Functional Safety at BE-ICS

Borja Fernández Adiego
Andrea Germinario
Enrique Blanco Viñuela
Frédéric Chapron
Peter Sollander

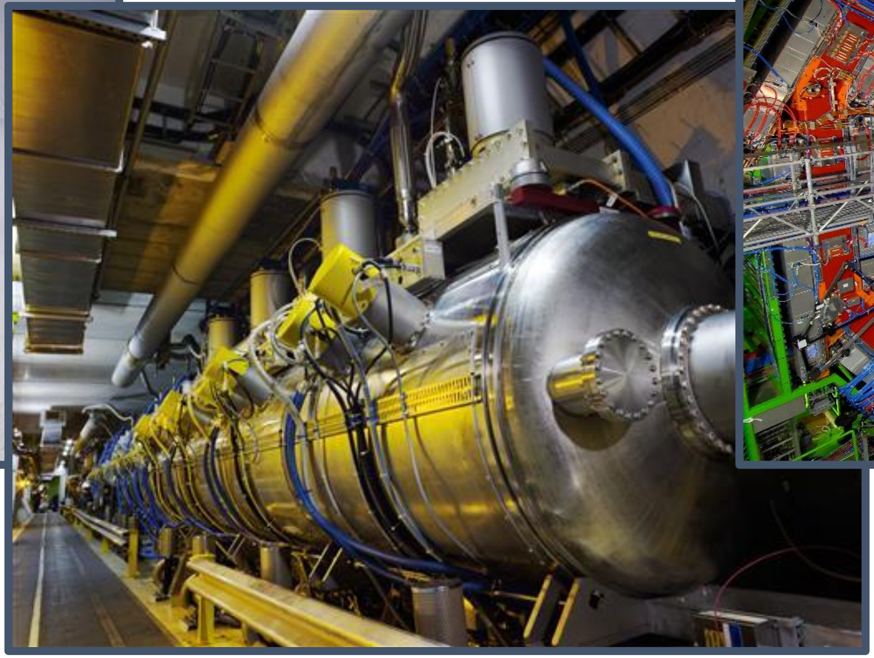
31/05/2023

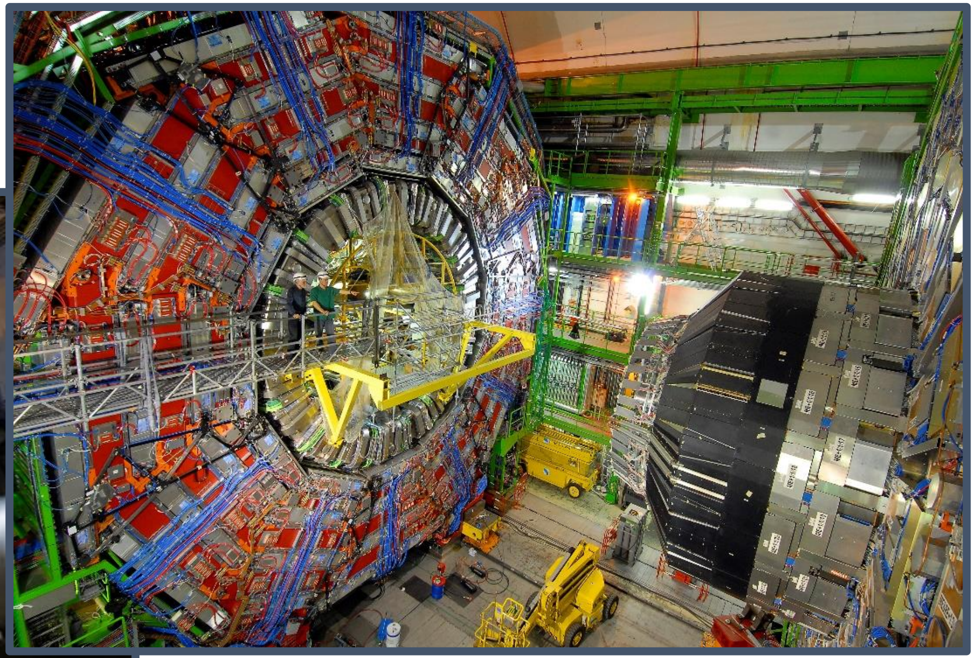
Agenda

- A few basic concepts about **Functional Safety**
- 2 Functional Safety projects at BE-ICS
- Management of Functional Safety projects at BE-ICS

Risks at the industrial installations at CERN

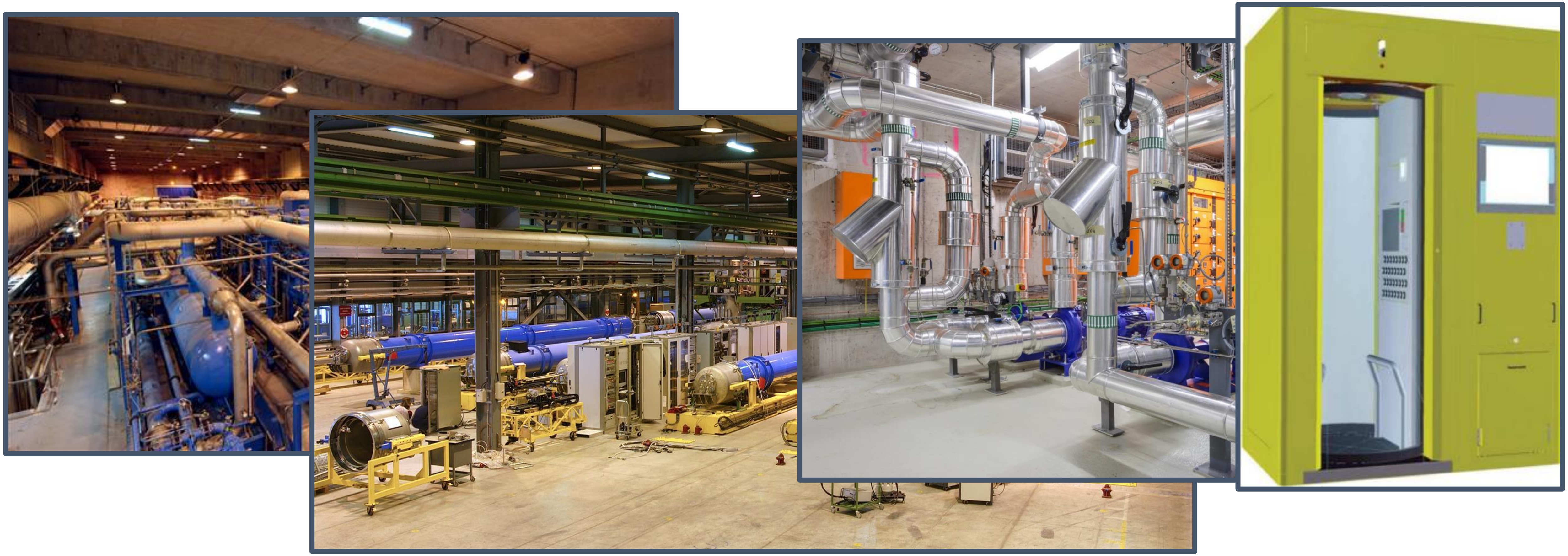
CERN particle accelerators





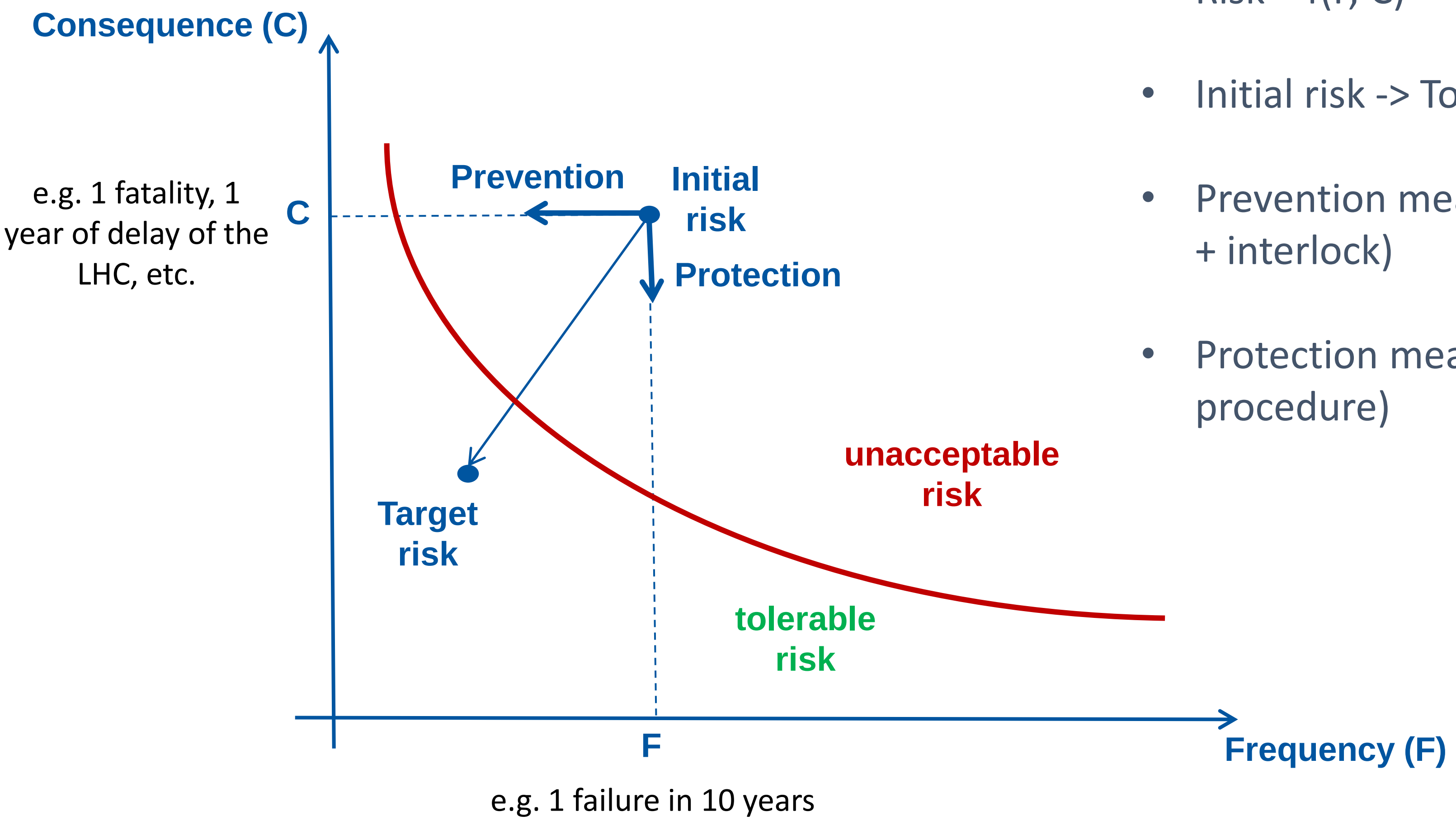
Risks at the industrial installations at CERN

CERN industrial facilities



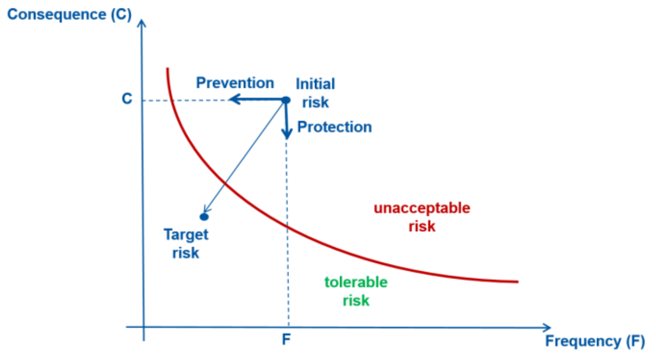
Risk for the **personnel**, the **installations** (economic losses), the **environment**, the **reputation** of the organization, etc.

Risk definition and risk reduction



- Risk = f(F, C)
- Initial risk -> Tolerable risk
- Prevention measures (gas leak detection + interlock)
- Protection measures (evacuation procedure)

Tolerable risk at CERN



HSE risk matrix
https://edms.cern.ch/document/1114042/2

Table 1 – Risk matrix

Risk evaluation		Probability of the hazardous event			
		Very low (1)	Low (2)	Medium (3)	High (4)
Potential severity	Minimal (A)	(A1)	(A2)	(A3)	(A4)
	Low (B)	(B1)	(B2)	(B3)	(B4)
	Medium (C)	(C1)	(C2)	(C3)	(C4)
	High (D)	(D1)	(D2)	(D3)	(D4)

Table 2 - Probability categories

Probability	Occurrence of the hazardous event
Very low (1)	Extremely unlikely to occur during task; once per year or less.
Low (2)	Unlikely to occur during task; more than once per year, maximum of once per month.
Medium (3)	Incident may occur during task; several times per month, maximum of once per week.
High (4)	Likely to occur several times during task several times per week.

Table 3 – Severity categories

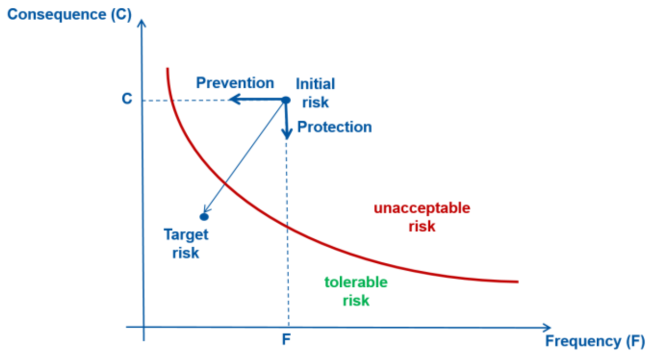
Severity		Severity description
Minimal (A)	People	Slight injuries, no treatment needed.
	Environment	Not applicable.
	Property	Not applicable.
Low (B)	People	Injuries or temporary, reversible illnesses not resulting in hospitalization and requiring only minor supportive treatment.
	Environment	Isolated and minor, but measurable, impact on some component(s) of a public resource.
	Property	Minor property damage in the facility.
Medium (C)	People	Injuries or temporary, reversible illnesses resulting in hospitalization of variable but limited period of disability.
	Environment	Serious impairment of the functioning of a public resource.
	Property	Major property damage in the facility.
High (D)	People	Death from injury or illness, permanent disability or chronic irreversible illness.
	Environment	Permanent or long term loss of a public resource (drinking water, air, etc.).
	Property	Loss off facility.

Table 4 - Action levels

Risk level	Action
Low (A1, A2, B1)	**Acceptable risk:** no actions need to be taken.
Medium (A3, A4, B2, B3, C1, C2, D1)	**Unacceptable risk:** actions are necessary to reduce the risk.
High (B4, C3, C4, D2, D3, D4)	**Unacceptable risk:** immediate actions are necessary to reduce the risk promptly.

Tolerable risk at CERN

CERN accelerators risk matrices (BE-MPE)
https://edms.cern.ch/document/2647881/1



LHC example

Failure mode consequence (severity) – LHC downtime

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	λ_1
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	λ_2
1/1000Years	A	A	A	A	A	A	A	A	A	A	A	

Risk reduction factor

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

$$RRF = \frac{1}{1y} / \frac{1}{100y} = 100$$

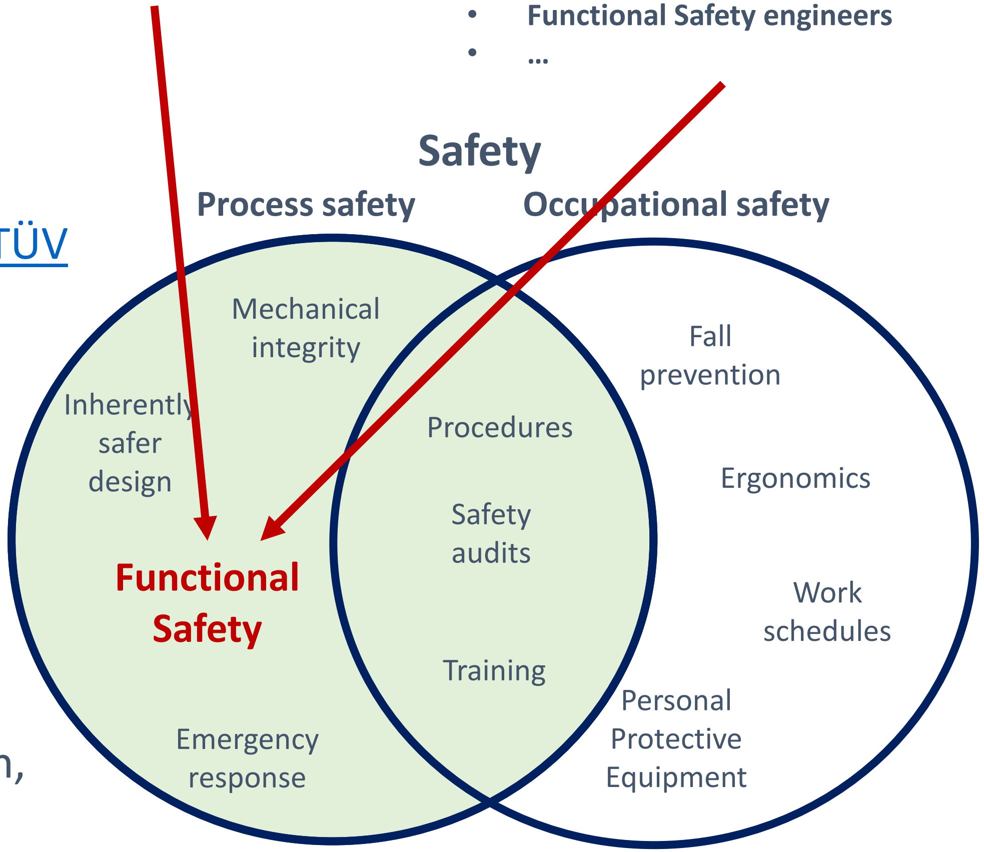
Related to SIL

Functional Safety

- The goal is to **ensure safety** in our industrial installations
- **Functional Safety** is, "**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 standards:
  - **IEC 61508**: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems
  - **IEC 61511**: specific for the process industry
  - IEC 62061: safety of machinery
  - IEC 13849: safety-related Parts of Control Systems
  - Specific industry standards (e.g chemical industry, radioprotection, etc.)
- Functional Safety certified courses (by [TÜV Rheinland]()):
  - [Safety Instrumented Systems]() and
  - [Process Hazard & Risk Analysis]()

- **HSE** (Health & Safety and Environmental) unit
- **DSO** (Department Security Officer)

- Process experts and responsible
- Control engineers
- Instrumentation engineers
- **Functional Safety engineers**
- …

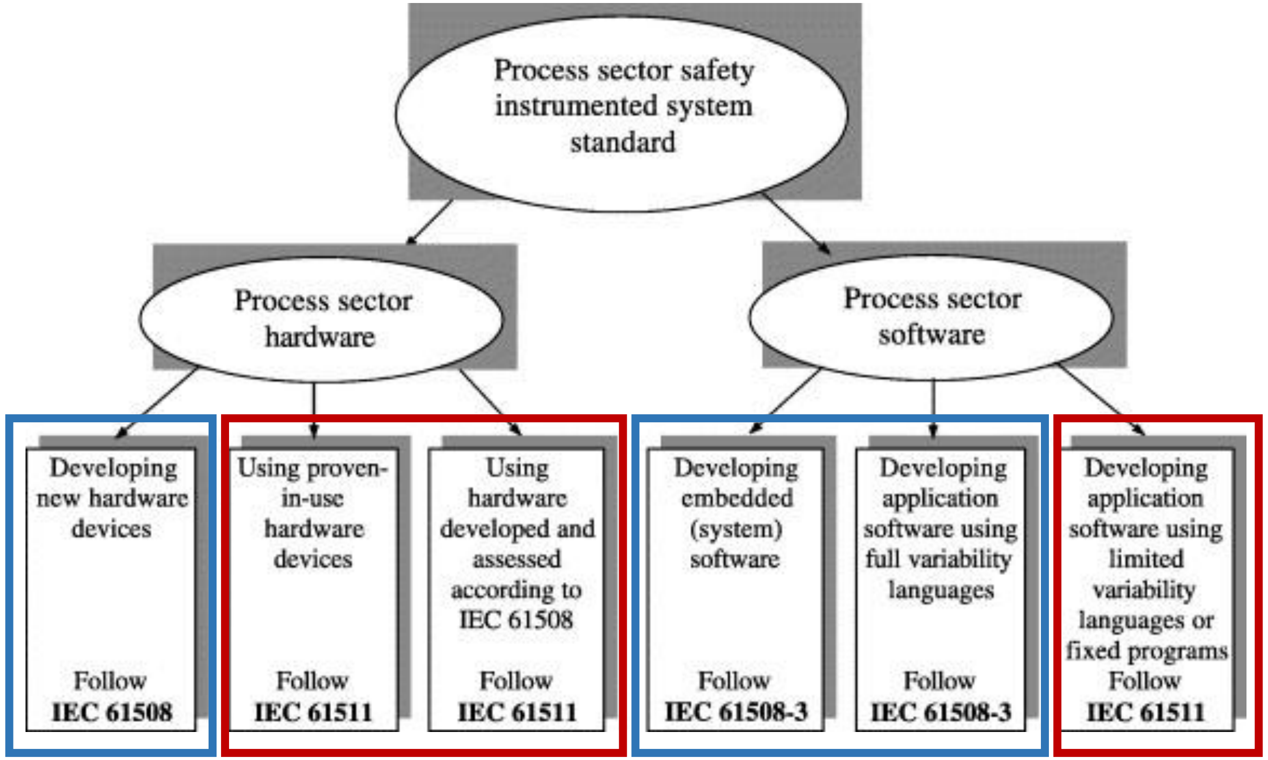


Risk for the people, the environment and the installations

Context – Functional Safety

Which standard should we use?

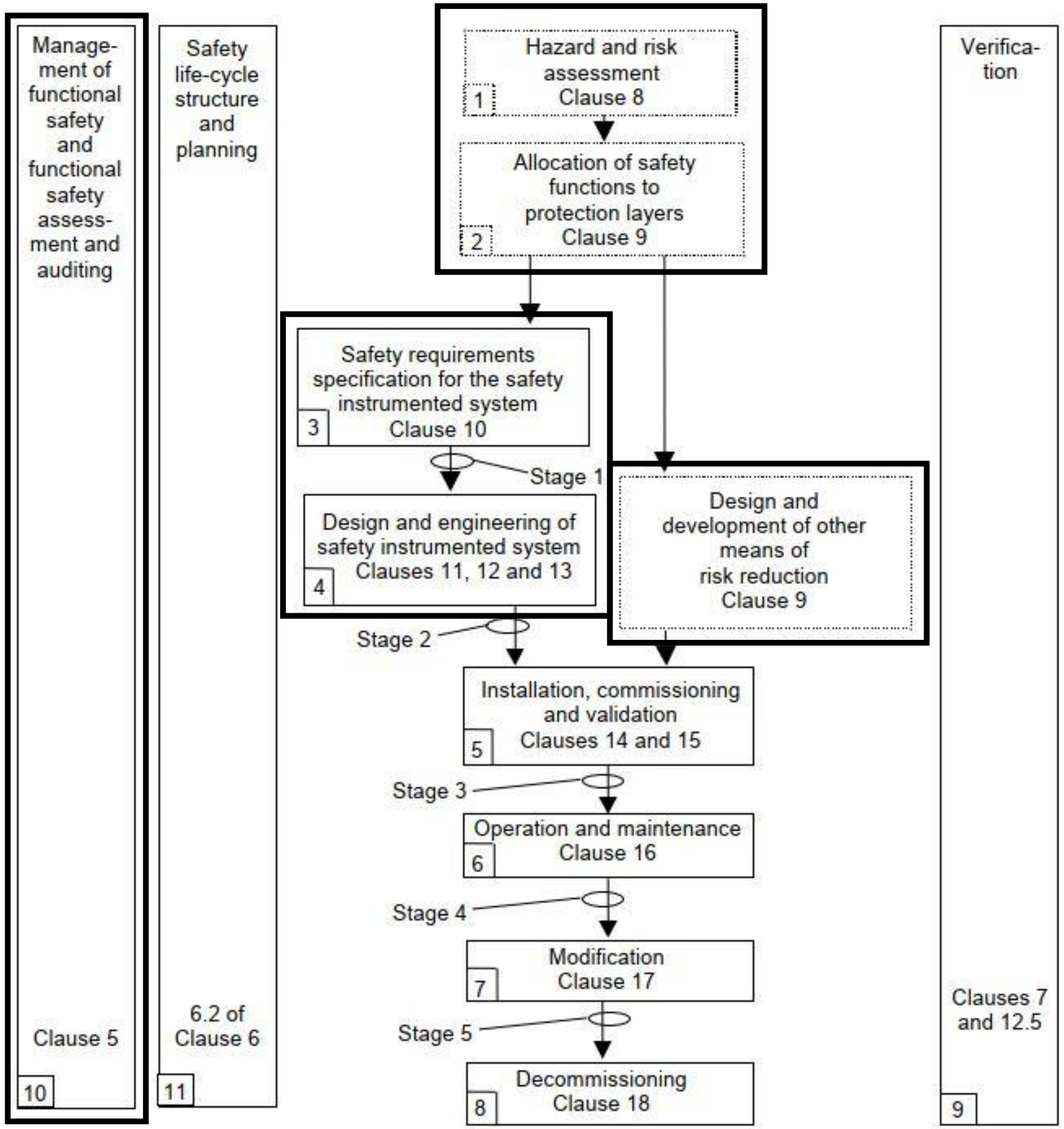
e.g. **Design a sensor** to be used in Safety systems for a chemical plant



e.g. **Design Safety system** for a chemical plant

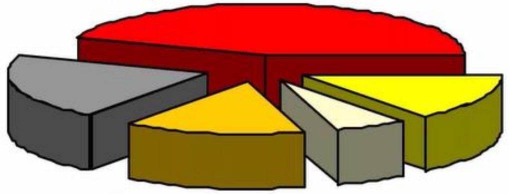
Context – IEC 61511

- IEC 61511 standard - SIS (Safety Instrumented Systems) for the industrial process sector
- It provides the safety life-cycle:
  - 11 phases (to complete the project)
  - 19 Clauses (requirements)
- Very challenging task to implement all the requirements (lots of resources and time-consuming)



Failures types

Failure per project phase



"Out of Control: Why Control Systems go Wrong and How to Prevent Failure,"
U.K.: Sheffield, Heath and Safety Executive, 1995 (Ed 2, 2003)

Failure types according their nature:

- **Random Hardware Failures**
  - From degradation mechanism
- **Systematic Failures**
  - Incorrect specification
  - Human errors
  - Software errors
  - Maintenance and modifications
  - ….

Failure types according their criticality and diagnostics:

- **Dangerous vs Safe**
- **Detected vs Undetected**

Functional Safety cares about **random and systematic** failures **but only** about the **dangerous undetected failures**

What about SIL?

SIL (Safety Integrity Level) = tool to **quantify the risk reduction**

Safety Integrity Level	Low-demand mode of operation	High-demand mode of operation
	Average probability of failure on demand (PFD_{avg}) / activation	Probability of dangerous failure per hour (PFH) /hour
SIL 4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$10^{-9} \leq PFH < 10^{-8}$
SIL 3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10^{-8} \leq PFH < 10^{-7}$
SIL 2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$10^{-7} \leq PFH < 10^{-6}$
SIL 1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$10^{-6} \leq PFH < 10^{-5}$

Low Demand: Safety Function demand rate is less than or equal to once a year

High Demand Mode: Safety Function demand rate is more than once a year

SIL	PFD_{avg}	RRF
4	$\geqslant 10^{-5}$ to $< 10^{-4}$	10000 to 100 000
3	$\geqslant 10^{-4}$ to $< 10^{-3}$	1000 to 10 000
2	$\geqslant 10^{-3}$ to $< 10^{-2}$	100 to 1000
1	$\geqslant 10^{-2}$ to $< 10^{-1}$	10 to 100

But it is **not only about hardware reliability**

What about SIL?

Process engineer
Safety officer
….

“agreement”

Risk reduction
Requirements = SIL

Functional Safety
engineer

FS standards

Risk analysis:

- **Identify** the risk
- **Evaluate** its criticality (consequence + frequency of the hazardous event)
- **Determine** the needed **risk reduction** (tolerable risk) = **SIL target**

e.g. **SIL2 Low demand** SIF (if the temp. is higher than 60°C, open the valve)

SIL2

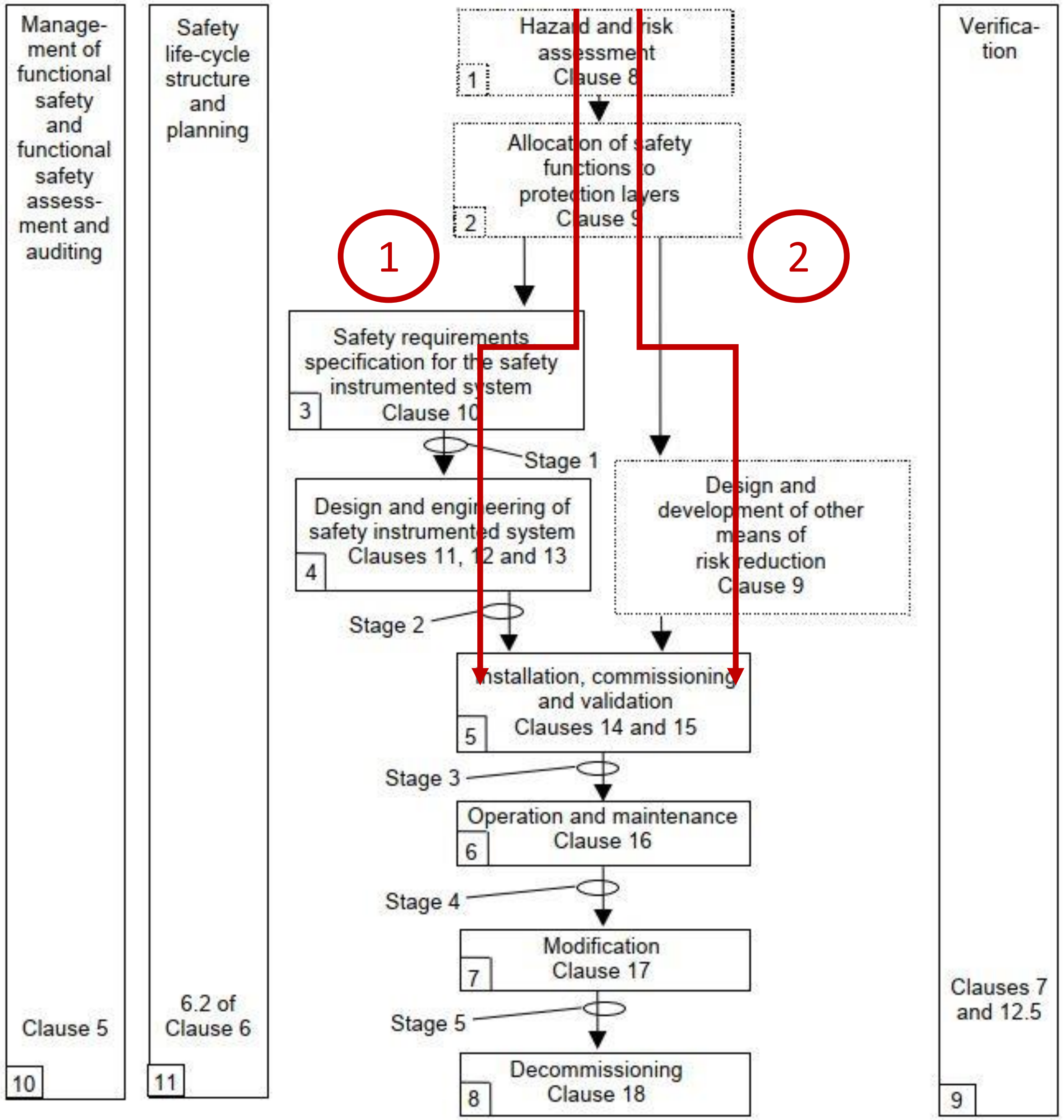
Design the SIL2 Low Demand SIF according to the IEC 61511 (or other) by following the **safety life cycle (hardware, software, communication protocols, architecture, etc.)**

it is **not only about hardware reliability**

CERN Safety systems examples

1. **Safety Instrumented System** for the SM18 cluster F (superconducting magnets test bench facility)

2. **Protection layers** for the HL-LHC Full Remote Alignment System (FRAS)



SM18 Cluster F Safety Instrumented System

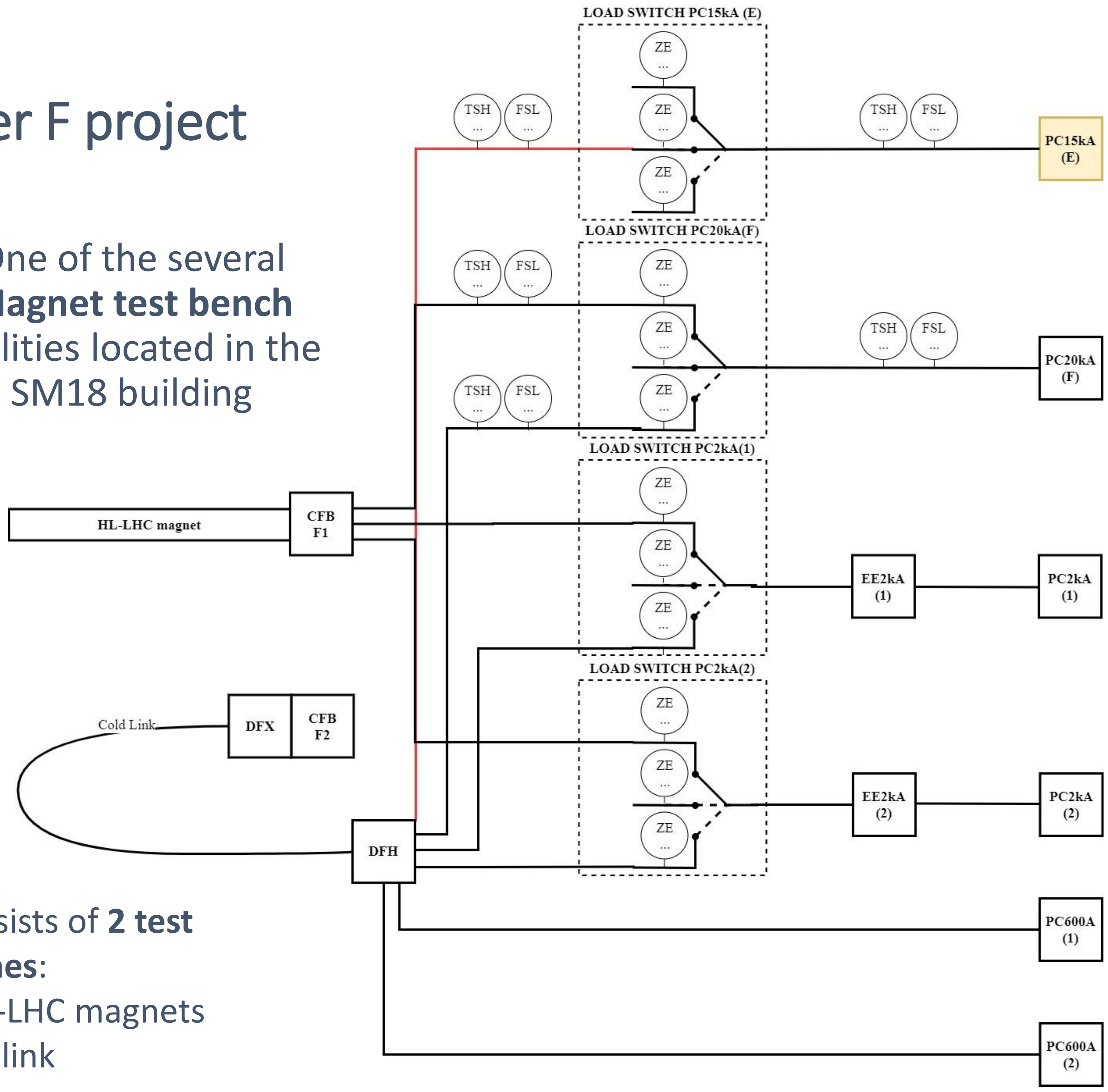
SM18 Cluster F project

Taken from https://cds.cern.ch/record/724733

Context – SM18 Cluster F project

One of the several **Magnet test bench** facilities located in the SM18 building

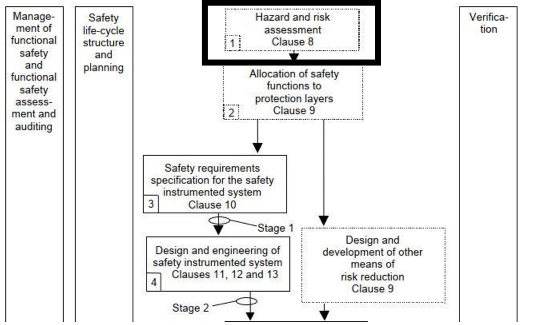
Electrical and cryogenics risks



6 power converters

It consists of **2 test benches**:

- HL-LHC magnets
- SC link



Risk analysis hazard identification – Personnel and machine protection

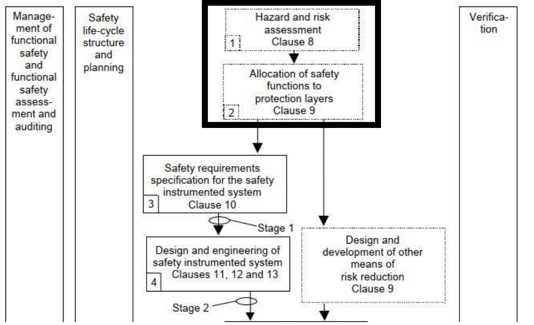
FMEA (Failure Mode and Effect Analysis)

Effects of the failure mode
Failure effect on

Subsystem		Failure mode		Effects of the failure mode		Causes of failure	Current mitigation measures for the failure mode or the hazard
				Failure effect on the system	Failure effect on the operators and other related persons		
Id	Description	Id	Description				
2	Bench Commutators	2.1	Incorrect indication of the position of the commutators	Power a (different) bench when potentially not all the "start-up" conditions are met - potential damage to the magnet, installation, PCs...	Operator does not know which bench is powered. Operator inadvertently exposed to electrical power - Electrocution	Failure of the feedback contacts of the commutator>Wrong wiring Accidental rupture of cable	

Other methods:

- **HAZOP**: when you analyze deviations (e.g. high temperature, high pressure)
- **FTA**: when you analyze the combination of multiple failures
- **What-if**: based on experience
- etc.

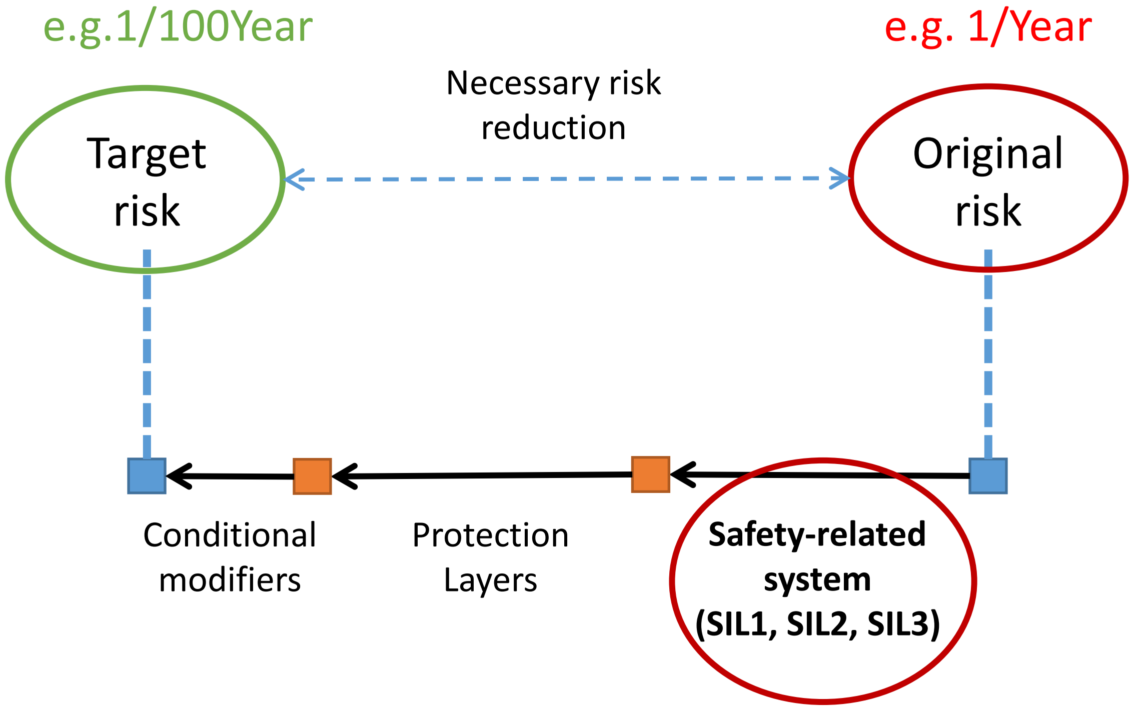


Risk assessment - Risk reduction and layers of protection

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

How?

- **Judgement** of the organization
- Based on the **IEC 61511 guidelines**



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

Estimation of the original failure frequency due to (for example):

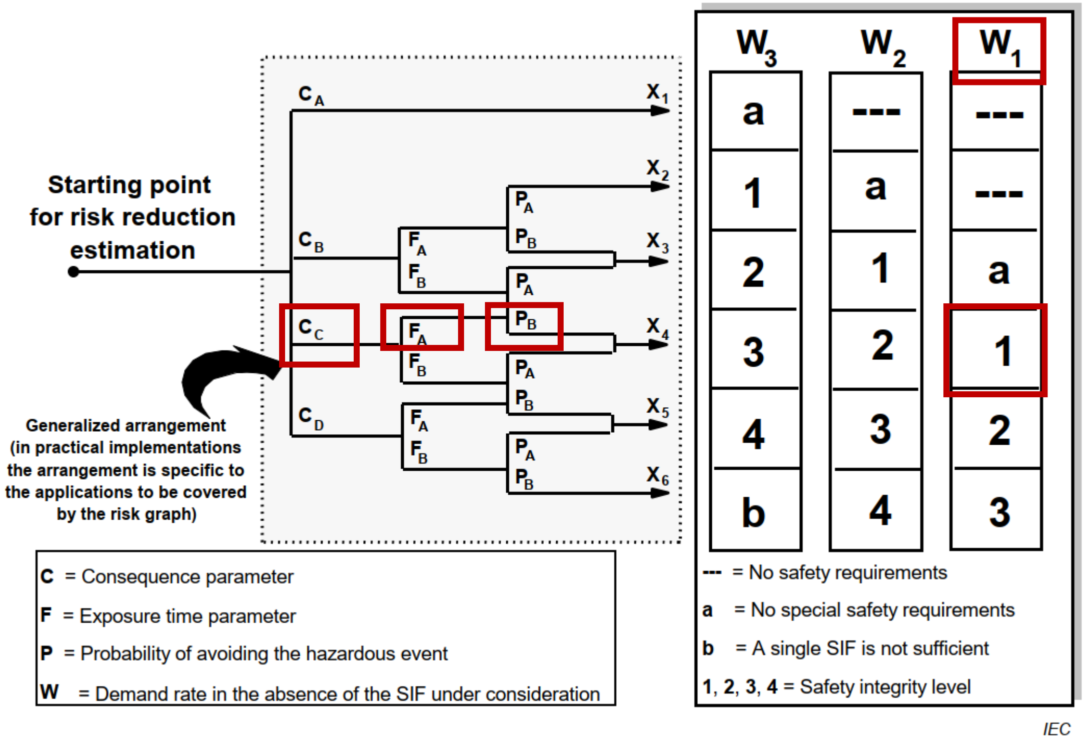
- Operator/expert command
- Software
- Hardware
- …

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 - 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 the HSE matrix)*
- Sometimes the necessary **risk reduction is bigger for machine protection** (mainly due to the F and P parameters)

SIL1 → necessary **Risk Reduction Factor** 10 < (RFF) ≤ 100

Calibrated Risk Graph – calibration (corporative decision)

Personnel protection:

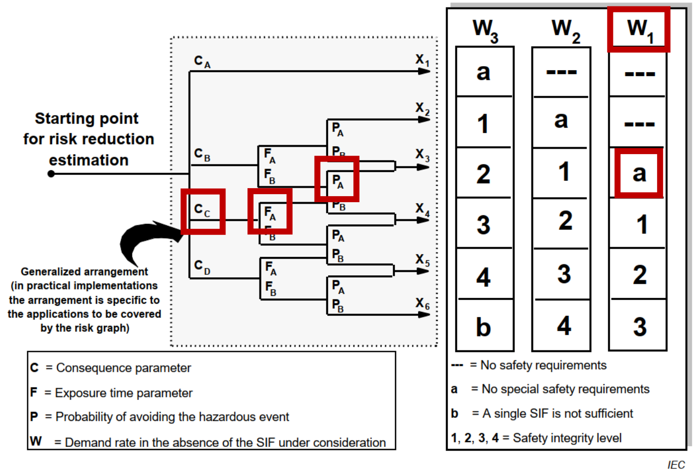
- Based on **examples** from IEC 61511-3:2016 Annex D or IEC 61508-5:2010 Annex E

OPERATORS		MACHINES	
Consequences:			
Minor injury is possible	CA	Delay of few minutes to few hours	CA
Permanent injury is possible	CB	Delay of several hours to few days	CB
One fatality is possible	CC	Delay of several days to several weeks	CC
Multiple fatalities are possible	CD	Delay of a month or more/ cancelation of test programmes	CD
Frequency of Exposition:			
less than 10% of working time	FA	Always	FB
more than 10% of working time	FB		
Possibility of avoidance:			
If there is any automatic control system capable of detecting the hazard and alerting the operators and/or prevent the hazard, in a way the harm can be avoided	PA	If there is any automatic control system capable of detecting the hazard and alerting the operators and/or prevent the hazard, in a way the harm can be avoided	PA
If not	PB	If not	PB
Probability of Failure			
less than 1 failure per 10 years	W1	less than 1 failure per 10 years	W1
less than 1 failure per year	W2	less than 1 failure per year	W2
more than 1 failure per year	W3	more than 1 failure per year	W3

Machine protection:

- Based on the operational **experience at CERN**

Calibrated Risk Graph vs HSE matrix



OPERATORS		MACHINES	
Consequences:			
Minor injury is possible	CA	Delay of few minutes to few hours	CA
Permanent injury is possible	CB	Delay of several hours to few days	CB
One fatality is possible	CC	Delay of several days to several weeks	CC
Multiple fatalities are possible	CD	Delay of a month or more/ cancelation of test programmes	CD
Frequency of Exposition:			
less than 10% of working time	FA	Always	FB
more than 10% of working time	FB		
Possibility of avoidance:			
If there is any automatic control system capable of detecting the hazard and alerting the operators and/or prevent the hazard, in a way the harm can be avoided	PA	If there is any automatic control system capable of detecting the hazard and alerting the operators and/or prevent the hazard, in a way the harm can be avoided	PA
If not	PB	If not	PB
Probability of Failure			
less than 1 failure per 10 years	W1	less than 1 failure per 10 years	W1
less than 1 failure per year	W2	less than 1 failure per year	W2
more than 1 failure per year	W3	more than 1 failure per year	W3

Table 1 – Risk matrix

Risk evaluation		Probability of the hazardous event			
		Very low (1)	Low (2)	Medium (3)	High (4)
Potential severity	Minimal (A)	(A1)	(A2)	(A3)	(A4)
	Low (B)	(B1)	(B2)	(B3)	(B4)
	Medium (C)	(C1)	(C2)	(C3)	(C4)
	High (D)	(D1)	(D2)	(D3)	(D4)

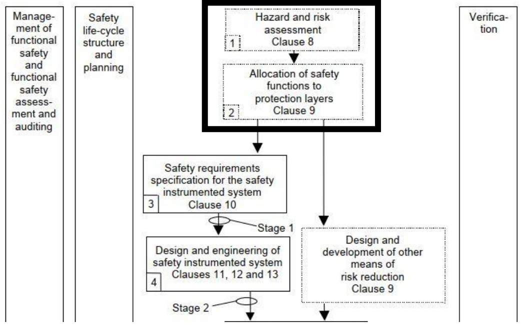
Table 3 – Severity categories

Severity		Severity description
Minimal (A)	People	Slight injuries, no treatment needed.
	Environment	Not applicable.
	Property	Not applicable.
Low (B)	People	Injuries or temporary, reversible illnesses not resulting in hospitalization and requiring only minor supportive treatment.
	Environment	Isolated and minor, but measurable, impact on some component(s) of a public resource.
	Property	Minor property damage in the facility.
Medium (C)	People	Injuries or temporary, reversible illnesses resulting in hospitalization of variable but limited period of disability.
	Environment	Serious impairment of the functioning of a public resource.
	Property	Major property damage in the facility.
High (D)	People	Death from injury or illness, permanent disability or chronic irreversible illness.
	Environment	Permanent or long term loss of a public resource (drinking water, air, etc.).
	Property	Loss off facility.

Table 2 - Probability categories

Probability	Occurrence of the hazardous event
Very low (1)	Extremely unlikely to occur during task; once per year or less.
Low (2)	Unlikely to occur during task; more than once per year, maximum of once per month.
Medium (3)	Incident may occur during task; several times per month, maximum of once per week.
High (4)	Likely to occur several times during task; several times per week.

Risk analysis hazard identification – Personnel and machine protection

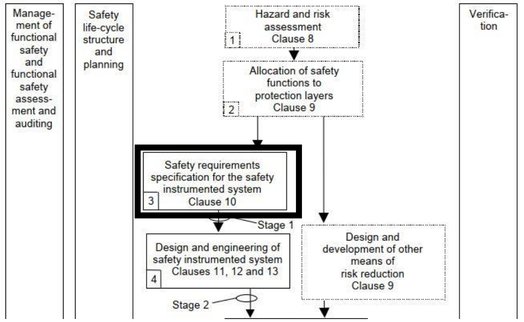


Determination of SIL								
Consequence		Occupancy (Frequency of Exposition)		Possibility of Avoidance		Base Probability of failure		SIL from Risk Graph
CA, CB, CC, CD		FA, FB		PA, PB		W1, W2, W3		-, 1, 2, 3
Choosen value	Comments or Justifications	Choosen value	Comments or Justifications	Choosen value	Comments and justifications	Choosen value	Comments and justifications	
CC	1 person might die due to eletrocution, since there is no insulation, or fire	FA	Operators are less than 10% of the time exposed to the hazardous zone	PB	The danger is not easily recognized by the operator and can scale quickly	W1	Less than once every 10 years	SIL 1

SIL1
necessary **Risk Reduction Factor 10 < RFF ≤ 100**

Risk graph calibration

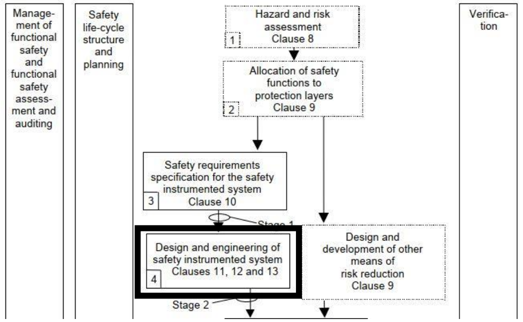
Safety Requirements Specification (SRS)



Very detailed (and tedious) document to specify all details of each Safety Instrumented Functions (SIF)

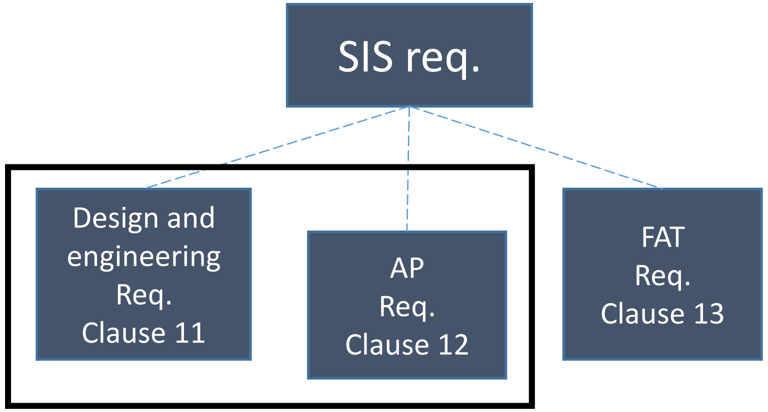
SIF DETAILS	
Tag	SIF-01
Description	Regarding any of the water cooling cables, upon detecting a high or a low flow, analyse the position of the associated load switch commutators and disable the associated power converter if the cable can be powered. To disable the power, disable the power permit and, after 1 minute, trigger the fast power abort command.
Sources of demand	Water Cooling Cable - Water temperature too high (Hazard 1.1): Water leak or wrong regulation of the Cooling System; Water Cooling Cable – Low flow (Hazard 1.3): Water leak or wrong regulation of the Cooling System.
Demand Rate	Less than once every 10 years for each of the two hazards which are source of demand.
Required Response Time	3 minutes after passing one of the threshold limits.
Output Actions	Disable the power converter by using two commands: the power permit and the fast power abort, the last one with a delay.
Criteria for Successful Operation	• Shutdown the power converter if the hazardous event occurs. • No damage to installations or personnel.
Conceptual Diagram of the SIF	Scheme on file "SIF-01 Block Diagram.drawio".
I/O functional relationship	Formal specification of the functional relationship found in the referenced document of Cause and Effect Matrix.
SIF Interfaces with any other system, BPCS or operator	• Operator: SCADA interface on the WinCCOA panel. • BPCS: Power converters will be shared between SIFs and Interlock Control.
Dangerous combinations of Output States	Not identified.
Mean time to repair	8 hours.

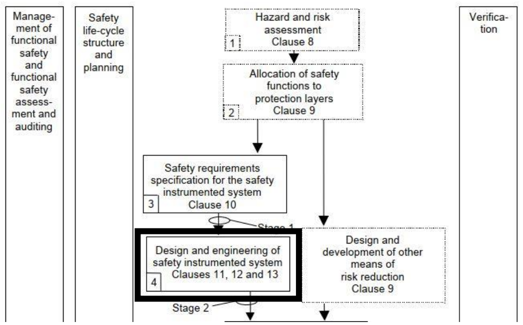
Common Cause Failures	
Type of failure	Description
Feedbacks of commutators	The feedbacks of the commutators are responsibility of SIF-03.
Commands to stop the power converters	Since the commands will act on the same power converter, it is possible that a failure on the power converter can cause both commands to fail.
Safety relays	The safety relays transform the output signals from the PLC to input signals for the actuators. Though they will be separated and isolated, the safety relays will be from the same model and thus can have a common cause of failure.
Process Details	
Safe State definition	The power converters related to the hazardous water-cooling cable are switched off, with no damage to installations or personnel.
Process Safety Time	5 minutes.
Individually safe process states which, when occurring concurrently, create a separate hazard	Not identified.
SIL Requirements	
Mode of Operation	Low demand
Target SIL	2
Test Proof Details	
Proof Test Requirements for inputs and final elements	
Sensor name or tag	All sensors and Actuators
Proof test interval	1 year
Test duration	1 hour
State of the tested device	Off-line
Detection of common cause failures	None
Prevention of errors	N/A



SIS design and engineering

- Design a SIS compliant with the SRS (Safety Requirements Specification)
- Challenges:
  1. **Design and engineering requirements**: *IEC 61511-1:2016 Clause 11*
     - **Hardware Fault Tolerance** (11.4)
     - Selection of the devices (11.5)
     - **Hardware random failures** (11.9)
     - Others (System behaviour on detection of a fault, field devices, interfaces, maintenance, etc.)
  2. **Application program (AP) Requirements** *IEC 61511-1:2016 Clause 12*
  3. Factory Acceptance Test (FAT) requirements *IEC 61511-1:2016 Clause 13*

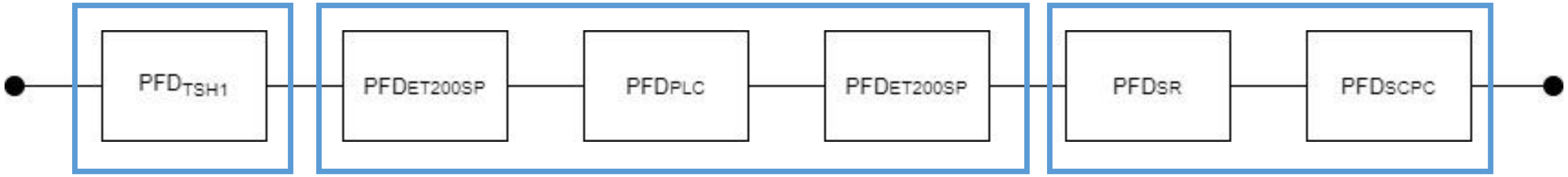




Hardware random failures analysis

No certified device (reliability calculation is needed)

Reliability block diagram



Example 1oo1

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

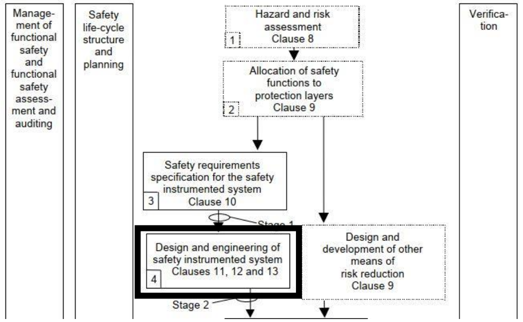
$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Average Probability of Failure On Demand for the sensor group

$$PFD_{avg} \approx PFD_{avg} + PFD_{avg} + PFD_{avg}$$

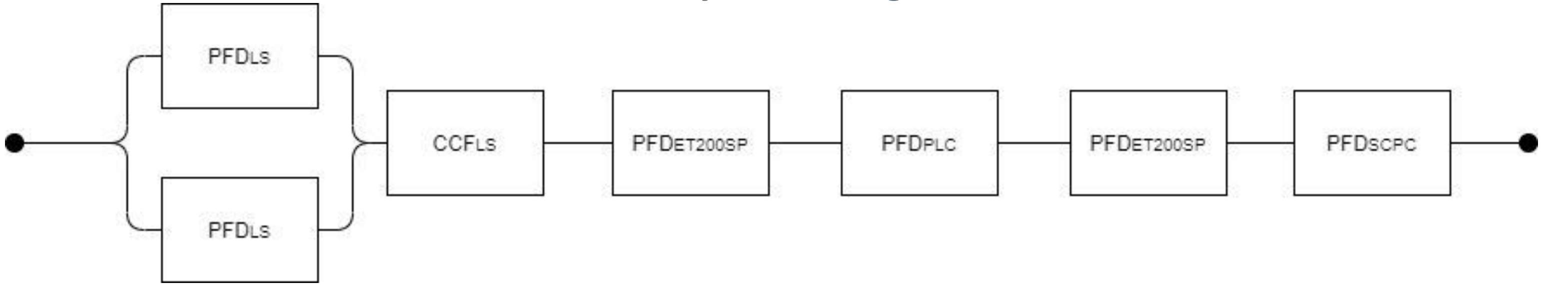
IEC 61508-6:2010 Annex B

Demand Mode of Operation		
Safety Integrity Level (SIL)	PFD_{avg}	Required risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10^4$ to $\leq 10^5$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 10^3$ to $\leq 10^4$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$> 10^2$ to $\leq 10^3$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$> 10^1$ to $\leq 10^2$



Hardware random failures analysis

Reliability block diagram



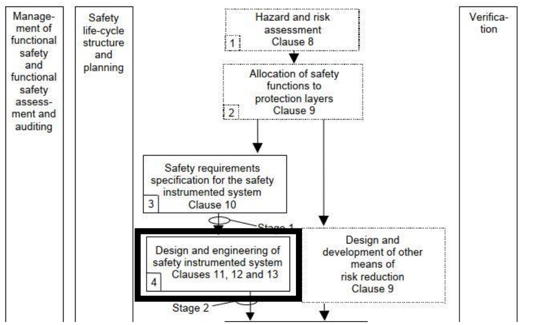
$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_{avg} \approx PFD_{avg} + PFD_{avg} + PFD_{avg}$$

IEC 61508-6:2010 Annex B

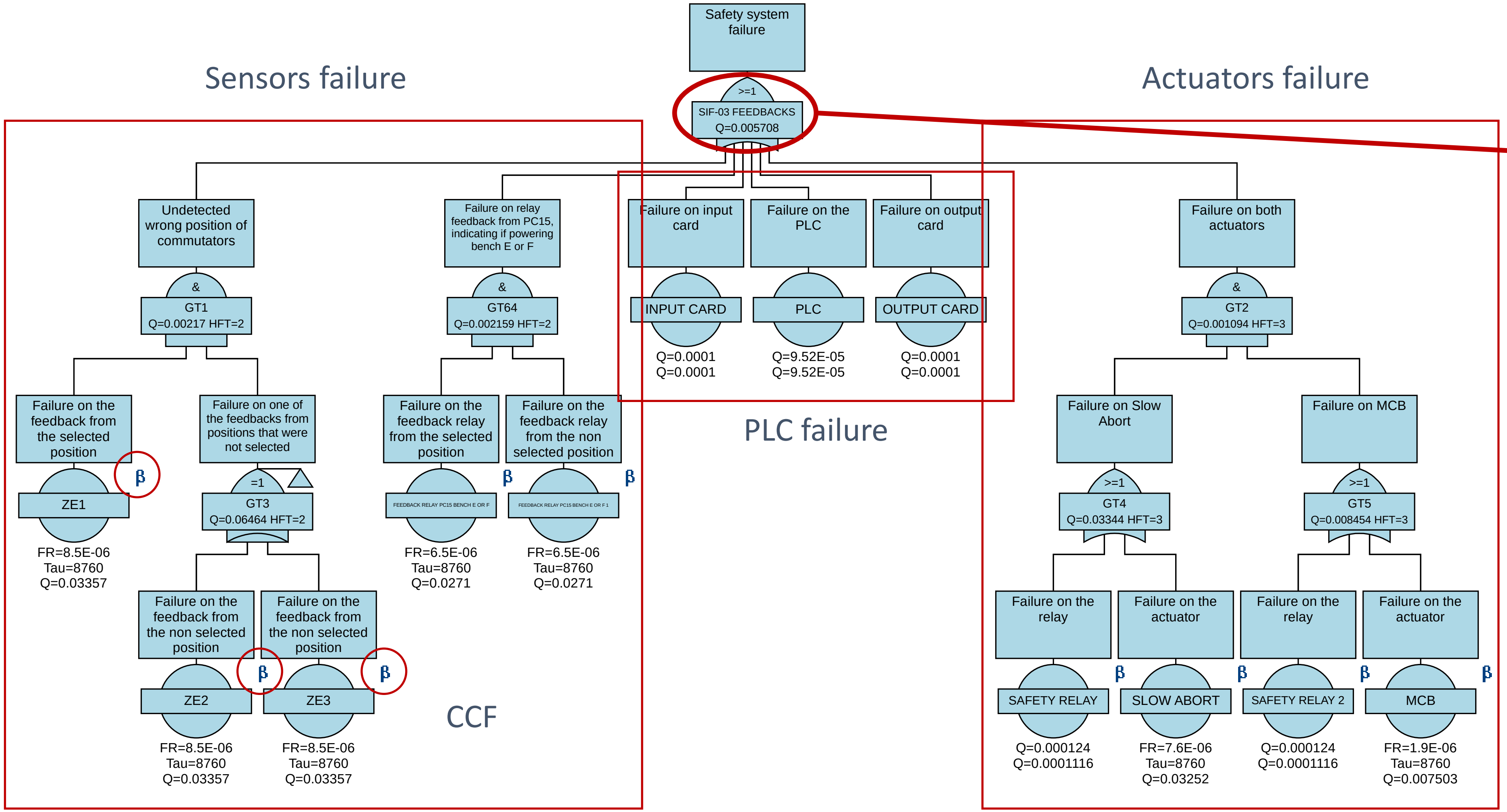
$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

Demand Mode of Operation		
Safety Integrity Level (SIL)	PFD_{avg}	**Required risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	$> 10^4$ to $\leq 10^5$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$> 10^3$ to $\leq 10^4$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$> 10^2$ to $\leq 10^3$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$> 10^1$ to $\leq 10^2$



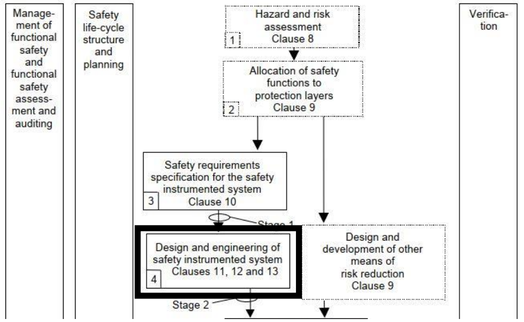
Hardware random failures analysis

Reliability Block Diagram (RBD) or **Fault Tree Analysis (FTA)** for SIFs **- ISOGRAPH**

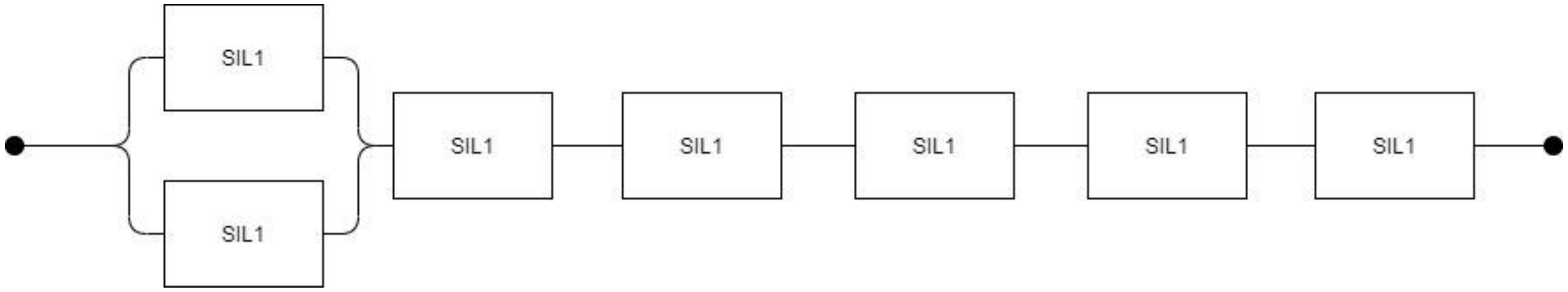


SIL	PFD_{avg}
4	$\geqslant 10^{-5}$ to $< 10^{-4}$
3	$\geqslant 10^{-4}$ to $< 10^{-3}$
2	$\geqslant 10^{-3}$ to $< 10^{-2}$
1	$\geqslant 10^{-2}$ to $< 10^{-1}$

Architectural constraints analysis



- Even if the prob. of failure is compliant with target SIL, we may need to apply redundancy
- Use the reliability model (sensors + controller + actuators) and analyze the SIF architecture

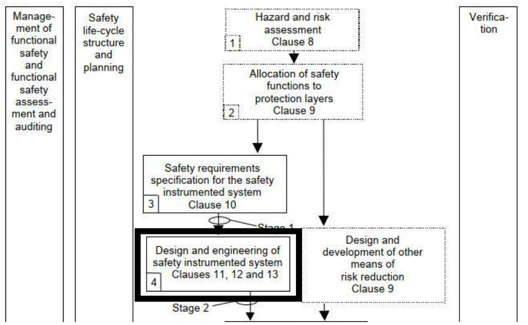


Redundancy is needed, if continuous mode

Hardware Fault Tolerance
IEC 61511-1:2016 Clause 11.4

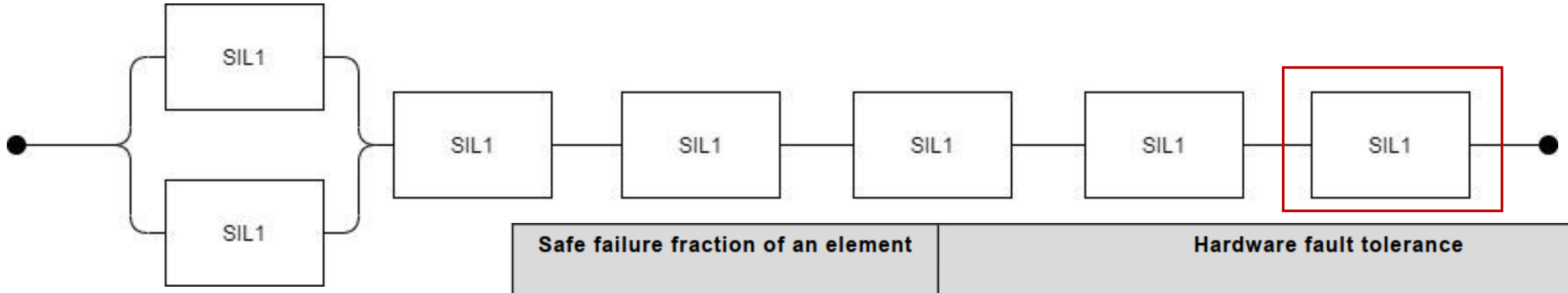
SIL	Minimun HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode) or continuous mode)	1
4 (any mode)	2

HFT (Hardware Fault Tolerance)



Architectural constraints analysis

- Route 1_H based on hardware fault tolerance and safe failure fraction concepts; or,
- Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.



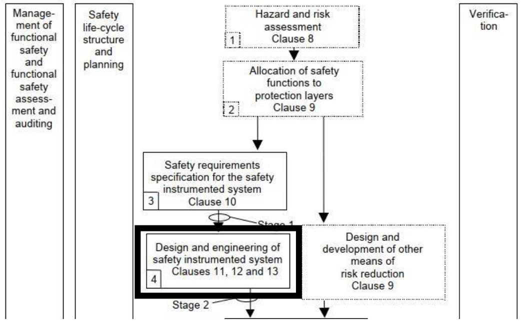
Architectural Constraints
IEC 61508-2:2010 Clause 7.4.4 Route 1H

Type A
(simple devices ≈ Mechanical devices)

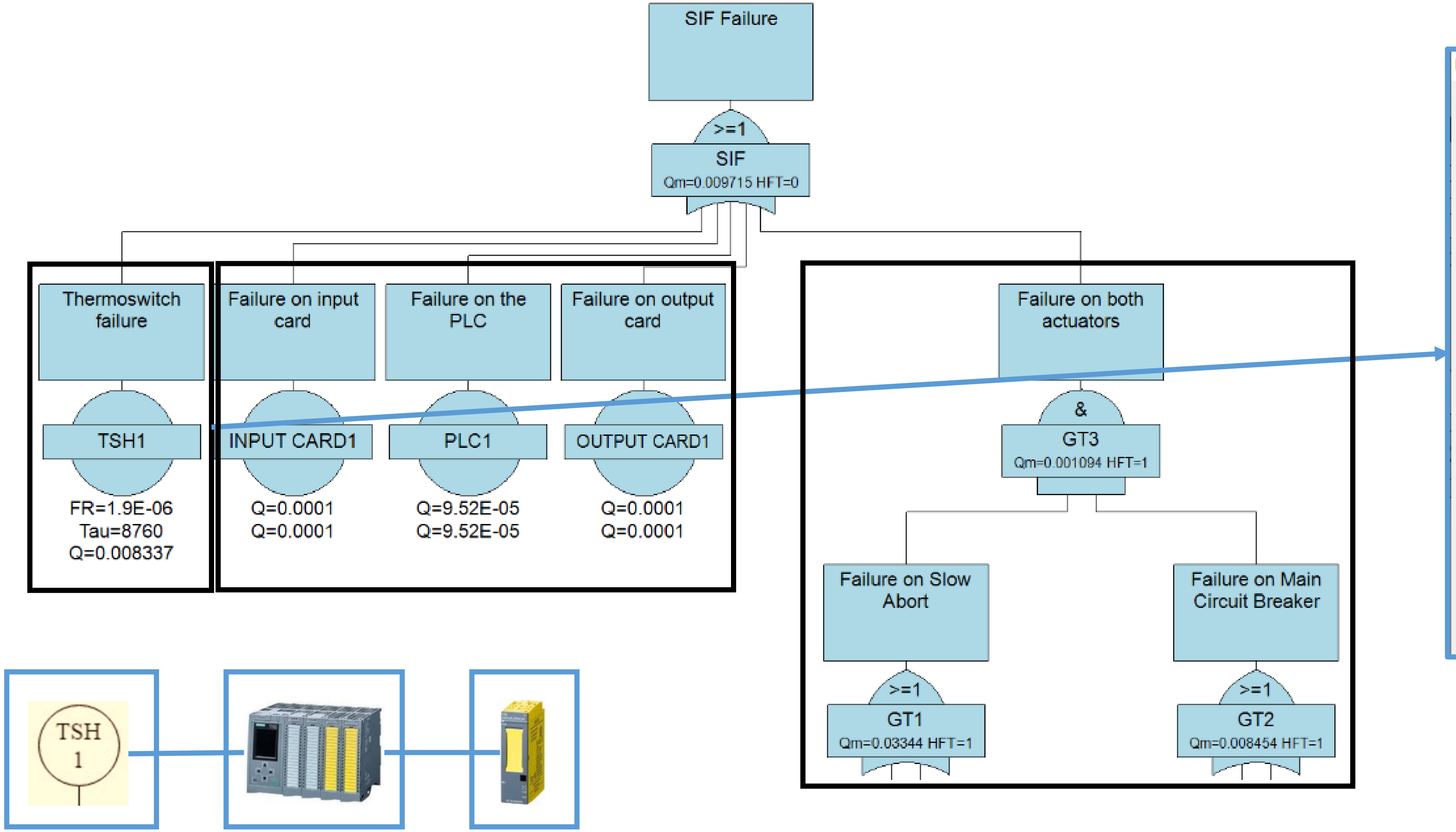
Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

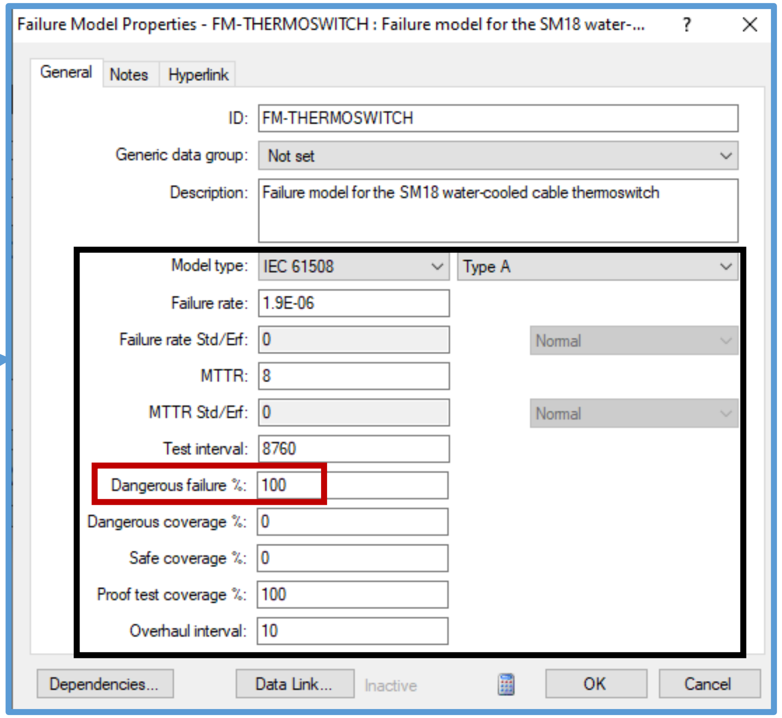
Type B
(complex devices ≈ contain microprocessors)

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4



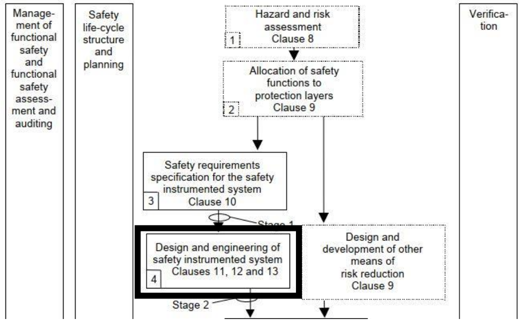
Architectural constrains analysis with Isograph





Related to SFF (Safe Failure Fraction)

Application Program



- IEC 61508-3 (2010). Software requirements
- IEC 61511-1 (2016). Clause 12. SIS application program development
- IEC 61511-2 (2016). Annex A and Annex B

12.2.3 The IEC 61511 series addresses programming in Limited Variability Languages (LVL) and the use of devices using Fixed Program Languages (FPL). The IEC 61511 series does not address Full Variability Language (FVL) and the IEC 61511 series does not address SIL 4 application programming. Where function blocks are written in FVL then these shall be developed and modified under IEC 61508-3:2010.

The traditional text based approach of safety AP specification is not efficient enough to handle the advanced, complex safety requirements commonly found in SIF specifications.

The most efficient tool to address these challenges is the Model-based design (MBD). MBD is a mathematical and visual method of addressing the problems associated with designing complex safety systems, and is being used successfully in many applications. It provides an efficient approach to overcome the difficulties of the development phase of the safety life-cycle. This approach and this example include the following steps:

The detailed functional safety requirements for each SIF can typically be defined by use of logic diagrams or cause and effect (see Figure D.2) drawings. In many cases, the

The models are independently run by the model checking tool in order to detect safe behavior violations. If errors are found by the model checker the concerned models are corrected and run again until they are free from these systematic design faults.

Testing and verification - Formal methods and the FS standards

IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems

Table A.1 – Software safety requirements specification

(See 7.2)

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1a	Semi-formal methods	Table B.7	R	R	HR	HR
1b	Formal methods	B.2.2, C.2.4	---	R	R	HR
2	Forward traceability between the system safety requirements and the software safety requirements	C.2.11	R	R	HR	HR
3	Backward traceability between the safety requirements and the perceived safety needs	C.2.11	R	R	HR	HR
4	Computer-aided specification tools to support appropriate techniques/measures above	B.2.4	R	R	HR	HR

Table A.5 – Software design and development – software module testing and integration

(See 7.4.7 and 7.4.8)

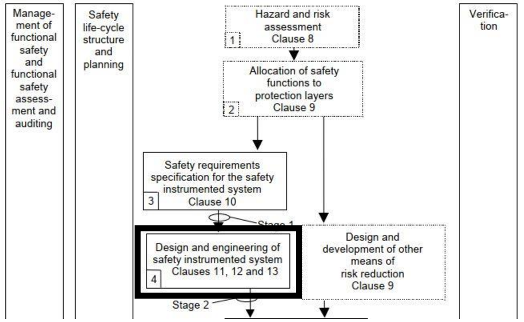
Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Probabilistic testing	C.5.1	---	R	R	R
2	Dynamic analysis and testing	B.6.5 Table B.2	R	HR	HR	HR
3	Data recording and analysis	C.5.2	HR	HR	HR	HR
4	Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	HR	HR	HR
5	Performance testing	Table B.6	R	R	HR	HR
6	Model based testing	C.5.27	R	R	HR	HR
7	Interface testing	C.5.3	R	R	HR	HR
8	Test management and automation tools	C.4.7	R	HR	HR	HR
9	Forward traceability between the software design specification and the module and integration test specifications	C.2.11	R	R	HR	HR
10	Formal verification	C.5.12	---	---	R	R

IEC 61511: Functional safety – Safety instrumented systems for the process industry sector

- several references to model checking. For example from IEC 61511-2:2016 Annex B:

*"… specification should be implemented in the graphical language of the **model checking** workbench environment…"*

Application Program

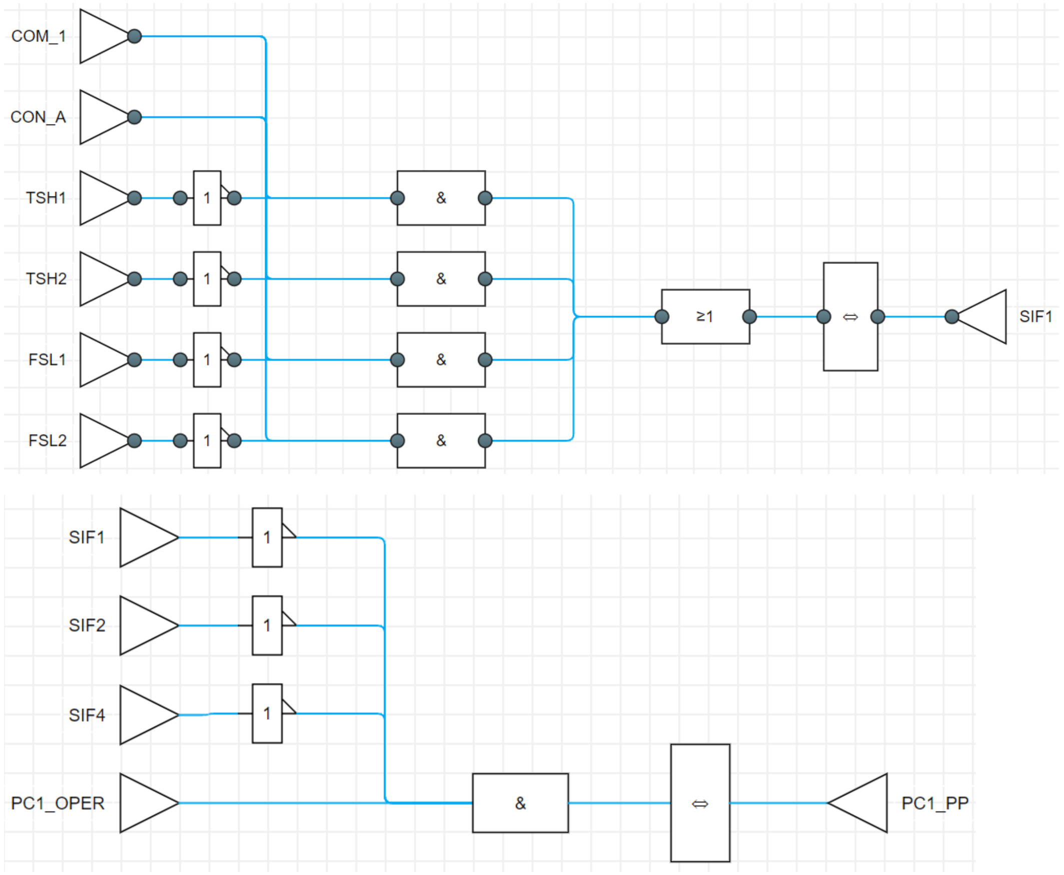


CEM (Cause and Effect Matrix) - **SISpec**
More details: MOPHA041

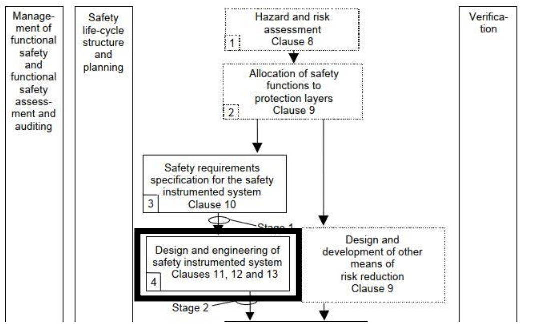
Cause \ Effect	SIF1
COM_1	A1,A2,A3,A4
CON_A	A1,A2,A3,A4
TSH1	NA1
TSH2	NA2
FSL1	NA3
FSL2	NA4

Cause \ Effect	PC1_PP
SIF1	NA1
SIF2	NA1
SIF3	
SIF4	NA1
PC1_OPER	A1

LD (Logic Diagrams) - **Grassedit**



Simulation, **test** and **verification** case generation and **code generation** are possible



Application Program

AP specification | *AP development* | *AP verification*

SISpec

(a) Top Operational CEM

Cause \ Effect	PC1_OPER	PC2_OPER
SEL_PC1	A1,A2,A3,A4,A5	
SEL_PC2		A1
TEST_A	A1	
TEST_B	A2	A1
TEST_C	A3	
TEST_D	A4	
TEST_E	A5	

(b) Top Safety CEM

Cause \ Effect	PC1_PP	PC2_PP
SIF1	NA1	
SIF2	NA1	
SIF3		NA1
SIF4	NA1	NA1
PC1_OPER	A1	
PC2_OPER		A1

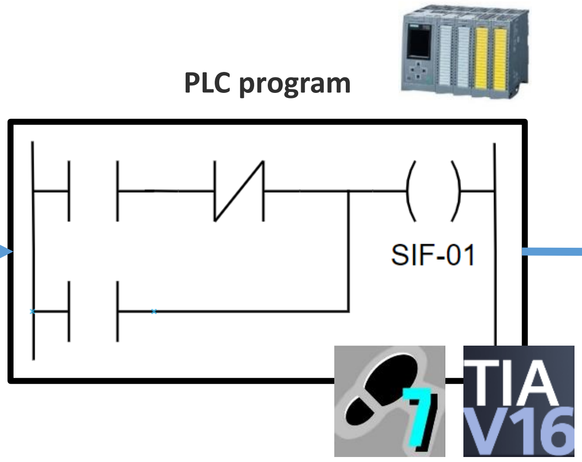
(c) Bottom Operational CEM

Cause \ Effect	TEST_A	TEST_B
SEL_TEST_A	A1	
SEL_TEST_B		A1
CRYO_A	A1	
CRYO_B		A1
DAQ_A	A1	
DAQ_B		A1

(d) Bottom Safety CEM

Cause \ Effect	SIF1	SIF2
COM_1	A1,A2,A3,A4	
CON_A	A1,A2,A3,A4	
TSH1	NA1	
TSH2	NA2	
FSL1	NA3	
FSL2	NA4	
...		...

PLC program

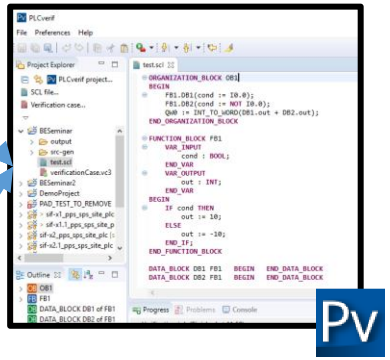


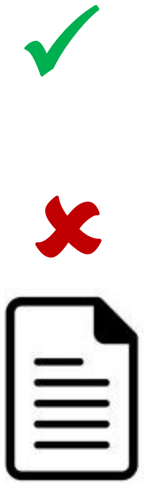
Exported source code

Verification cases

```
//#ASSERT(
    (
        NOT Inputs.In1 OR
        NOT Inputs.In2
    )
    --> (Out1 = FALSE)
): SIF01;
```

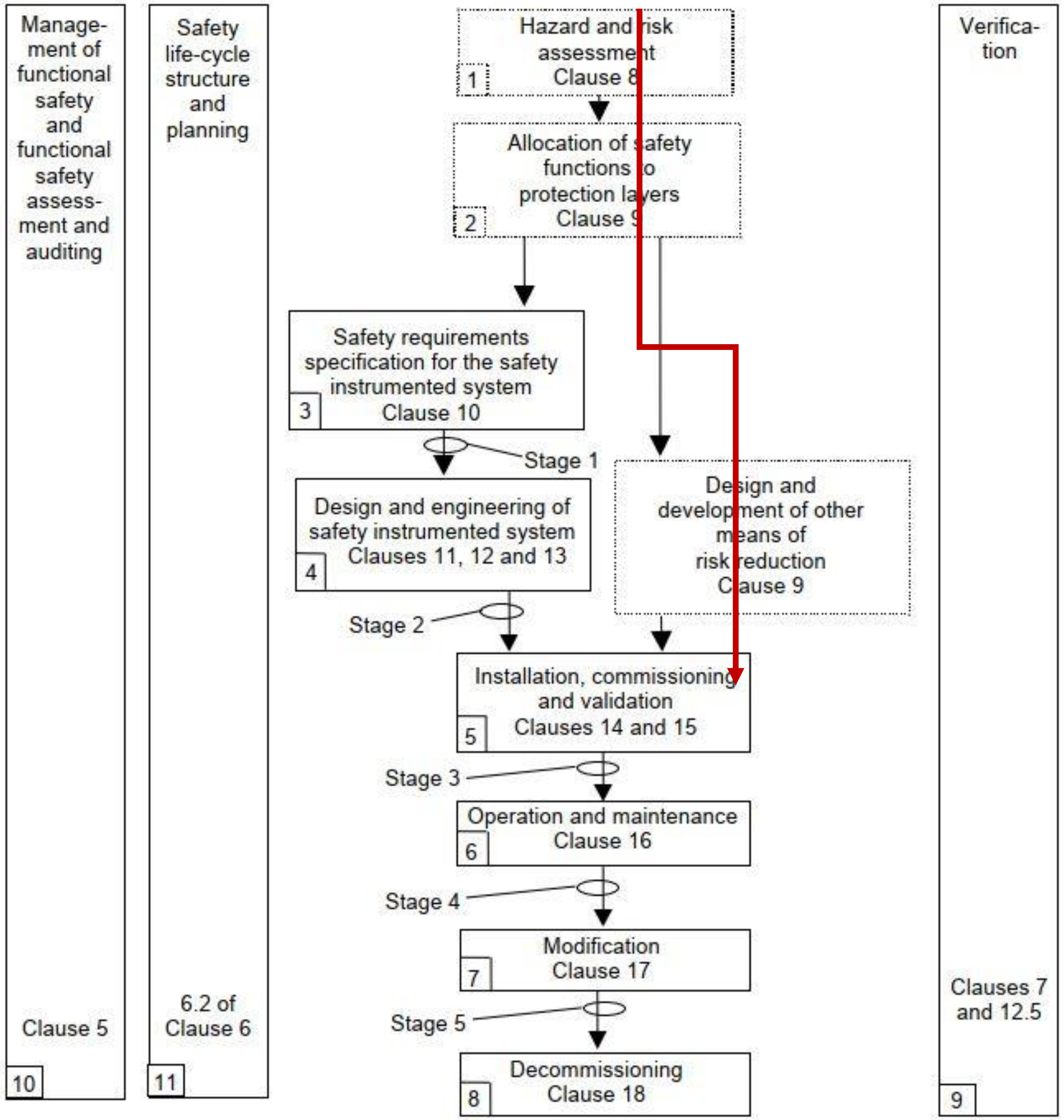
PLCverif



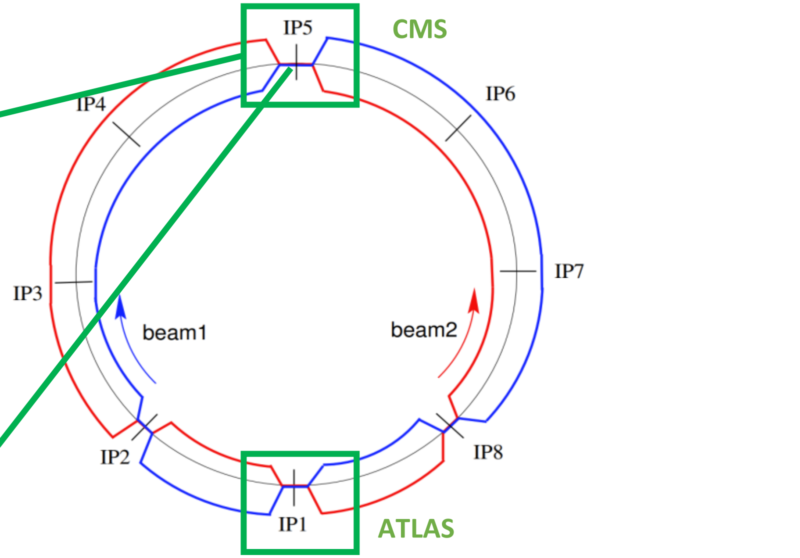


PLCverif more details:
https://cern.ch/plcverif
MOPV042, WEPV042, etc.

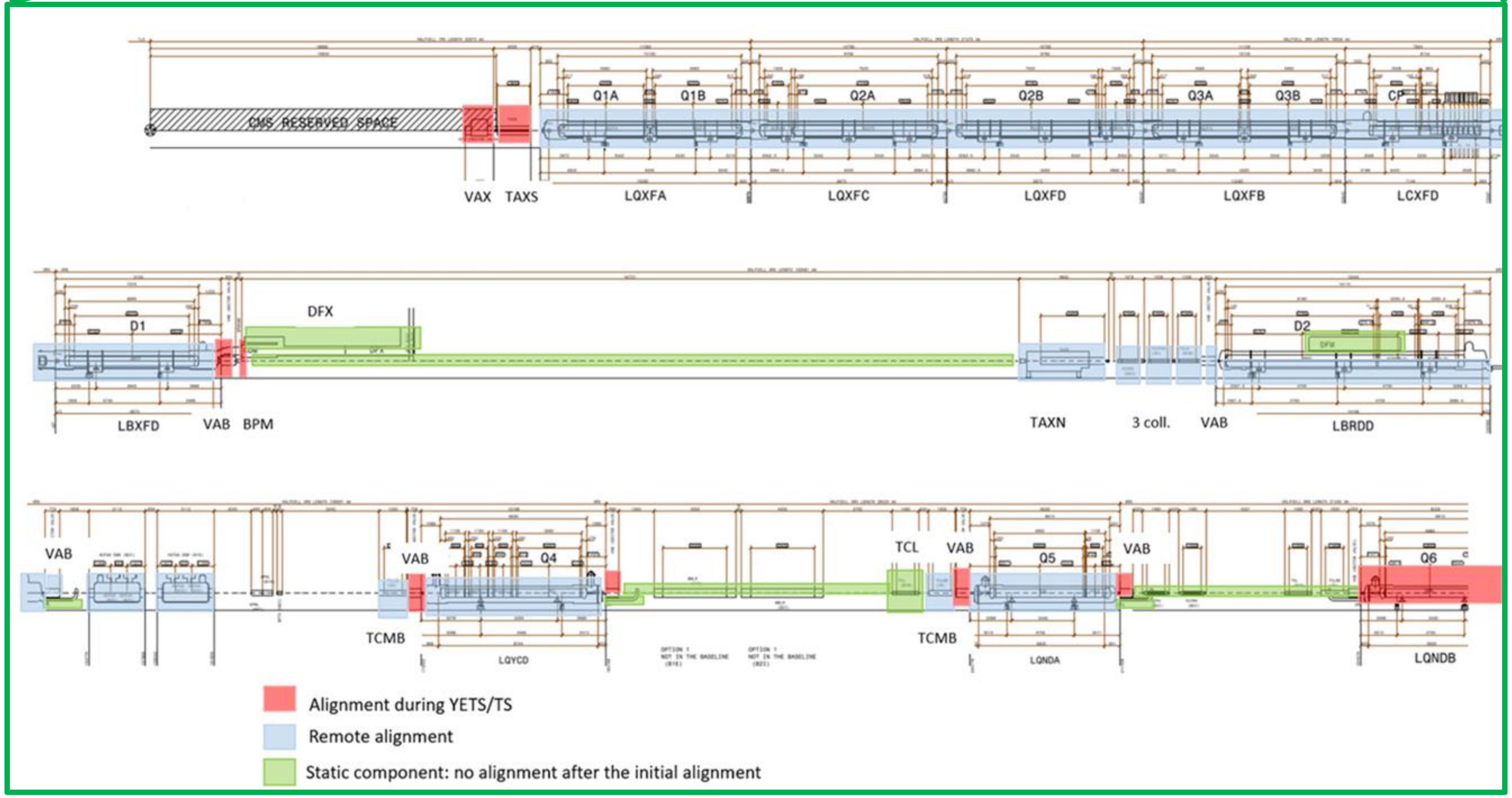
FRAS Protection Layers design



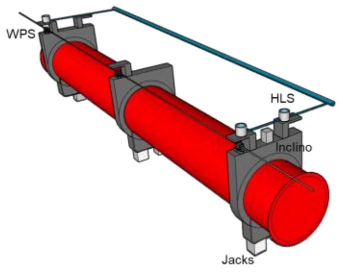
Context – FRAS



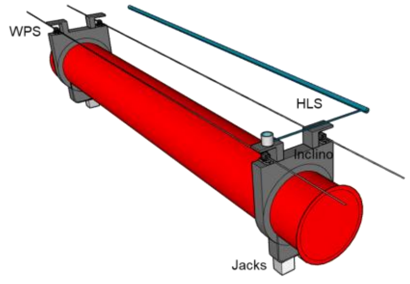
- **F**ull **R**emote **A**lignment **S**ystem for the **HL-LHC** [EDMS 2166298]
- Installed in **both** Long Straight Sections (**LSS**) **of IP1** (ATLAS) **and IP5** (CMS)



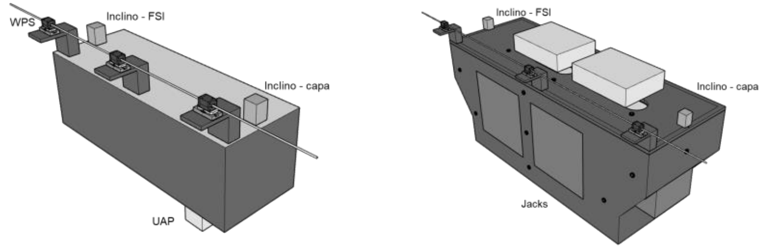
Q45-D2: Q4, Q5, D2



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



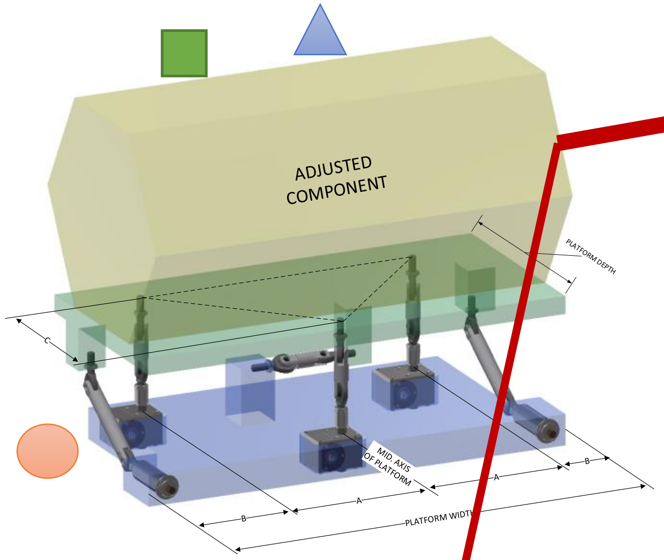
CMCT: Collimators, Q4/5 masks, Crab-cavities, TAXN

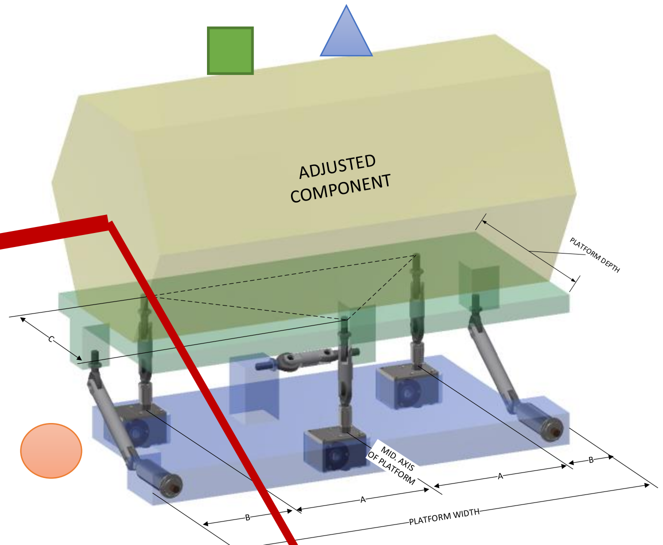


Context – FRAS

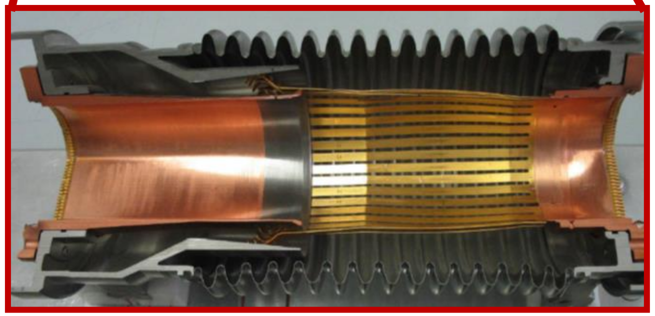
4 IP sides and each of them contains:

- **17 components** for remote alignment
- **Capacitive sensors**:
  - 54 WPS (Wire Positioning System)
  - 10 Inclinometers
- **FSI** (Frequency Scanning Interferometer) **sensors**:
  - 27 HLS (Hydrostatic Levelling Sensors)
  - 16 FSI inclinometers
- **Resolvers** (5 motors per component):
  - 85 resolvers
- **21 bellows**





- Universal Adjustment Platform (UAP)
- 5 Motorized jacks
- v ≤ 20 µm/s



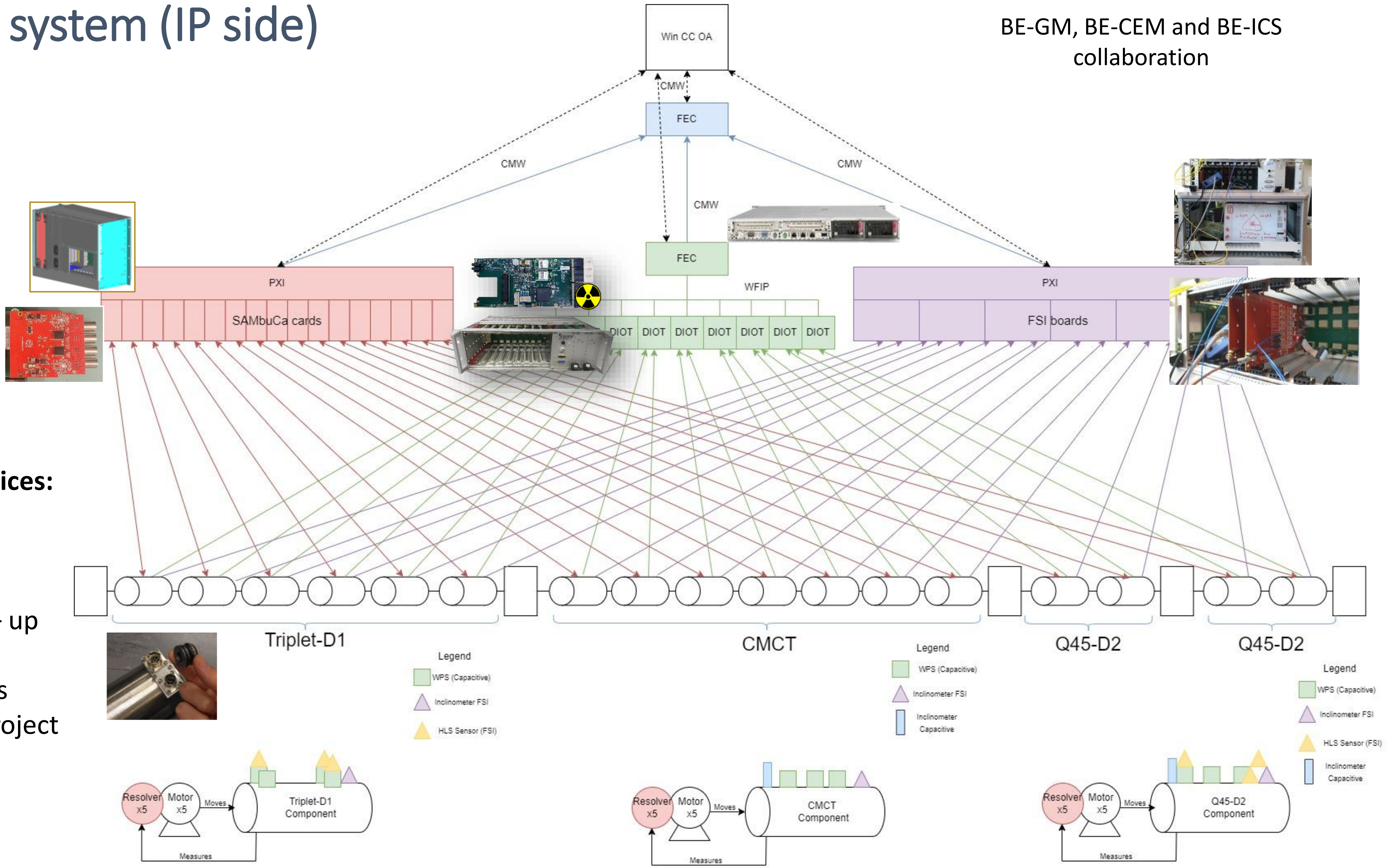
Bellow **deformation limits**
+/- 2.5 mm
1 mrad

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

FRAS control system (IP side)

BE-GM, BE-CEM and BE-ICS collaboration

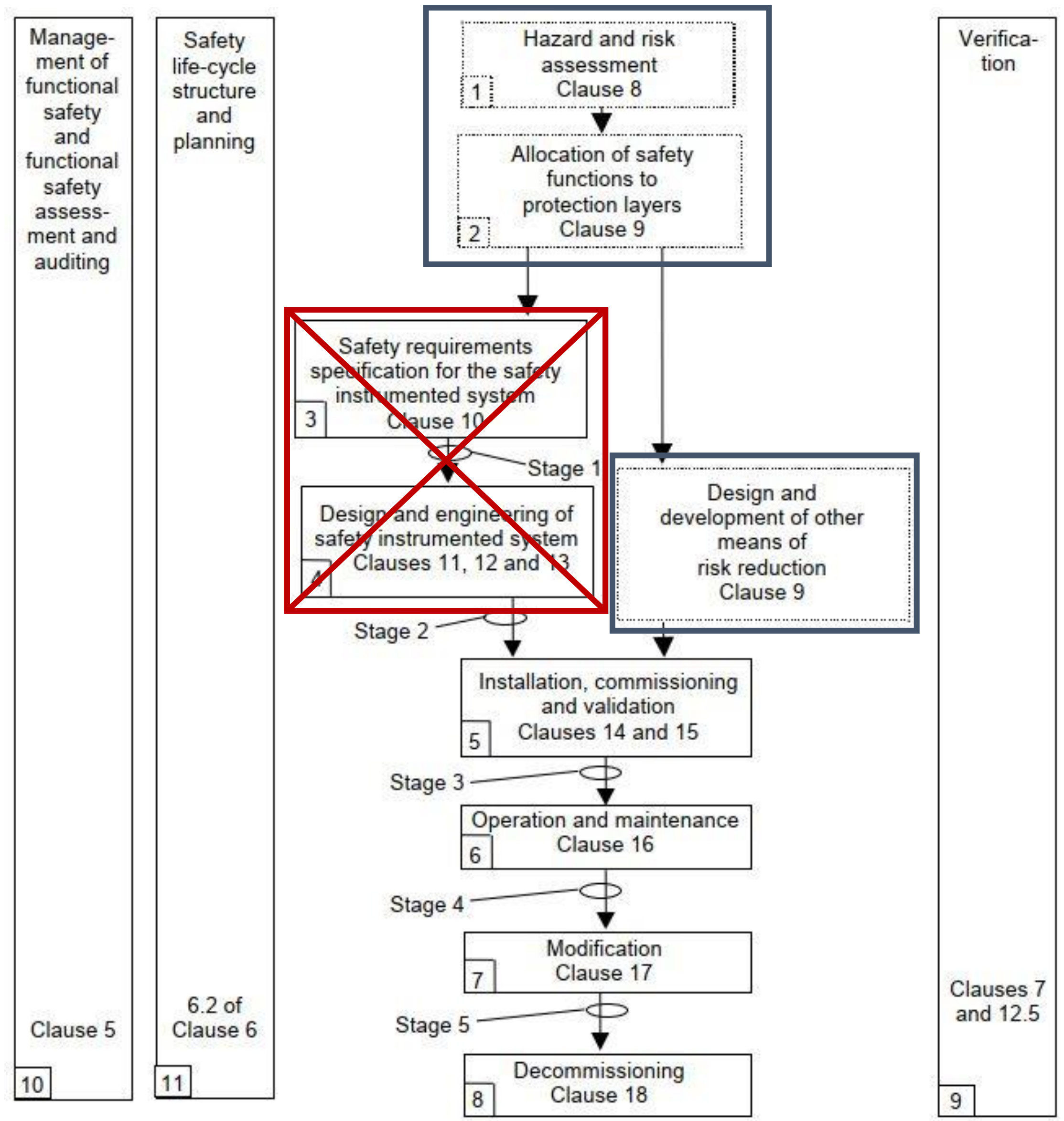
- **17 components**
- **21 bellows**
- **Sensors:**
  - 54 WPS
  - 10 Cap. inclin.
  - 27 HLS FSI
  - 16 FSI inclin.
- 17x5 = **85 motors**
- **85 resolvers**
- **Controllers and IO devices:**
  - 2 FECs
  - 9 DIOTs
  - 2 PXI
  - 1 Inter FSI crate – up to 8 FSI boards
  - 17 Sambuca cards
- **1 WinCCOA server** / project



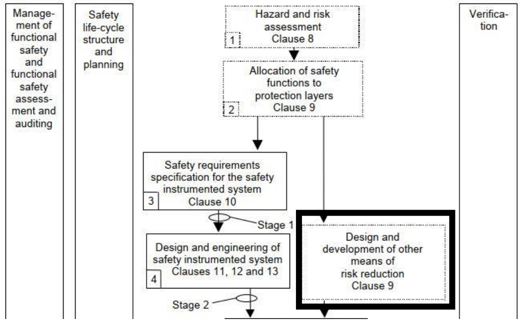
IEC 61511 Safety Life Cycle

Safety Instrumented System requirements

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



Protection Layers requirements



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	1
100	2
1000	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.

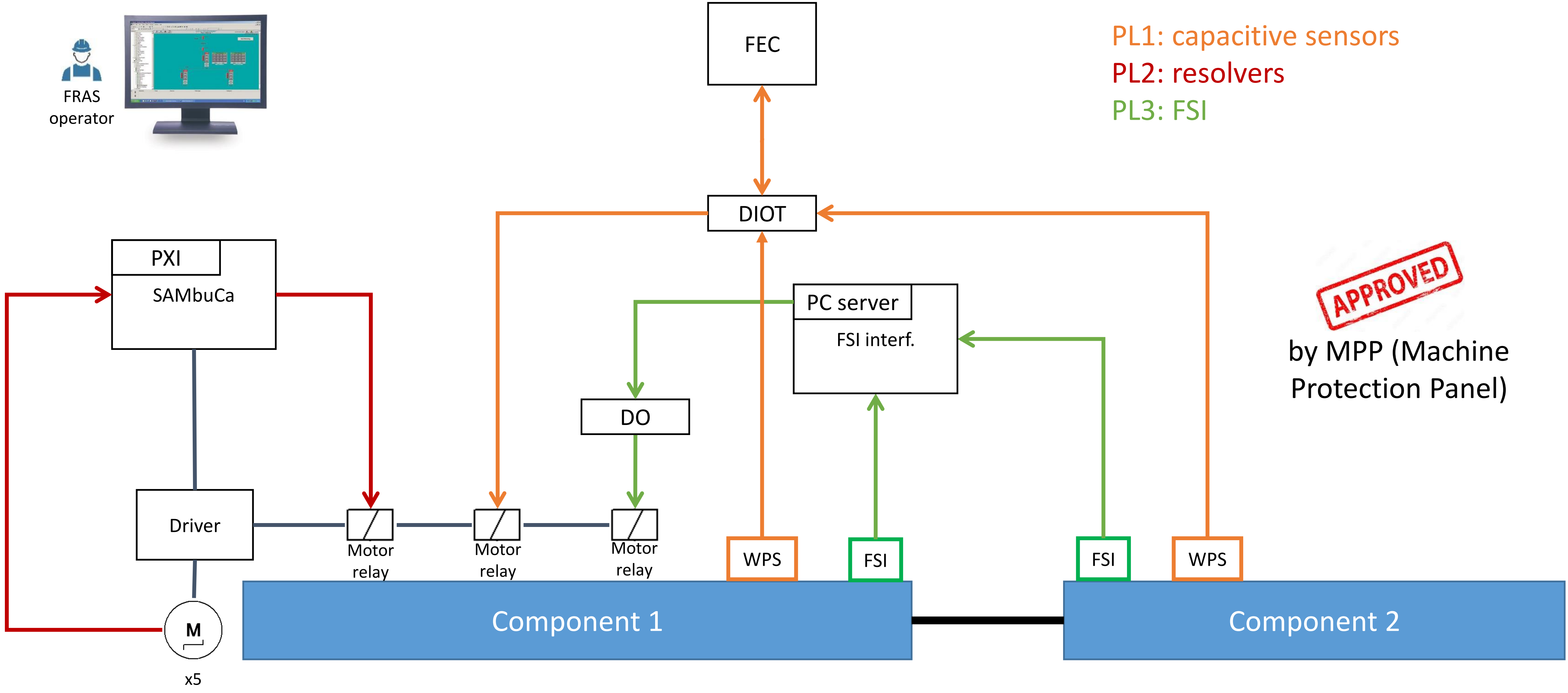
are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative unless 9.2.7 applies.

NOTE A definition of dependent failure is provided in 3.2.12.

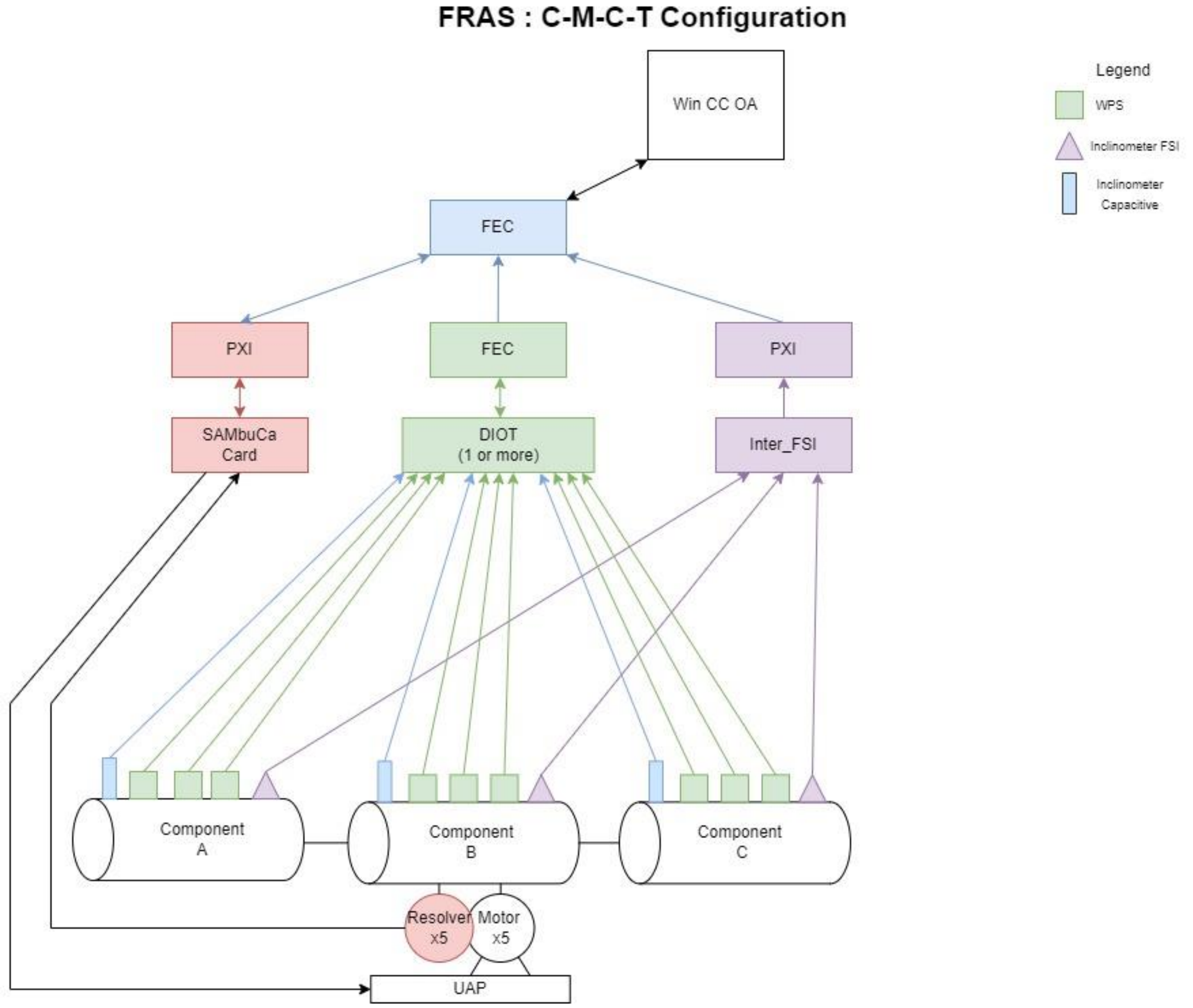
9.4.2 The assessment shall consider the following:

- 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.

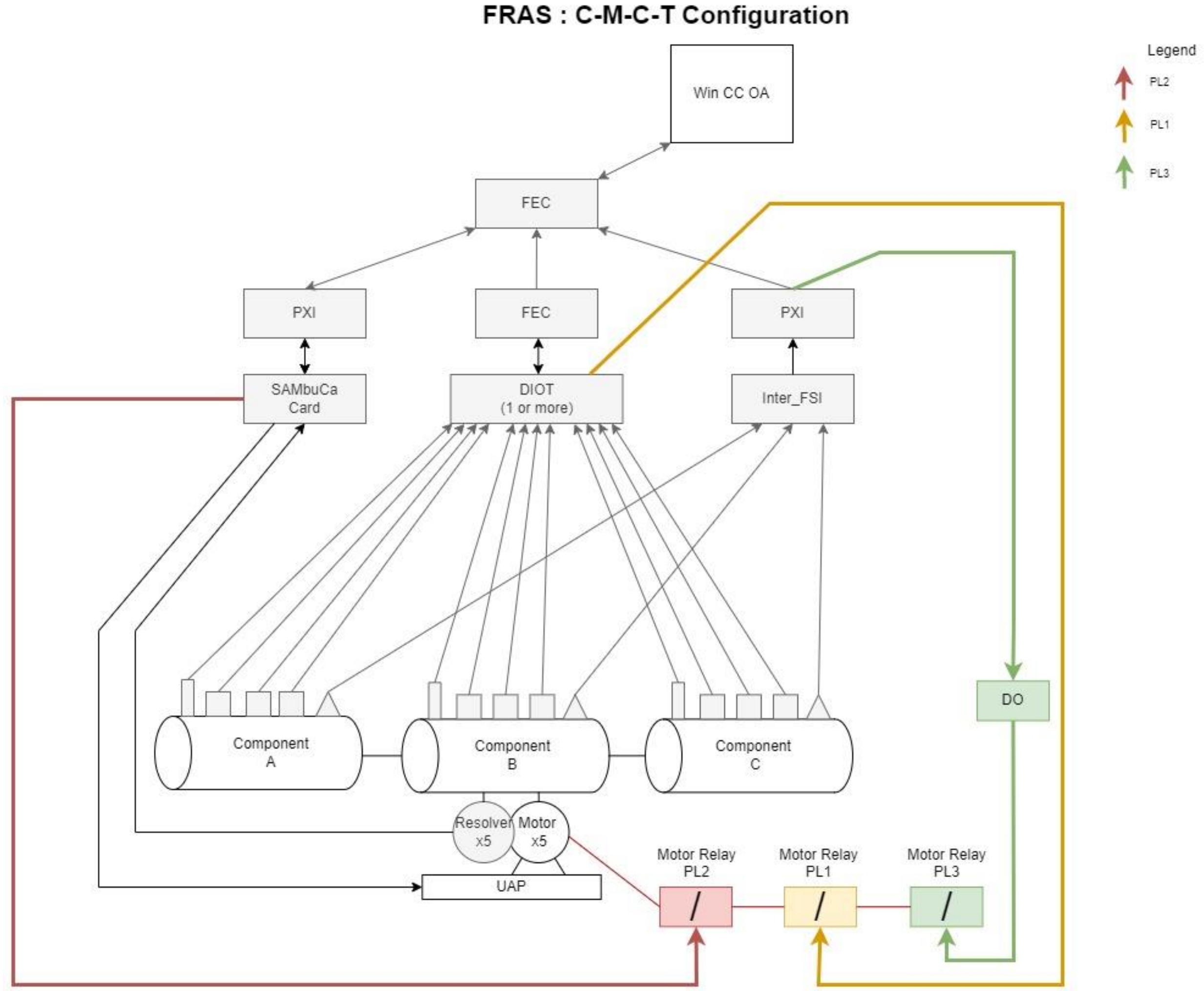
Protection layers proposal for bellow and personnel protection (functional schema)



FRAS control system vs FRAS Protection Layers



New hardware



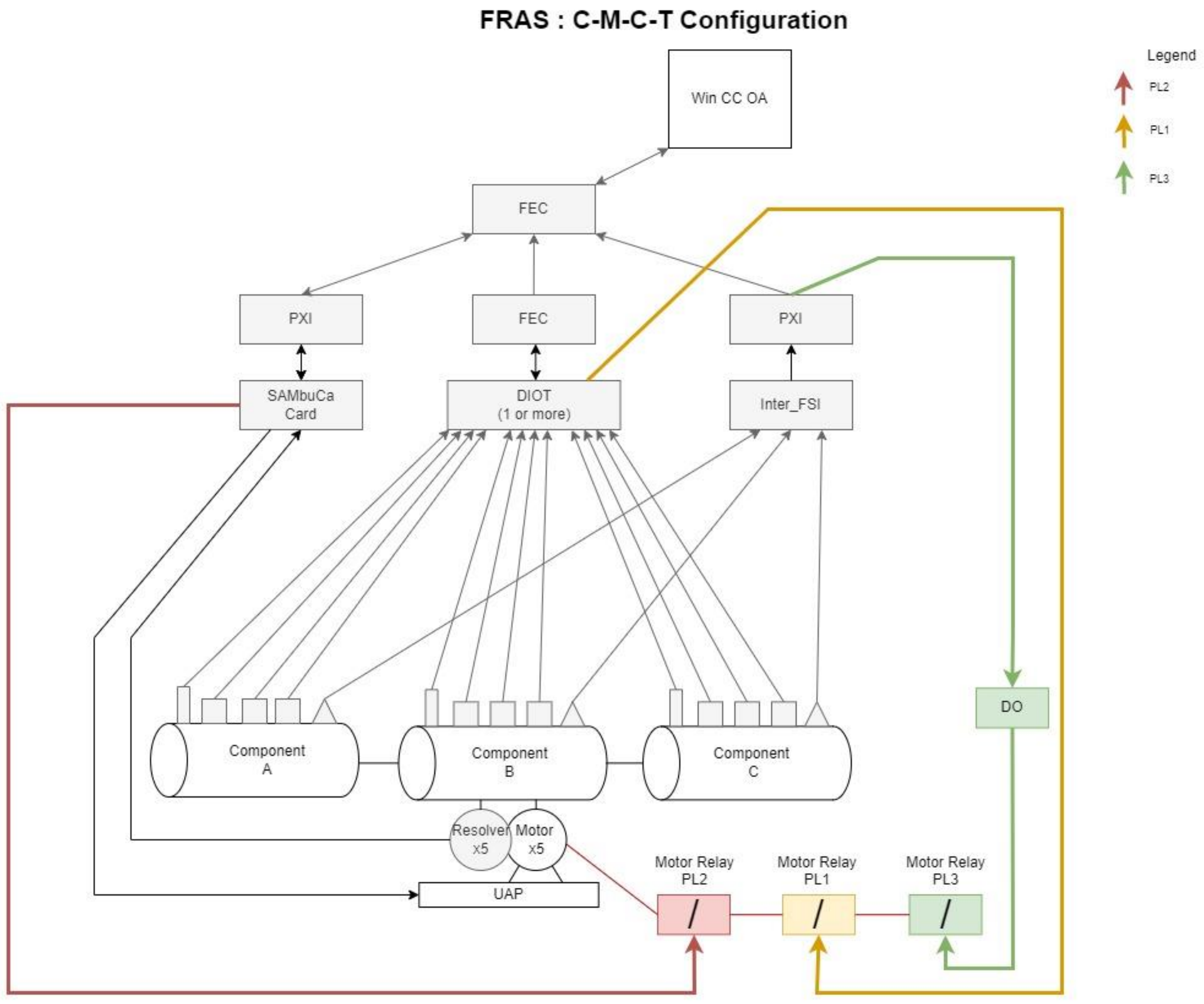
FRAS control system vs FRAS PLs

- PLs and the FRAS control system **share most of the components**

- We need to analyze the different FRAS control system failures and **asses which protection layer protects from specific failures**

- **Functional safety analysis:**
  1. **FMEA** to analyze **component** failures
  2. **FTA** to analyze **system** failures
  3. **LOPA** to analyze the efficiency of our PLs and assess if we meet the risk reduction target

New hardware



Reliability data

Source of information:

1. Failure records
2. Reliability studies
3. Standard recommendations
4. Operator errors (HEART method)

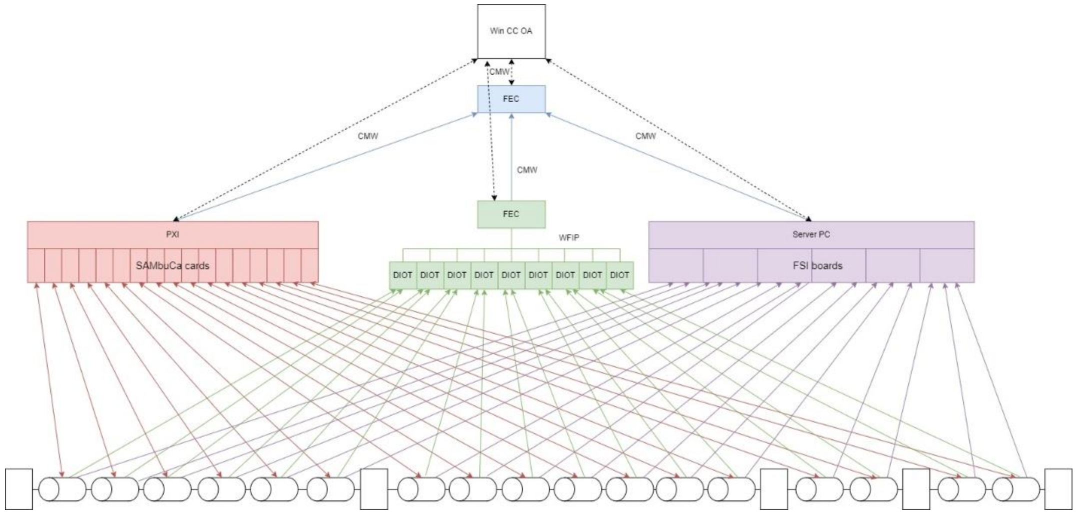
For safety analysis, we only care about **dangerous undetected failures**

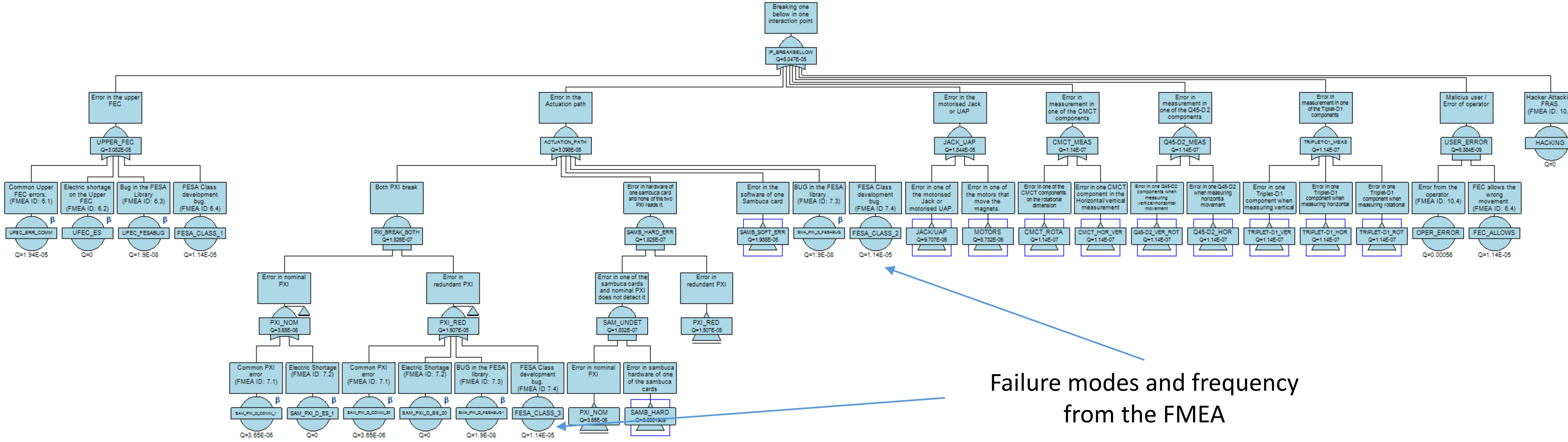
FMEA – Individual component failures

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
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

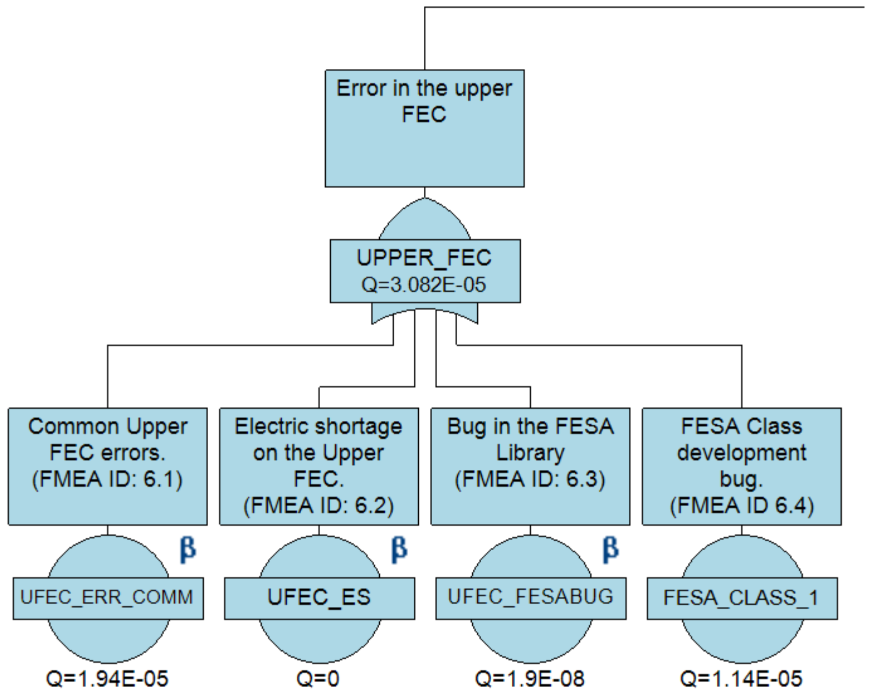
Isograph reliability workbench





Failure modes and frequency from the FMEA

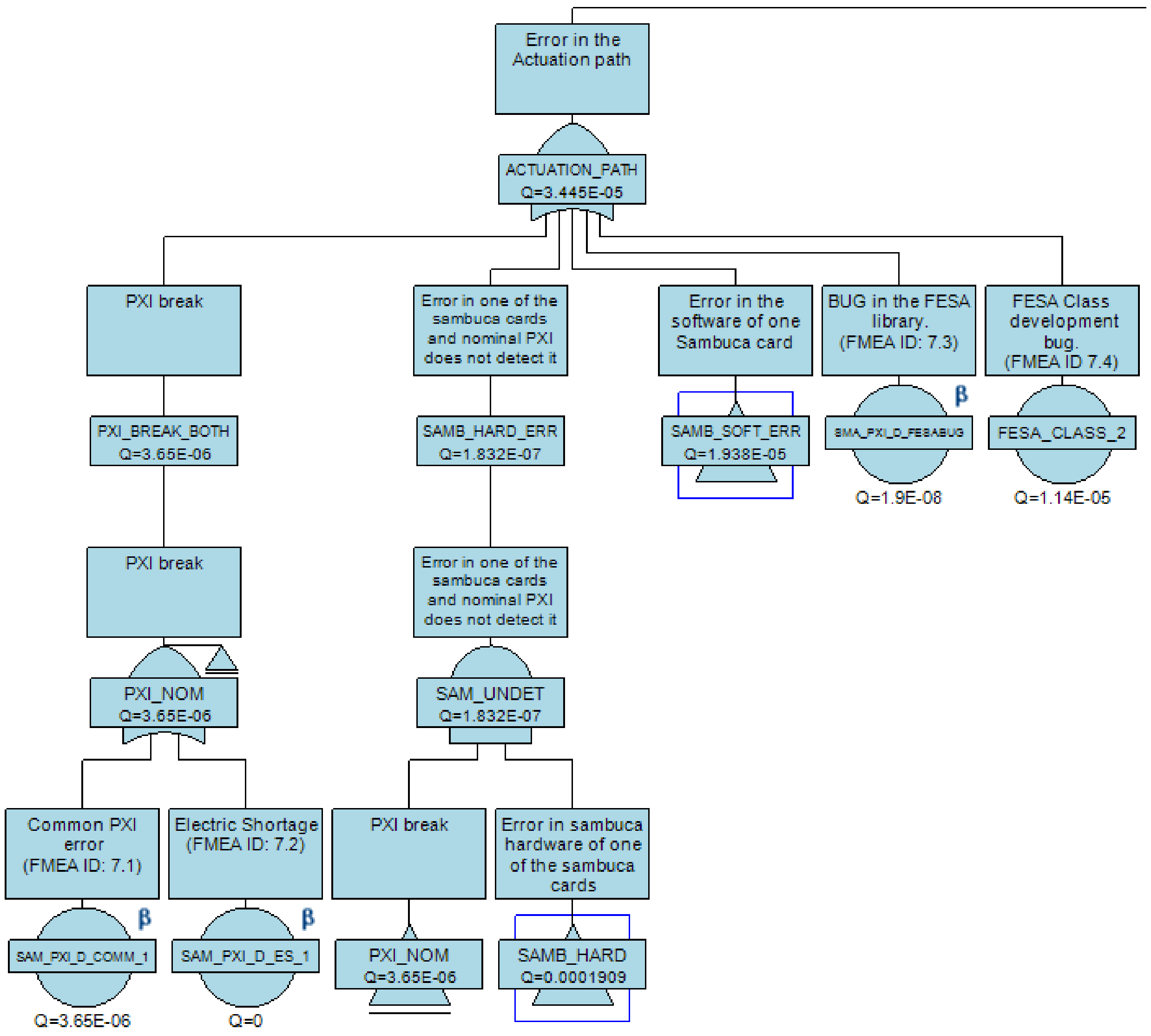
FTA – top FEC

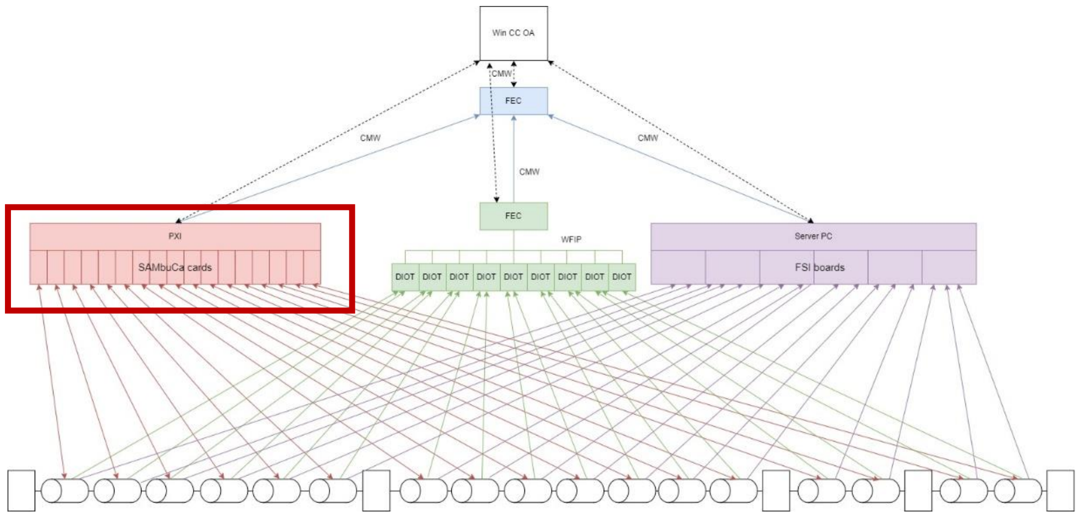


Notes:

- **All** failures records are considered **dangerous undetected failures**
- However, many of them could be detected (e.g. most hardware errors)

FTA – actuation path

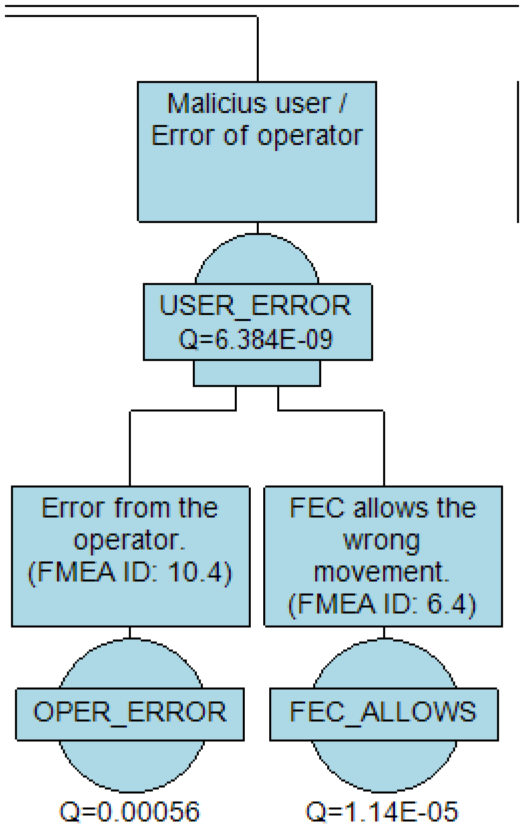


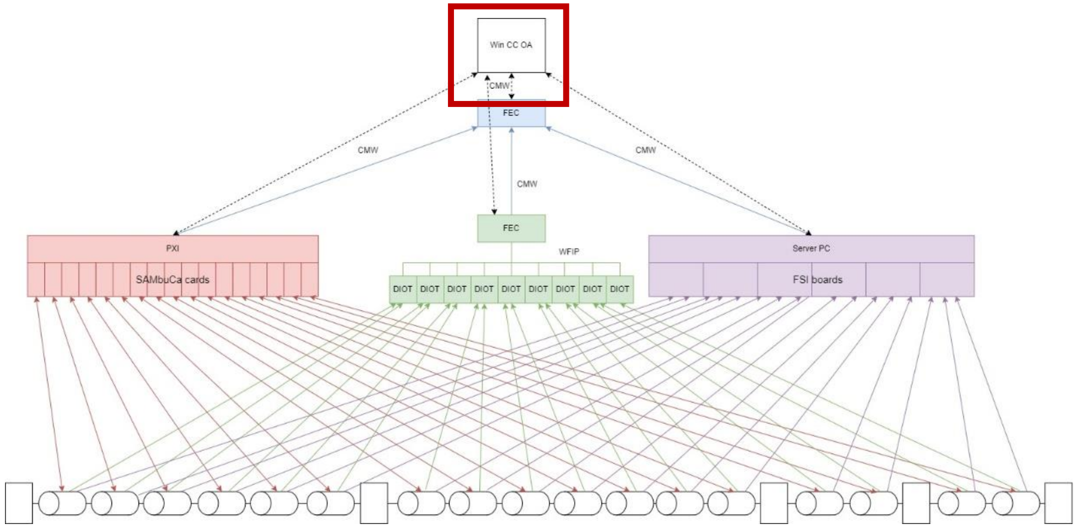


Notes:

- A hardware failure in the SAMBUCA cards would be detected by the PXI
- A **software/logic error won't be detected**

FTA – Operator mistake





Notes:

- If the operator makes a mistake, the **top FEC should avoid the wrong command to be transmitted**
- The **HEART** method was used to evaluate, the probability of the human failure

Operator mistakes
HEART (Human Error Analysis Reduction Technique) method

From "*Critical evaluation of quantitative human error estimation methods in light of different incident causation models and Hollnagel's research on performance variability*"
by Esme Fowler (University of Aberdeen)
https://downloads.opito.com/downloads/Critical-evaluation-of-quantitative-human-error-estimation-methods-in-light-of-different-incident-causation-models-2018.pdf?mtime=20181029151433

4.2.1 - Reasons for use

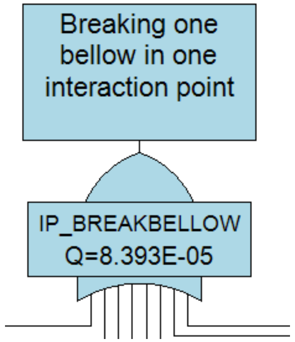
From the comparison of HRA tools is seems that HEART is the most appropriate op
as it meets the following requirements:

- It is a widely validated tool across different industries.
    - It was revalidated by the UK Health and Safety Laboratory in 2016
- It provides its own nominal HEPs linked to 9 different task types. The nominal probabilities were initially developed in the 1980's, however, in 2017 they were updated based on literature published in the 30yrs since its development [66]. The updated values for the nominal probabilities will be used here.
- It provides a list of 38 PSFs with multipliers for each one
- The calculation used to combine the PSFs and nominal HEPs is very simple to understand.

4.2.2 - Performance Shaping Factors

HEART provides an extensive list of PSFs with their relative multipliers to be used in the calculation. The sources for the data for the multipliers are predominantly from ergonomics and psychology journals in addition to technical reports and conference

Conclusions FTA



TE-MPE risk matrices for the LHC (EDMS2647876)

	[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

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

$$RRF = \frac{7.35}{10} / \frac{1}{100} = 73.5 \approx 100$$

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

- The biggest contributors to this risk are:
  - **the top FEC**: λ = 0.27 y^{-1} (**FESA class** is the biggest contributor)
  - **Actuation path**: λ = 0.30 y^{-1} (**SAMBUCA** cards and **FESA software** error are the biggest contributors here)
  - **Motors and UAPs**: λ = 0.16 y^{-1} (~ 50% each)

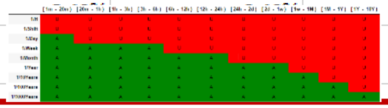
- The PLs share most of the hardware (and **software**) with the FRAS control system, **LOPA is a good choice to assess scenarios risk and the adequacy of the PLs**

Layers of Protection Analysis (LOPA)

Initiating events and frequency from the FTA

Assuming independent (and diverse) PLs

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		ror 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	10										10
	PL3	10	10	10								10
Operation Time	36.5	10	10	10	10	10	10	10	10	10	10	10
Procedures / Alarms												
Cybersecurity: TN + RBAC												0
Physical Limit Switches		0	0	0	0	0	0	0	0	0		0
Cumulative		10000	1000	1000	10	10	10	10	10	10	10	10000
	Intermediate event frequency	0.000027	0.000302	0.00016153	0.0000999	0.0000999	0.00009986	0.00009986	0.00009986	0.00009986	0.00009986	0.00000001
	Weight over the overall frequency	2.27%	25.37%	13.58%	8.40%	8.40%	8.40%	8.40%	8.40%			0.00%
	Total mitigated event frequency						0.00119					
	Tolerable Event Frequency - LHC						0.01000					
	Tolerable Event Frequency - IP side						0.00250					
	Tolerable Event Frequency - Bellow						0.000119048					
	Residual Risk						0.00131063					



Target from MPE matrices

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
					Error 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	36.5	10	10	10	10	10	10	10	10	10	10	10
Procedures / Alarms												
Cybersecurity: TN + RBAC												0
Physical Limit Switches		0	0	0	0	0	0	0	0	0		0
Cumulative		100	100	100	10	10	10	10	10	10	10	100
	Intermediate event frequency	0.002700	0.003018	0.00161534	0.0000999	0.0000999	0.00009986	0.00009986	0.00009986	0.00009986	0.00009986	0.00000056
	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						0.00803					
	Tolerable Event Frequency - LHC						0.01000					
	Tolerable Event Frequency - IP side						0.00250					
	Tolerable Event Frequency - Bellow						0.000119048					
	Residual Risk						-0.00553260					

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
					Error 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					

Conclusions

About FRAS control system:

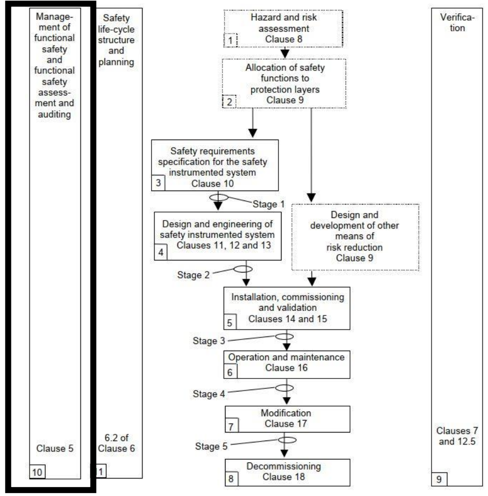
1. The biggest contributors to this risk are:
   - **the top FEC**: $\lambda = 0.27\ y^{-1}$ (**FESA class** is the biggest contributor)
   - **Actuation path**: $\lambda = 0.30\ y^{-1}$ (**SAMBUCA** cards and **FESA software** error are the biggest contributors here)
   - **Motors and UAPs**: $\lambda = 0.16\ y^{-1}$ (~ 50% each)
2. Software errors can be minimized by “exhaustive” functional testing

About the PLs:

1. **We don’t meet all the requirements from IEC 61511 to claim a risk reduction of 10 per PL**, therefore we only claim a maximum of 10 risk reduction for all PLs protecting from a specific event
2. According to this data, if the risk is present (motors are powered) **more than 11 full days** per year, we don’t meet the tolerable risk target
3. According to this data, if FRAS components are operated less than 11 days, **we do NOT need to provide diversity and replace the PL1 FEC by a PLC** (if a PLC is installed in PL1, full independence between 2 PLs can be achieved)
4. Human errors are analyzed by the **HEART** method, but it is not a critical source of danger
5. Cybersecurity issues will be addressed with different methods (determinist methods)

Functional safety projects management

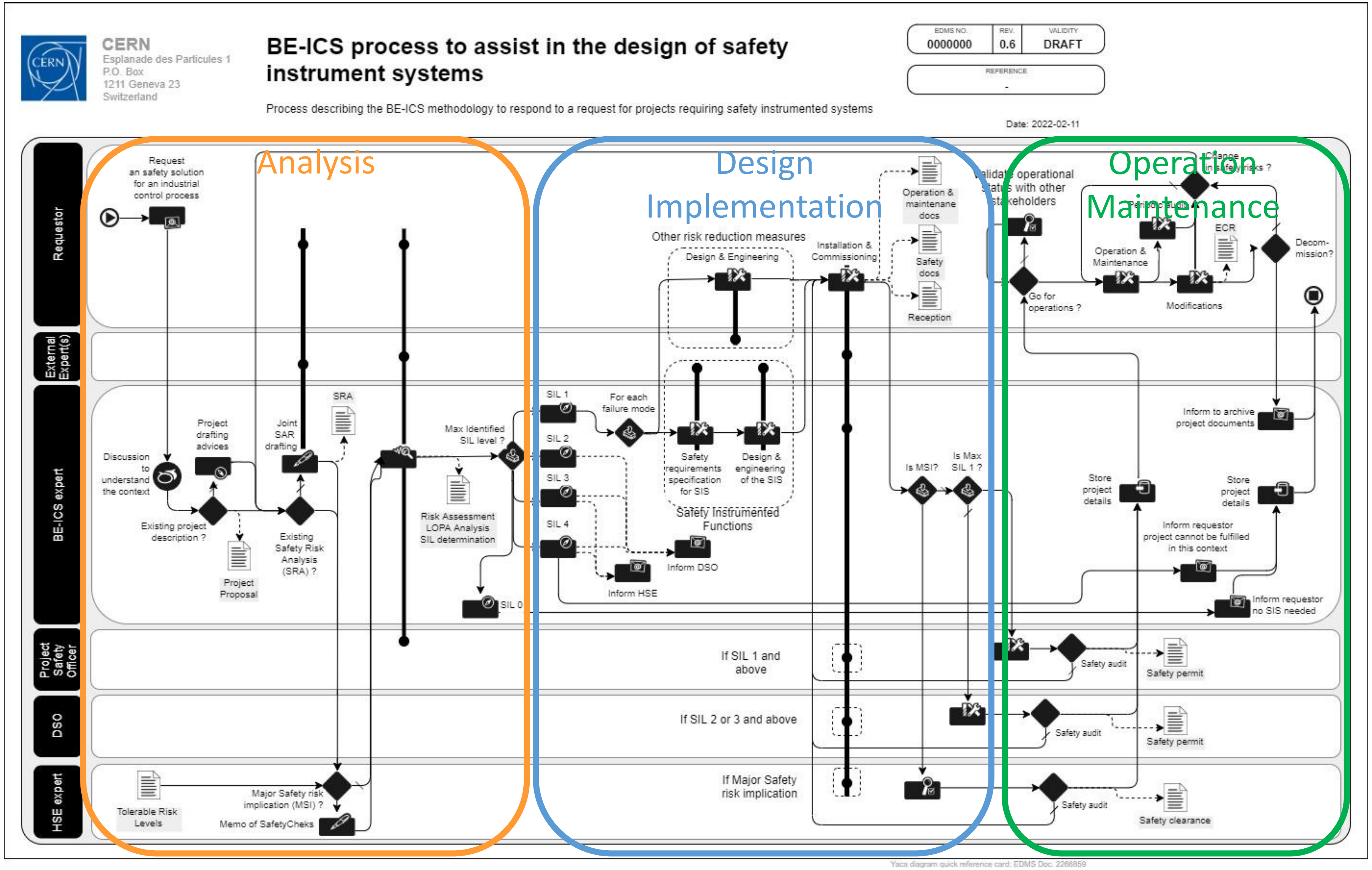
Management of Functional Safety projects

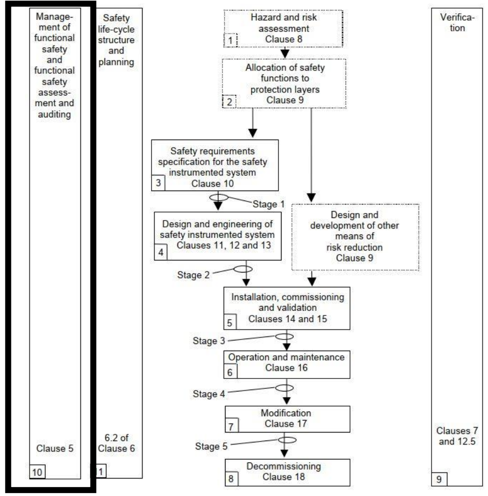


- **Challenges:**
  - Define the **roles** and **responsibilities** of the project members
  - Define the **workflow** and **documentation to coordinate all project members**

Role	**Responsibilities**
Functional Safety (FS) expert	Apply the FS standards
Process expert	Process knowledge and risk analysis
Instrumentation and controls expert	Design and implementation of the safety system
Departmental Safety Officer (DSO)	Risk graph calibration and safety support
Health & Safety and Environmental Protection (HSE) unit representative	Safety support and safety audits

Management of Functional Safety projects (workflow)





Functional Safety tools

Table 1: Safety Life-cycle Tools and Software Suites.

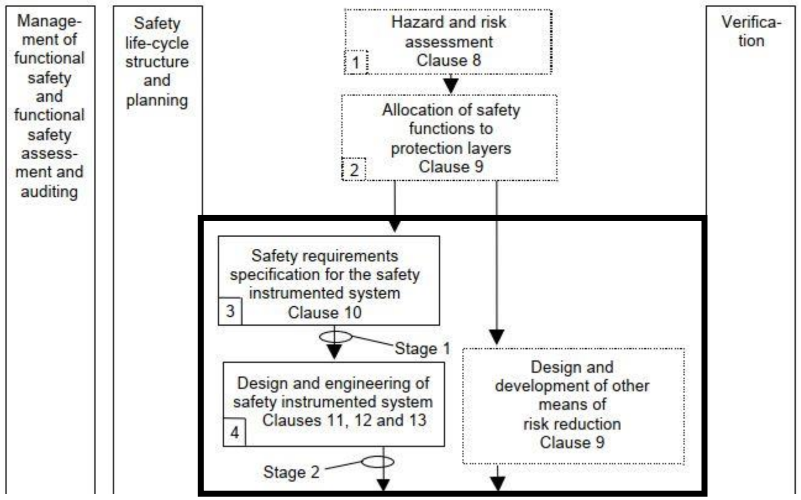
Tool	Safety life-cycle coverage	Reference
exSILentia® (Exida)	All phases	https://www.exida.com/
Safeguard Profiler	Phases 1, 2, 3, 4 and 6 (Bowtie, LOPA analysis, SRS, SIS design, SIL verification, Proof test analysis)	https://www.acm.ca/safeguard-profiler/
SISsuite	All phases	https://www.sissuite.com/
SLM V2	All phases	https://mangansoftware.com/slm-v2/
Vertigo™	Phases 3 and 4 (Equipment failure rate database, SRS and SIL verification)	https://www.kenexis.com/software/sis-lifecycle-management-and-sil-verification/
SIL Solver®	Phase 4 (SIL verification)	https://sis-tech.com/applications/sil-solver/
Isograph's Reliability Workbench	Phase 4 (SIL verification)	https://www.isograph.com/software/reliability-workbench/
Siemens Safety Matrix Engineering Tool	All phases	https://assets.new.siemens.com/siemens/assets/api/uuid:f18dcad1-9faf-4f33-8c20-c8390d176993/safetymatrixflyerfinal-300.pdf
SILcet	Phase 4 (SIL verification)	https://safetyandsis.com/sil-verification/

More details in https://inspirehep.net/files/fcdeb3597bbefa61732b5fdbb53c53e6

Many more tools for phase 4 (SIL verification)

Conclusions / tips

- FS is about **proving** that **your design, development and operation meet** the risk reduction target (**SIL**)
- The SIL (risk reduction target) can be achieved (mainly) by:
  - a **SIS** (IEC 61511-1 clauses 10, 11, 12 and 13)
  - or **independent protection layers** (IEC 61511-1 clause 9)
- If SIS, then:
  - Reliability calculations (random hardware failures)
  - Architectural analysis
  - Systematic failures analysis (e.g Operators, EMC, etc.)
  - Software design and verification
  - …



- If PLs, then: specificity, independence, dependability, auditability and diversity (when possible)
- **Multidisciplinary teams** (Safety engineers, process engineers, automation engineers, functional safety engineers, …)
- **Proof tests** (periodic test to maintain the SIL over the life of the industrial plant)

Future work at BE-ICS

Regarding management aspects:

- **Traceability** (explore commercial tools)
- **Workflow** procedures for functional safety projects (coordination and responsibilities of the different groups)
- Functional safety **service** definition

Regarding technical aspects:

- **Code generation** of application programs (Siemens safety LADDER code for TIA portal)
- **Integration** in our frameworks (e.g. UNICOS)
- Frequency estimation of software errors (?)

CERN