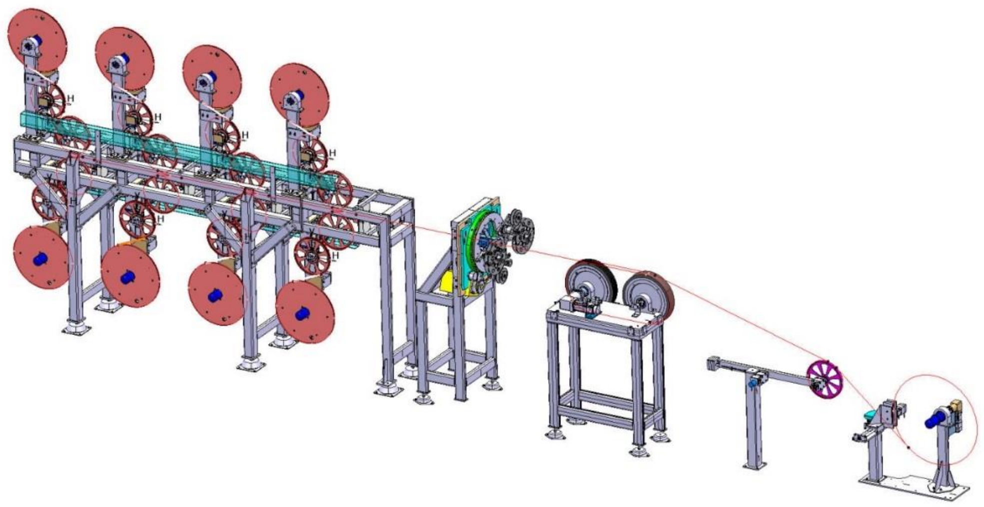
Functional Safety Activities (2)

ALBA – CERN workshop

Borja Fernández Adiego BE/ICS

Some examples of Safety Systems

- HTS (high temperature superconducting) winding machine (IEC 62061 standard)
    - Siemens Safety PLC + SINAMICS + Profisafe
    - Safety Evaluation Tool for machine safety (https://www.industry.siemens.com/topics/global/de/safety-integrated/maschinensicherheit/safety-evaluation-tool/seiten/default.aspx)



- Several magnet test benches
    - "SM18" test benches
    - **"B311 Switchboard" test bench**
    - **"FAIR" test bench**

- **AWAKE experiment (industrial process)**

In all of them ICS developed the control system (**using UNICOS**) and safety system

Switchboard installation

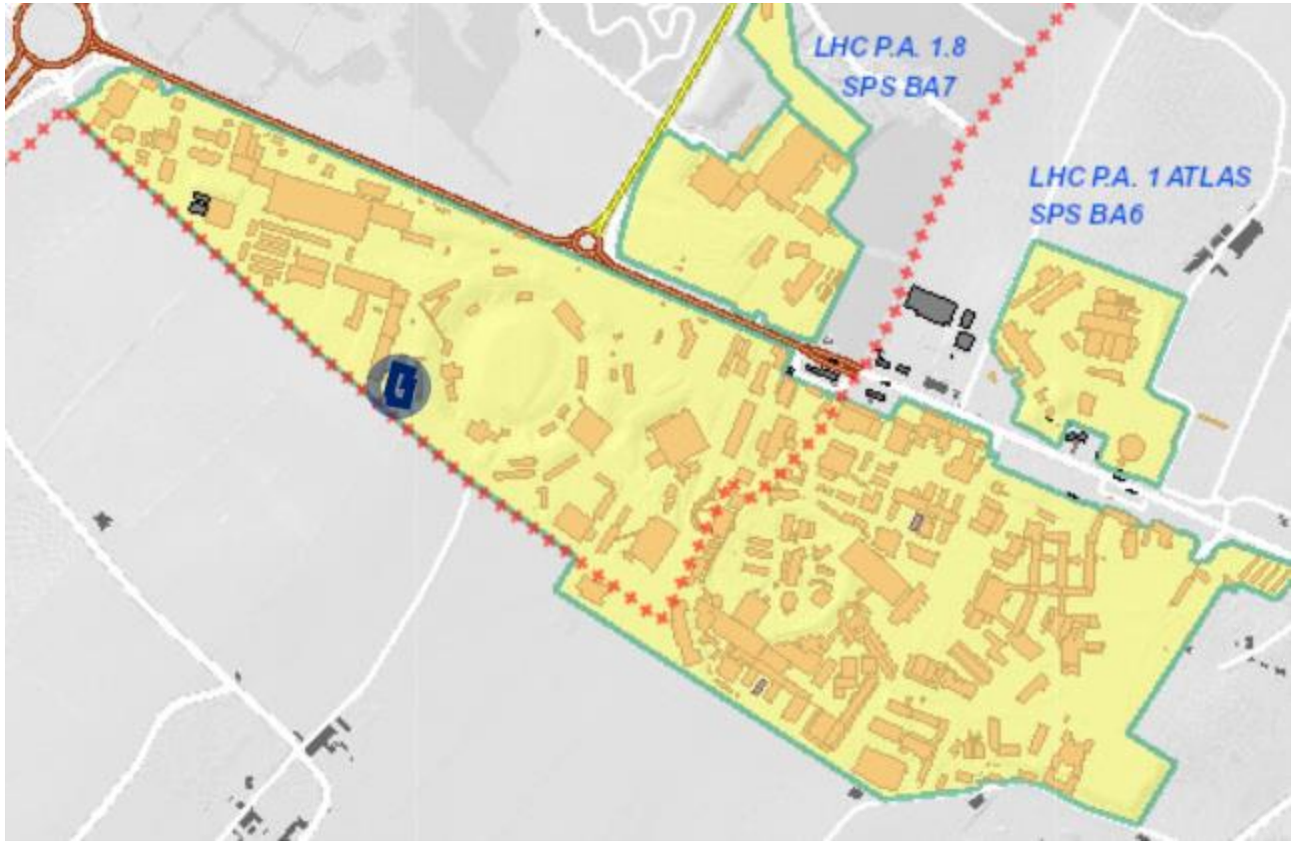
- New magnet test bench facility in building 311

- Different test benches to **measure the field** of normal conducting **electro-magnets**

- Magnets will be powered with DC or quasi-DC current up to **1000 A**

- The **current** provided by each converters must be **multiplexed** to the test benches by **a dedicated electro-mechanical switches assembly** (hereafter named “**switchboard**”)

- **Project managed by TE/MSC**



Switchboard installation

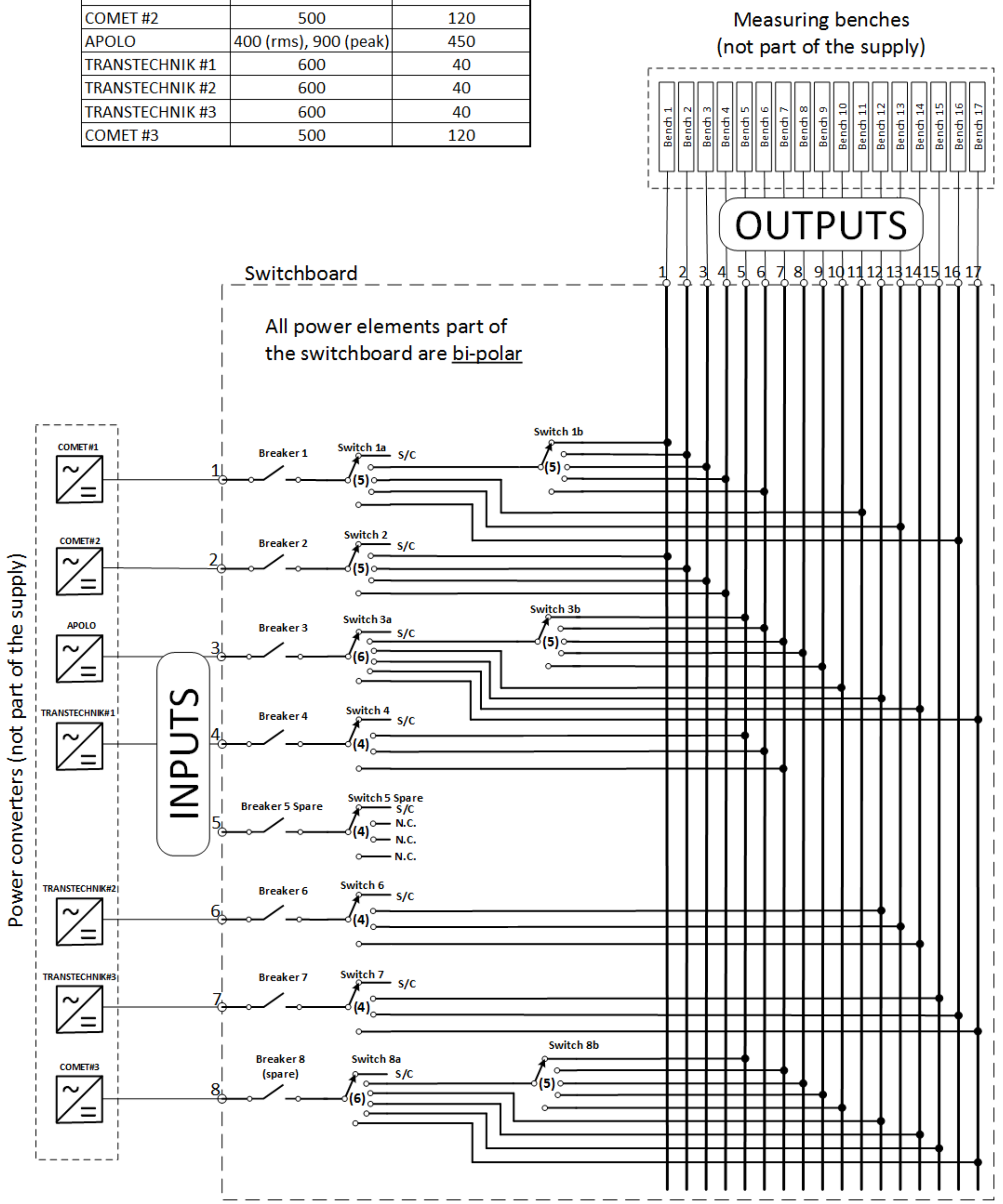
Switchboard installation

- **17 Measuring benches**
- **7 Power converters**
  - 3 COMET
  - 1 Apolo
  - 3 Transtechnik

- **Switchboard** assembled by the company Boffetti http://www.boffettigroup.com/

- Switchboard **main components**:
  - **ABB** Emax **circuit-breakers**
  - **Mersen** (FLOHE Foulileret SAS) **circular commutators**

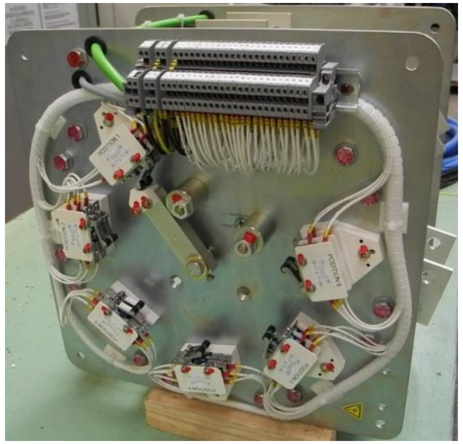
CONVERTERS		
Type	**Max. current [A]**	**Max. voltage [V]**
COMET #1	750	120
COMET #2	500	120
APOLO	400 (rms), 900 (peak)	450
TRANSTECHNIK #1	600	40
TRANSTECHNIK #2	600	40
TRANSTECHNIK #3	600	40
COMET #3	500	120



Switchboard installation

ABB Emax circuit-breakers

Mersen circular conmutators



Risk analysis

- **FMEA** (Failure Mode and Effect Analysis)
- High level analysis: focusing on the design
- 4 items were analysed
  - Magnet
  - Interbox
  - Switchboard
  - Power converter

Electrical risk

Need of an **interlock system** to mitigate this risk

Item	Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity (S)	Potential Cause(s) of Failure	Occurrence (O)	Occurrence Current Design(Prevention)	Detection (D)	Current Design Controls (Detection)	Risk Priority Number (RPN)	Recommended Action(s)	FMEA unique identifier number
1.3	Switchboard	blade position switch	open circuit under power	10	switch indicates closed position	3	tests during installation	8	regular switching tests without load	240	installation of a redundant switch	NBS#69
1.1	Magnet	Thermal interlock	Wrong connections	10	mix between thermal (NC) versus water (NO) interlock wrong connectors interlock scheme	5	standard interlock system (CERN OK, External institute NOK)	8	none	400		NBS#39

ICS contribution to the project

- Development of an **control system** which allows the operator **to select the switchboard setup** for the tests
- **Development of a protection** (interlock) **system** to prevent some hazardous events (monitoring the switchboard, the power converters and the bench signals)

Activities:

1. **Risk analysis**: **FMEA** (signal level of the existing design) + **Brainstorming** (What if method)
2. Definition of the control strategy: **UNICOS** Functional Analysis
3. Definition of **Safety Functions (IEC 61508)**
4. **Implementation** Control system + Safety Instrumented System
5. **“Proof” of compliance** with the requirements (**best effort**)
6. Safety report: including proof test coverage catalogue and recommendations

Risk Analysis (FMEA) + Brainstorming

Item / Function	Potential Failure Mode(s)	Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls (how can the potential failure be detected?)	Det	RPN	Recommended Action(s)
TSH01(NC)	No communication	TSH01(NC)	No communication	Safety input card (SIL3) will detect it and move to passivation	3	broken cable	1	PLC will detect it	9	27	
	Fails to open		Fails to open	Safety problem: damage the bench	10	Contact failure	3 (need MTTF)	no redundant information : It seems that the signal is serial chain of all magnet TSH	3	90	SIF checking the temperature of the bench
	Fails to close		Fails to close	No Safety problem	1	Contact failure	3 (need MTTF)	no redundant information : It seems that the signal is serial chain of all magnet TSH	3	9	

- *The **configuration from the SCADA is not very critical** as we have **feedback from all switches***
- ***Powering with two (or more) power converters the same bench will rise a critical situation** (damage to the installation and eventually to the workers)*
- ***All safety functions will act on the power converters***

Safety Functions (families)

1. **Coherence switches**: all feedbacks from the switch must be coherent (a.k.a one signal *TRUE* and all the rest *FALSE*)
2. **Breaker status**: Breaker must be closed in order to allow to the PC to provide the power to the bench
3. **Bench configuration**: never more than 1 PC can power the same bench
4. **Bench status signals**: all “bench signals” (EMXX, PBXX, FSLXX, TSHXX and ZSLXX) must be “OK” in order to allow to the PC to provide the power to the bench
5. **Overcurrent protection**: The current of COMET#3 PC should be limited.

Remarks:

- SIFs are **independent of the test bench selection** (SCADA)
- All safety functions will **stop the Power Converters** (PC_FPAXX and PC_PERMXX)

Safety Instrumented Function definition

- **Risk to mitigate:** Electrical risk (short-circuit) due to wrong Switchboard configuration. Potential power converters damage, magnet damage and human damage.

- **Functionality**: Each bench should be powered by **only 1 Power Converter**
- **Mode:** Low demand operation mode
- **Safety Integrity Level:** SIL2

Risk evaluation [R]		Probability of the hazardous event			
		1	2	3	4
Potential severity	A	A1	A2	A3	A4
	B	B1	B2	B3	B4
	C	C1	C2	C3	C4
	D	D1	D2	D3	D4

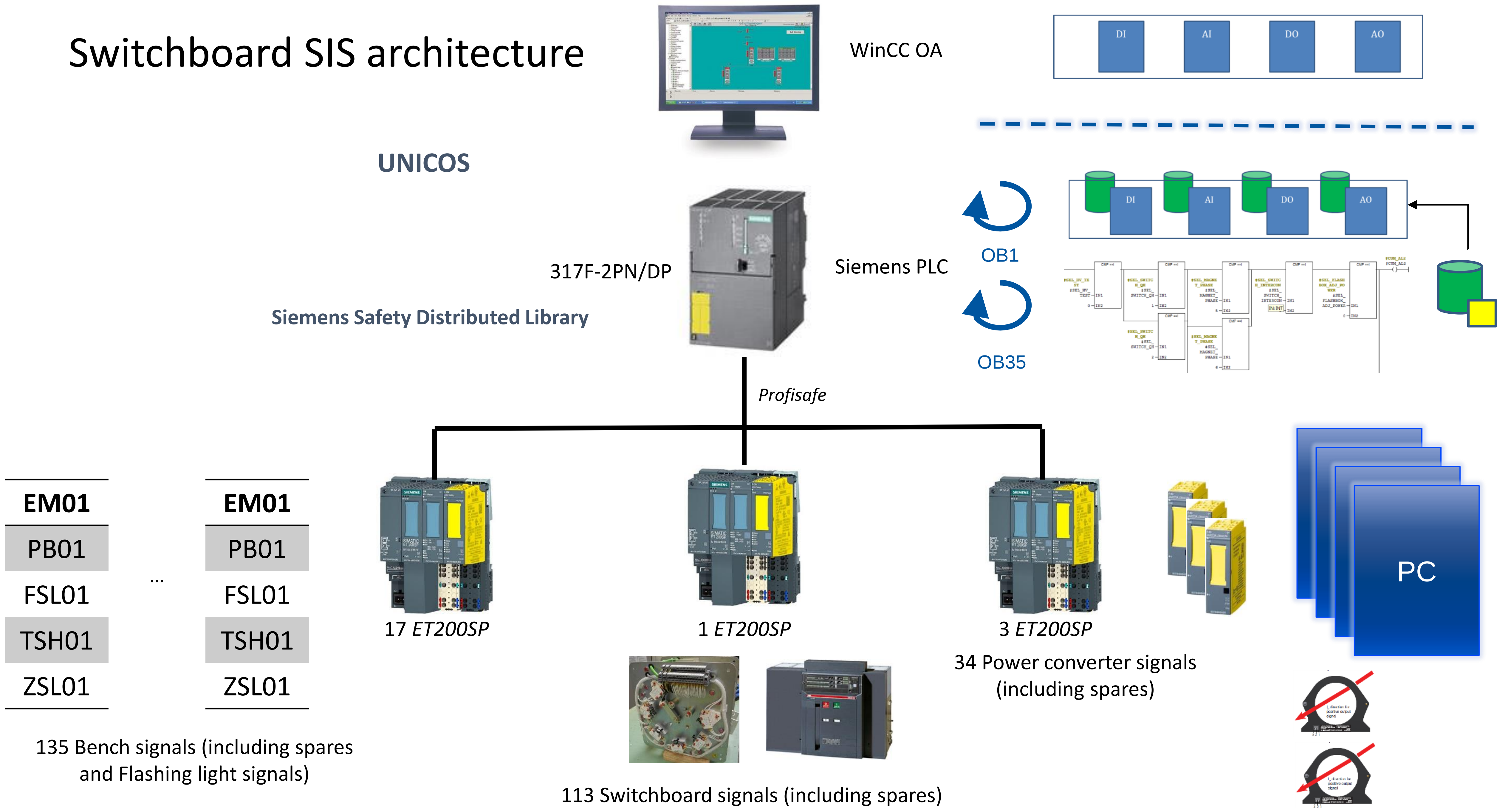
Risk evaluation table

SIF must be compliant with:

- SIL2 **Hardware** Safety Integrity requirements:
  - Architectural constrains
  - Hardware random failures
- SIL2 **Systematic** Safety Integrity requirements:
  Mechanical Stress, EM interference, Software errors, etc.

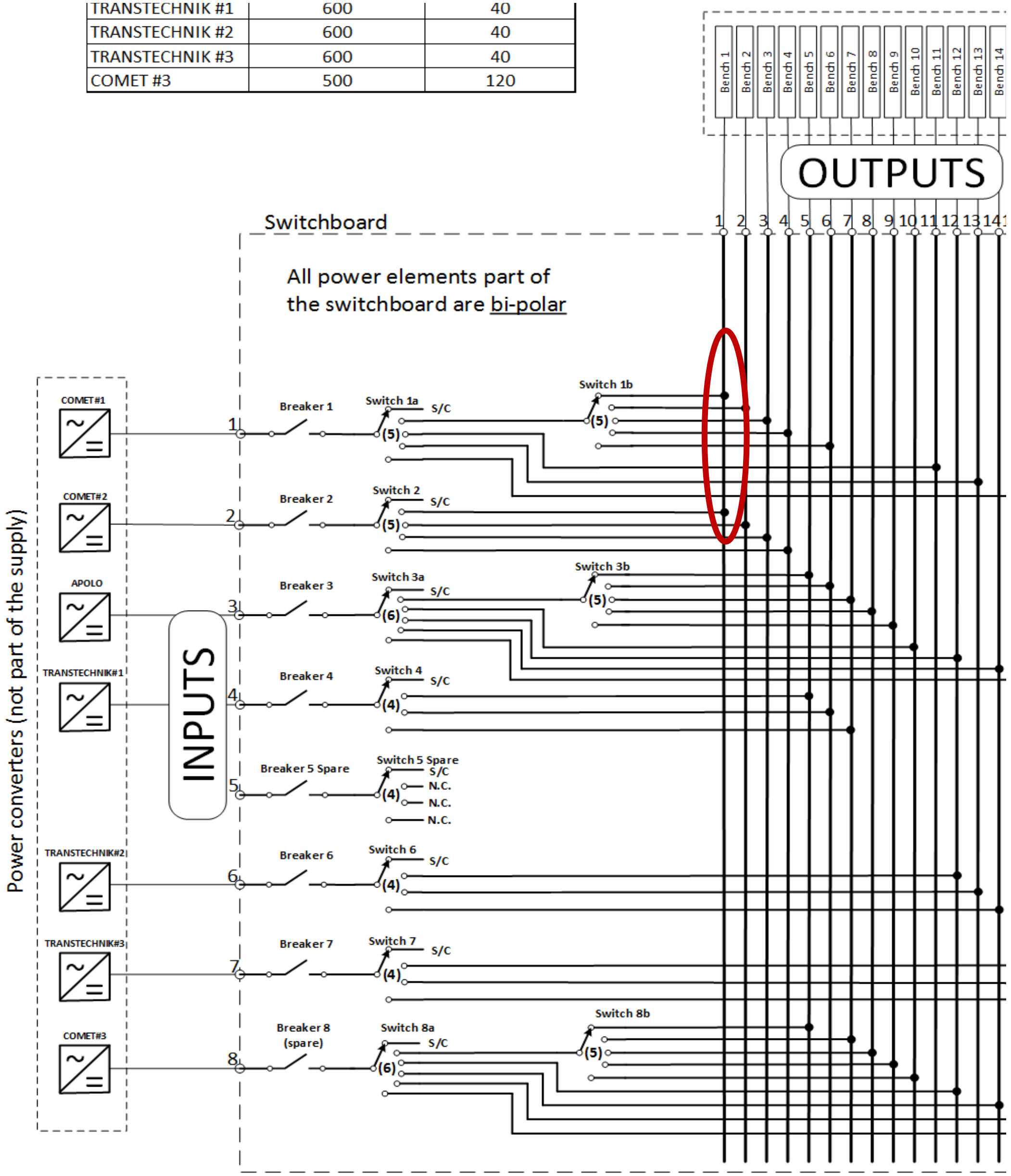
SIL4	$PFD_{avg} < 10^{-4}$	TRR < 10000
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

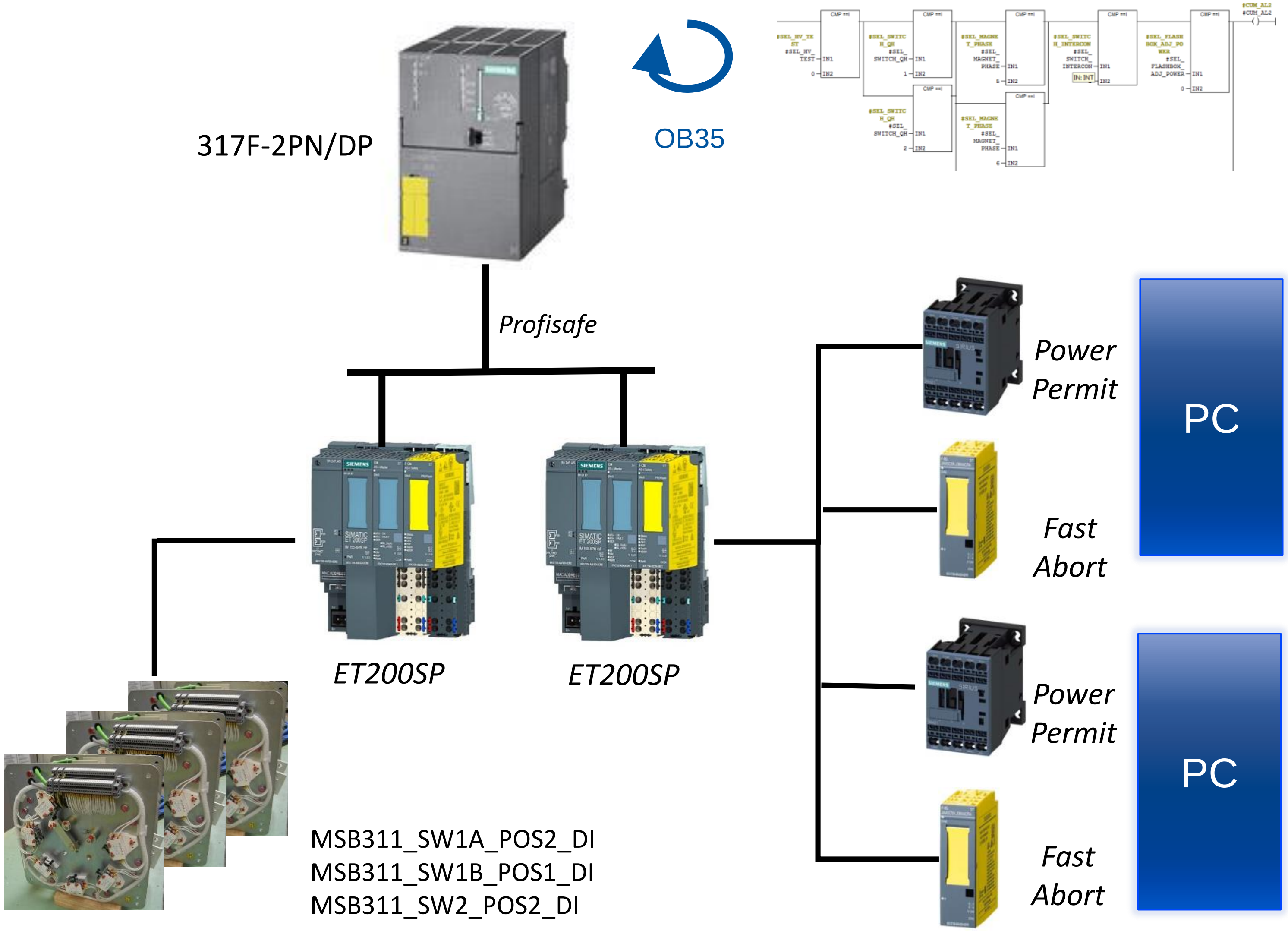
Switchboard SIS architecture



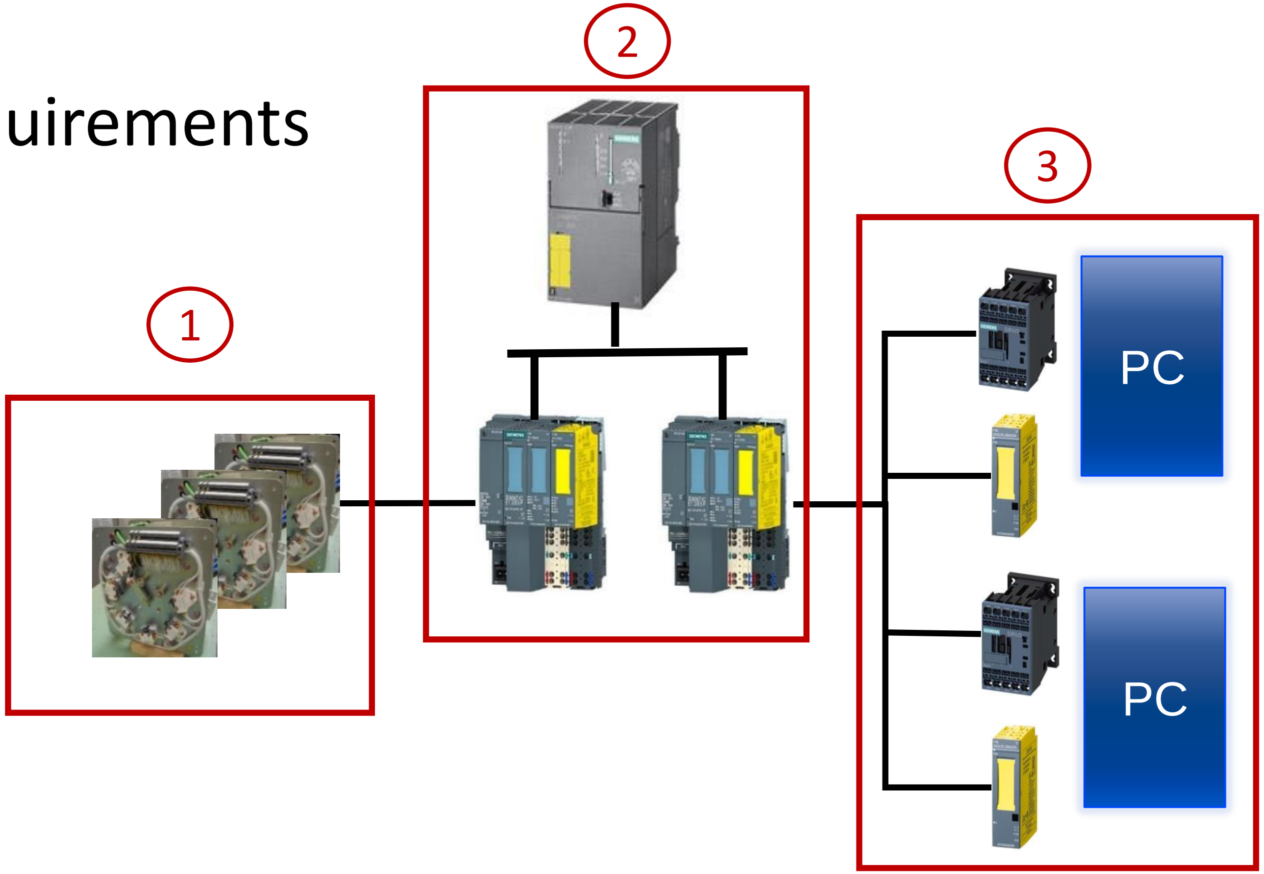
Implementation of SIF

TRANSTECHNIK #1	600	40
TRANSTECHNIK #2	600	40
TRANSTECHNIK #3	600	40
COMET #3	500	120



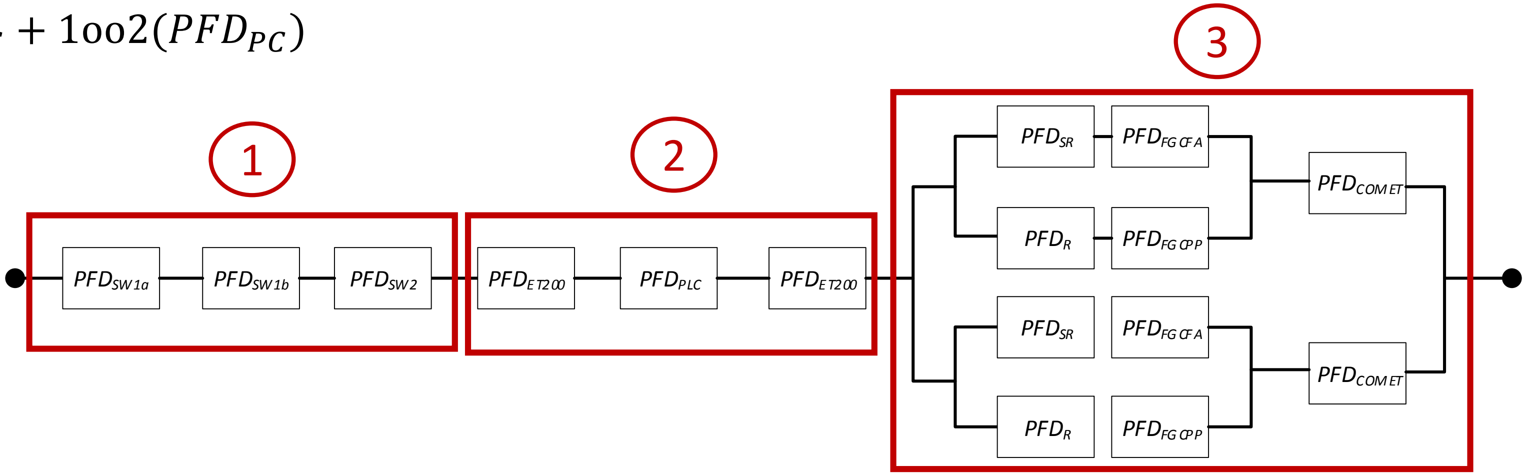


Hardware Safety Integrity requirements



Reliability Block Diagram

$$PFD_{SIF} = 3 * (PFD_{sw}) + 2 * PFD_{ET200} + PFD_{PLC} + 1oo2(PFD_{PC})$$



Source of Information (IEC 61508)

1. **Site specific (CERN)**
    - Power converters team (TE-EPC)

2. **Industry specific**
    - Test bench facilities (e.g. SM18)

3. **Generic (large number of applications)**
    - Boffetti, ABB, Mersen

4. **Manufacturer data**
    - ABB – circuit breakers
    - Mersen (FLOHE) - Switches

Why so important:

1. **Hardware** Safety Integrity requirements:
    - Hardware random failures (**Failure rate, MTTF**, etc.)
    - Architectural constrains
        - Route 1 :**SFF** (Safe Failure Fraction)
        - Route 2 : **Feedback** from the users

2. **Systematic** Safety Integrity requirements:
    - **Proven in use**

Meeting the Safety Integrity requirements

IEC 61508

1. **Hardware Safety Integrity**
   - Quantify the **random hardware failures** for the specific SIL: PFD or PFH calculations.

   AND

   - Comply with the **architectural constrains** for the specific SIL: Route 1_H (SFF and HFT) or Route 2_H (field feedback, …)

2. **Systematic Safety Integrity**
   - Comply with requirements for systematic safety integrity for the specific SIL: Route 1_S

   OR

   - Comply with requirements for **Proven in Use** (PIU) for the specific SIL: Route 2_S

IEC 61511

1. **Hardware Safety Integrity**
   - Quantify the **random hardware failures** for the specific SIL: PFD or PFH calculations.

   AND (

   - Comply with the **HFT requirements (IEC 61511)**

   OR

   - Comply with the **HFT requirements (IEC 61508)**

)

2. **Systematic Safety Integrity**
   - Comply with **Application Program requirements for LVL & FPL**

   AND (

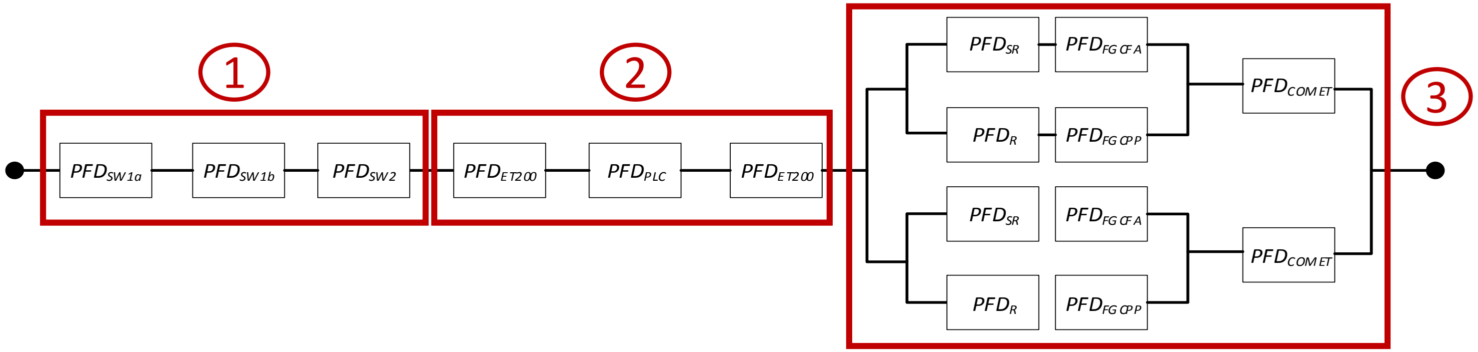
   - Comply with requirements based on **Prior Use** (IEC 61511)

   OR

   - Comply with requirements for systematic safety integrity (IEC 61508)

)

Hardware random failures



$$PFD = \lambda_D . \frac{T}{2}$$

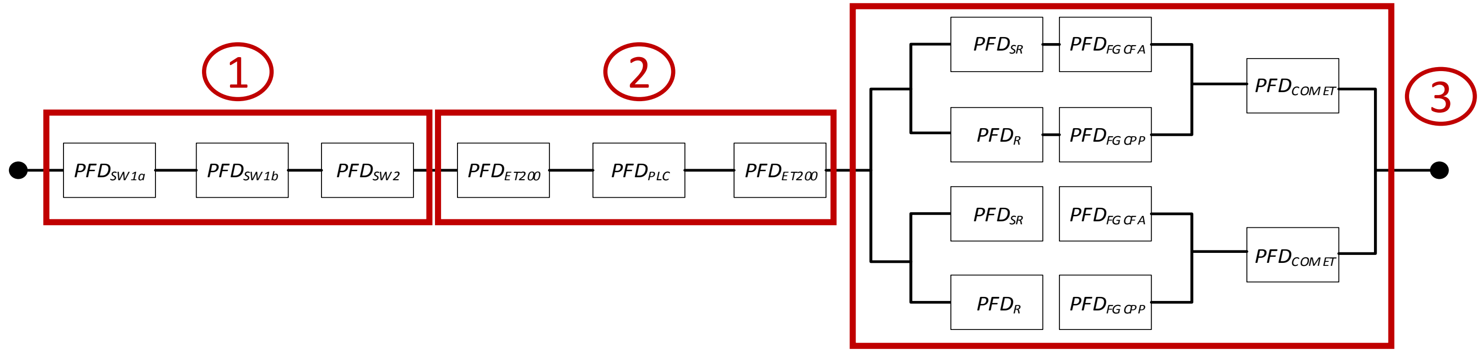
$$MTTF = 1/\lambda_D$$

$$MTBF = MTTF + MTDF + MTTR$$

Where:

- $\boldsymbol{\lambda_D}$ is the (dangerous) failure rate. We consider constant failure rate $\lambda(t) = \lambda$
- $\boldsymbol{T}$ is the period of time between the manual tests
- No automatic tests C = 0

Hardware random failures



$$PFD = \lambda_D . \frac{T}{2}$$

PFD for block 1:

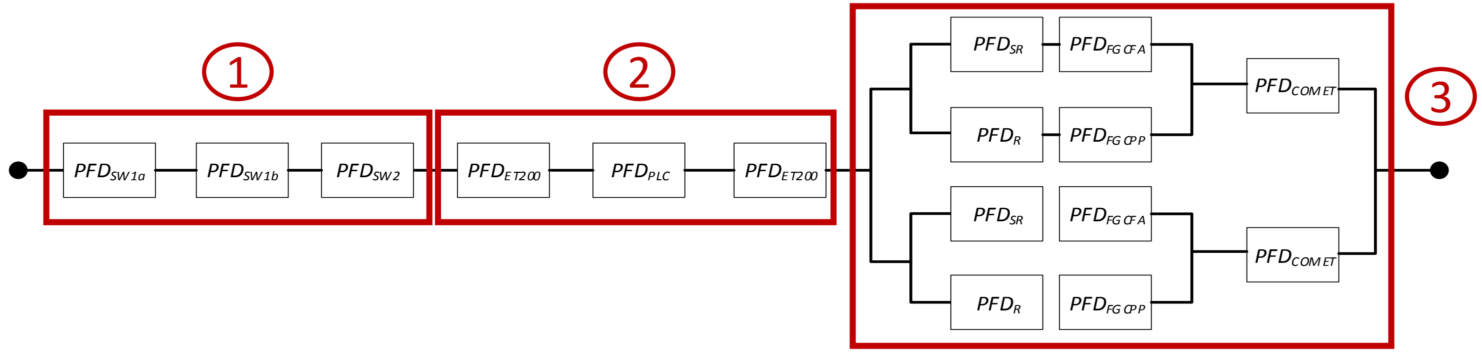
- Information provided by manufacturer (Mersen): λ **= 0.9 E-03**
- **Assumptions**:
  - $\lambda = \lambda_D$ (Failure rate = Dangerous failure rate)
  - **C = 0** (No automatic tests)
  - **SIL2**
- If **PFD_1 = 1 E-03**, then **T = 0.741 years = 270 days**
- If **PFD_1 = 1 E-02**, then **T = 7.41 years**

Failure mode	Rate of occurrence	MTBF	MTTR	Effects on OCS	Effects on LV
	(%)	(hour)	(hour)		
MAIN CIRCUIT					
Mechanical defect	2,2 E-3	20 E6	3,00	No high voltage on OCS	NA
MOTOR					
Mechanical defect	4,4 E-3	10 E6	1,50	No possibility to commutate	NA
INTERLOCKING					
Mechanical defect	2,2 E-3	20 E6	1,00	No possibility to commutate	NA
AUXILIARY CONTACTS					
Auxiliary contacts	0,9 E-3	50 E6	0,50	Signalisation	NA
	9,7 E-3	4,5 E6	6,00		

SIL4	**$PFD_{avg} < 10^{-4}$**	**TRR < 10000**
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

Hardware random failures

$$PFD = \lambda_D . \frac{T}{2}$$



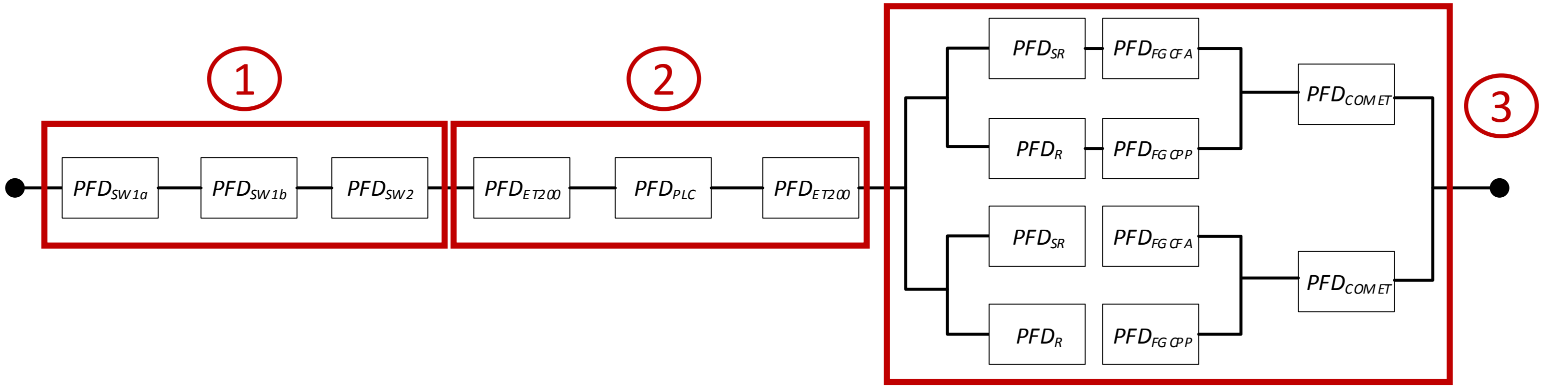
PFD for block 2:

- Information provided by manufacturer (Siemens): **SIL3** certified devices
- **No significant to reach SIL2 for this SIF**

SIL4	**$PFD_{avg} < 10^{-4}$**	**TRR < 10000**
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

Hardware random failures

$$PFD = \lambda_D \cdot \frac{T}{2}$$

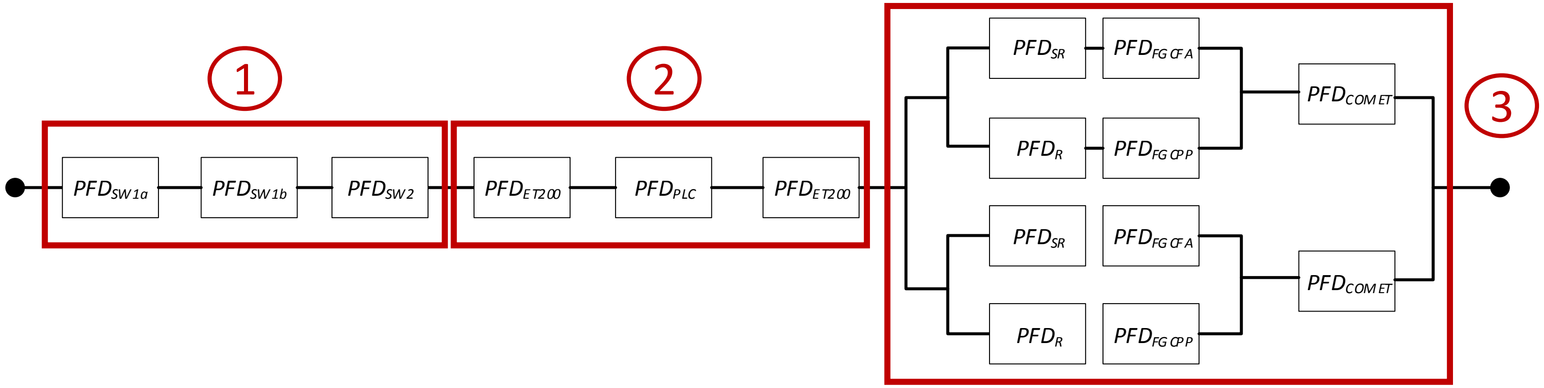


PFD for block 3:

- **Safety relay**: Information provided by manufacturer (Siemens): **SIL3**
- **Power Converters**: **No valid information** to guarantee SIL
  - Large number of PC installed at CERN (around 2000 PCs)
  - New Function Generator Controller (FGC3)
- Redundant signals
  - Fast Abort (**safe signal, redundant architecture**)
  - Power Permit
- Redundant Architecture
  - Stop both power converters
  - Possibility to add hardware interlock (recommendation given to SM18 test bench facilities)

SIL4	**$PFD_{avg} < 10^{-4}$**	**TRR < 10000**
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

Architectural constrains



2 options:

- **Route 1_H**: Based on hardware fault tolerance (HFT) and safety failure fraction(SFF)

	Type A			Type B		
HFT / SFF	0	1	2	0	1	2
<60%	SIL 1	SIL 2	SIL 3	N/A	SIL 1	SIL 2
60% ≤ 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% ≤ 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

- **Route 2_H**: HFT and Feedback of users (Boffetti, Mersen and the Power converter team)

Systematic Safety Integrity

- **We focus on the software (PLC program) reliability**: IEC 61511 verification of application software

- All the SIFs were formally verified using the **PLCverif tool:** https://cern.ch/PLCverif
  - This tool applies model checking to the PLC programs

- During the development of the PLC program, **PLCverif found "discrepancies"** between the SIFs specification (desired functionality) and the SIFs implementation (PLC program)

- The 5 SIFs are expressed in 94 verification properties. **The PLC program has $2^{174} \approx 6*10^{51}$ input combinations.** "Impossible" to check all of them with testing

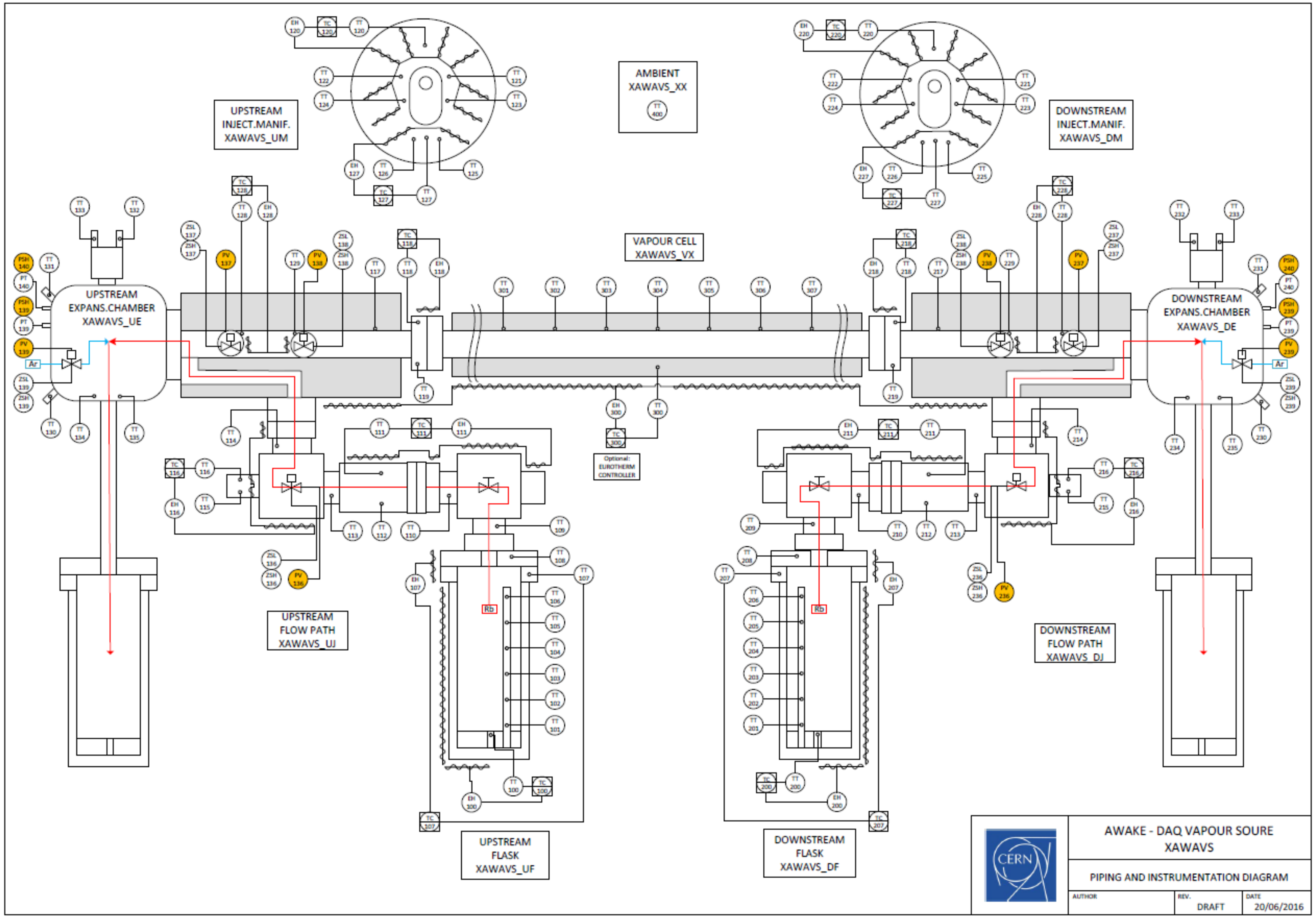
AWAKE (Advanced Wakefield Experiment)

"…an approach to accelerate an electron beam to the TeV energy regime in a single plasma section…"

http://awake.web.cern.ch/awake/

International collaboration:

- Several groups at CERN (TE/VSC, HSE/SEE, BE/ICS)
- Max-Planck-Institut für Physik https://www.mpp.mpg.de/
- WDL http://www.wrightdesign.net/



Risk Analysis (FMEA)

RISK ASSESSMENT											
	Hazard	Causes	Hazardous Event(s)	Consequences	Control measure(s)	P	S	R	Action(s)	Further prevention measure(s) required	Further mitigation measure(s) required
	Flammable	Accidental contact with oxygen source during system operation	Failure of vapour source structure leading to ingress of air into the vapour source	Injury to personnel due to fire in experimental area Significant damage to local infrastruture due to fire Respiratory damage to personnel due to release of rubidium combustion products	Joints and interconnects following UHV best practice RGA completed during HWC to verify leak rate less than 2 x 10-10mbarls-1 CERN beamline valve interlocks if pressure exceeds 1 x 10-5 mbar isolating vapour source system	1	D	D1	**Unacceptable risk: actions are necessary.**	**SIF2**: Secondary protection of density viewports using automatic valves **SIF2**: Place system into emergency shutdown state if fault (loss of vacuum) detected (*calculate safe inlet pressure of argon assuming worst case heating*)	**SOP: CERN firefighting procedure needed (i.e use of class D fire extinguishers)**

Safety Instrumented Function definition

- **Risk to mitigate:** ignition risk due to the contact of rubidium and the air.

- **Functionality**: Isolate the **rubidium** inside the plasma cell by closing the valves behind the viewports once a leak of the plasma cell is detected
- **Mode:** Low demand operation mode
- **Safety Integrity Level:** SIL2

Risk evaluation [R]		Probability of the hazardous event			
		1	2	3	4
Potential severity	A	A1	A2	A3	A4
	B	B1	B2	B3	B4
	C	C1	C2	C3	C4
	D	D1	D2	D3	D4

Risk evaluation table

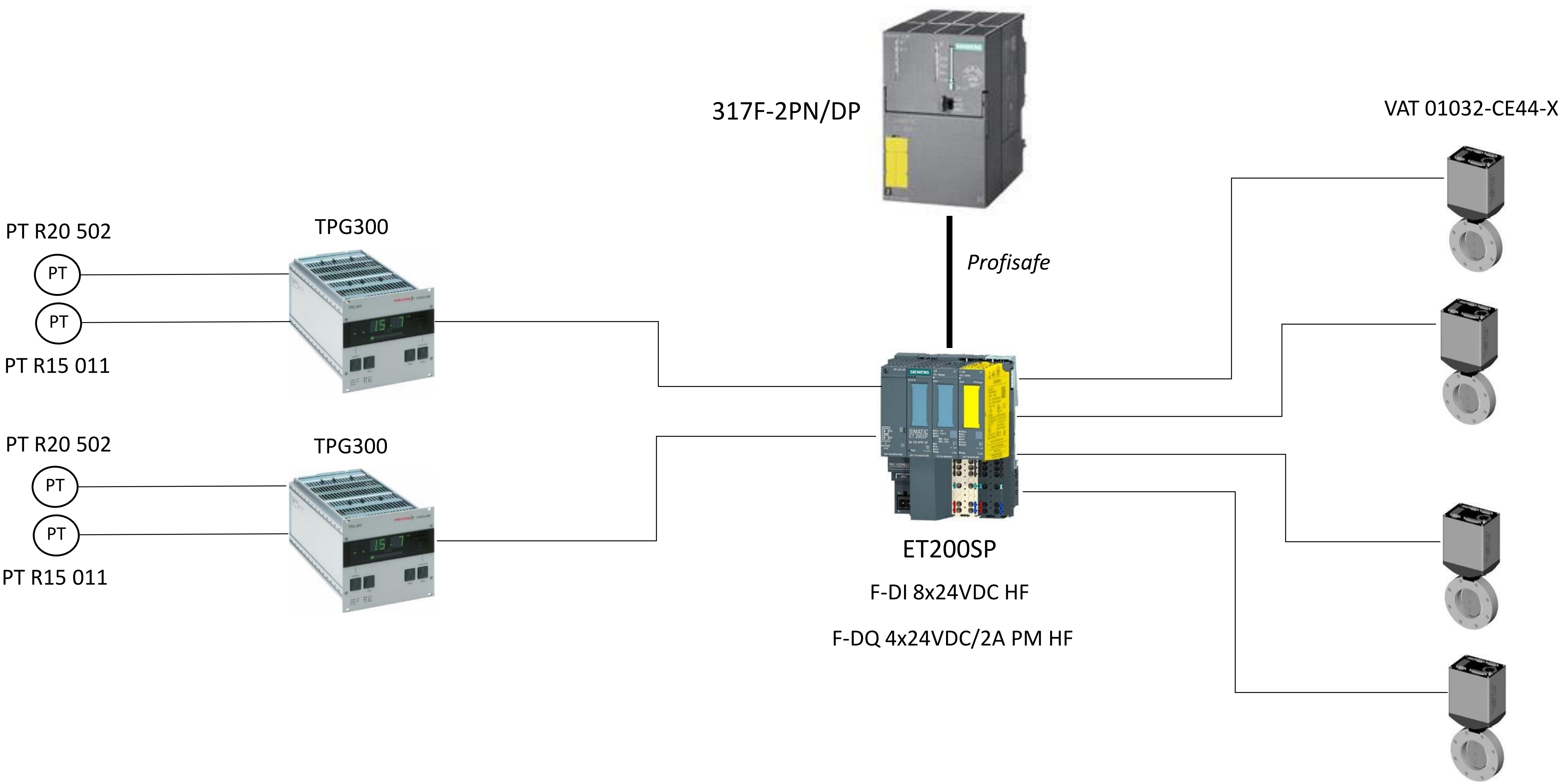
SIF must be compliant with:

- SIL2 **Hardware** Safety Integrity requirements:
  - Architectural constrains
  - Hardware random failures
- SIL2 **Systematic** Safety Integrity requirements: Mechanical Stress, EM interference, Software errors, etc.

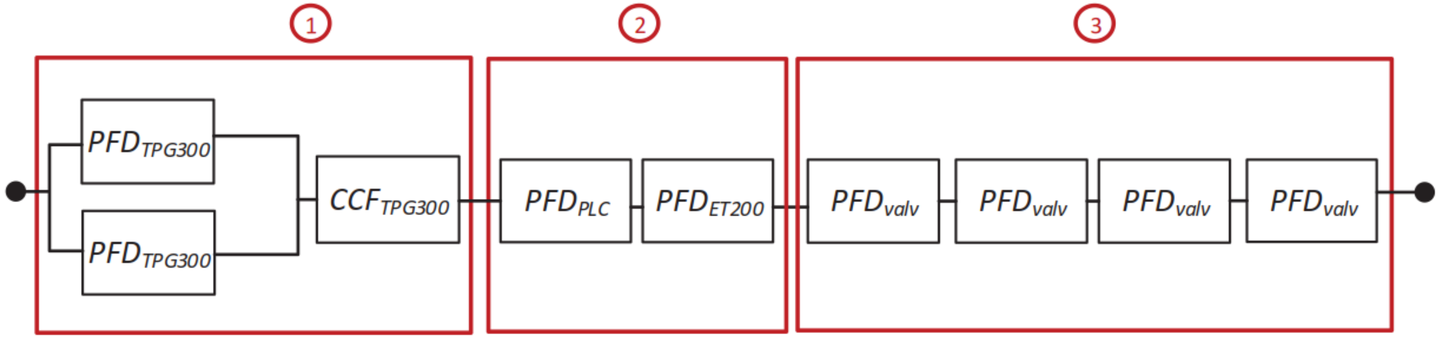
SIL4	**$PFD_{avg} < 10^{-4}$**	**TRR < 10000**
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

AWAKE SIF architecture

UNICOS + Distributed Safety library



Hardware random failures



$$PFD = \lambda_D . \frac{T}{2}$$

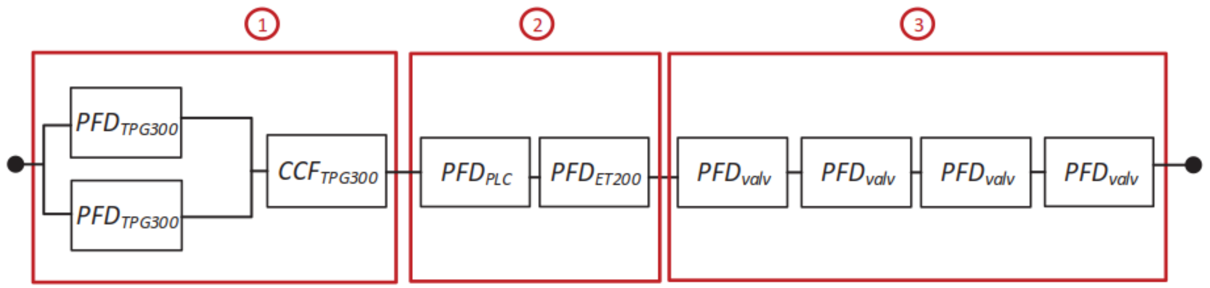
$$MTTF = 1/\lambda_D$$

$$MTBF = MTTF + MTDF + MTTR$$

Where:

- $\boldsymbol{\lambda_D}$ is the (dangerous) failure rate. We consider constant failure rate $\lambda(t) = \lambda$
- $\boldsymbol{T}$ is the period of time between the manual tests
- No automatic tests C = 0

Hardware random failures



$$PFD_1 = \frac{\lambda_D^2 * T^2}{3} + \beta \frac{\lambda_D * T}{2}$$

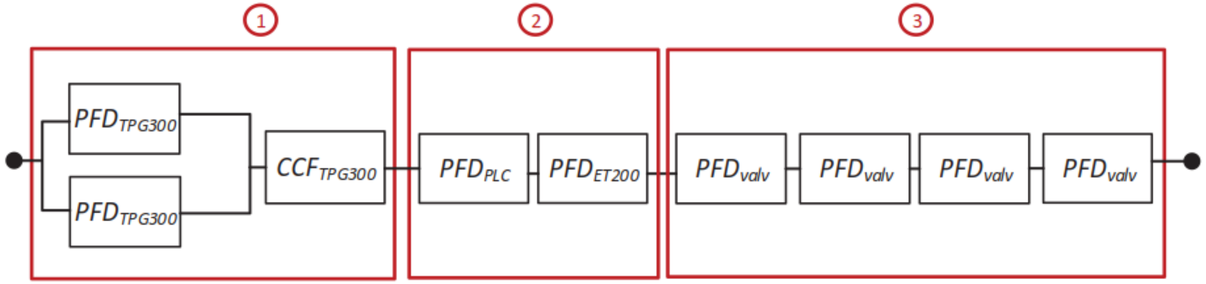
PFD for block 1:

- Information provided by manufacturer (Mersen): $MTTF$ **= 156 years**
- **Assumptions**:
  - λ = λ_D (Failure rate = Dangerous failure rate)
  - **C = 0** (No automatic tests)
  - B = 25%
  - **SIL2**
  - **T = 4 weeks**
- **PFD_1 = 6.15 E-05**

SIL4	**$PFD_{avg} < 10^{-4}$**	**TRR < 10000**
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

Hardware random failures

$$PFD = \lambda_D . \frac{T}{2}$$



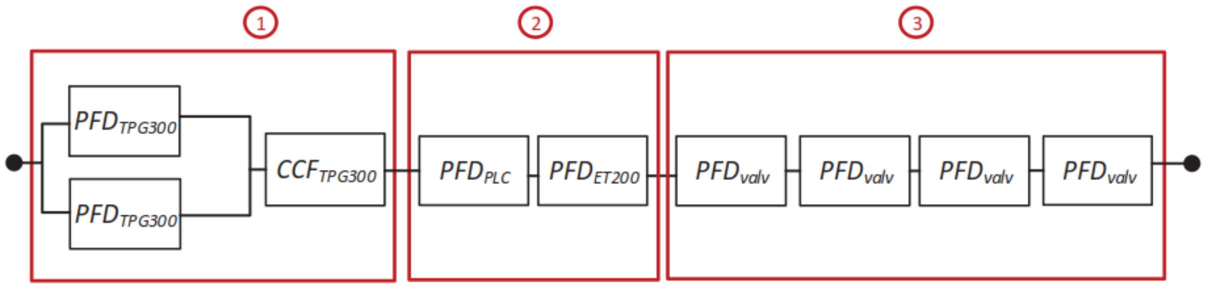
PFD for block 2:

- Information provided by manufacturer (Siemens): **SIL3** certified devices
- **No significant to reach SIL2 for this SIF**

SIL4	**$PFD_{avg} < 10^{-4}$**	**TRR < 10000**
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

Hardware random failures

$$\lambda_{D_{valve}} = PFD_3/(2 * T)$$



PFD for block 3:

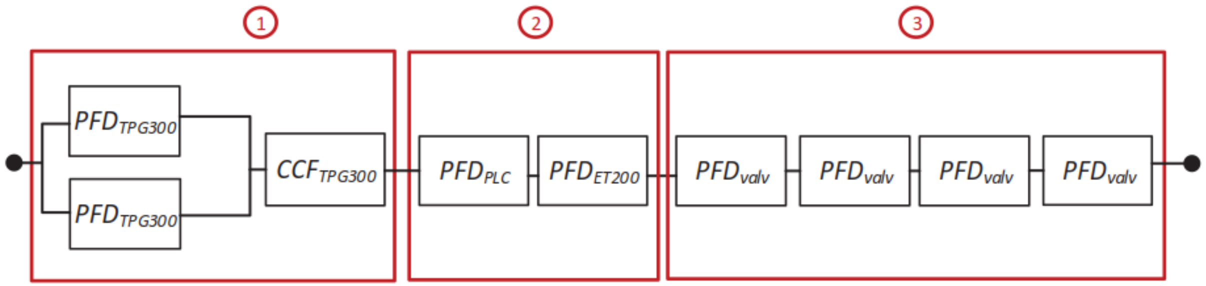
- Information provided by manufacturer: **50000 cycles until the first service**
- **No safety relevant information**

SIL4	**$PFD_{avg} < 10^{-4}$**	**TRR < 10000**
SIL3	$10^{-4} < PFD_{avg} < 10^{-3}$	TRR < 1000
SIL2	$10^{-3} < PFD_{avg} < 10^{-2}$	TRR < 100
SIL1	$10^{-2} < PFD_{avg} < 10^{-1}$	TRR < 10
SIL0	No Safety	

Table 3: Valve SIL 2 PFD Boundaries

PFD_3	**PFD_{valve}**	**λ_D**	**MTTF**
10^{-2}	$PFD_3/4=0.0025$	$6.518*10^{-2}$	15.34
10^{-3}	$PFD_3/4=0.00025$	$6.518*10^{-3}$	154

Architectural constrains



2 options:

- **Route 1_H**: Based on hardware fault tolerance (HFT) and safety failure fraction(SFF)

	Type A			Type B		
HFT / SFF	0	1	2	0	1	2
<60%	SIL 1	SIL 2	SIL 3	N/A	SIL 1	SIL 2
60% ≤ 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% ≤ 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

- **Route 2_H**: HFT and Feedback of users

1
TPG300
Type B: complex
HFT=1
Unknown SFF

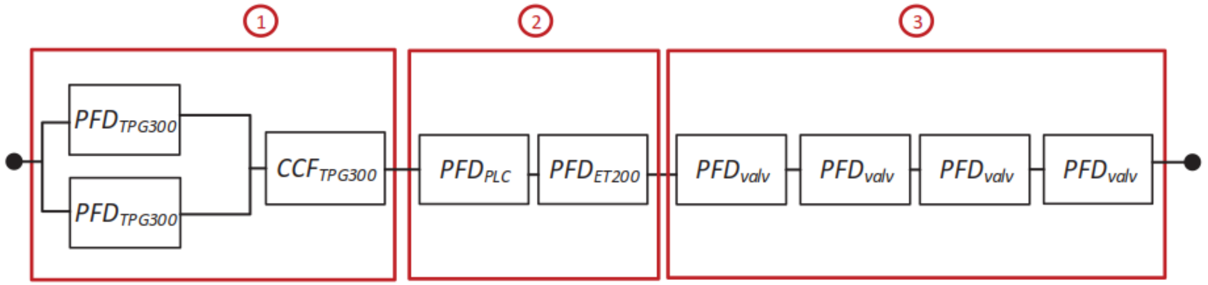
Constraint:
SFF > 60%

3
Solenoid valves
Type A: simple
HFT=0
Unknown SFF

SFF > 60%
Otherwise need **redundancy**

Systematic Safety Integrity

- **We focus on the software (PLC program) reliability**: IEC 61511 verification of application software
- The SIF was formally verified using the **PLCverif tool:** https://cern.ch/PLCverif
  - This tool applies model checking to the PLC programs



1

TPG300
SC1 compliant
Design (EMI, env. stress, online monitoring)
Separated and redundant TPG300
SC1 -> SC2

2

S7-315F (fail safe PLC)
SIL 3 compliant for systematic fail.

(IEC 61511) Application software must be SIL2
- **Low variability Language (ladder)**
- **Verification by formal methods***

3

Solenoid valves
Basic information from supplier

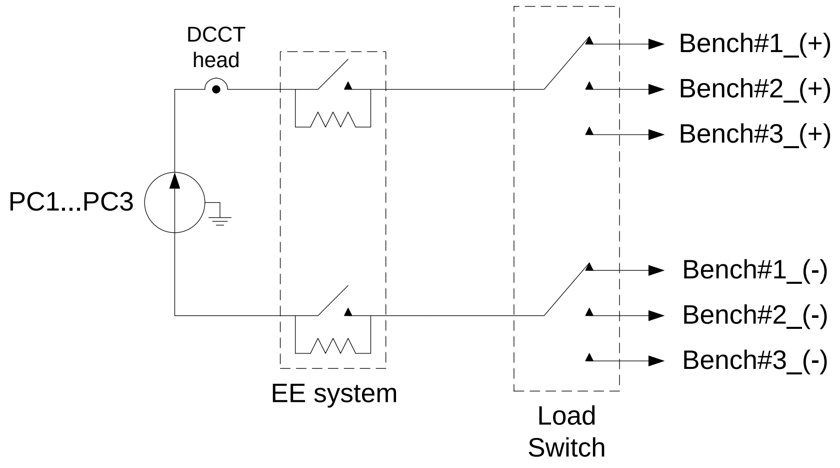
The four valves must have an **SC2 to claim the required SIL 2**

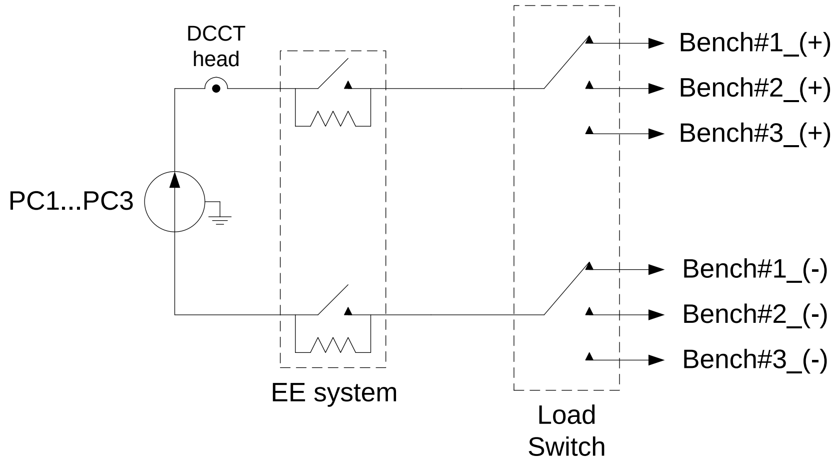
FAIR test bench

*Building 180 is hosting the test bench facility for all magnets from the **FAIR project at GSI**.*

The functionality of this installation is very similar to the already existing test bench facility in the SM18 building at CERN.

The installation is composed by 3 different test benches where up to 9 magnets can be tested at the same time. Six kind of tests can be performed in this installation





Risk Analysis (FMEA) provided by HSE

Electrical risk

Risk Assessment												
ID	Hazards	Causes	Hazardous Events	Consequences	Control measures (Preventive and Protective)	P	S				R	Risk Level
							People	Environment	Property	Operational		
	Electricity	Stored Energy in Magnet	Change of connection to load can leave stored energy in magnet	People - Electrocution Property - Overheating	Preventive: Risk considered in design, Hardware Interlock	2	B	A	B	B	B2	**Moderate risk: actions are recommended to reduce the risk.**

Cryogenic risk

Risk Assessment												
ID	Hazards	Causes	Hazardous Events	Consequences	Control measures (Preventive and Protective)	P	S				R	Risk Level
							People	Environment	Property	Operational		
	Cryogenic fluid	*Commissioning/Operation:* Exhaust of GN2 precooler, located near filling area of N2 tanks	Exhaust gas in area of operators/drivers around N2 precooler exhaust	People - cyrogenic fluid	Preventive - Add external piping to B180 to vent precooler exhaust higher up	2	B	A	A	A	B2	**Moderate risk: actions are recommended to reduce the risk.**

Risk Analysis (FMEA) provided by HSE

Conclusions:

- **Cryogenic safety**:
  - “Other control measures”: Cryogenics control system, including the pressure and temperature regulation, heaters control, etc.
  - **SIF**: in case of losing the cryogenic conditions, stop the PCs. Risk B2 -> **SIL1** (?) -> Low demand (?) (P = 2). Severity to people B = low
- **Electrical and electromagnetic safety**:
  - **SIF:** protection of people from direct contact. Risk D1 -> **SIL2** (?) -> Low demand (?) (P = 1) Severity to people D = high
  - **SIF:** protection from Quench. Risk B4 -> **SIL2** (?) -> High demand (?) (P = 4) Severity to people B = low
- Mechanical safety:
  - No SIFs needed.
- Ergonomic:
  - No SIFs needed.
- Non ionizing radiation:
  - No SIFs needed.

Interlock specification

- Provide by the client (TE/MSC group at CERN)
- **Contains functionality and safety conditions**
- PLC program is based on this specification (complex logic)

	A	B	C	D	K	L	M	N	O
1					BENCH 1				
2					TYPE OF TEST TO SELECT				
3-4	TEST CONFI			Signal name	Power PCx (x= 1 to 9)	HV at warm	Continuity	HV at cold	QPS signal compensation at cold
5		Par.		MIN_Q_CURx (*9 PCs)	xxx A				
42	INPUT VALUES TO BE CHECKED	72 DIGITAL INPUTS	31	PC8_STATUS	1 if x=8, NA if x≠8	NA	NA	NA	NA
43			32	PC9_STATUS	1 if x=9, NA if x≠9	NA	NA	NA	NA
44			33	PCs_MCB_STATUS	NA	NA	NA	NA	NA
45			34	MANUAL_STOP	1	NA	NA	NA	NA
46			35	AUE_PC_ALL	1	1	1	1	1
47			36	TB1_ELEC_DOOR_OPENED	0	0	0	0	0
48			37	TB1_CRYO_DOOR_OPENED	0	0	0	0	0
49			38	TB2_ELEC_DOOR_OPENED	NA	NA	NA	NA	NA
50			39	TB2_CRYO_DOOR_OPENED	NA	NA	NA	NA	NA
51			40	TB3_ELEC_DOOR_OPENED	NA	NA	NA	NA	NA
52			41	TB3_CRYO_DOOR_OPENED	NA	NA	NA	NA	NA
53			42	TB1_ELEC_DOOR_CLOSED	1	1	1	1	1
54			43	TB1_CRYO_DOOR_CLOSED	1	1	1	1	1
55			44	TB2_ELEC_DOOR_CLOSED	NA	NA	NA	NA	NA
56			45	TB2_CRYO_DOOR_CLOSED	NA	NA	NA	NA	NA
57			46	TB3_ELEC_DOOR_CLOSED	NA	NA	NA	NA	NA
58			47	TB3_CRYO_DOOR_CLOSED	NA	NA	NA	NA	NA
59			48	TB1_TOWER_ELEC_FREE	1	1	1	1	1
60			49	TB2_TOWER_ELEC_FREE	NA	NA	NA	NA	NA
61			50	TB3_TOWER_ELEC_FREE	NA	NA	NA	NA	NA
62			51	TB1_TOWER_CRYO_FREE	1	1	1	1	1
63			52	TB2_TOWER_CRYO_FREE	NA	NA	NA	NA	NA
64			53	TB3_TOWER_CRYO_FREE	NA	NA	NA	NA	NA
65			54	COM1_TB1	1 if x=1, NA if x≠1	0	0	0	0
66			55	COM1_TB2	0 if x=1, NA if x≠1	0 or 1	0 or 1	0 or 1	0 or 1
67			56	COM1_TB3	0 if x=1, NA if x≠1	1 or 0	1 or 0	1 or 0	1 or 0
68			57	COM2_TB1	1 if x=2, NA if x≠2	0	0	0	0
69			58	COM2_TB2	0 if x=2, NA if x≠2	0 or 1	0 or 1	0 or 1	0 or 1
70			59	COM2_TB3	0 if x=2, NA if x≠2	1 or 0	1 or 0	1 or 0	1 or 0
71			60	COM3_TB1	1 if x=3, NA if x≠3	0	0	0	0
72			61	COM3_TB2	0 if x=3, NA if x≠3	0 or 1	0 or 1	0 or 1	0 or 1
73			62	COM3_TB3	0 if x=3, NA if x≠3	1 or 0	1 or 0	1 or 0	1 or 0
74			63	COM4_TB1	1 if x=4, NA if x≠4	0	0	0	0
75			64	COM4_TB2	0 if x=4, NA if x≠4	0 or 1	0 or 1	0 or 1	0 or 1
76			65	COM4_TB3	0 if x=4, NA if x≠4	1 or 0	1 or 0	1 or 0	1 or 0
77			66	COM5_TB1	1 if x=5, NA if x≠5	0	0	0	0
78			67	COM5_TB2	0 if x=5, NA if x≠5	0 or 1	0 or 1	0 or 1	0 or 1
79			68	COM5_TB3	0 if x=5, NA if x≠5	1 or 0	1 or 0	1 or 0	1 or 0
80			69	COM6_TB1	1 if x=6, NA if x≠6	0	0	0	0
81			70	COM6_TB2	0 if x=6, NA if x≠6	0 or 1	0 or 1	0 or 1	0 or 1
82			71	COM6_TB3	0 if x=6, NA if x≠6	1 or 0	1 or 0	1 or 0	1 or 0
83			72	COM7_TB1	1 if x=7, NA if x≠7	0	0	0	0
84			73	COM7_TB2	0 if x=7, NA if x≠7	0 or 1	0 or 1	0 or 1	0 or 1
85			74	COM7_TB3	0 if x=7, NA if x≠7	1 or 0	1 or 0	1 or 0	1 or 0
86			75	COM8_TB1	1 if x=8, NA if x≠8	0	0	0	0
87			76	COM8_TB2	0 if x=8, NA if x≠8	0 or 1	0 or 1	0 or 1	0 or 1
88			77	COM8_TB3	0 if x=8, NA if x≠8	1 or 0	1 or 0	1 or 0	1 or 0
89			78	COM9_TB1	1 if x=9, NA if x≠9	0	0	0	0

Risk Analysis (FMEA) + Brainstorming

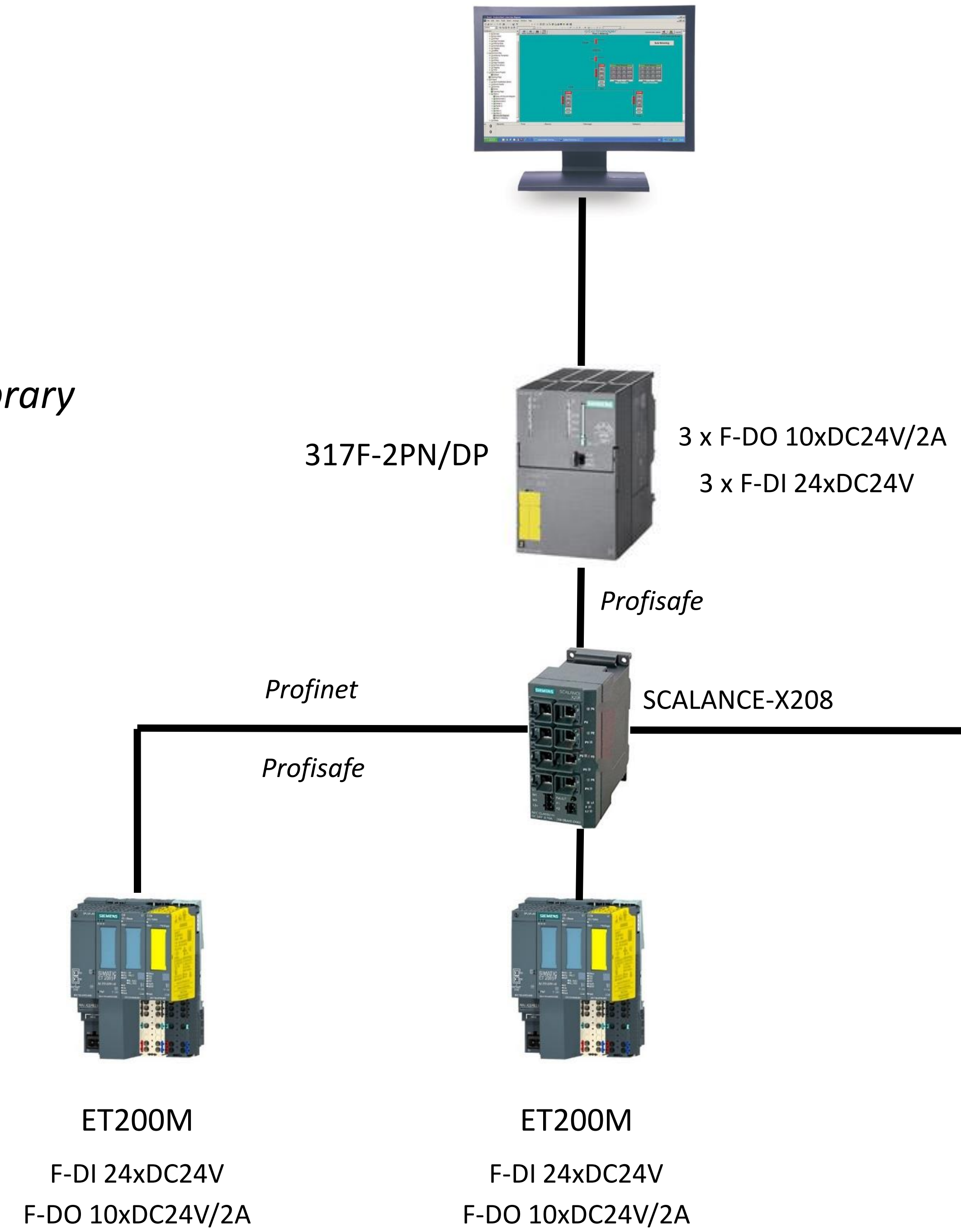
Item / Function	Potential Failure Mode(s)	Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls (how can the potential failure be detected?)	Det	RPN	Recommended Action(s)
TSH01(NC)	No communication	TSH01(NC)	No communication	Safety input card (SIL3) will detect it and move to passivation	3	broken cable	1	PLC will detect it	9	27	
	Fails to open		Fails to open	Safety problem: damage the bench	10	Contact failure	3 (need MTTF)	no redundant information : It seems that the signal is serial chain of all magnet TSH	3	90	SIF checking the temperature of the bench
	Fails to close		Fails to close	No Safety problem	1	Contact failure	3 (need MTTF)	no redundant information : It seems that the signal is serial chain of all magnet TSH	3	9	

Why?

- ***Identification of safety critical signals*** *to mitigate the risks*
- *Sometimes (very few),* ***we can select the instrumentation***
- *We can take decisions about the* ***architecture*** *(e.g. redundancy) and identify weak points of our SIS.*

FAIR SIS architecture

UNICOS + Distributed Safety library



PCs & commutators signals:

- PC Fast abort commands
- PC Slow abort commands
- PC feedbacks
- MCB commands
- Commutators feedbacks
- …

Bench signals:

- Emergency stops
- Door commands
- Door feedbacks
- Safety mat
- Auxiliary Power supplies
- …

FAIR SIFs

- **16 SIFs** were extracted to mitigate the cryogenic and electrical risks:

- Here an example for electrical risk:

__SIF5__: shutdown the PCs if the coherence of the commutator feedbacks is not respected (one signal TRUE and all the rest FALSE).

- ***Functionality****: if (NOT ((COM1_TB1=1 AND COM1_TB2=0 AND COM1_TB3=0) OR (COM1_TB1=0 AND COM1_TB2=1 AND COM1_TB3=0) OR (COM1_TB1=0 AND COM1_TB2=0 AND COM1_TB3=1))) then (PC1_PERMIT=0 AND FCL1_CLOSE_CMD=0)*
- ***Safety Integrity Level****: SIL2*
- ***Mode****: Low demand*

Repeat for the other eight power converters.