FRAS

Protection Layers analysis according with the IEC 61511 standard

Borja Fernández Adiego **(BE-ICS)**

Mateusz Sosin **(BE-GM)**

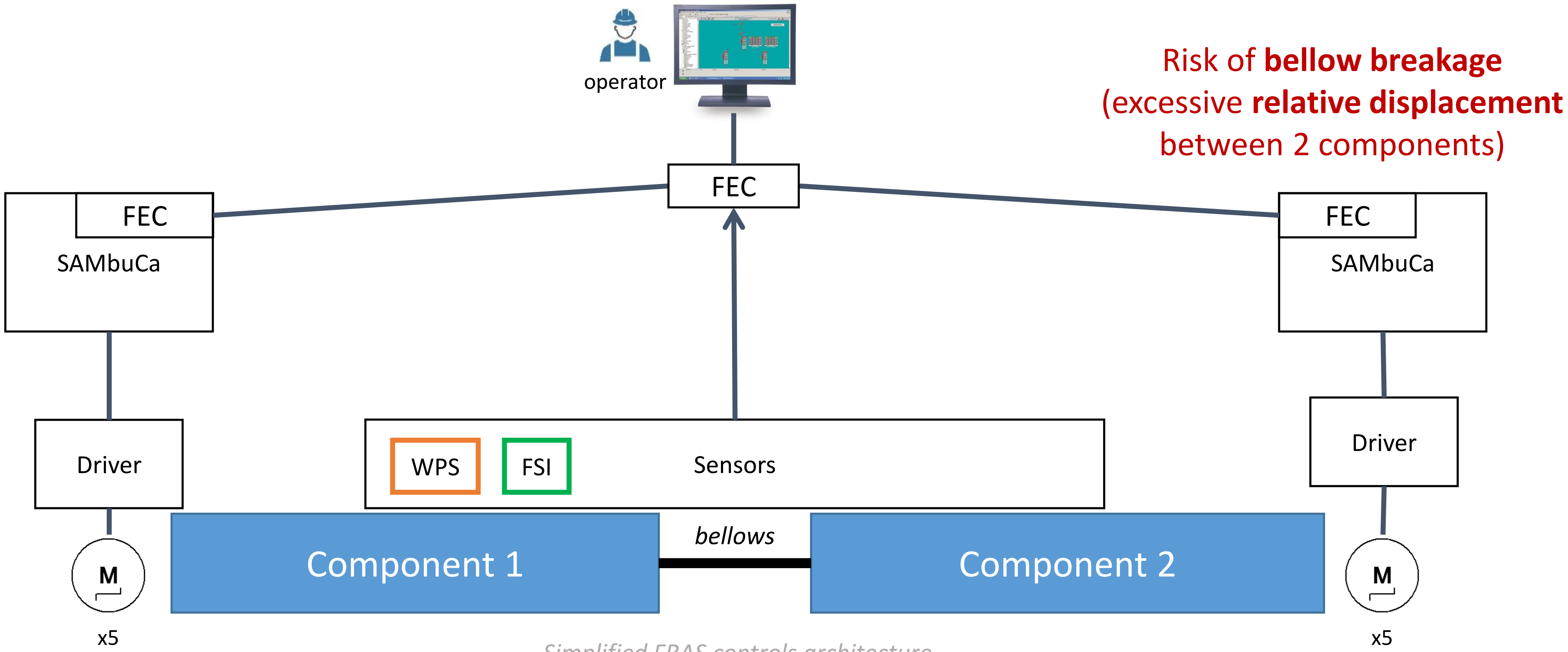
Contains joint work of several members of the

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

Contents

Context - FRAS

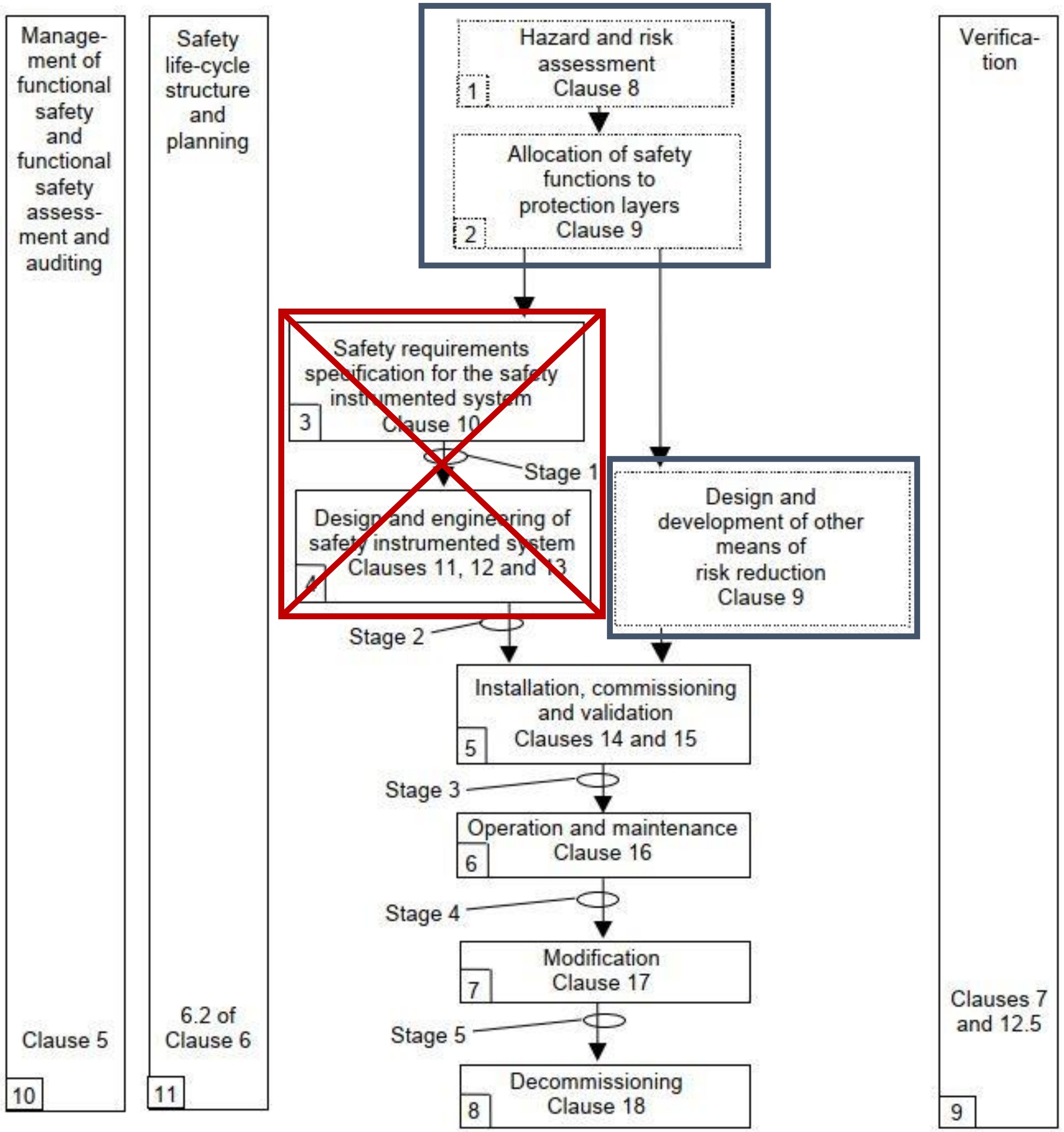
- The HL-LHC Full Remote Alignment System
- https://indico.cern.ch/event/806637/contributions/3487466/attachments/1925359/3186588/FRAS_MG.pdf



Simplified FRAS controls architecture

Context – IEC 61511 Safety Life Cycle

Safety Instrumented System requirements

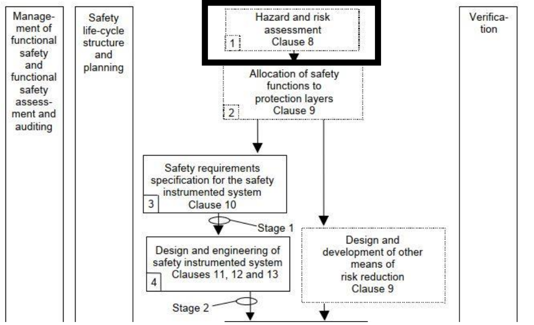


Protection Layers requirements

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)**



Summary from the hazard identification

- Risk analysis based on the **FMEA** (Failure Mode and Effect Analysis)

- **3 failure modes were identified** (vertical, horizontal and rotational displacement)

- **The 3 FRAS operational modes** were analyzed ("remote alignment", "maintenance" and "standby" modes)

- The **worst effect for machine protection** is the breakage of the bellows and potential 1 year of delay for the LHC

- The **worst effect for personnel** is potentially a 1 fatality by helium intoxication

- The potential **causes** are:
  - **Operator** or **expert** mistake ("depending of the operational mode")
  - **Software/communication** error on "FRAS control system" (FEC, Sambuca, etc.)
  - **Hardware** error on the "FRAS control system" (motor, FEC, Sambuca driver, etc.)

Summary from the hazard identification – Machine protection

Subsystem		Failure mode	Effects of the failure mode on the system	Causes of failure
Id	Description	Description		
REMOTE ALIGNMENT MODE				
1	magnets, masks and collimators	vertical displacement (exciding the bellow limits)	Bellows damage, break of insulation vacuum, Break of beam vacuum. Possibility of the helium spill if He-interconnection lines damaged (only for magnets)	Software error, communication error, hardware error (motor driver, sambuca, FEC, etc.), wrong command (operator mistake)
		horizontal displacement (exciding the bellow limits)	Bellows damage, break of insulation vacuum, Break of beam vacuum. Possibility of the helium spill if He-interconnection lines damaged (only for magnets)	Software error, communication error, hardware error (motor driver, sambuca, FEC, etc.), wrong command (operator mistake)
		rotational displacement (exciding the bellow limits)	Bellows damage, break of insulation vacuum, Break of beam vacuum. Possibility of the helium spill if He-interconnection lines damaged (only for magnets)	Software error, communication error, hardware error (motor driver, sambuca, FEC, etc.), wrong command (operator mistake)

- For all failure modes, all FRAS operational modes and both personnel and machine protection, **the causes of failure are the same (same hazardous event)**

Why do we analyze 3 failure modes?

- To mitigate a failures mode, we need to equip the accelerator with sensors that can detect a specific displacement
- the **available sensors** (FSI, resolvers, Inclinometers, etc.) **detect different type of displacements** (vertical, horizontal and rotational)
- Not all sensors are available for all **LHC component configurations**

Summary from the hazard identification – Personnel protection

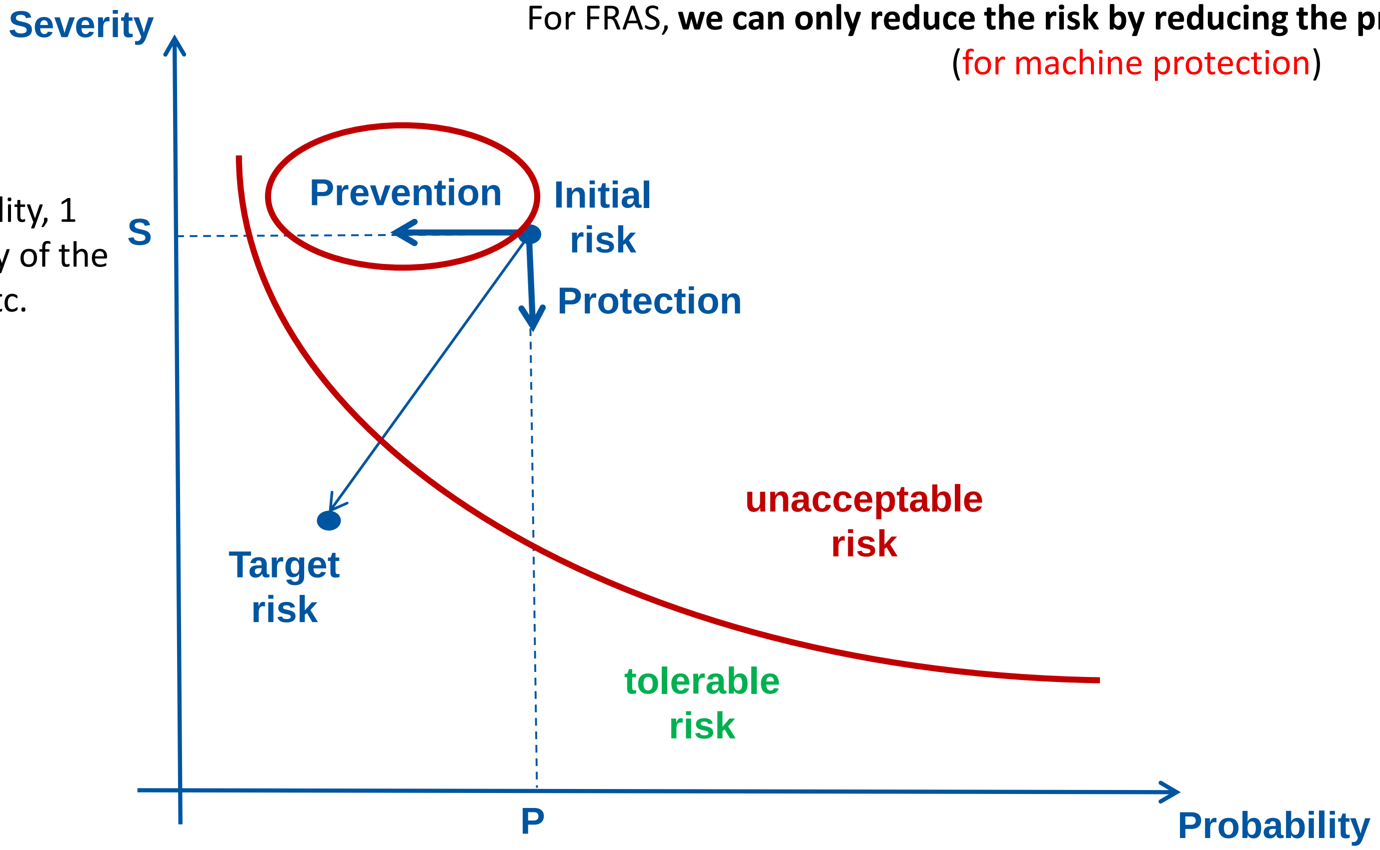
Subsystem		Failure mode	Effects of the failure mode on the system	Causes of failure
Id	Description	Description		
MAINTENANCE MODE Maintenance mode is a Remote alignment mode, with experienced FRAS operator working in				
1	magnets, masks and collimators	vertical displacement (exciding the bellow limits)	one fatality due to helium spill and asphyxion	Software error, communication error, hardware error (motor driver, sambuca, FEC, etc.), wrong command (operator mistake)
		horizontal displacement (exciding the bellow limits)	one fatality due to helium spill and asphyxion	Software error, communication error, hardware error (motor driver, sambuca, FEC, etc.), wrong command (operator mistake)
		rotational displacement (exciding the bellow limits)	one fatality due to helium spill and asphyxion	Software error, communication error, hardware error (motor driver, sambuca, FEC, etc.), wrong command (operator mistake)

Same potential **cause** of failure

Risk assessment - Risk reduction and layers of protection

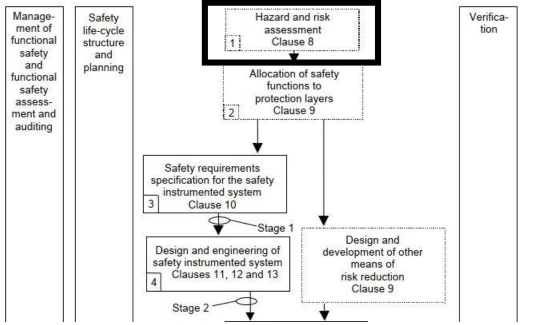
For FRAS, **we can only reduce the risk by reducing the probability of occurrence** (for machine protection)

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



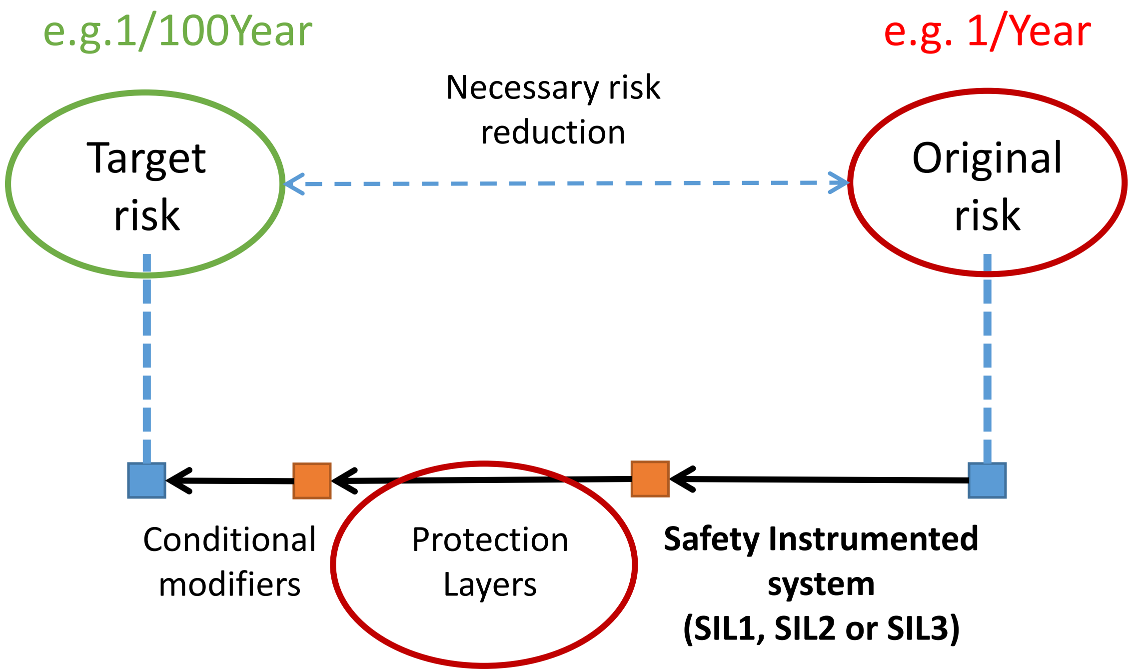
e.g. 1 failure in 10 years

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?
based on the **"LHC risk matrices"** provided by BE-MPE ([EDMS **2647876**]) and **the IEC 61511-3 methods**



Estimation of the original failure frequency due to:

- Operator/expert command
- Software
- Hardware
- …

How?
based on the **IEC 61511-3 guidelines** and the operational experience (BE-GM and BE-CEM)

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

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	CCC operator, 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.

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.

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

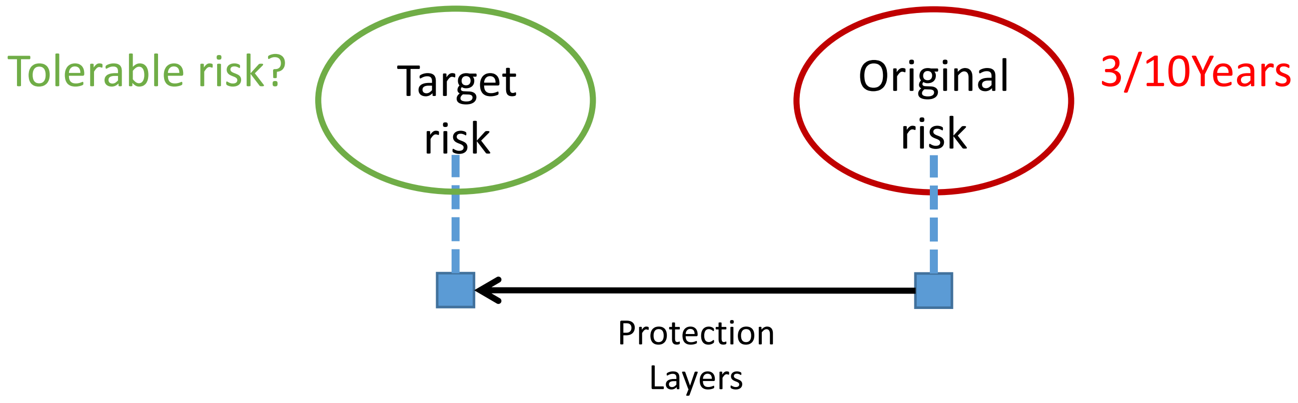
Worst case scenario

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

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 - Tolerable risk (1st approach for 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)

Risk reduction factor $RRF = \frac{\lambda_1}{\lambda_2}$

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

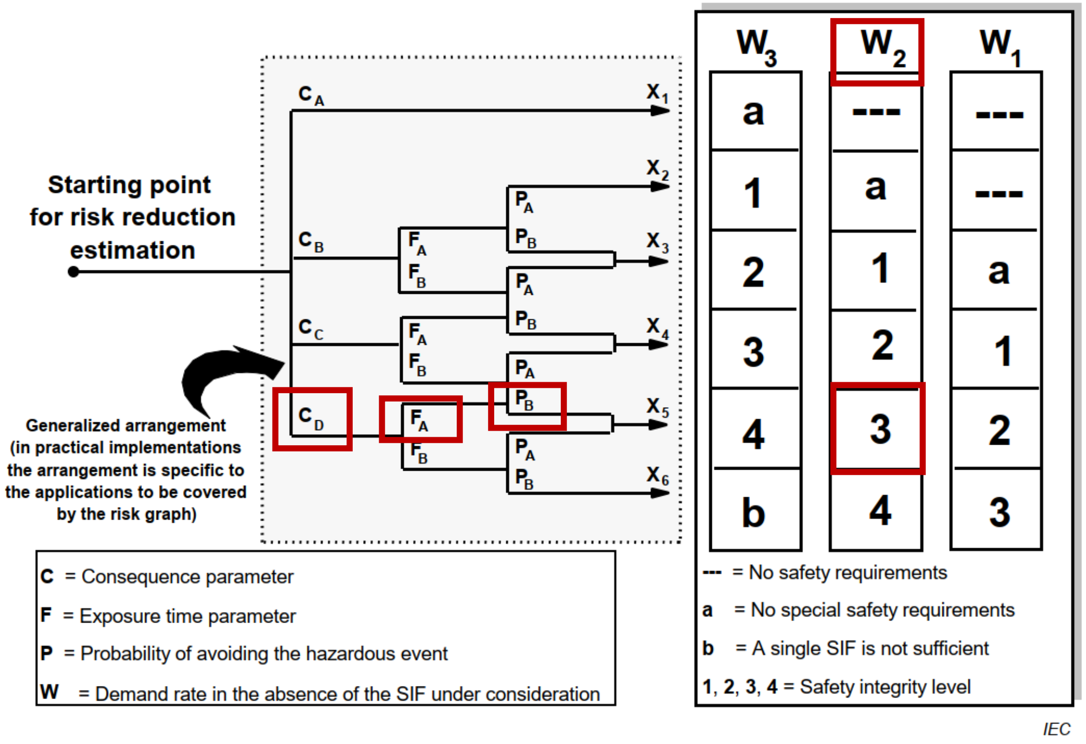
$$RRF = \frac{3}{10} / \frac{1}{1000} = 300 \approx 1000$$

Considering 1/10Year < $\boldsymbol{\lambda_1}$ < 1/Year:

- the necessary **Risk Reduction Factor (RRF) is 100** (for a expected LHC delay < 1 year) – equivalent to SIL2
- the necessary **Risk Reduction Factor (RRF) is 1000** (for a expected LHC delay ≥ 1 year) – equivalent to SIL3

Risk assessment - Tolerable risk (2nd approach for machine protection)

IEC 61511-3 Annex D - Calibrated Risk Graph (**qualitative** method)



- **C**: the **consequence** of the hazardous event
- **F**: the **occupancy** (probability that the exposed area is occupied)
- **P**: the **probability of avoiding** the hazardous situation
- **W**: the **demand rate** (number of times per year that the hazardous situation would occur in the absence of the SIF being considered)

necessary **Risk Reduction Factor (RRF) = 1000** (equivalent SIL3)

Risk assessment - Tolerable risk (3rd approach for machine protection)

IEC 61511-3 Annex C: Safety Layer Matrix (**qualitative** method)

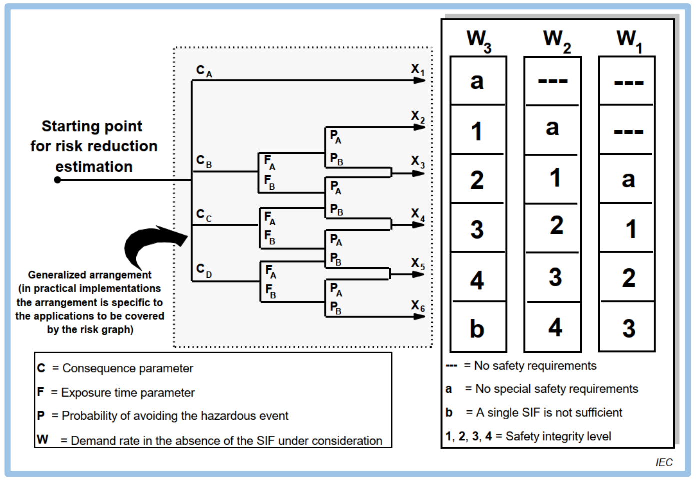
Number of existing PLs	Required SIL								
3							c)	1	1
2	c)	c)	1	c)	1	2	1	2	3 b)
1	c)	1	2	1	2	3 b)	3 b)	3 b)	3 a)
Hazardous event likelihood	Low	Med	High	Low	Med	High	Low	Med	High
	Minor			Serious			Extensive		
	Hazardous event severity rating								

IEC

- **Severity** = consequence (C)
- **Likelihood** = demand rate (W)
- No occupancy is considered (F)
- PLs are equivalent to probability of avoiding (P)

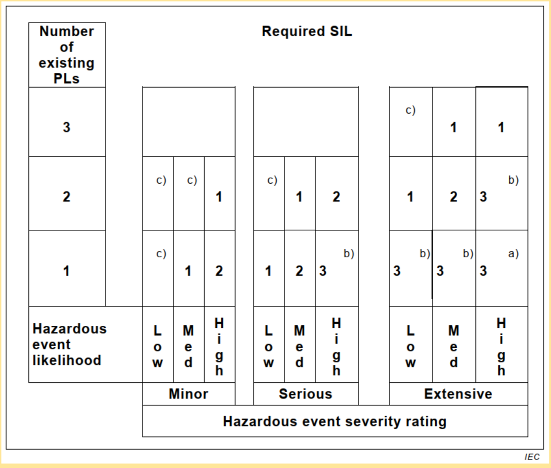
necessary **Risk Reduction Factor (RRF) = 1000** (equivalent SIL3)

Risk assessment - Tolerable risk (comparing the 3 methods)



Risk graph (IEC 61511-3 Annex D):

- C = consequence
- W = failure rate
- F and P are not considered



Risk matrix (IEC 61511-3 Annex C):

- Severity
- likelihood
- Number of existing PLs

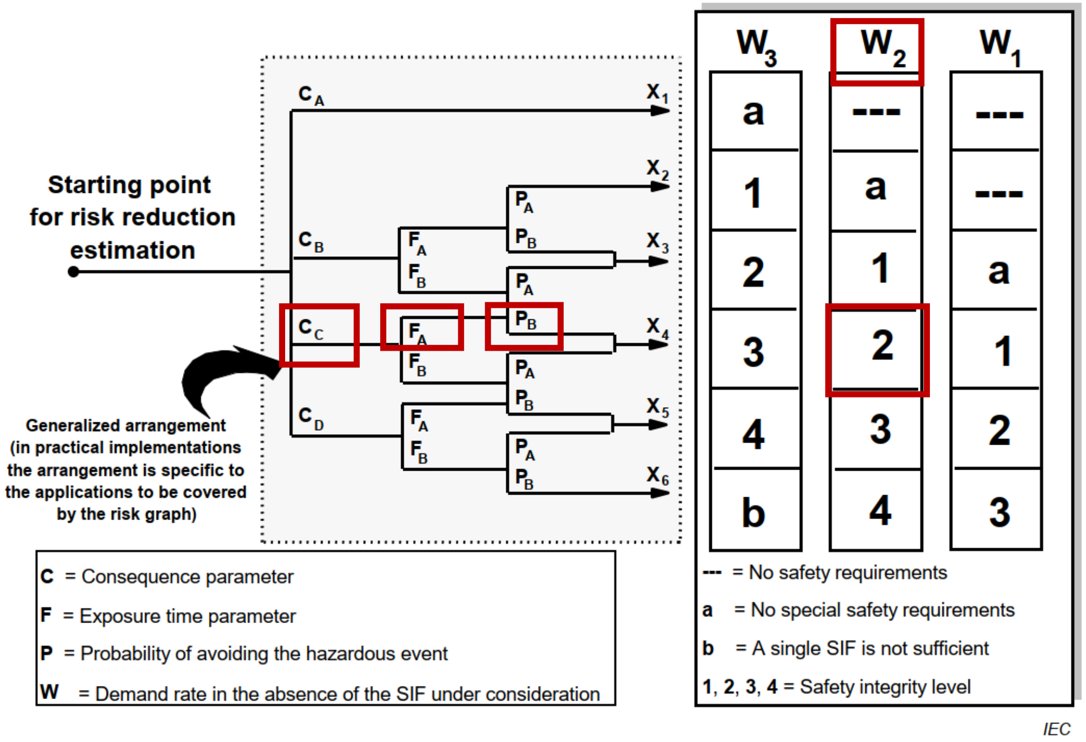
			Minor					Serious				Extensive	
			CA		CB					CC		CD	
			[1m - 20m)	[20m - 1h)	[1h - 3h)	[3h - 6h)	[6h - 12h)	[12h - 24h)	[24h - 2d)	[2d - 1w)	[1w - 1M)	[1M - 1Y)	[1Y - 10Y)
High	W3	1/H	U	U	U	U	U	U	U	U	U	U	U
		1/Shift	U	U	U	U	U	U	U	U	U	U	U
		1/Day	A	U	U	U	U	U	U	U	U	U	U
		1/Week	A	A	A	A	U	U	U	U	U	U	U
Med		1/Month	A	A	A	A	A	A	U	U	U	U	U
Low	W2	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
	W1	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

Failure mode consequence (severity)

Failure mode frequency

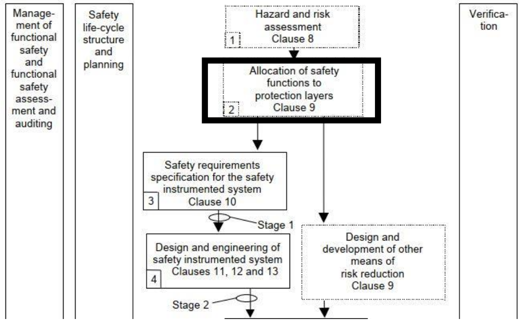
Risk assessment - Tolerable risk (Personnel protection)

IEC 61511-3 Annex D - Calibrated Risk Graph (**qualitative** method)



- **Calibration** based on the IEC 61508 and IEC 61511 examples and applied to other CERN projects (e.g. SM18 cluster F)
- The necessary **risk reduction is bigger for machine protection**
- The same protection layers will protect both machine and personnel

necessary **Risk Reduction Factor (RFF) = 100** (equivalent SIL2)



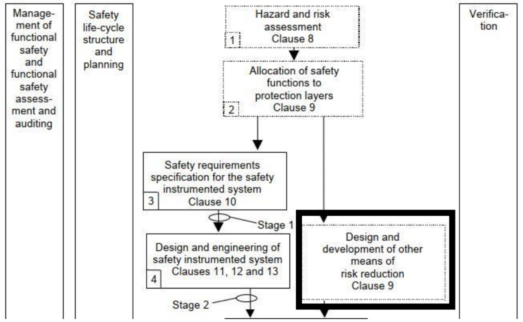
Tolerable risk for FRAS (summary)

- The necessary **risk reduction is 100 or 1000** (Machine protection establishes the max. risk reduction)

- This can be achieved by:
  - A SIL2 or SIL3 Safety Instrumented System (certified devices, very strict safety requirements, etc.)
  - **2 or 3 independent Protection Layers** according to the IEC 61511-3 Annex G

- **Due to some technical** (and economical) **challenges** like the sensors technology, devices under radiation, available certified devices, etc., **we propose the Protection Layers alternative** (following the IEC 615111-3 Annex C and Annex F guidelines)

Analysis of the Protection Layers (IEC 61511-3 Annex C and F)



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
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:

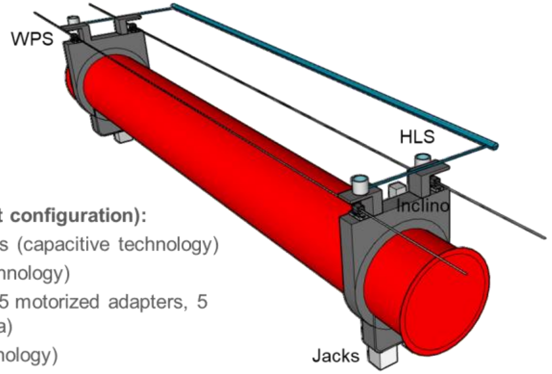
- independence between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS.

Analysis of the (existing) Protection Layers

- Represented as **Reliability Block Diagrams** (RBD) using the *Isograph Reliability Workbench*
- Classified by the **sensor technology**:
  - **PL1**: Capacitive sensors - Wire Positioning Sensors (WPS) and Inclinometers
  - **PL2**: Resolvers
  - **PL3**: Frequency Scanning Interferometry (FSI) - Hydrostatic Levelling Sensors, Inclinometers
- Assigned to one or several **failure modes** (from risk analysis):
  - **V**: exceeding bellow **Vertical** displacement limit
  - **H**: exceeding bellow **Horizontal** displacement limit
  - **R**: exceeding bellow **Rotational** displacement limit
- Enabled for all FRAS **operational modes:**
  - **1**: Remote alignment mode
  - **2**: Maintenance mode
  - **3**: Standby mode (LHC operation)
- Available for one or several **FRAS component configurations**:
  - **Triplet-D1**: Q1, Q2a, Q2b, Q3, CP and D1
  - **Q45-D2**: Q4, Q5 and D2
  - **C-M-C-T**: Collimators, masks, Crab-cavities and TAXN

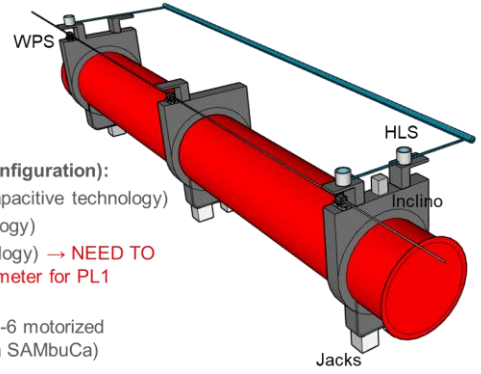
FRAS components configurations

- **Triplet-D1**: Q1, Q2a, Q2b, Q3, CP and D1



Sensor systems (current configuration):
- 2 wires, 4 WPS sensors (capacitive technology)
- 3 HLS sensor (FSI technology)
- Supported by 3 jacks (5 motorized adapters, 5 resolvers via SAMbuCa)
- Inclinometer (FSI technology)

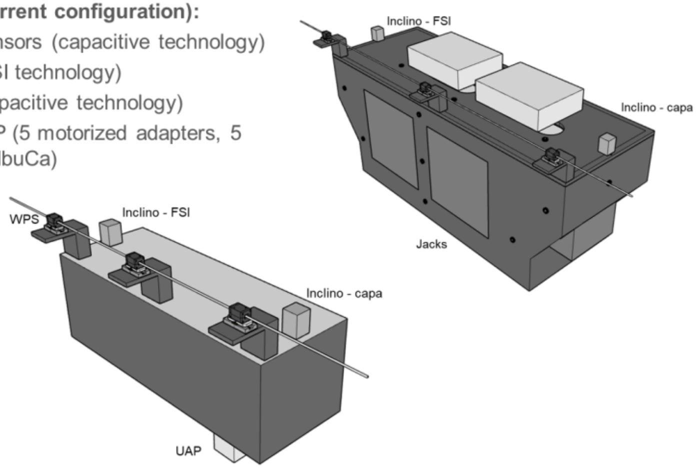
- **Q45-D2**: Q4, Q5 and D2



Sensor systems (current configuration):
- 1 wire, 3 WPS sensors (capacitive technology)
- 3 HLS sensor (FSI technology)
- 1 inclinometer (FSI technology) → NEED TO ADD CAPACITIVE Inclinometer for PL1 capacitive
- Supported by 3(4) jacks (5-6 motorized adapters, 5-6 resolvers via SAMbuCa)

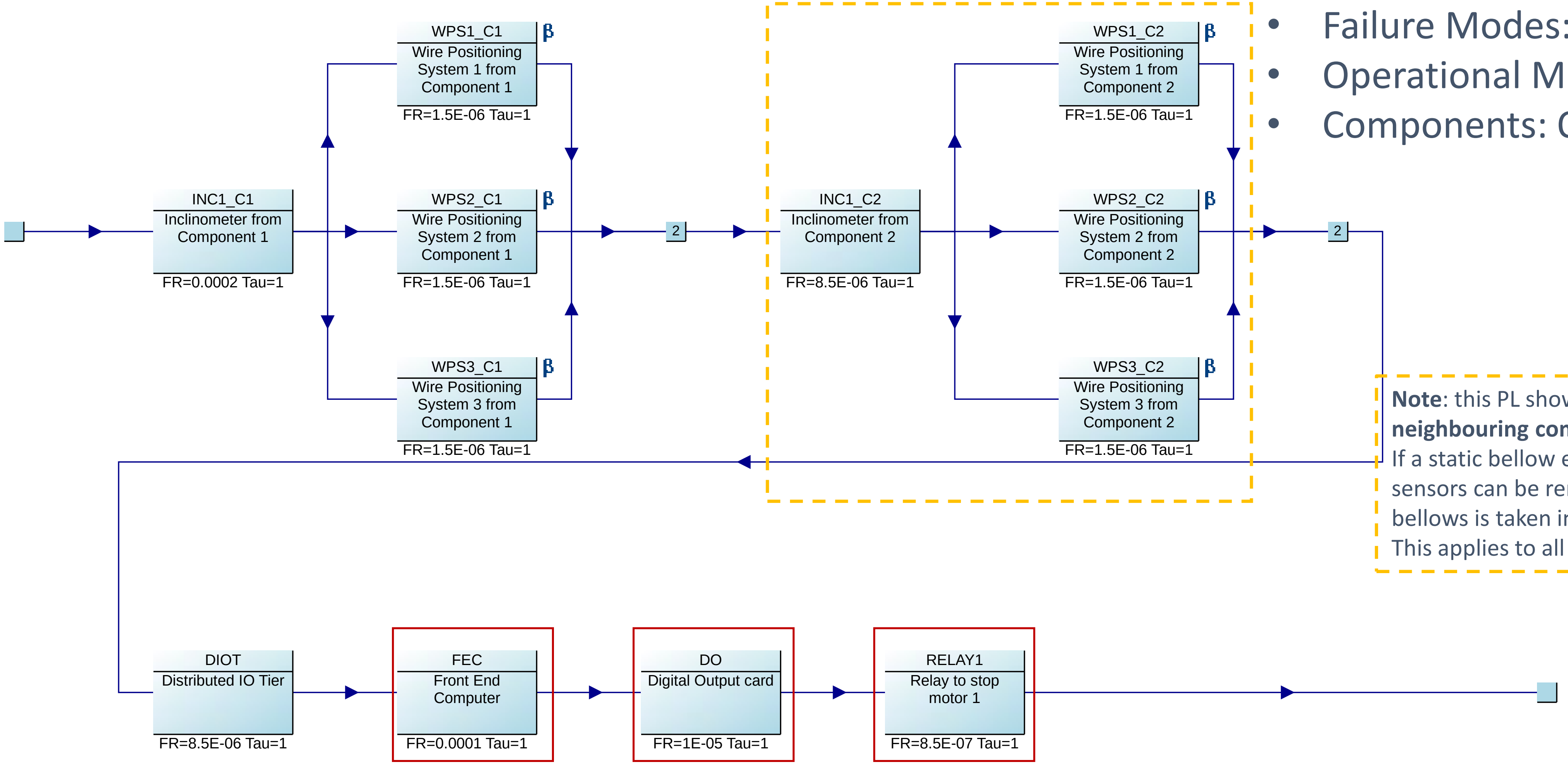
- **C-M-C-T**: Collimators, masks, Crab-cavities and TAXN

Sensor systems (current configuration):
- 1 wire, 3 WPS sensors (capacitive technology)
- 1 inclinometer (FSI technology)
- 1 inclinometer (capacitive technology)
- Supported by UAP (5 motorized adapters, 5 resolvers via SAMbuCa)



Slides from Vivien RUDE and Mateusz Sosin

PL1.1: Capacitive sensors



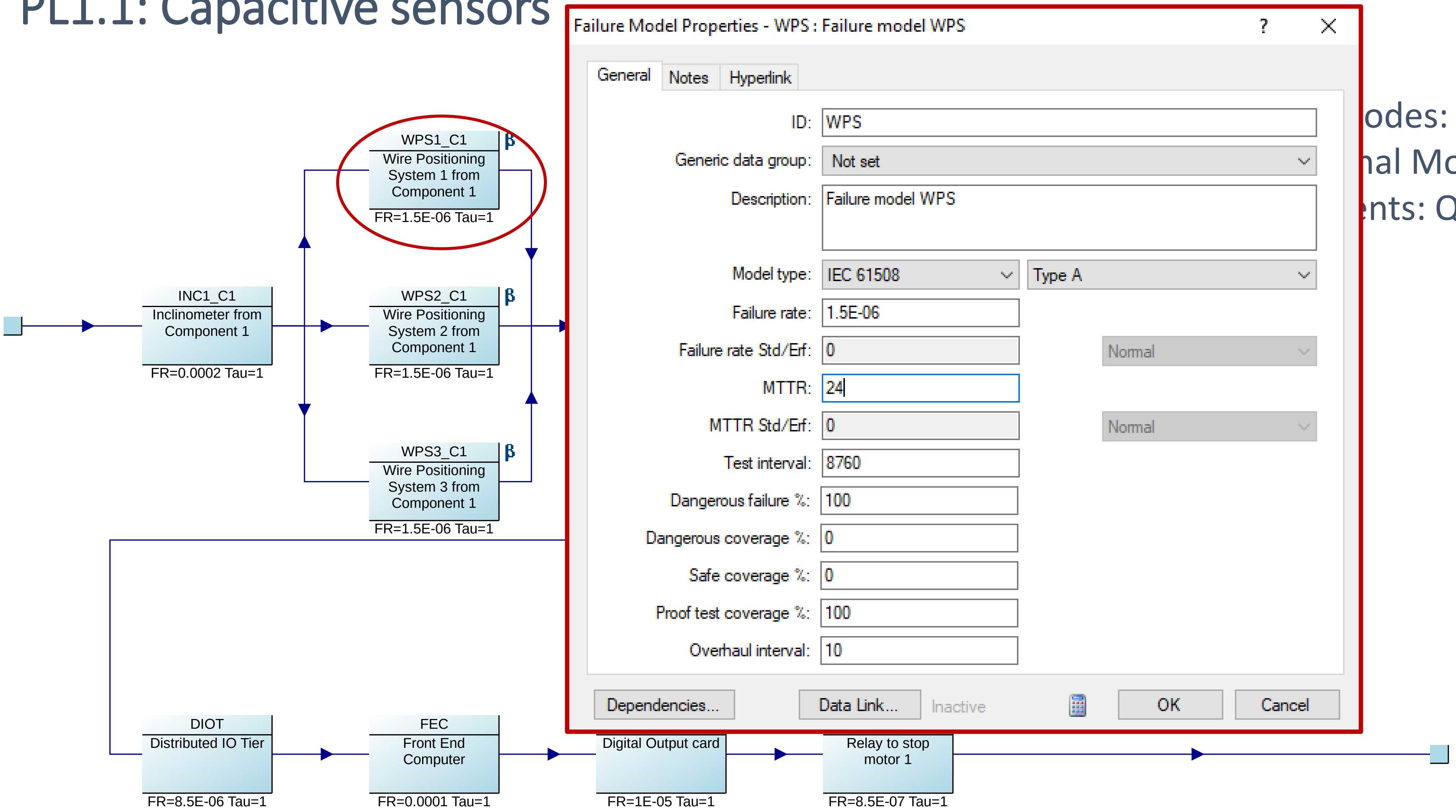
- Failure Modes: V, H and R
- Operational Modes: 1, 2 and 3
- Components: Q45-D2 and C-M-C-T

Note: this PL shows the **configuration for 2 neighbouring components that can move**.
If a static bellow exists on one side half of sensors can be removed as initial setting of bellows is taken into account.
This applies to all PLs

Potential common cause of failure devices

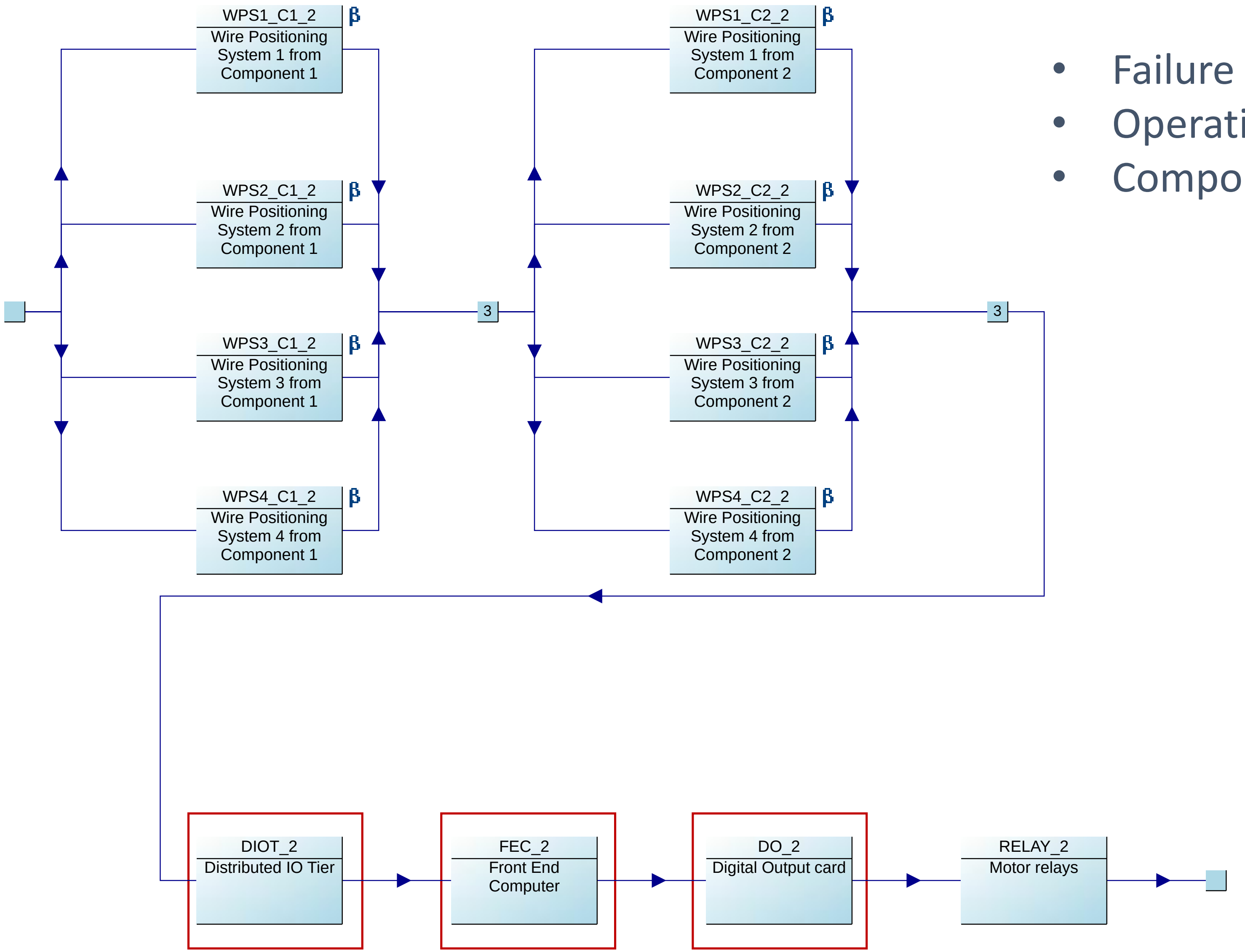
PL1.1: Capacitive sensors

odes: V, H and R
nal Modes: 1, 2 and 3
nts: Q45-D2 and C-M-C-T



Note: possibility for safety and reliability analysis of these models (Isograph reliability workbench)

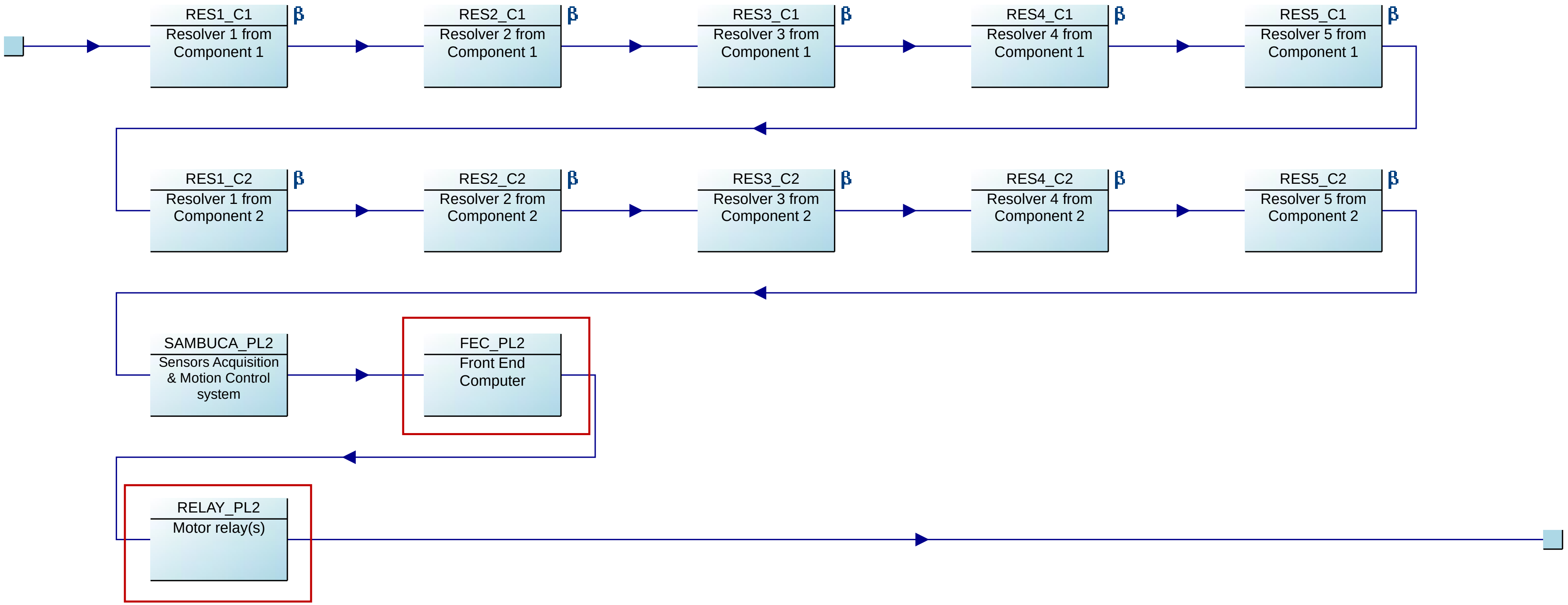
PL1.2: Capacitive sensors



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

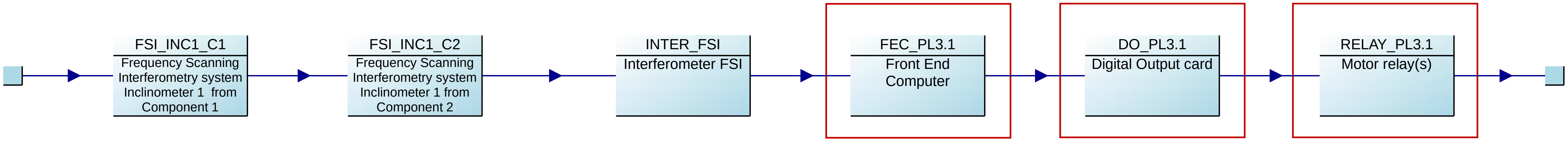
PL2: Resolvers

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



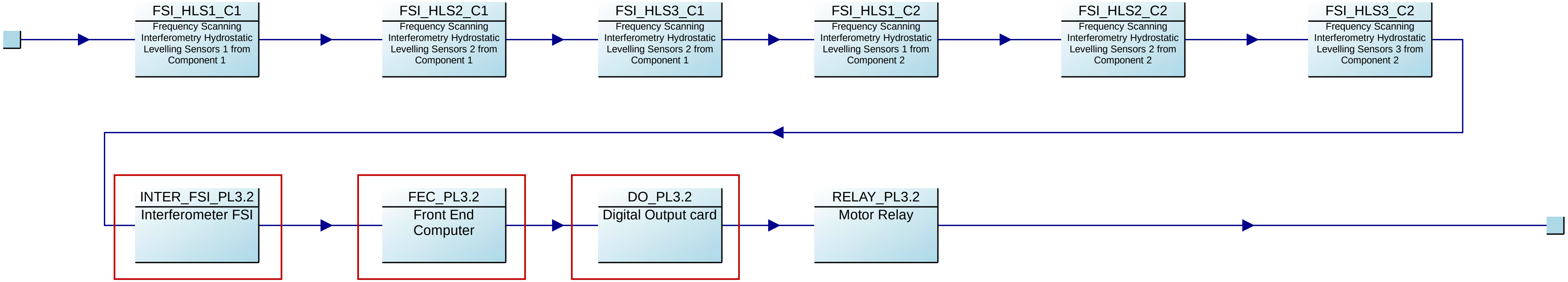
PL3.1: FSI sensors

- Failure Modes: R
- Operational Modes: 1, 2 and 3
- Components: All

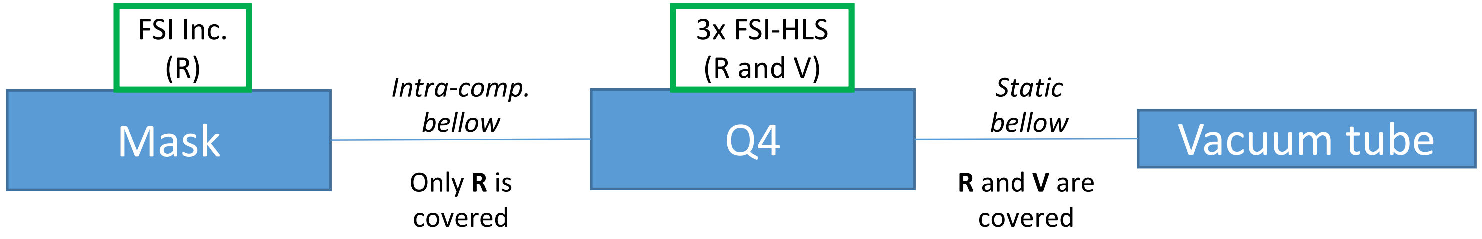


PL3.2: FSI sensors

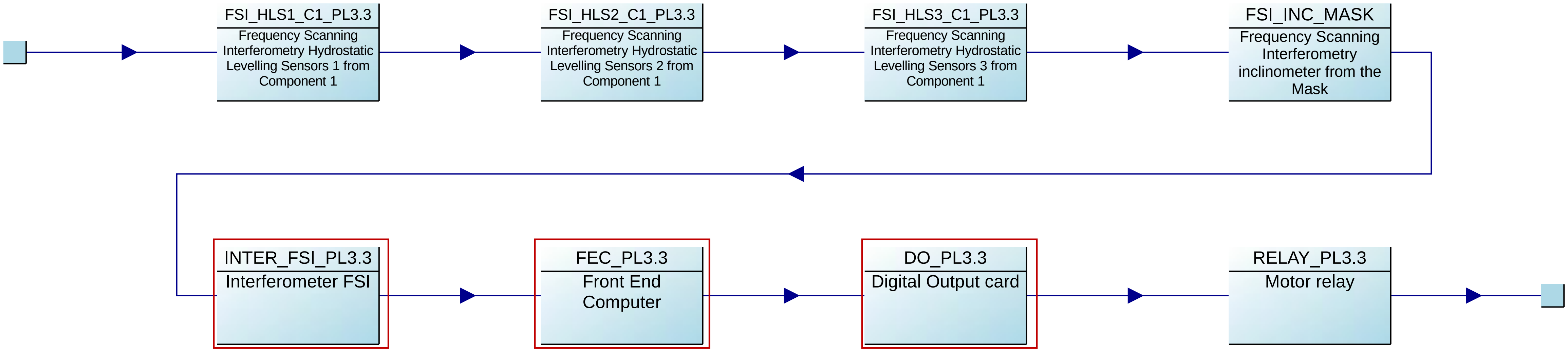
- Failure Modes: V and R
- Operational Modes: 1, 2 and 3
- Components: Triplet-D1



PL3.3: FSI sensors



- Failure Modes: V (excludig bellow between Q4/5 and masks) and R
- Operational Modes: 1, 2 and 3
- Components: Q45-D2



PLs summary

Sensor technology	Protection Layer	Failure Modes	FRAS operational Modes	FRAS Components
Capacitive	PL1.1	V, H and R	1, 2 and 3	Q45-D2 and C-M-C-T
	PL1.2	V, H and R	1, 2 and 3	Triplet-D1
Resolver	PL2	V, H and R	1, 2 and 3	Triplet-D1, Q45-D2 and C-M-C-T
FSI	PL3.1	R	1, 2 and 3	Triplet-D1, Q45-D2 and C-M-C-T
	PL3.2	V and R	1, 2 and 3	Triplet-D1
	PLP3.3	V (ex. Q4/5-Mask) and R	1, 2 and 3	Q45-D2

PLs and risk reduction summary

FRAS component	Failure mode	Available PLs	Achieved risk reduction*
C-M-C-TAX	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”)
Q45-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-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

Conclusions and recommendations (1)

- **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

- We need an **agreement** (between BE-CEM, BE-GM and BE-ICS) about the initial risk and the tolerable, followed by the MPP (Machine Protection Panel) **approval**
  - **If risk reduction = 100** (SIL2), **no need of extra PLs**
  - **If risk reduction = 1000** (SIL3), we (may) **need extra PLs**
    - For **H failure mode** in all components
    - for **V failure mode** in C-M-C-T

- Potential **Common Cause of Failures**:
  - **Hardware**: use different devices for each PLs (FECs, SAMbuCa, DIOTs, Motor relays, etc.)
  - **Power supplies**: guarantee that a common power failure won't deactivate/disable 2 or more PLs at the same time (any power failure of PLs shall disable the use of the motors)
  - **Radiation**: analyze if 2 PLs could be affected at the same time by radiation (located in the same area) – **Not in FRAS?**
  - **Software**: develop specific "FESA classes" for each PL. However the FESA framework libraries will be shared. An hypothetically dangerous undetected failure (λ_{DU}) in FESA could affect all PLs
  - **Diagnostics**: provide "status signals" from the different protection layers (e.g. watchdogs)
  - **Diversity**: use different technologies whenever possible

Conclusions and recommendations (2)

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:

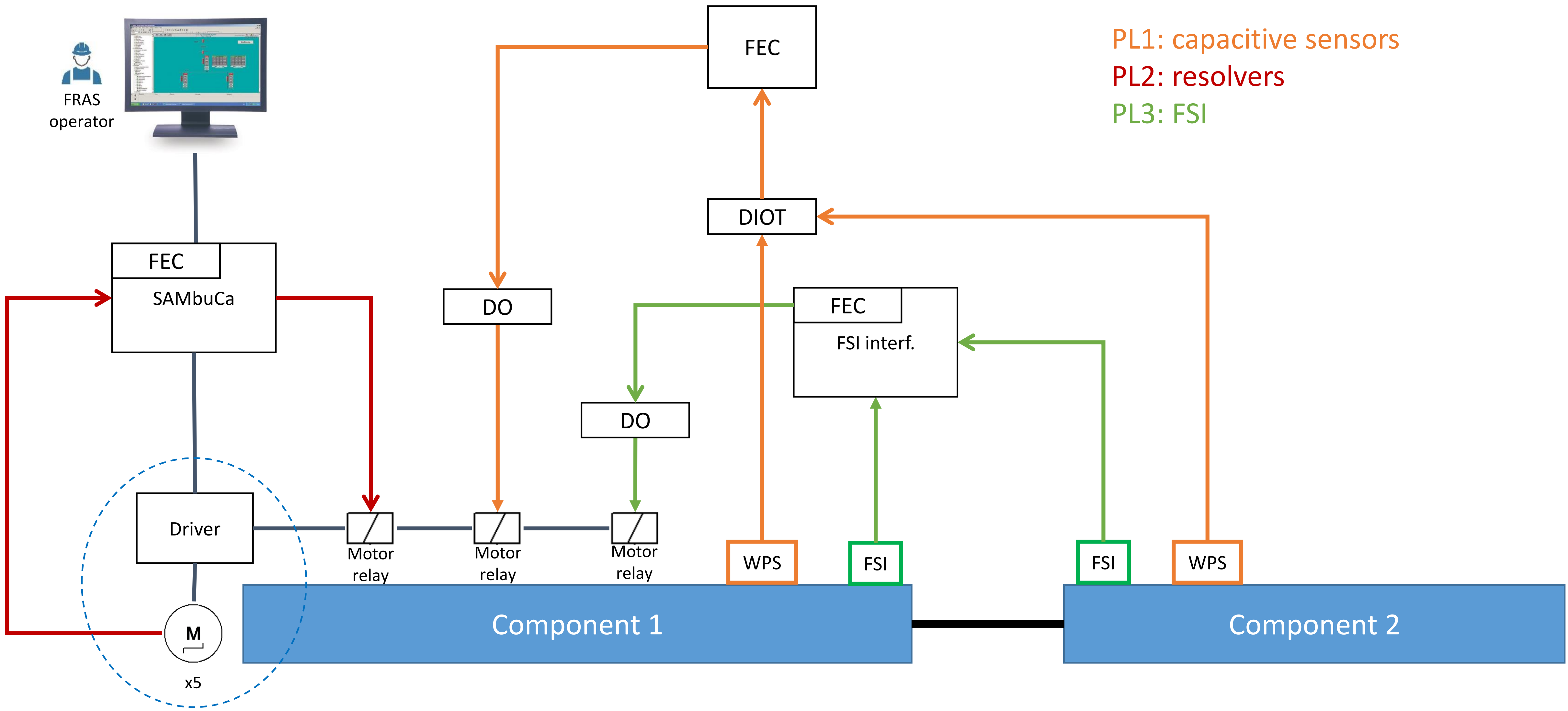
- Specificity – a PL is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a PL.
- Independence – a PL is independent of other protection layers if it 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

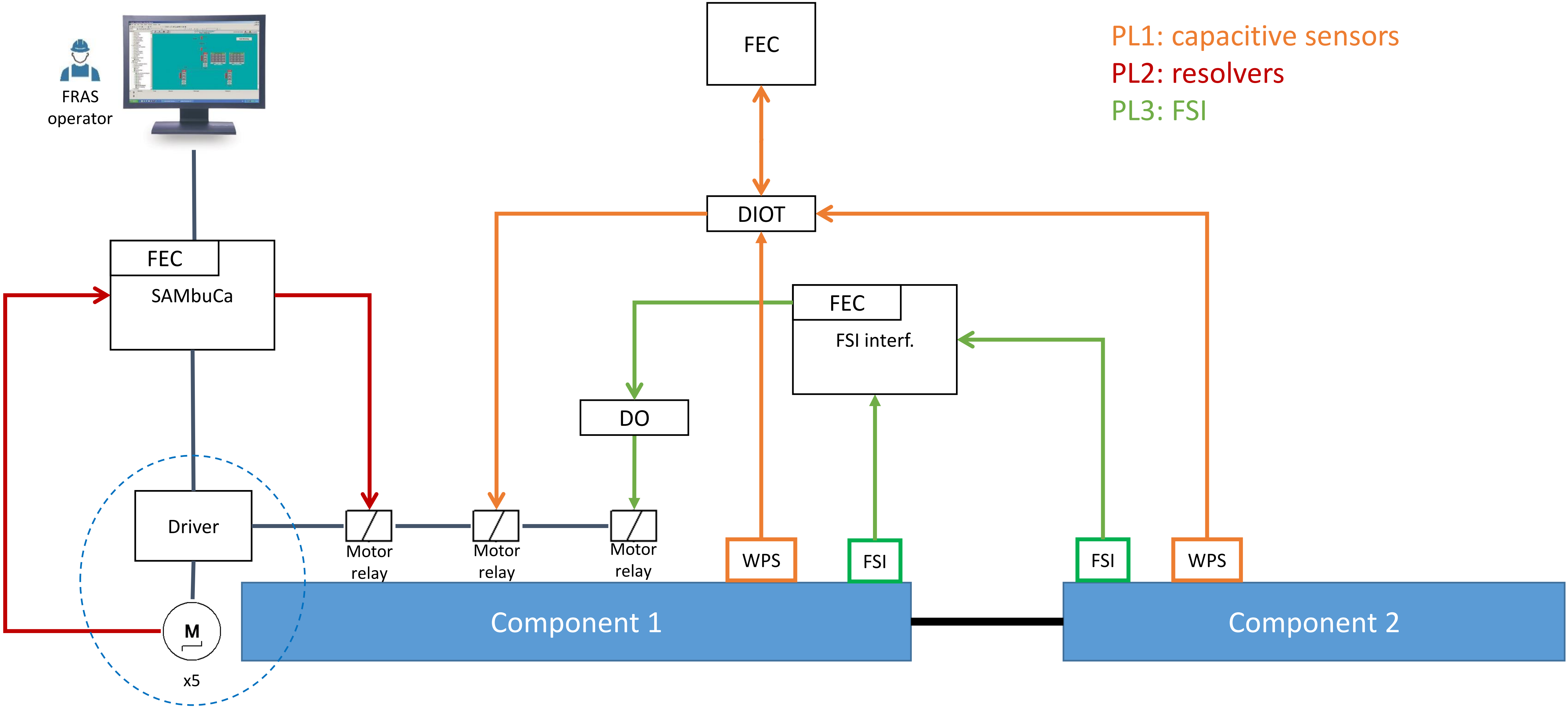
- diversity between protection layers – the aim should be diversity between protection layers and the BPCS but this is not always achievable. Some diversity can be achieved by using equipment from different manufacturers but if SIS and BPCS sensors are connected to the process using the same type of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

FECs and FESA

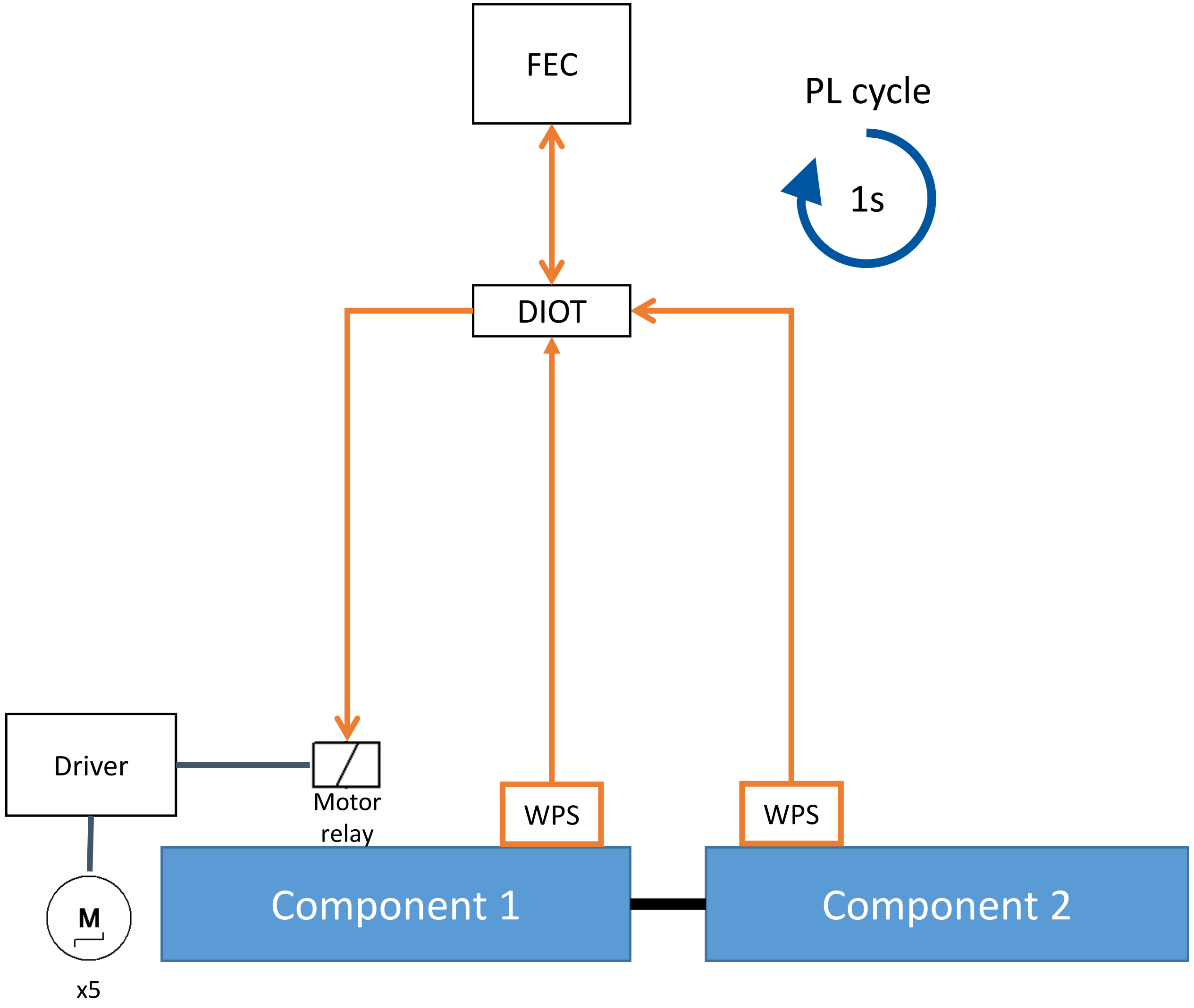
Potential PLs functional schema 1



Potential PLs functional schema 2 (requires new developments)



PL1 (Schema 2) functional software logic



FEC

1. FEC **computes the thresholds** for capacitive sensors (WPS/inclinometer) based on the previous cycle measurements.
   These "cyclic" thresholds are narrow (allows for small portion of motion, i.e. +/-50um; ultimate speed of motion os 20um/s)

2. Updated thresholds are send to DIOT every cycle (1s)

WordFIP communication

DIOT

1. Every cycle (1s) DIOT watchdog logic checks if new thresholds has arrived or if communication between FEC and DIOT is still working. If the communication has failed, **the motor interlock is triggerred**

2. If the thresholds arrive, the DIOT logic compares them with the WPS/inslinometer sensors measurements and **if limits are violated triggers the motor interlock**

If bad thresholds computed by FEC (software error):

- Other protection layers will trigger the interlock, or
- The DIOT will trigger the interlock anyway, as thresholds represents 3D component position and bad calculations will not represent real sensors state (sensors out of thresholds anyway)