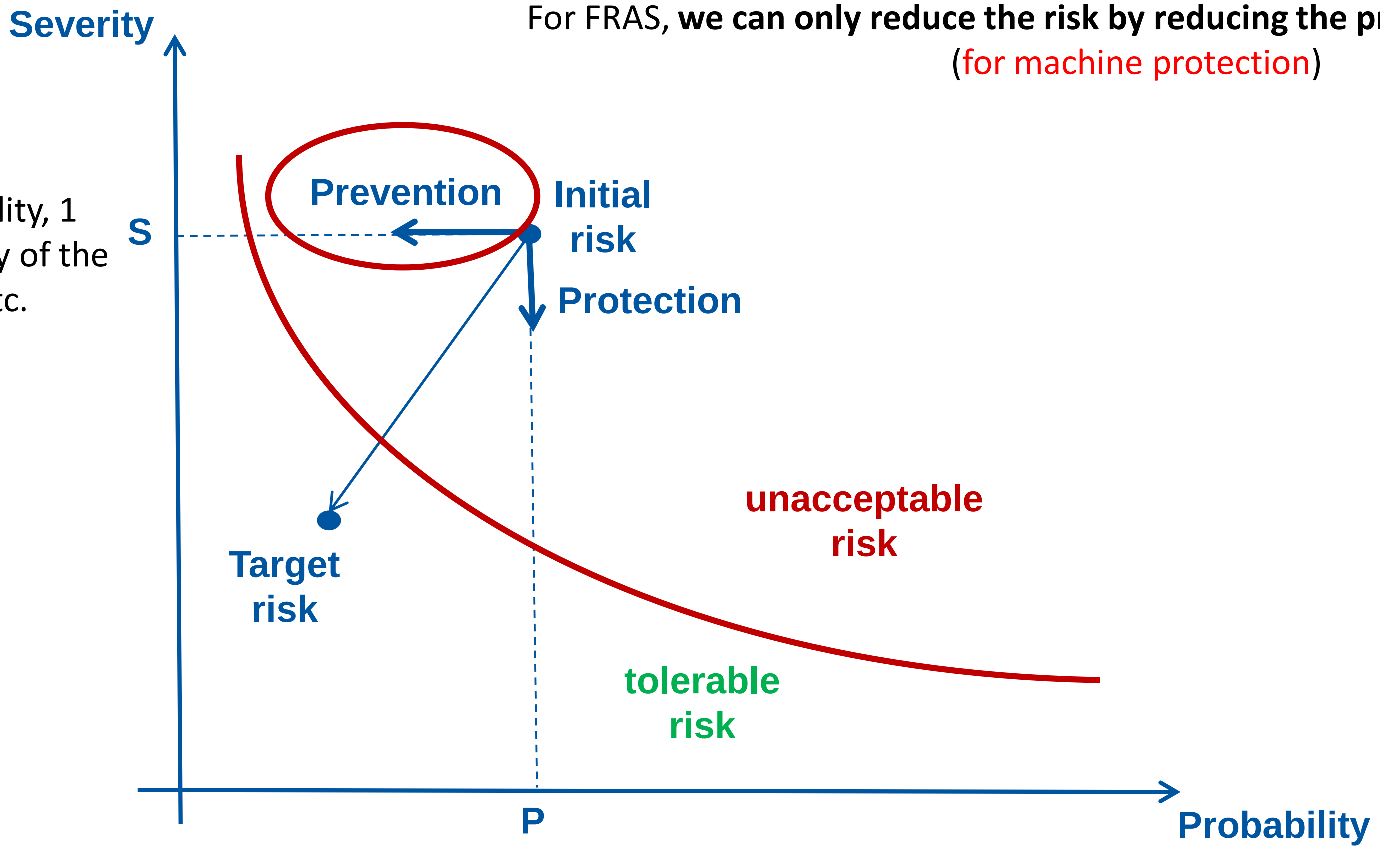
* The corresponding failure mode should never occur in this scenario

Risk assessment
(evaluation of the necessary risk reduction)

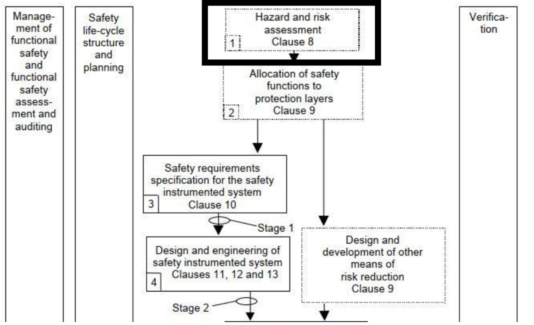
Risk assessment - Risk reduction and layers of protection

For FRAS, **we can only reduce the risk by reducing the probability of occurrence** (for machine protection)

e.g. 1 fatality, 1 year of delay of the LHC, etc.



e.g. 1 failure in 10 years

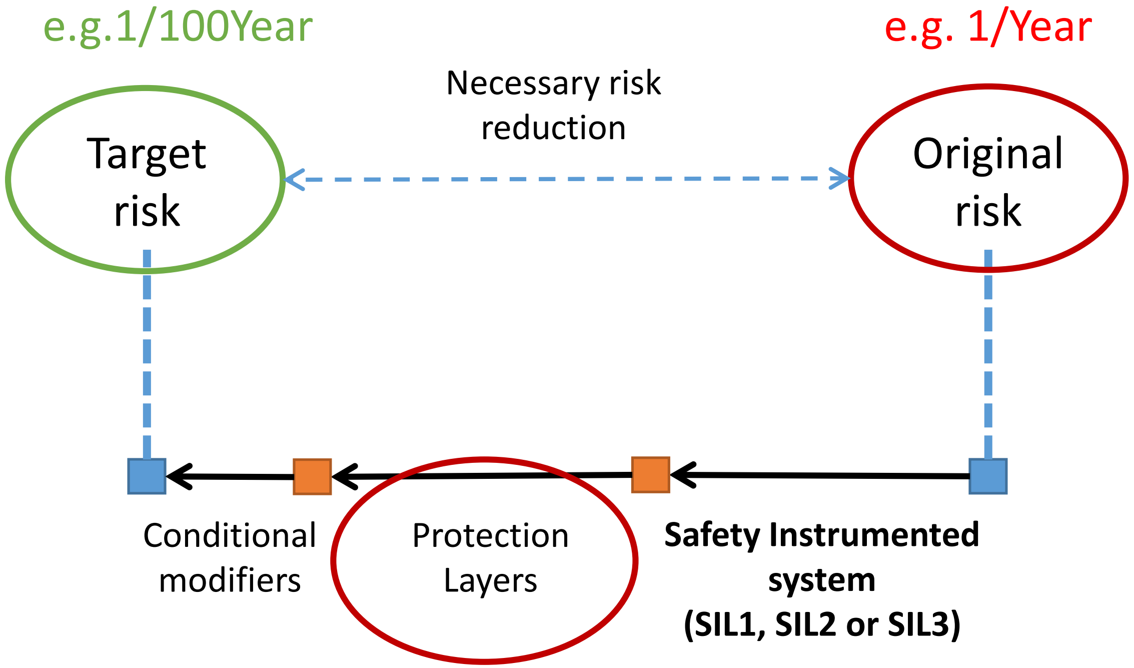


Risk assessment - Risk reduction and layers of protection

Depends on the definition of **tolerable risk** (combination of frequency and the severity of the risk)

How?

- **Judgement** of the organization
- based on the **"LHC risk matrices"** provided by BE-MPE (EDMS 2647876) and **the IEC 61511-3 methods**



According to the Functional Safety Standards
IEC 61508, IEC 61511 or IEC 62061

Estimation of the original failure frequency due to:

- Operator/expert command
- Software
- Hardware
- Quench
- …

How?

- Collected data from similar systems and operational experience
- Reliability predictions (e.g. MIL-HDBK-217) https://www.isograph.com/software/reliability-workbench/prediction-software/mil-hdbk-217/)
- Based on the **IEC 61511-3 guidelines**

Risk assessment - Estimation of initial risk frequency

IEC 61511-3 Annex G: Layer of protection analysis using a risk matrix

Table G.3 – Example initiating causes and associated frequency

Initiating cause	Conditions	MTBF[a] in years	
Basic Process Control Loop (BPCS)	Complete instrumented loop, including the sensor, controller, and final element.	10	HMI + FEC + Sambuca + Driver + Motor
Operator Action (SOP)	Action is performed daily or weekly per procedure. The operator is trained on the required action. {This value can be reduced by a factor of 10 (value=1 in 10 years) based on experience. The team should document job aids, procedures, and/or training used to achieve 1 in 10 years.}	1	
	Action is performed monthly to quarterly per procedure. The operator is trained on the required action.	10	FRAS operator
	Action is performed yearly, after turnaround or temporary shutdown per procedure. The operator is trained on the required action.	100	FRAS expert
Instrumented Safety Device (OTHER)	Instrumented safety device spuriously operates, e.g., closure of block valve, pump shutdown, and opening of vent valve.	10	other devices?

[a] The initiating causes listed can be assumed to occur more frequently (e.g., changed from 1/100 year to 1/10 year based on process experience. The values cannot be made less frequent without additional justification and approval by process safety. Additional analysis should be submitted as part of the justification. This would include human factors analysis, failure modes and effects analysis (FMEA), event tree analysis or fault tree analysis.

Risk assessment - Estimation of initial risk frequency

List of identified causes	Estimated frequency	
(1) Software or communication error	1/10Y	Based on the IEC 61511 guidelines
(2) Controls hardware failure	1/10Y	
(3) Wrong operator command	1/10Y	
(4) Losing jack support	1/10Y	*Based on the operational experience (feedback required)
(5) Quench	1/M	
(6) Ground motion bigger than alignment limits	1/10Y	
(7) Power failure	1/Y	

* Initial proposal - Estimation to be validated/corrected

Estimation of initial risk frequency

IEC 61511-3 Annex G: Layer of protection analysis using a risk matrix

Table G.3 – Example initiating causes and associated frequency

Initiating cause	Conditions	MTBF[a] in years
Basic Process Control Loop (BPCS)	Complete instrumented loop, including the sensor, controller, and final element.	10
Operator Action (SOP)	Action is performed daily or weekly per procedure. The operator is trained on the required action. {This value can be reduced by a factor of 10 (value=1 in 10 years) based on experience. The team should document job aids, procedures, and/or training used to achieve 1 in 10 years.}	1
	Action is performed monthly to quarterly per procedure. The operator is trained on the required action.	10
	Action is performed yearly, after turnaround or temporary shutdown per procedure. The operator is trained on the required action.	100
Instrumented Safety Device (OTHER)	Instrumented safety device spuriously operates, e.g., closure of block valve, pump shutdown, and opening of vent valve.	10

[a] The initiating causes listed can be assumed to occur more frequently (e.g., changed from 1/100 year to 1/10 year based on process experience. The values cannot be made less frequent without additional justification and approval by process safety. Additional analysis should be submitted as part of the justification. This would include human factors analysis, failure modes and effects analysis (FMEA), event tree analysis or fault tree analysis.

$$\lambda_{DU} = \frac{1}{MTBF}$$

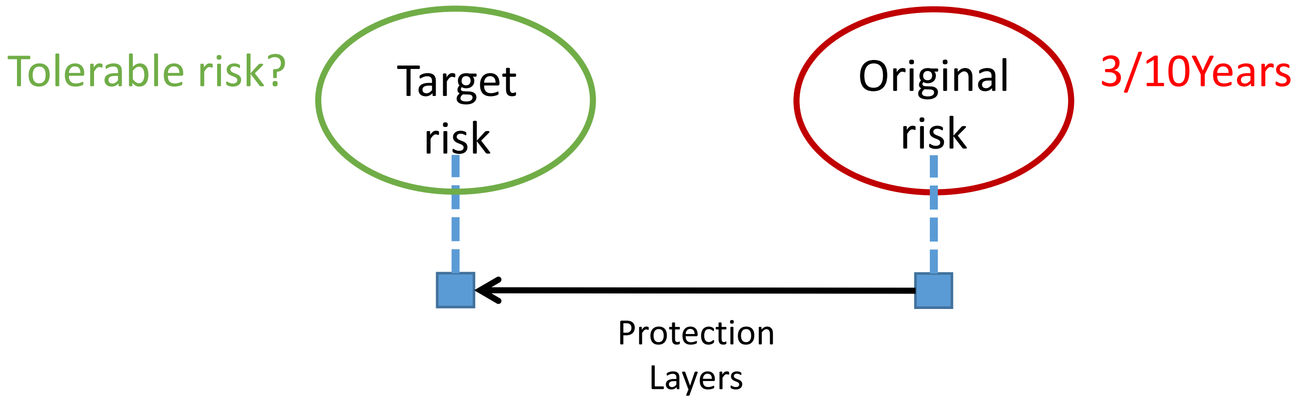
Worst case scenario

$$\lambda_{DU} = \frac{1}{10} + \frac{1}{10} + \frac{1}{10} = \frac{3}{10}$$

3 potential **failures** every **10 years** (CCC operator)

$$\lambda_{DU} = \frac{1}{10} + \frac{1}{100} + \frac{1}{10} = \frac{21}{100}$$

2.1 potential **failures** every **10 years** (FRAS expert)



Risk assessment - Estimation of the effect damage (LHC downtime)

List of identified consequences for the LHC	Estimated LHC downtime
(1) Bellow damage	1M - 1Y
(2) Component damage (in the next injection)	1Y - 10Y

Initial proposal - Estimation to be validated/corrected

Risk assessment - Tolerable risk (machine protection)

Data-driven risk matrix for LHC

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

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

λ_2

Machine protection:

- Based on experience of the MPE group at CERN – risk matrices for the LHC (EDMS2647876)

Example of "exceeding the bellow limits" Failure Mode

Risk reduction factor

$$RRF = \frac{\lambda_1}{\lambda_2}$$

$$RRF = \frac{3}{10} / \frac{1}{100} = 30 \approx 100$$

Considering the initial freq. (λ_1) between 1/Year and 1/10Year and an expected LHC delay between 1 month and 1 year, then the necessary **Risk Reduction Factor (RRF) is 100** – equivalent to SIL2

Risk assessment - Tolerable risk (machine protection)

Subsystem		Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard	Determination of Acceptability				Acceptability	
						Consequence (for the system)		Base Probability of failure		Matrix Result	Distance
Id	Description	Description				In terms of time delay		In terms of 1/time			
						Chosen value	Comments or Justifications	Chosen value	Comments and justifications	A = Acceptable U = Unacceptable	Distance from the first acceptable state on the Y-
REMOTE ALIGNMENT MODE (NO BEAM)											
1	All components (magnets, masks and collimators)	vertical displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command		1M-1Y	Delay of several to repair the interconnection bellow	1/Year	Estimated according the IEC 61511 guidelines	U	2
		horizontal displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command		1M-1Y	Delay of several to repair the interconnection bellow	1/Year	Estimated according the IEC 61511 guidelines	U	2
		rotational displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command		1M-1Y	Delay of several to repair the interconnection bellow	1/Year	Estimated according the IEC 61511 guidelines	U	2

Necessary **Risk Reduction of 100**

Subsystem		Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard	Determination of Acceptability				Acceptability	
						Consequence (for the system)		Base Probability of failure		Matrix Result	Distance
Id	Description	Description				In terms of time delay		In terms of 1/time			
HIGH INTENSITY BEAM											
3	All components (magnets, masks and collimators)	Component position out of alignment limits	(2) Component damage	(6) Ground motion bigger than alignment limits	(7) FRAS motors will be unpowered (3) BLM interlock if missalignment too big (BEAM DUMP)	1Y-10Y	Delay of 1 year or more to replace the component	1/100Years	Estimation: significant ground moion AND BLM interlock failure	U	1

Necessary **Risk Reduction of 10**

Risk assessment - Tolerable risk (machine protection)

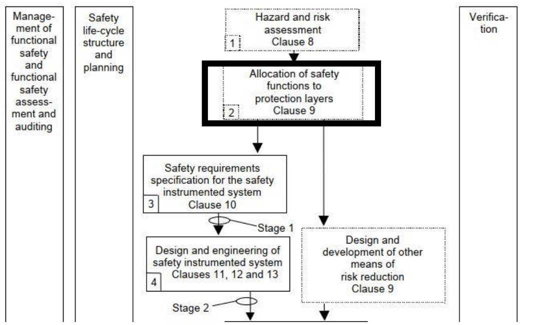
Subsystem		Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard	Determination of Acceptability				Acceptability	
						Consequence (for the system)		Base Probability of failure		Matrix Result	Distance
Id	Description	Description				In terms of time delay		In terms of 1/time			
HIGH INTENSITY BEAM											
3	All components (magnets, masks and collimators)	Component position out of alignment limits	(2) Component damage	(6) Ground motion bigger than alignment limits	(7) FRAS motors will be unpowered (3) BLM interlock if missalignment too big (BEAM DUMP)	1Y-10Y	Delay of 1 year or more to replace the component	1/100Years	Estimation: significant ground moion AND BLM interlock failure	U	1

Necessary Risk **Reduction of 10**

Not considering the BLM risk reduction

Subsystem		Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard	Determination of Acceptability				Acceptability	
						Consequence (for the system)		Base Probability of failure		Matrix Result	Distance
Id	Description	Description				In terms of time delay		In terms of 1/time			
HIGH INTENSITY BEAM											
3	All components (magnets, masks and collimators)	Component position out of alignment limits	(2) Component damage	(6) Ground motion bigger than alignment limits	(7) FRAS motors will be unpowered	1Y-10Y	Delay of 1 year or more to replace the component	1/10Years	Estimation: significant ground moion	U	2

Necessary Risk **Reduction of 100**



Tolerable risk for FRAS (summary)

- The necessary **risk reduction is 100 or 10 according with the current estimations** (frequency and LHC delay time)

- Machine protection establishes the max. risk reduction (more critical than personnel protection)

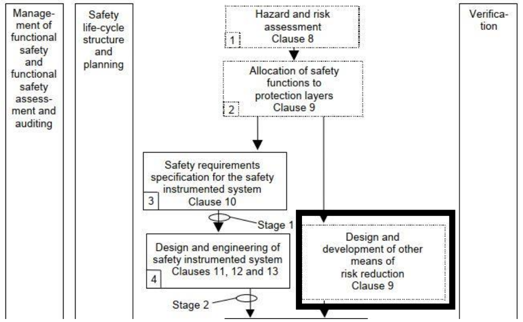
- A risk reduction of 100 can be achieved by:
  - A SIL2 Safety Instrumented System (certified devices, very strict safety requirements, etc.)
  - **2 independent Protection Layers** if we meet the requirements of the IEC 61511-3 Annex C

- **Due to some technical** (and economical) **challenges, we don't recommend to develop a Safety Instrumented System (SIS). Some** of these challenges are:
  - The sensor technology: radiation tolerant and SIL certified devices, etc.
  - The software requirements: usage of FVL (Full Variability Language) – IEC 61508-3 requirements

- **We propose the Protection Layers alternative** (following the IEC 615111-3 Annex C guidelines)

Protection Layers design (IEC 61511)

Protection Layers design (IEC 61511-3 Annex C)



a) A protection layer consists of a grouping of equipment and/or administrative controls that function in concert with other protection layers to control or mitigate process risk.

b) A protection layer (PL) meets the following criteria:

- Reduces the identified risk by at least a factor of 10;
- Has the following important characteristics:
  - Specificity – a PL is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a PL.
  - Independence – a PL is independent of other protection layers if it can be demonstrated that there is no potential for common cause or common mode failure with any other claimed PL.
  - Dependability – the PL can be counted on to do what it was designed to do by virtue of addressing both random failures and systematic failures in its design.
  - Auditability – a PL is designed to facilitate regular validation of the protective functions.

c) A safety instrumented system (SIS) protection layer is a protection layer that meets the definition of a SIS in IEC 61511-1:2016 Clause 3.2.69 (“SIS” was used when safety layer matrix was developed).

Necessary Risk Reduction	Number of PLs
10 (SIL1)	1
100 (SIL2)	2
1000 (SIL3)	3

Analysis of the Protection Layers (IEC 61511-2 Annex A)

9.4 Requirements for preventing common cause, common mode and dependent failures

9.4.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between:

- protection layers;
- protection layers and the BPCS.

are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.

NOTE A definition of dependent failure is provided in 3.2.12.

9.4.2 The assessment shall consider the following:

- 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.

Mitigation proposal – Protection layers (machine protection)

Id	Subsystem	Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard	Determination of Acceptability: Consequence (for the system)		Determination of Acceptability: Base Probability of failure		Acceptability: Matrix Result	Acceptability: Distance	FRAS Control system actions	Mitigation proposal: Independent Protection Layers (IPLs)	Mitigation proposal: Safety Instrumented Function (SIF)
	Description	Description				In terms of time delay		In terms of 1/time						
						Chosen value	Comments or Justifications	Chosen value	Comments and justifications	A = Acceptable U = Unacceptable	Distance from the first acceptable state on the Y-			
REMOTE ALIGNMENT MODE (NO BEAM)														
1	All components (magnets, masks and collimators)	vertical displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command		1M-1Y	Delay of several to repair the interconnection bellows	1/Year	Estimated according the IEC 61511 guidelines	U	2		2 PLs are needed - PL1 and PL2 will be available (also PL3 in some components)	
		horizontal displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command		1M-1Y	Delay of several to repair the interconnection bellows	1/Year	Estimated according the IEC 61511 guidelines	U	2		2 PLs are needed - PL1 and PL2 will be available	
		rotational displacement (exceeding the bellow limits)	(1) Bellow damage	(1) Software or communication error, or (2) Controls hardware failure, or (3) Wrong operator command		1M-1Y	Delay of several to repair the interconnection bellows	1/Year	Estimated according the IEC 61511 guidelines	U	2		2 PLs are needed - PL1, PL2 and PL3 will be available	

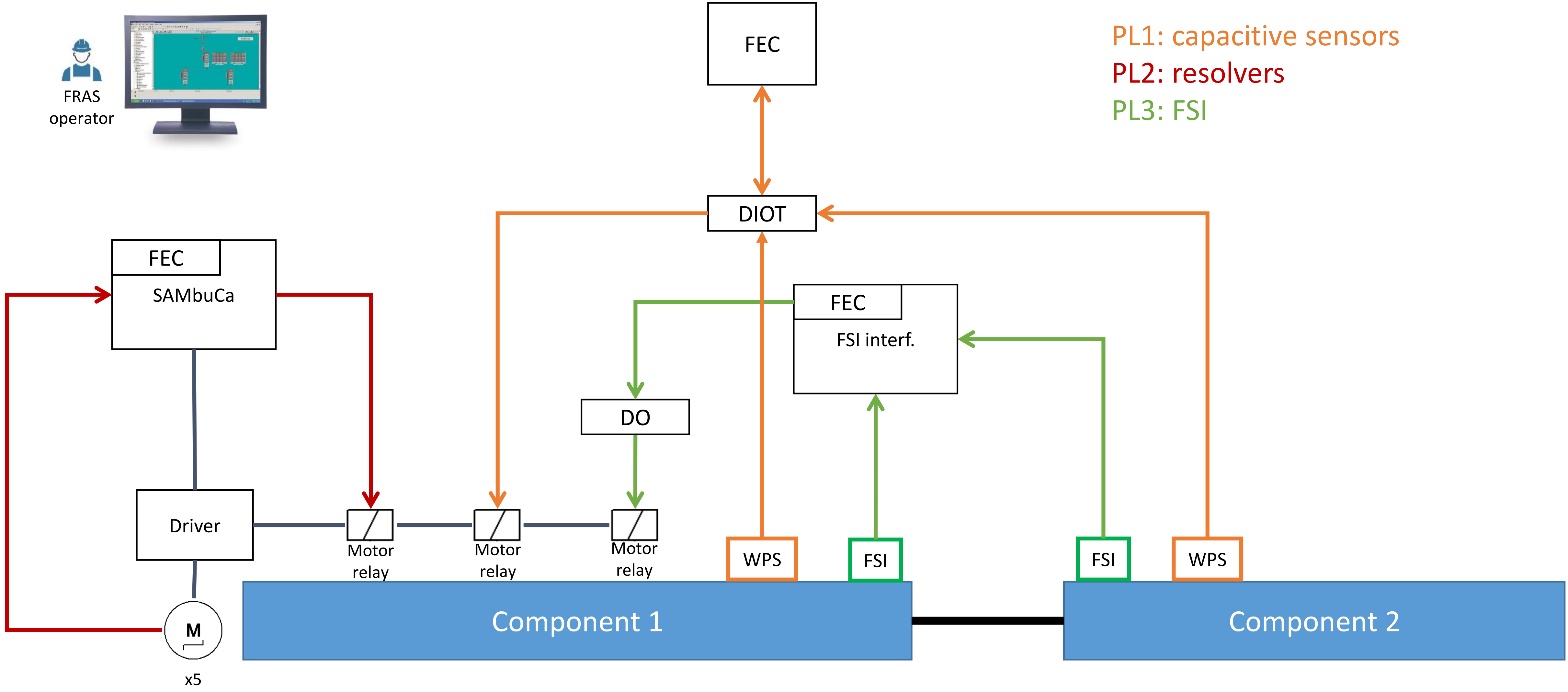
2 Layers of Protection

Id	Subsystem	Failure mode	Effects of the failure mode on the system	Causes of failure	Current mitigation measures for the failure mode or the hazard	Determination of Acceptability: Consequence (for the system)		Determination of Acceptability: Base Probability of failure		Acceptability: Matrix Result	Acceptability: Distance	FRAS Control system actions	Mitigation proposal: Independent Protection Layers (IPLs)	Mitigation proposal: Safety Instrumented Function (SIF)
	Description	Description				In terms of time delay		In terms of 1/time						
HIGH INTENSITY BEAM														
3	All components (magnets, masks and collimators)	Component position out of alignment limits	(2) Component damage	(6) Ground motion bigger than alignment limits	(7) FRAS motors will be unpowered (3) BLM interlock if missalignment too big (BEAM DUMP)	1Y-10Y	Delay of 1 year or more to replace the component	1/100Years	Estimation: significant ground moion AND BLM interlock failure	U	1		**1 PL is needed**: interlock (Machine missaligned) sent to the **BIS OR SIS**	

1 Layers of Protection

Protection Layers
to protect bellow breakage

Protection layers proposal for bellow protection (functional schema)



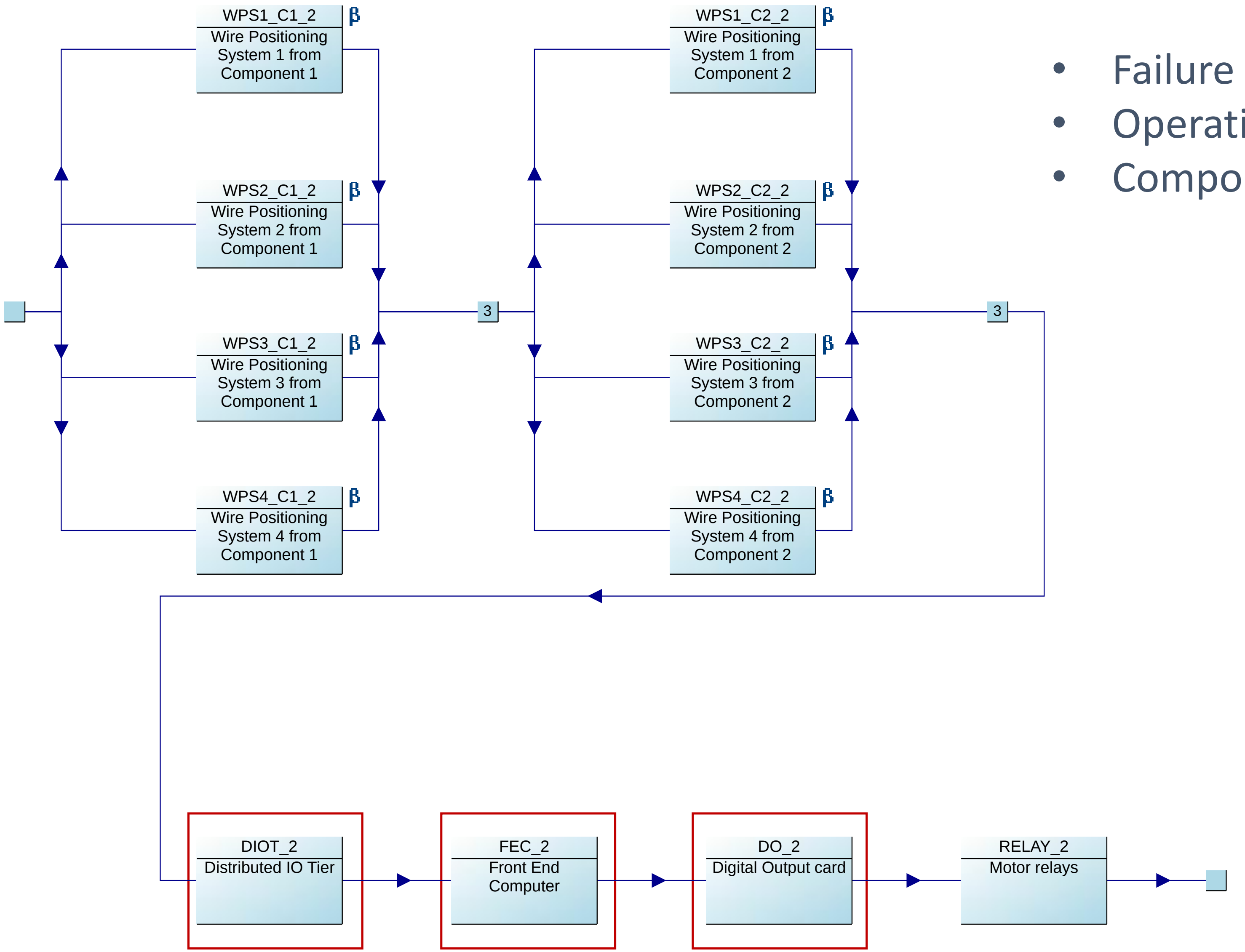
PLs and risk reduction summary

FRAS component	Failure mode	Available PLs	Achieved risk reduction*
Collimators, Masks, Crab Cavity, TAXN	R (rotational)	PL1.1, PL2 and PL3.1	1000 (“SIL3”)
	V (vertical)	PL1.1 and PL2	100 (“SIL2”)
	H (horizontal)	PL1.1 and PL2	100 (“SIL2”)
Q4, Q5, D2	R (rotational)	PL1.1, PL2, PL3.1 (and PL3.3 ex. Q4/5-Mask)	1000 (“SIL3”)
	V (vertical)	PL1.1, PL2 and PL3.3	1000 (“SIL3”)
	H (horizontal)	PL1.1 and PL2	100 (“SIL2”)
Triplet zone (Q1-D1)	R (rotational)	PL1.2, PL2, PL3.1 (and PL3.2)	1000 (“SIL3”)
	V (vertical)	PL1.2, PL2 and PL3.2	1000 (“SIL3”)
	H (horizontal)	PL1.2 and PL2	100 (“SIL2”)

PL1: capacitive sensors
PL2: resolvers
PL3: FSI

*if the IEC 61511-3 Annex C requirements are met

PL1.2: Capacitive sensors – Isograph model

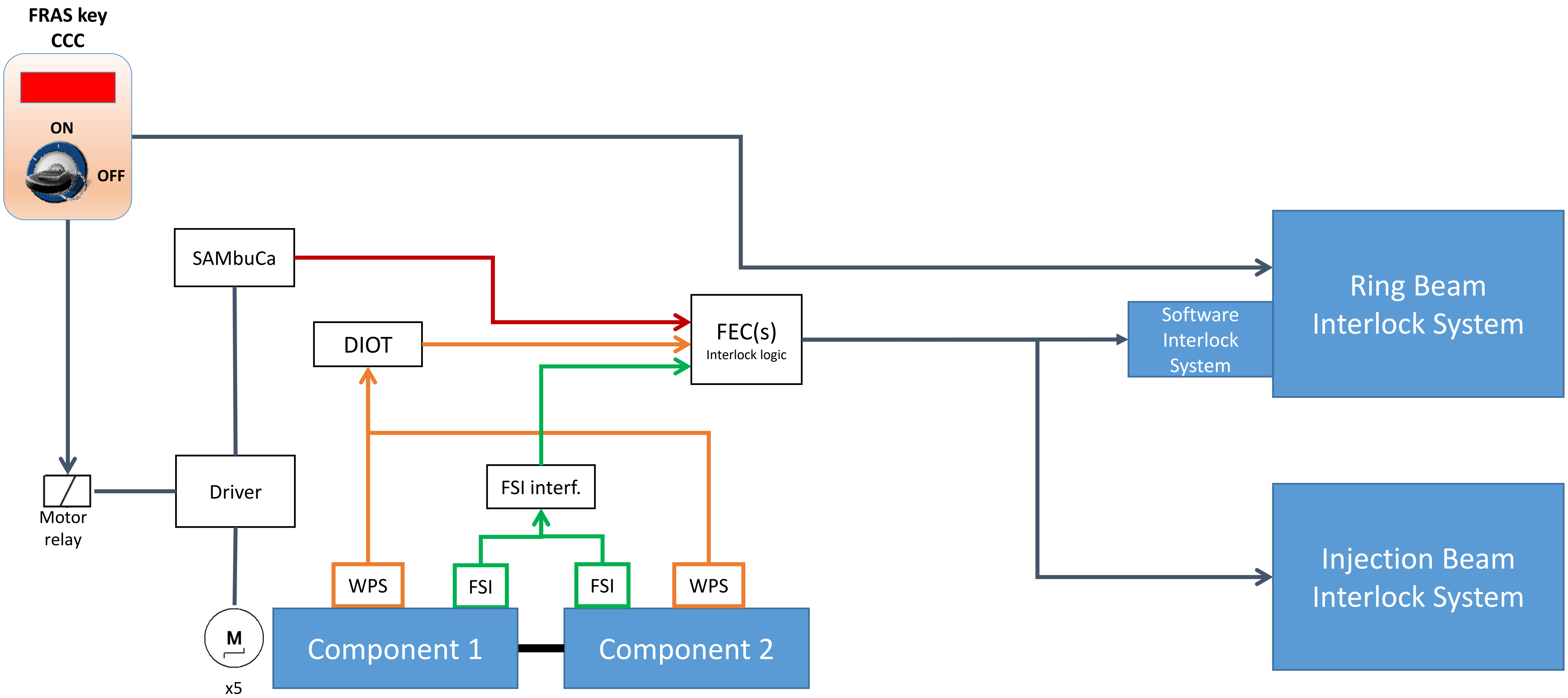


- Failure Modes: V, H and R
- Operational Modes: 1, 2 and 3
- Components: Triplets-D1

Protection Layers
to protect component damage

Protection layers proposal for component protection (functional schema)

Beam Interlock System for the LHC https://edms.cern.ch/ui/file/567256/0.2/LHC-CIB-ES-0001-00-10.pdf



Conclusions

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

- The **“calibration” of the risk graph and the estimations** of the consequence 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** (we can provide 3 in many component configurations)
  - We need **1 extra PL for component protection**:
    - FRAS key to avoid a misalignment provoked by FRAS – ring BIS
    - Software interlock signal to SIS and Injection BIS if a misalignment is detected

- Potential **Common Cause of Failures between the different layer must be analyzed**

- We are currently exploring the possibility of replacing the FEC by a PLC for the PL1 (capacitive sensors)

Conclusions

a) A protection layer consists of a grouping of equipment and/or administrative controls that function in concert with other protection layers to control or mitigate process risk.

b) A protection layer (PL) meets the following criteria:

- Reduces the identified risk by at least a factor of 10;
- Has the following important characteristics:
  - Specificity – a PL is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a PL.
  - Independence – a PL is independent of other protection layers if it can be demonstrated that there is no potential for common cause or common mode failure with any other claimed PL.
  - Dependability – the PL can be counted on to do what it was designed to do by virtue of addressing both random failures and systematic failures in its design.
  - Auditability – a PL is designed to facilitate regular validation of the protective functions.

Special attention to the PL software and radiation

- diversity between protection layers – the aim should be diversity between protection layers and the BPCS but this is not always achievable. Some diversity can be achieved by using equipment from different manufacturers but if SIS and BPCS sensors are connected to the process using the same type of hook up, then the diversity may be of limited value;

FECs and FESA