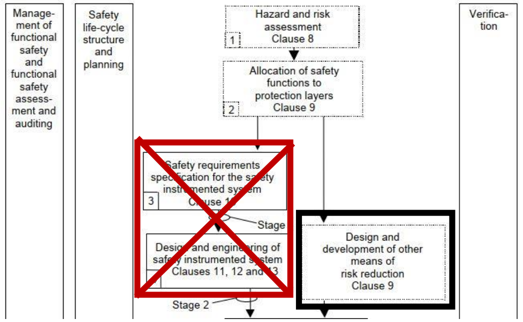
FRAS project

Updates in the PL design

Contents



Protection Layers design (IEC 61511)

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.

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

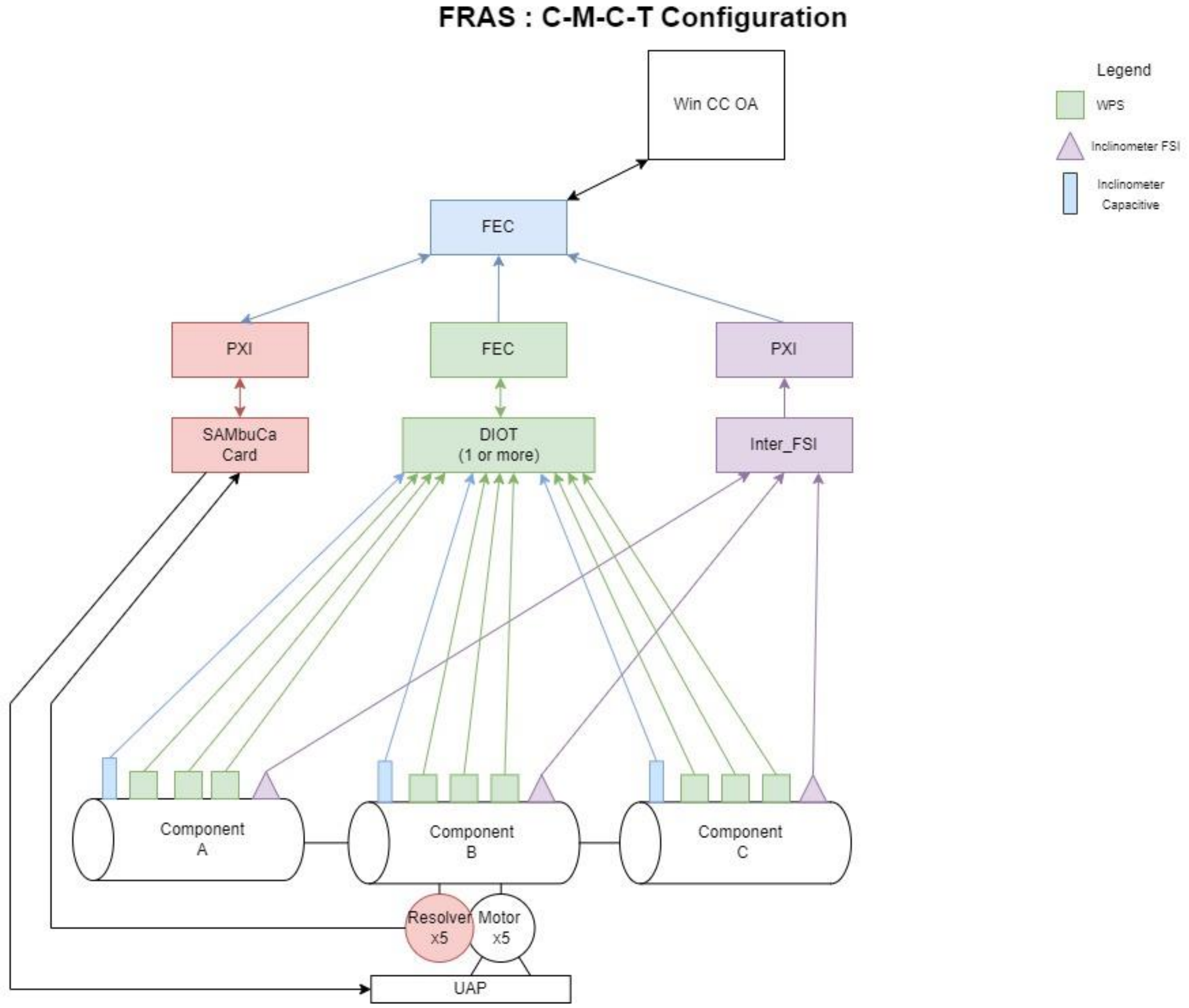
9.4.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between:

- protection layers;
- protection layers and the BPCS.

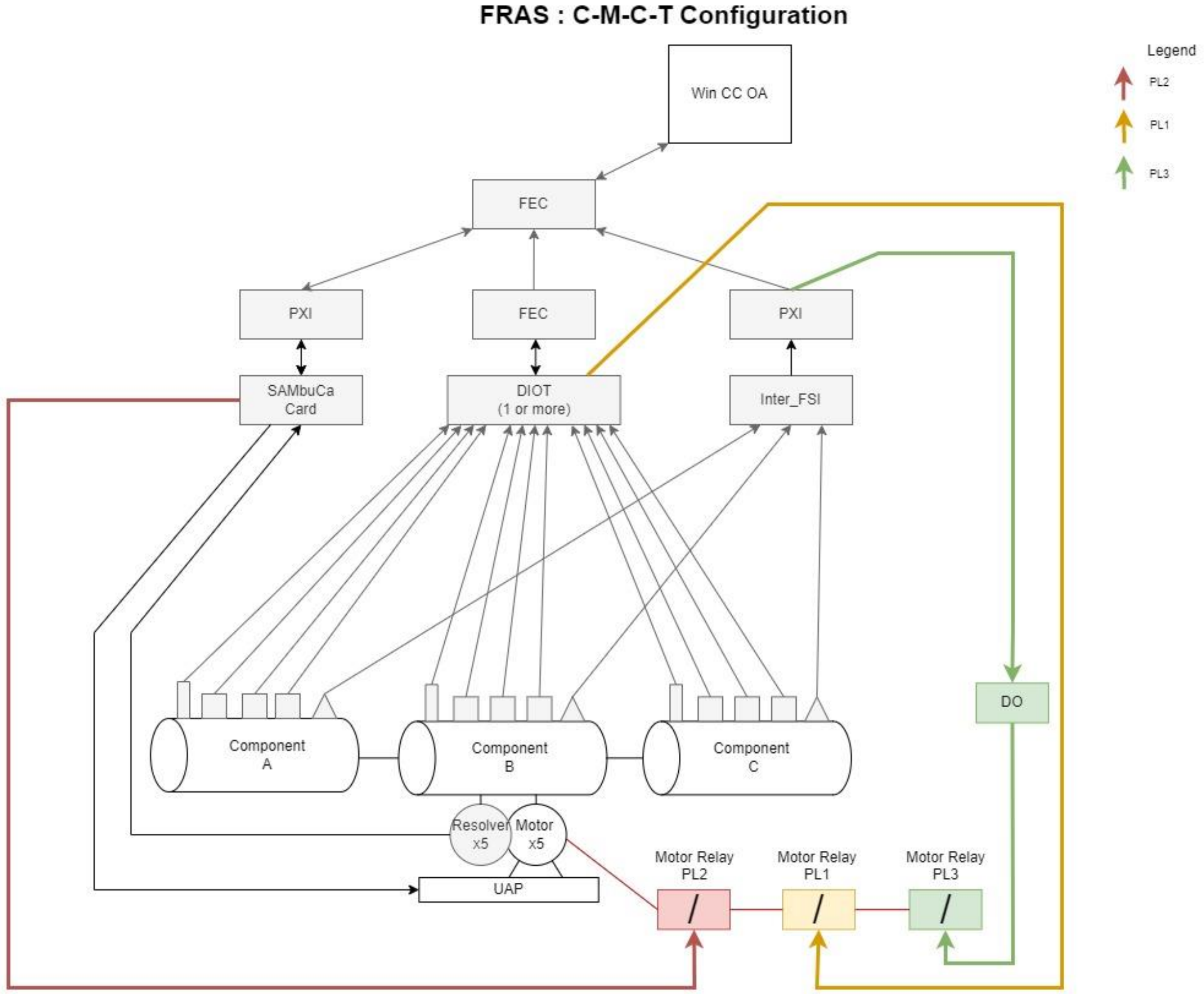
are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.

Necessary Risk Reduction	Number of PLs
> 10 (SIL1)	2
> 100 (SIL2)	3

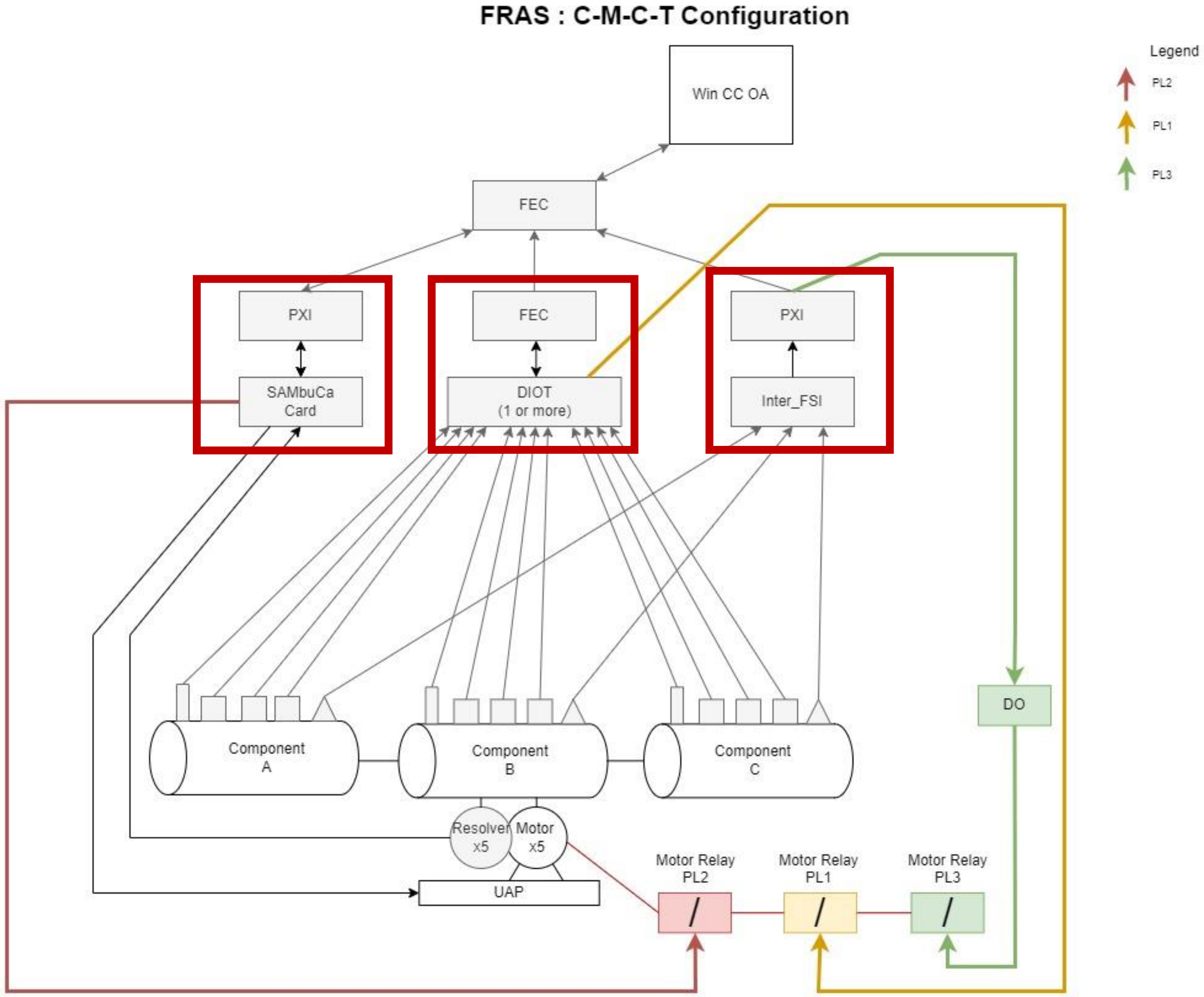
FRAS control system vs FRAS PLs



New hardware



FRAS control system vs FRAS PLs



"Independent" Protection Layers

(except for the FESA framework dependency)

No more diversity was proposed since the **LOPA results** showed that we can achieve the tolerable risk with the current architecture

Contents

Contents

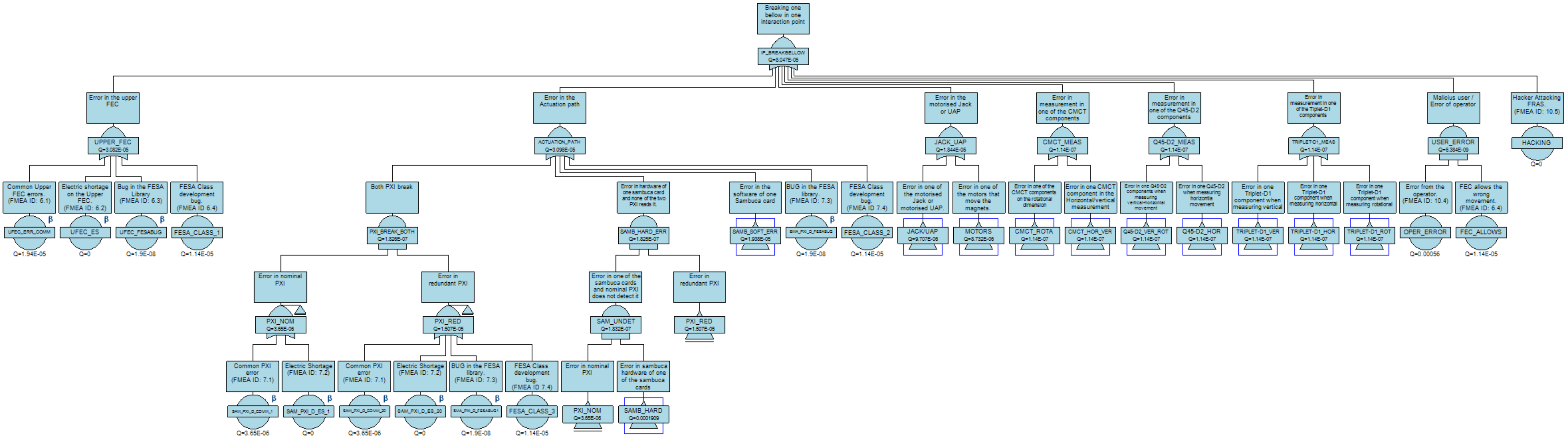
1. **FMEA (device failures)**

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

2. FTA review (System failures)
3. LOPA + safety matrix (do we achieve the tolerable risk?)

Contents

1. FMEA (device failures)
2. **FTA review (System failures)**
3. LOPA + safety matrix (do we achieve the tolerable risk?)



Contents

1. FMEA (device failures)
2. **FTA review (System failures)**
3. **LOPA + safety matrix** (do we achieve the tolerable risk?)

	[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

Layers of Protection Analysis (LOPA)

We don't meet the independence and diversity requirements
From the IEC 61511 standard

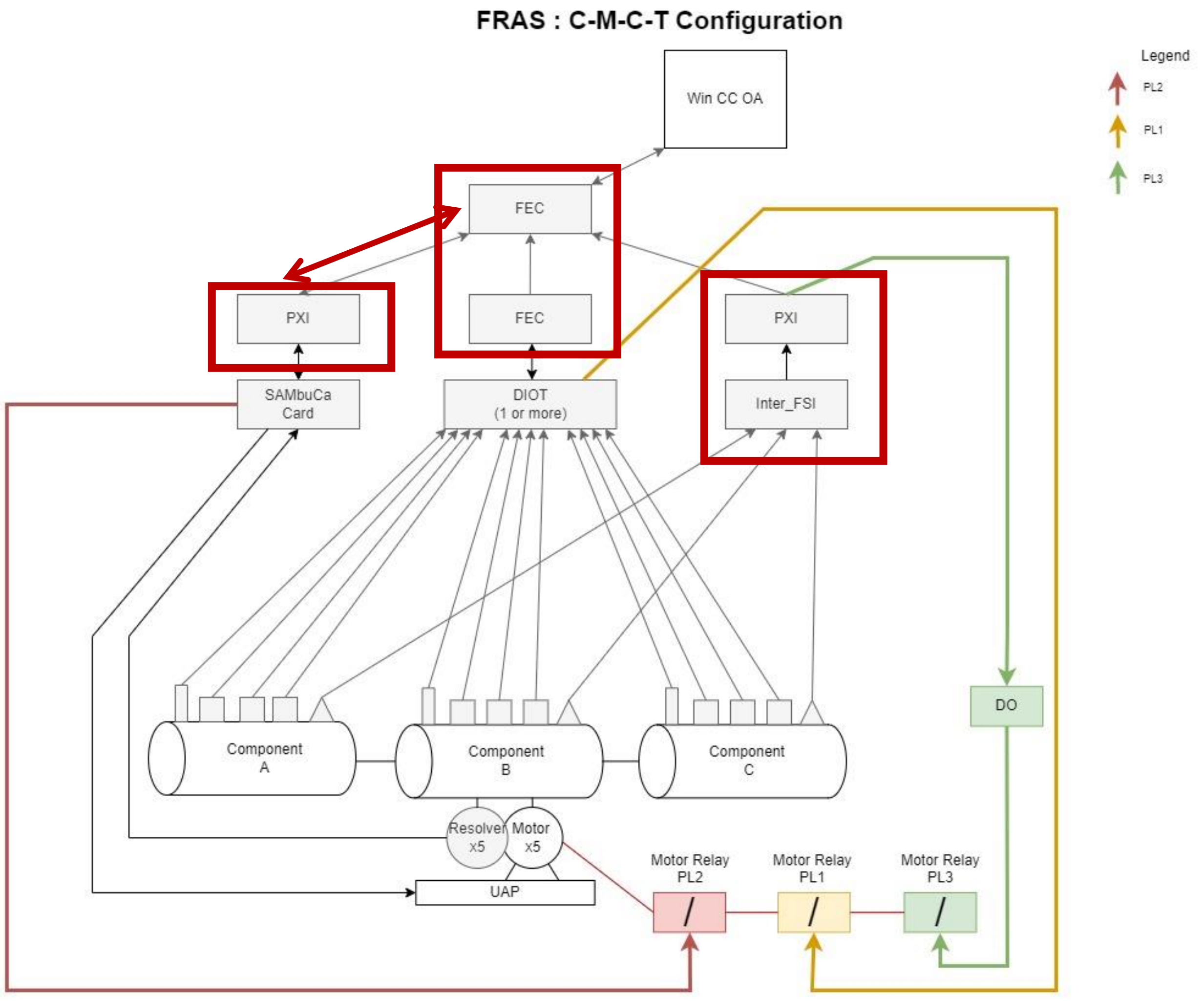
Impact Event		Initiating Cause 1	Initiating Cause 2	Initiating Cause 3	Initiating Cause 4		Initiating Cause 5		Initiating Cause 6			Initiating Cause 7
					rror measurement one CMCT componen		rror measurement one Q45-D2 componer		Error measurement one Triplet-D1 component			
IP side Break Bellow		Upper 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
	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
	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
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
Procedures / Alarms												
Cybersecurity: TN + RBAC												0
Physical Limit Switches		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
	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
	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%
	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										

What have we changed?

1. FMEA (device failures)

2. **FTA review (System failures)**
3. **LOPA +** safety matrix **(do we achieve the tolerable risk?)**

FRAS PLs changes



Changes:

1. **Capacitive sensors path**: we must use the LGC algorithm (same as top FEC) with different "parameters/configuration"

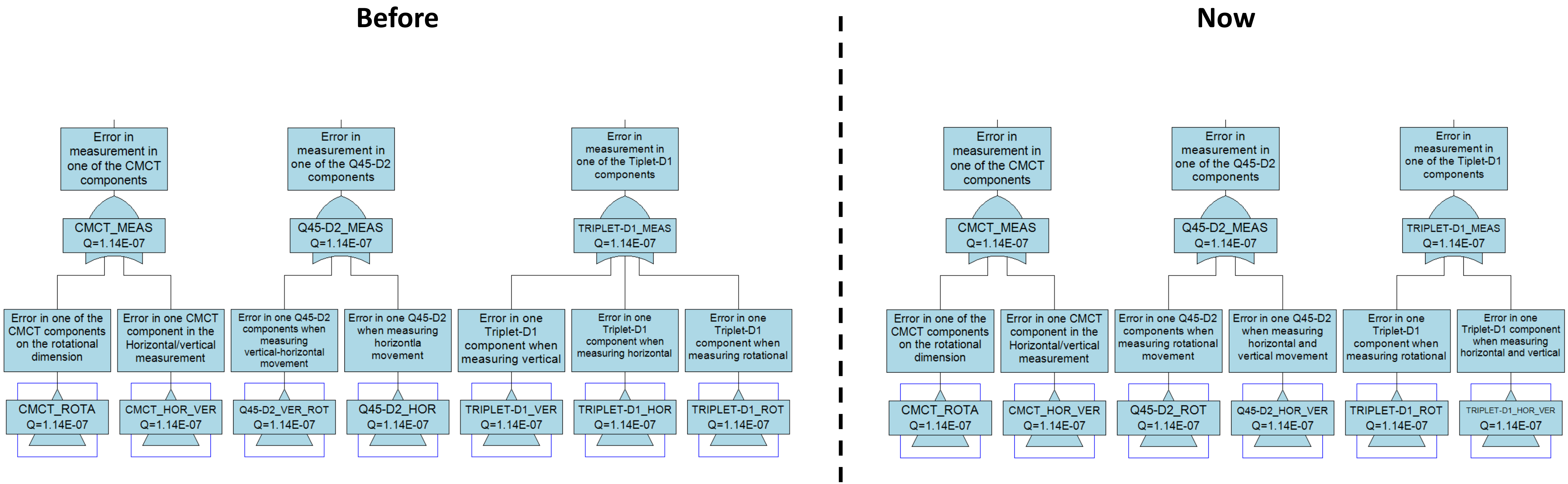
2. **Resolvers path**: initial position (before movement) given by the top FEC

3. **FSI sensors path**: it can only measure (and then protect from) rotational movement

Changes in the FTA

Change: FSI can only measure rotational

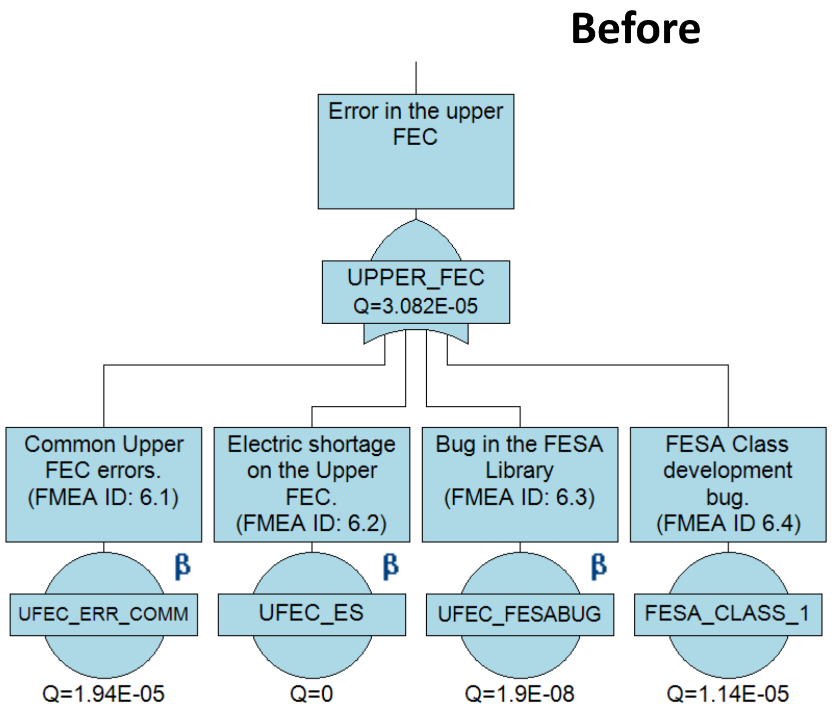
Conclusion: failure frequencies barely change

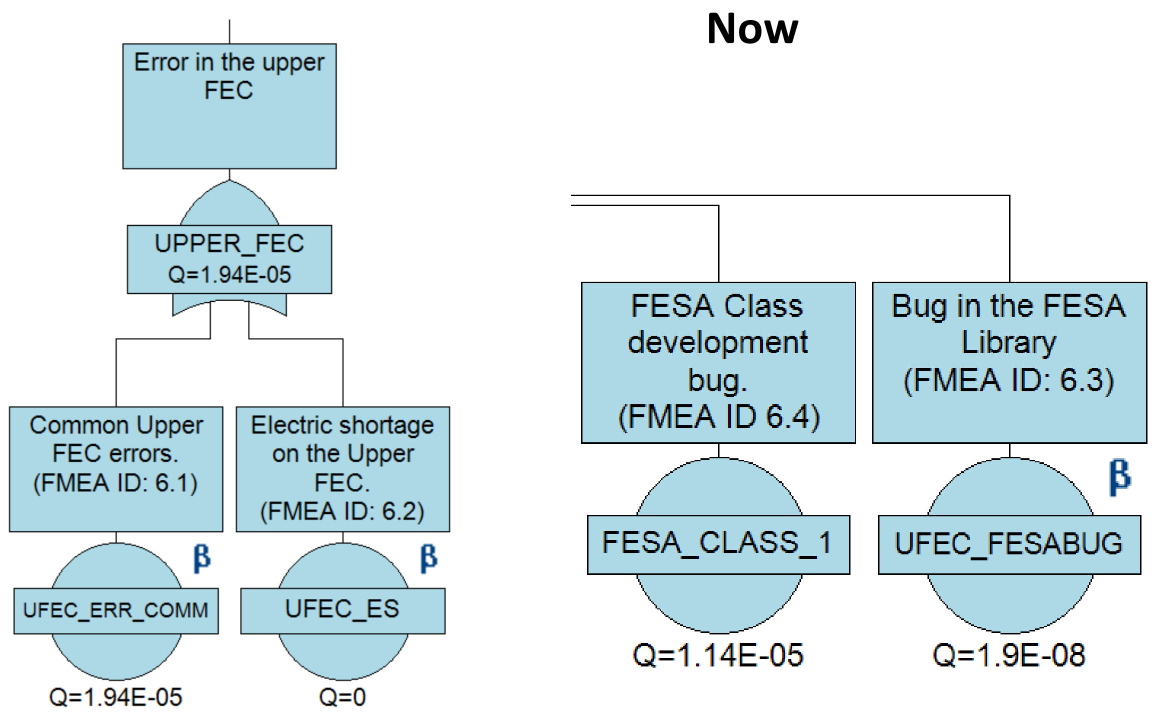


FRAS PLs changes

Change: Dependencies with top FEC – we split the failure modes

Conclusion: more granularity for the LOPA analysis

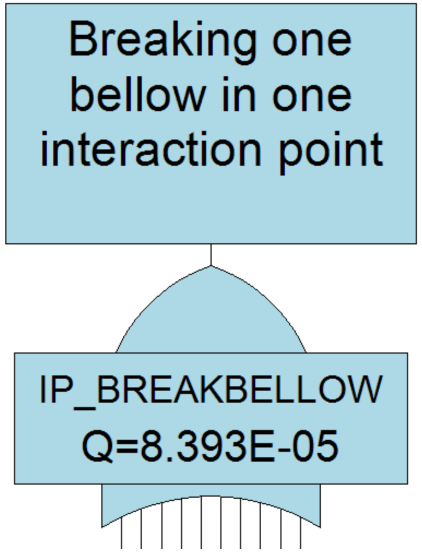




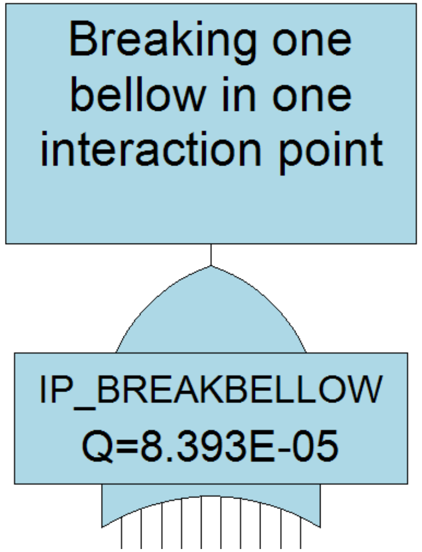
FRAS PLs changes

Conclusion: global failure rate does not change. We just got more granularity for the LOPA analysis

Before



Now



FRAS PLs changes

Change: more granularity for the top FEC failures

Conclusion: (conservative approach) some relevant (according to the assumptions) failure modes are not protected

Before

Impact Event		Initiating Cause 1
IP side Break Bellow		Upper FEC
	Event Frequency (1/h	3.08E-05
	Event Frequency (1/y	0.27
Protection and mitigation layers	PL1	10
	PL2	
	PL3	

Now

Impact Event		Initiating Cause 1.0	Initiating Cause 1.1	Initiating Cause 1.2
IP side Break Bellow		Upper FEC common (hardware)	Upper FEC FESA framework	Upper FEC User Software (LGC + FESA class)
	Event Frequency (1/h	1.94E-05	1.90E-08	1.14E-05
	Event Frequency (1/y	0.17	0.00017	0.10
Protection and mitigation layers	PL1	10		
	PL2			
	PL3			

FRAS PLs changes

Impact Event		Initiating Cause 1.0	Initiating Cause 1.1	Initiating Cause 1.2	Initiating Cause 2	Initiating Cause 3	Initiating Cause 4		Initiating Cause 5				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 common (hardware)	Upper FEC FESA framework	Upper FEC User Software (LGC + FESA class)	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	1.94E-05	1.90E-08	1.14E-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	6.38E-09	0.00E+00
	Event Frequency (1/y	0.17	0.00017	0.10	0.30	0.161534	0.00099864	0.00099864	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	5	73	73	73	73	73	73	73	73	73	73	73	73	73
Procedures / Alarms														
Cybersecurity: TN + RBAC													0	100
Physical Limit Switches		0	0	0	0	0	0	0	0	0	0		0	0
Cumulative		730	73	73	730	730	73	73	73	73	73	73	730	7300
	Intermediate event frequency	0.000233	0.000002	0.001368	0.000413	0.00022128	0.0000137	0.0000137	0.00001368	0.00001368	0.00001368	0.00001368	0.00000008	0.00000000
	Weight over the overall frequency	10.04%	0.10%	58.96%	17.82%	9.54%	0.59%	0.59%	0.59%	0.59%	0.59%	0.59%	0.00%	0.00%
	Total mitigated event frequency								0.00232					
	Tolerable Event Frequency - LHC								0.01000					
	Tolerable Event Frequency - IP side								0.00250					
	Tolerable Event Frequency - Bellow								0.000119048					
	Residual Risk								0.00017984					

FRAS PLs changes

However,

Purely systematic failures (e.g., software failures) will not be affected by the operation time

Therefore,

We should not consider this risk reduction in LOPA

These failures will be treated separately, following the risk reduction recommendations for software from the IEC standards (including testing, procedures, runtime monitors, specification, etc.)

FRAS PLs changes

Impact Event		Initiating Cause 1.0	Initiating Cause 1.1	Initiating Cause 1.2	Initiating Cause 2	Initiating Cause 3	Initiating Cause 4		Initiating Cause 5				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 common (hardware)	Upper FEC FESA framework	Upper FEC User Software (LGC + FESA class)	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	1.94E-05	0.00E+00	0.00E+00	3.45E-05	1.84E-05	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	0.17	0.00000	0.00	0.30	0.161534	0.00099864	0.00099864	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	12	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667
Procedures / Alarms														
Cybersecurity: TN + RBAC													0	100
Physical Limit Switches		0	0	0	0	0	0	0	0	0	0	0	0	0
Cumulative		304.1666667	30.41666667	30.41666667	304.1666667	304.1666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	30.41666667	304.1666667	3041.666667
	Intermediate event frequency	0.000559	0.000000	0.000000	0.000992	0.00053107	0.0000328	0.0000328	0.00003283	0.00003283	0.00003283	0.00003283	0.00000018	0.00000000
	Weight over the overall frequency	24.53%	0.00%	0.00%	43.52%	23.30%	1.44%	1.44%	1.44%	1.44%	1.44%	1.44%	0.01%	0.00%
	Total mitigated event frequency	0.00228												
	Tolerable Event Frequency - LHC	0.01000												
	Tolerable Event Frequency - IP side	0.00250												
	Tolerable Event Frequency - Bellow	0.000119048												
	Residual Risk	0.00022030												

Conclusions

- Same reliability data as before (**same assumptions**)
- PLs cannot protect from all failures
- **New** single point of failure -- LGC logic:
    - 58% of chances of breaking the bellow (according with the data)
    - **Testing, runtime monitors (?) and procedures should be put in place**
- Max. **operation time** limit = **12 days** – assuming a **perfect** mechanism/procedure to switch off the motors and **excluding pure software failures from the top FEC**

RAC3 PLs changes

Impact Event		Initiating Cause 1.0	Initiating Cause 1.1	Initiating Cause 1.2	Initiating Cause 2	Initiating Cause 3	Initiating Cause 4	Initiating Cause 5	Initiating Cause 6	Initiating Cause 7	Initiating Cause 8
Triplet-D1 Config Break Bellow		Upper FEC (hardware)	Upper FEC FESA framework	Upper FEC User Software (LGC + FESA class)	Error in actuation path PXI - SAMbuCa	Error in actuation path Motors	Error measuring V	Error measuring H	Error measuring R	Malicius user / Error of operator	Hacker attack
	Event Frequency (1/h)	1.94E-05	1.90E-08	1.14E-05	1.85E-05	1.01E-05	3.42E-05	3.42E-05	1.14E-07	6.38E-09	0.00E+00
	Event Frequency (1/y)	0.17	0.00017	0.10	0.16	0.088651	0.29959200	0.2995920	0.0009986	0.0000559	0.0000000
	PL1	10			10	10					
	PL2										
	PL3										
Operation Time	4	91.25	91.25	91.25	91.25	91.25	91.25	91.25	91.25	91.25	91.25
Procedures / Alarms											
Cybersecurity: TN + RBAC											100
Physical Limit Switches											
Cumulative		912.5	91	91.25	912.5	912.5	91.25	91.25	91.25	91.25	9125
	Intermediate event frequency	0.000186	0.000001824	0.001094	0.000178	0.00009715	0.0032832	0.00328320	0.00001094	0.00000061	0.00000000
	Weight over the overall frequency	2.35%	0.02%	13.77%	2.23%	1.22%	41.31%	41.31%	0.14%	0.01%	0.00%
	Total mitigated event frequency	0.00814									
	Tolerable Event Frequency - LHC	0.01000									
	Tolerable Event Frequency - Bellow	0.000119048									
	Residual Risk	0.00186									

RAC3 PLs changes

However,

Purely systematic failures (e.g., software failures) will not be affected by the operation time

Therefore,

We should not consider this risk reduction in LOPA

These failures will be treated separately, following the risk reduction recommendations for software from the IEC standards (including testing, procedures, runtime monitors, specification, etc.)

RAC3 PLs changes

Triplet-D1 Config Break Bellow		Upper FEC (hardware)	Upper FEC FESA framework	Upper FEC User Software (LGC + FESA class)	Error in actuation path PXI - SAMbuCa	Error in actuation path Motors	Error measuring V	Error measuring H	Error measuring R	Malicius user / Error of operator	Hacker attack
	Event Frequency (1/h)	1.94E-05			1.85E-05	1.01E-05	3.42E-05	3.42E-05	1.14E-07	6.38E-09	0.00E+00
	Event Frequency (1/y)	0.17	0.00000	0.00	0.16	0.088651	0.29959200	0.2995920	0.0009986	0.0000559	0.0000000
	PL1	10			10	10					
	PL2										
	PL3										
Operation Time	5	73	0	0	73	73	73	73	73	73	73
Procedures / Alarms											
Cybersecurity: TN + RBAC											100
Physical Limit Switches											
Cumulative		730	1	1	730	730	73	73	73	73	7300
	Intermediate event frequency	0.000233	0.000000000	0.000000	0.000222	0.00012144	0.0041040	0.00410400	0.00001368	0.00000077	0.00000000
	Weight over the overall frequency	2.72%	0.00%	0.00%	2.59%	1.42%	47.91%	47.91%	0.16%	0.01%	0.00%
	Total mitigated event frequency	0.00880									
	Tolerable Event Frequency - LHC	0.01000									
	Tolerable Event Frequency - Bellow	0.000119048									
	Residual Risk	0.00120									