Functional Safety, Formal methods and Neural Networks at BE-ICS

Xaver Eugen Fink

Borja Fernández Adiego

On behalf of BE-ICS

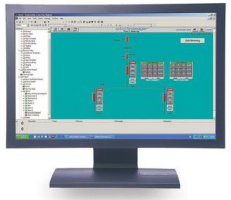
03/07/2023

BE-ICS in a nutshell

- "BE-ICS provides the **technology, frameworks, engineering** and CERN-wide **support** for systems and projects in all domains using standard **industrial control** solutions" https://be-dep-ics.web.cern.ch

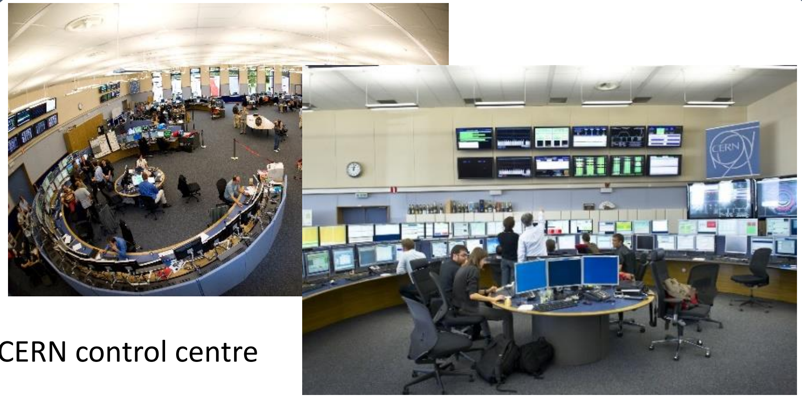
- BE-ICS is in charge of the design and development of industrial **control** and **safety** systems

WinCCOA

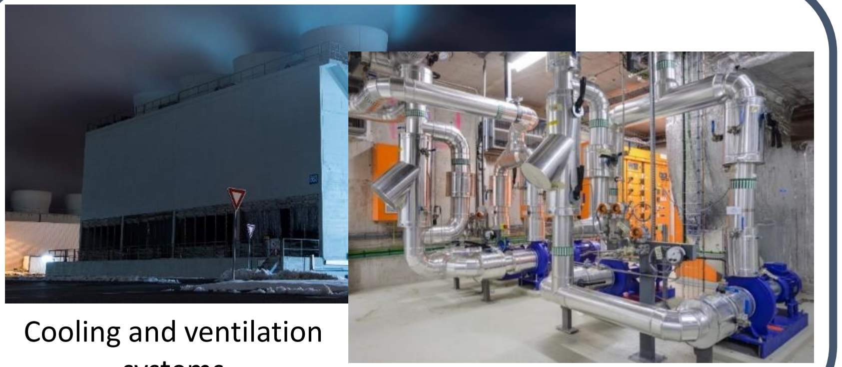


Industrial PCs (FEC)

Programmable Logic Controllers (PLC)



CERN control centre



Cooling and ventilation systems

Superconducting magnet test benches

Cryogenics plants

Images from cds.cern.ch

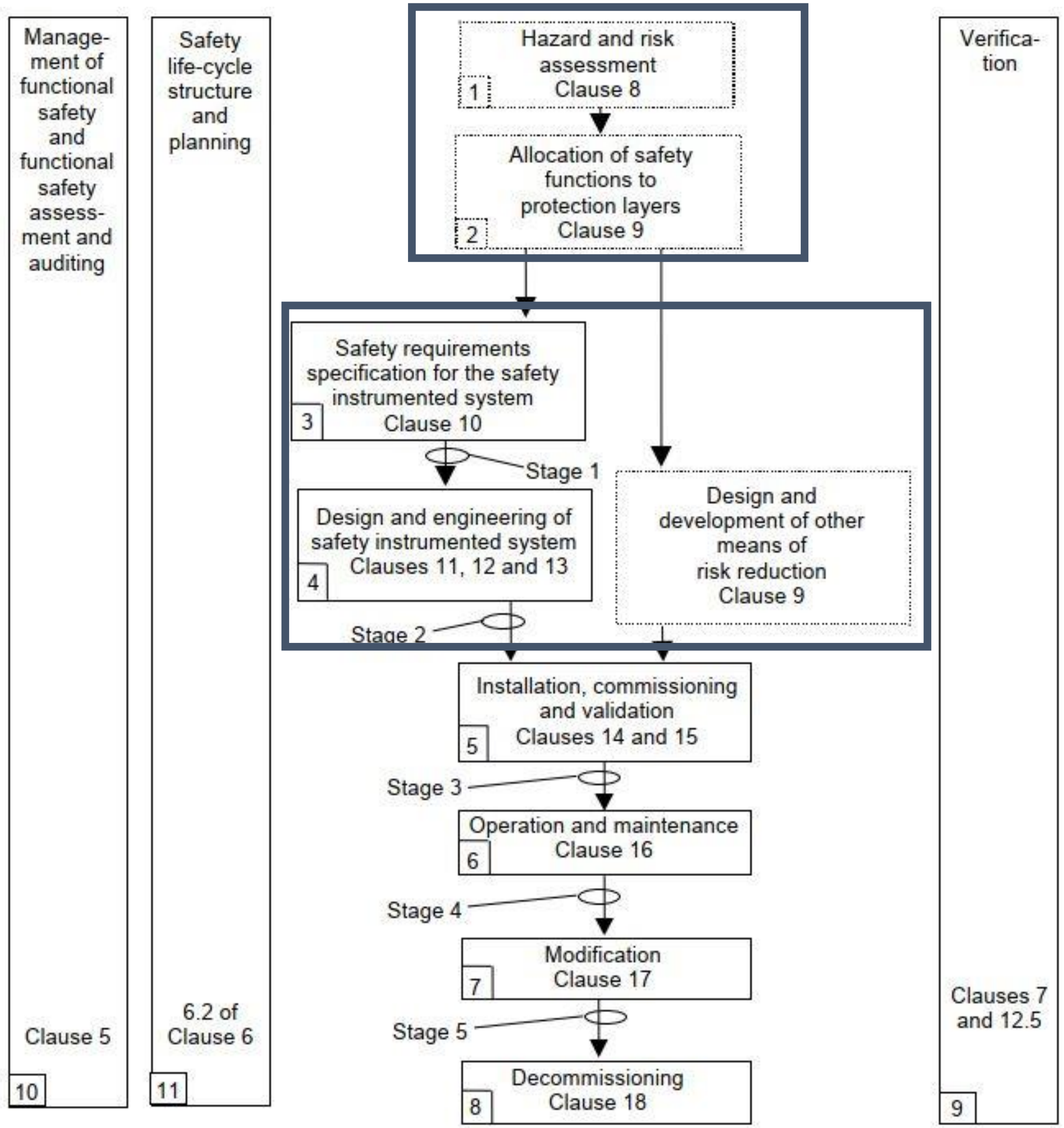
1. Functional Safety activities

- We apply the **Functional Safety standards** in our projects to protect the **personnel, the installations and the environment**
  - IEC 61508
  - **IEC 61511** (specific for the process industry)
  - IEC 62061

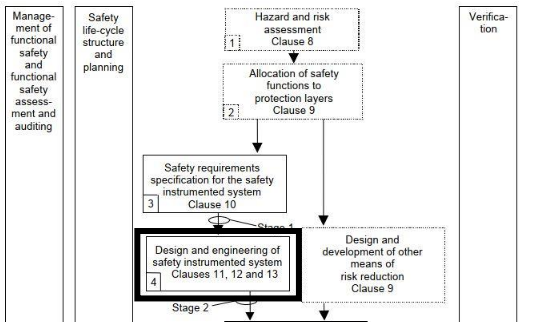
- We follow the **Safety Life Cycle**
  1. **Risk analysis and assessment**
  2. **Design and engineering** of the safety system
  3. Commissioning, operation and maintenance
  4. Planning, management and verification

- We use **SIL** (**Safety Integrity Level**)
  - It gives us the necessary **risk reduction**
  - And the **requirements to design and develop our safety system** (hardware, software, architecture, testing, etc.)

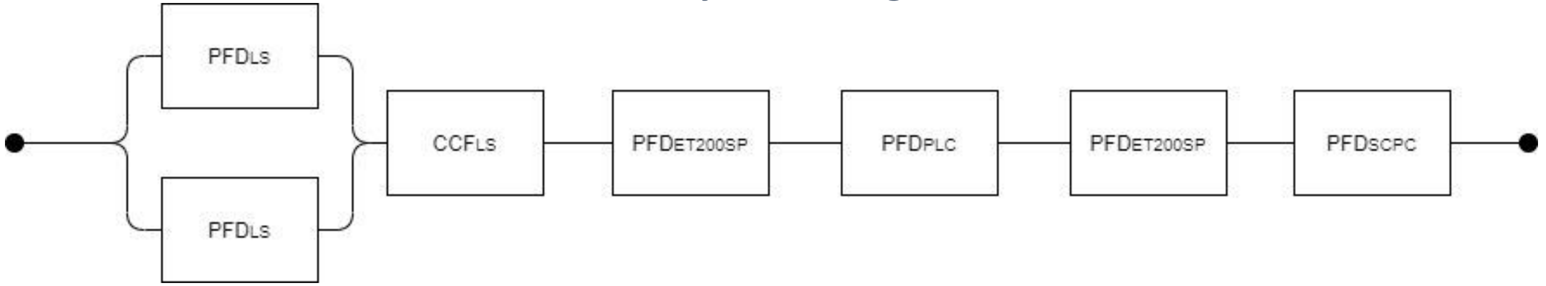
Risk assessment  SIL  SIS design



Safety Instrumented Systems design



Reliability block diagram



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

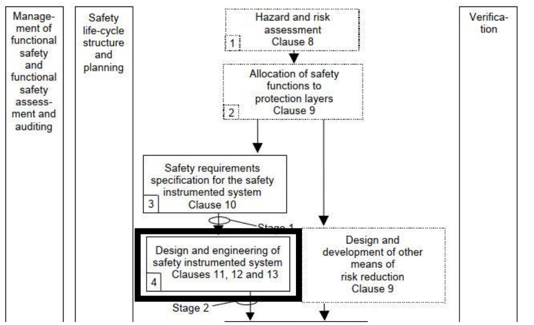
$$PFD_{avg} \approx PFD_{avg} + PFD_{avg} + PFD_{avg}$$

IEC 61508-6:2010 Annex B

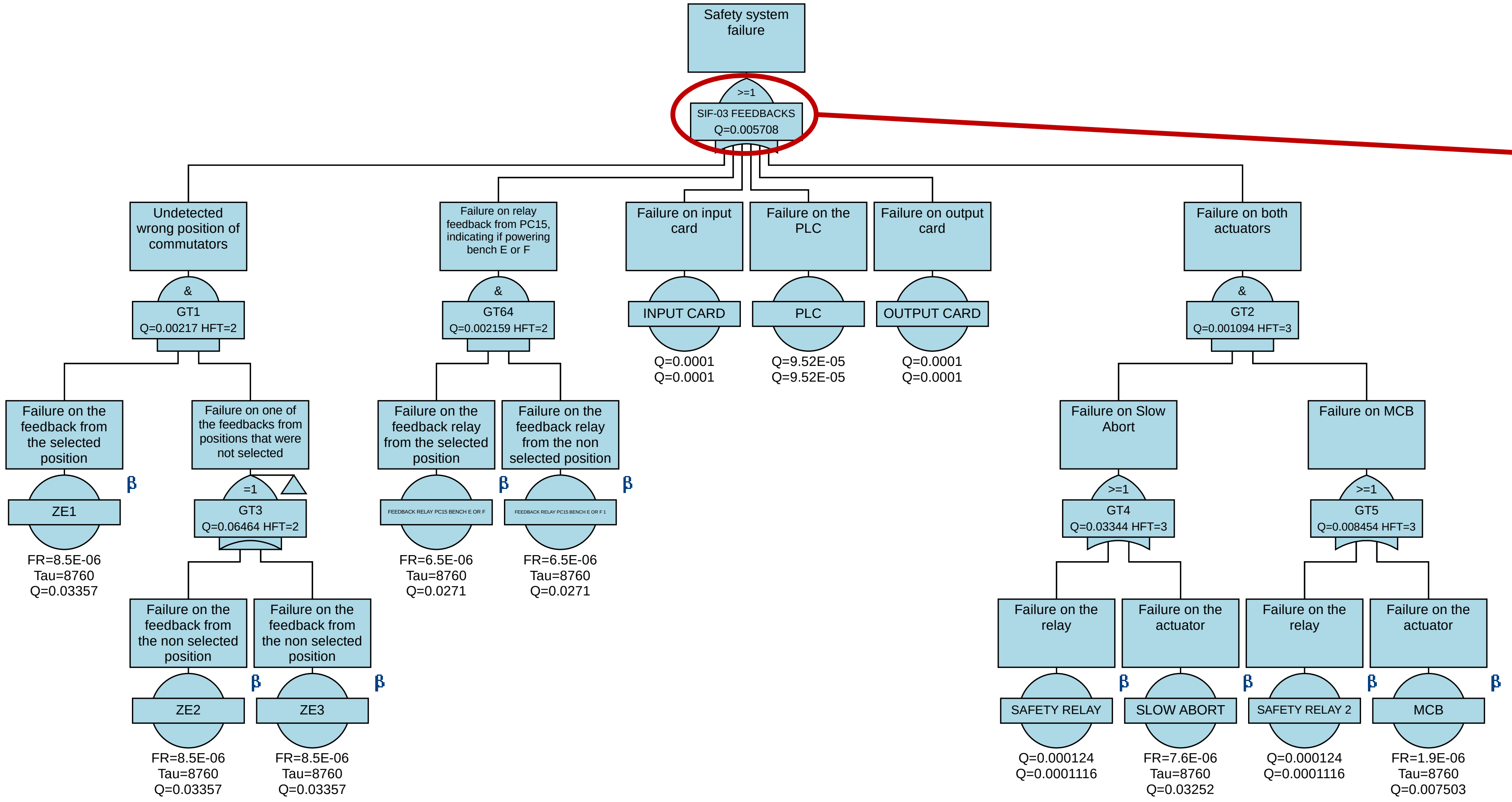
$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

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 $\leq 10^2$

Safety Instrumented Systems design



Reliability Block Diagram (RBD) or **Fault Tree Analysis (FTA)** for SIFs **– ISOGRAPH reliability workbench**



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 $< 10^{-1}$

Safety design: Hazard and risk assessment via LOPA

- **Risk assessment** methods

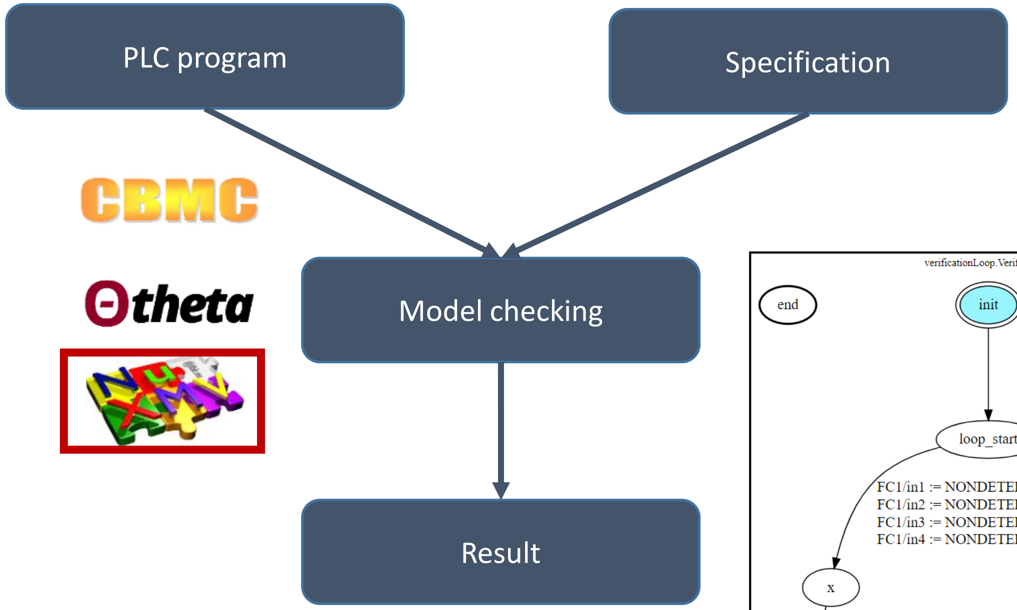
Layers of Protection Analysis (LOPA)
recommended by the IEC 61511-3

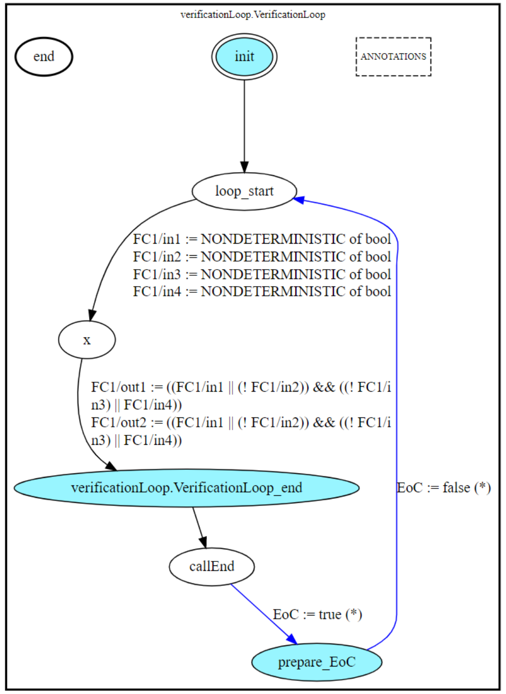
Impact Event		Initiating Cause 1	Initiating Cause 2	Initiating Cause 3	Initiating Cause 4		Initiating Cause 5		Initiating Cause 6			Initiating Cause 7
					Error measurement one CMCT component		rror measurement one Q45-D2 componen		Error measurement one Triplet-D1 component			
IP side Break Bellow		Upper FEC	Error in actuation path PXI - SAMbuCa	Error in actuation path Jack / UAP and motors	Rotational	Horizontal-Vertical	Vertical-Rotational	Horizontal	Vertical	Horizontal	Rotational	Operator mistake
	Event Frequency (1/h)	3.08E-05	3.10E-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	0.27	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	10
	PL2	10										10
	PL3	10	10	10		10		10		10		10
Operation Time		10	10	10	10	10	10	10	10	10	10	10
Procedures / Alarms												
Cybersecurity: TN + RBAC												0
Physical Limit Switches				0	0	10	0	10	10	10		0
Cumulative		10000	1000	1000	10	1000	10	1000	100	1000	100	10000
	Intermediate event frequency	0.000027	0.000271	0.00016153	0.0000999	0.0000010	0.00009986	0.00000100	0.00000999	0.00000100	0.00000999	0.00000001
	Weight over the overall frequency	3.96%	39.76%	23.66%	14.63%	0.15%	14.63%	0.15%	1.46%	0.15%	1.46%	0.00%
	Total mitigated event frequency						0.00068					
	Tolerable Event Frequency - LHC						0.01000					
	Tolerable Event Frequency - IP side						0.00250					
	Tolerable Event Frequency - Bellow						0.000119048					
	Residual Risk						0.00181738					

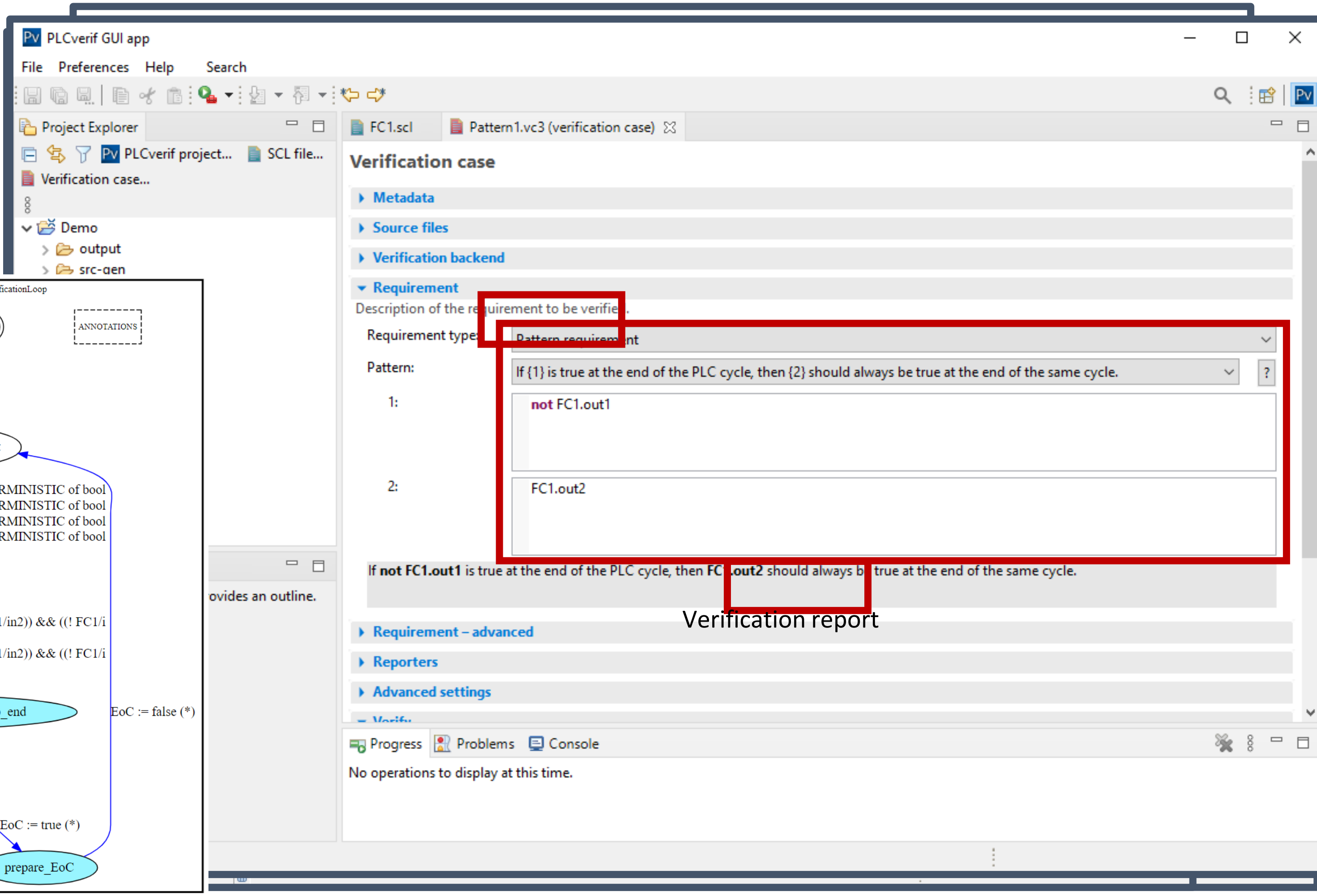
2. Formal method and verification for software

PLC verification framework PLCverif

- We apply formal methods and formal verification (e.g. **model checking**) to guarantee that **PLC programs are compliant with their specifications** (**PLCverif** tool)





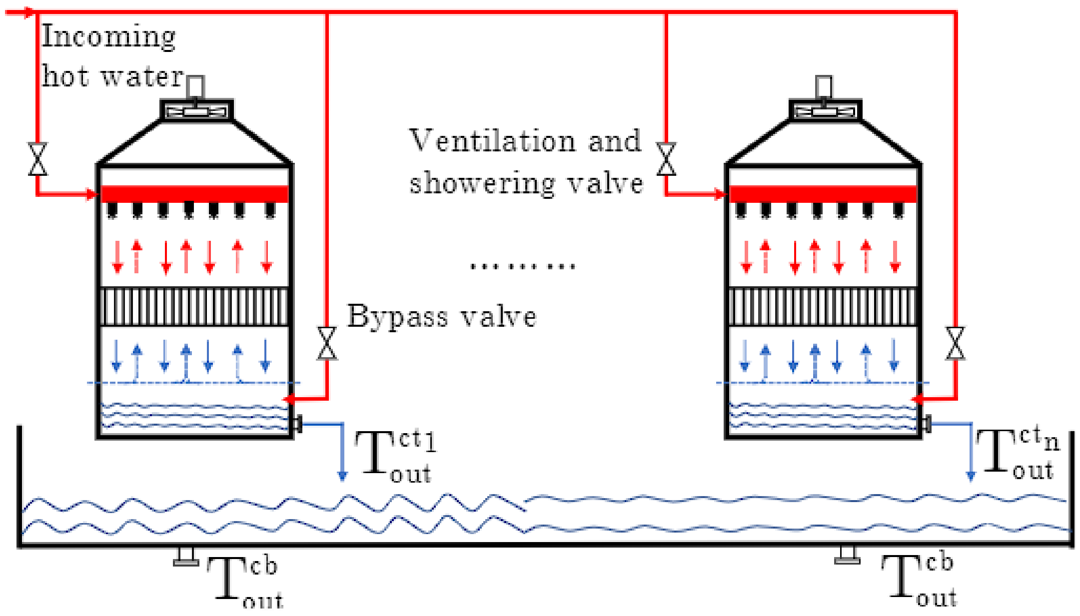


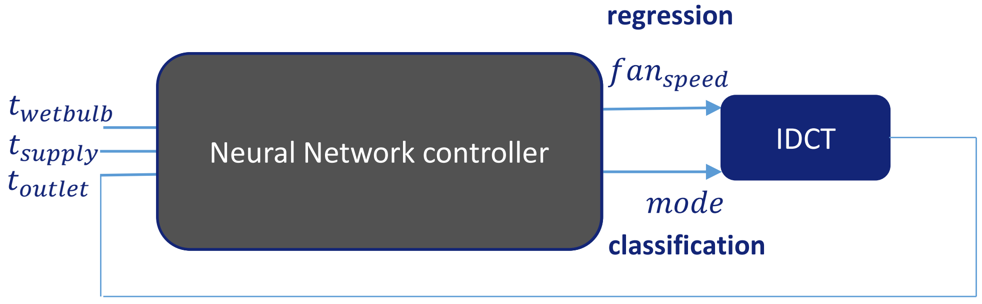
PLCverif references:
https://gitlab.com/plcverif-oss and
www.cern.ch/plcverif

3. Neural network controllers: Verification case study

LHC cooling towers control

- Induced draft cooling towers (IDCTs)
- **Provide cold water** for different LHC subsystems (e.g. cryogenics, chillers, air handling units, etc.)
- **Control actions:**
  - **Mode selection**:
    1. Ventilation
    2. Showering
    3. Bypass
  - **Fan speed**
- **Control objective**:
  - Keep **outlet water temperature within strict limits**
  - Utilize **minimum amount of energy**





Ghawash, F., Hovd, M., Schofield, B.: ***Model predictive control of induced draft cooling towers in a large scale cooling plant***. IFAC-PapersOnLine 55(7), 161–167 (2022) https://www.sciencedirect.com/science/article/pii/S2405896322008394

The idea was **replacing** the **MPC** by a **NN**

But the NN is NOT DEPLOYED YET!!

WORK IN PROGRESS

3. Neural network controllers: Verification case study

How to verify these properties?

Different methods were applied and compared:

1. **nnenum**: an open-source **NN verification** tool for **ReLU** NNs from Stony Brook University https://github.com/stanleybak/nnenum
2. **Z3**: an open-source **theorem prover** from Microsoft Research https://github.com/Z3Prover/z3
3. **PLCverif**: an open-source formal **verification tool for PLC programs** from CERN https://gitlab.com/plcverif-oss
4. **Testing:** traditional testing techniques

nnenum

Keras

NN design

Pv

PLC source code

Executable

*Ignacio D. Lopez-Miguel et al. "**Verification of Neural Networks Meets PLC Code: An LHC Cooling Tower Control System at CERN**". In EANN 2023: Engineering Applications of Neural Networks conference*
https://link.springer.com/chapter/10.1007/978-3-031-34204-2_35

Formal methods research activity – recent publications

Latest research activities (BE-ICS) related to **formal specifications** and **formal verification of Neural Networks**

- Extending the integration of **FRET** in **PLCverif**. *"Verifying PLC Programs via Monitors: Extending the Integration of FRET and PLCverif". X. Fink et al.* Paper accepted at the **NASA Formal Methods 2024** conference https://conf.researchr.org/home/nfm-2024

- Integration of a **new specification method/tool** called **FRET** in **PLCverif**. *"From Natural Language Requirements to the Verification of Programmable Logic Controllers: Integrating FRET into PLCverif". Z. Adam et al.* Paper accepted at the **NASA Formal Methods 2023** conference https://conf.researchr.org/home/nfm-2023

- Formal **verification of a Neural Network** running on a PLC. *"Verification of neural networks meets PLC code: An LHC cooling tower control system at CERN". I.D. Lopez et al.* Paper accepted at the **Engineering Applications and Advances of Artificial Intelligence 2023** conference https://eannconf.org/2023/