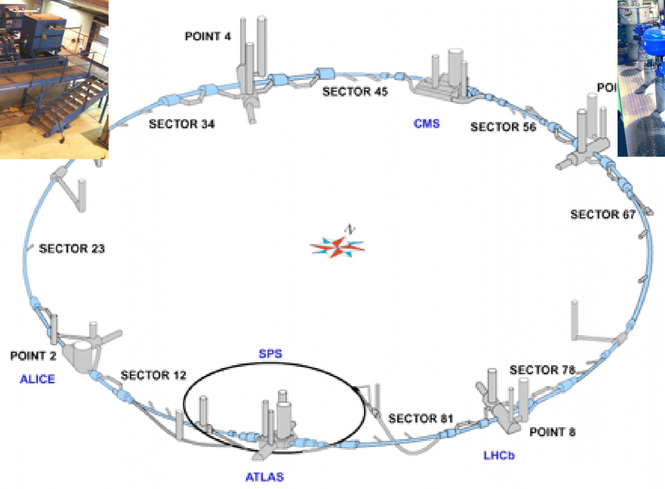
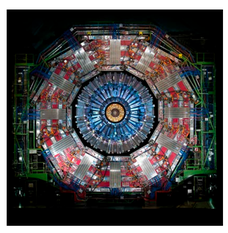
Automated Formal Verification for PLC Control Systems

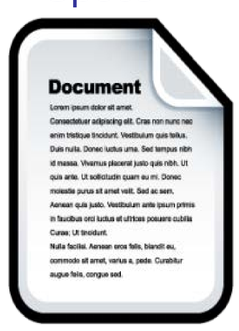




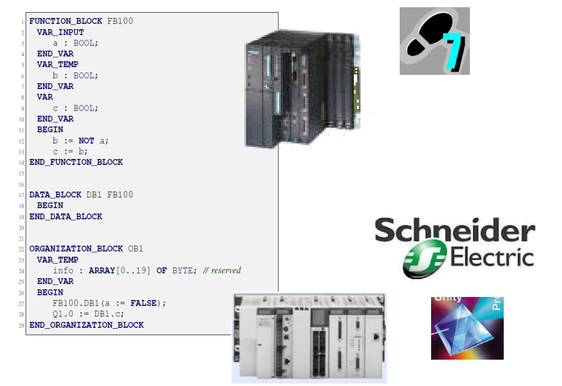
Many industrial process at **CERN** are controlled by Programmable Logic Controllers (**PLCs**): Cryogenics, Vacuum, Gas, C&V systems, etc.
The **UNICOS** framework is a standard for the Industrial Control System development.

How to develop **safe and robust** Control Systems, **guarantying** that the **PLC programs** fulfils the **specifications**?
Some standards, like **IEC 61508,** provide some guidelines, but how…

Specs



PLC code

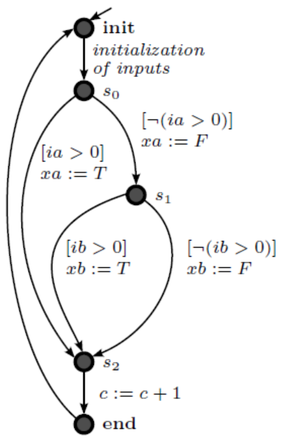


SIEMENS

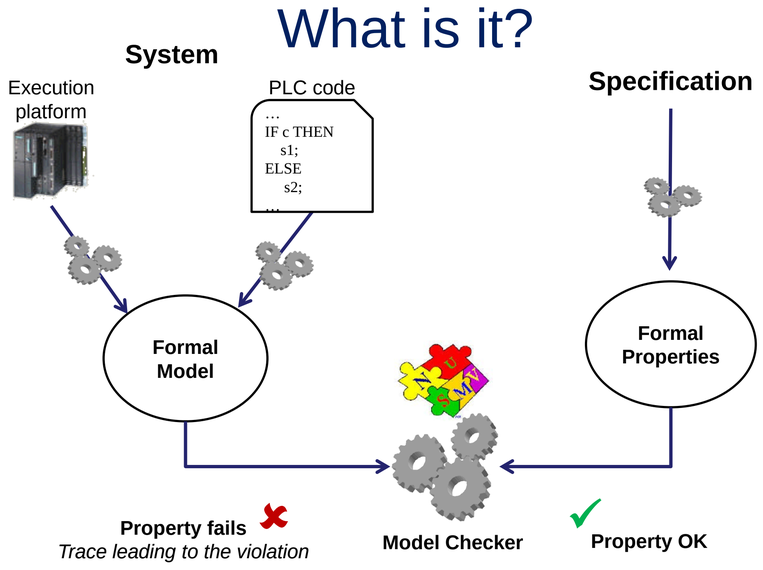
Schneider Electric

Formal Verification: Model Checking

Formal Models:
Petri Nets, **Automata**, etc.



What is it?



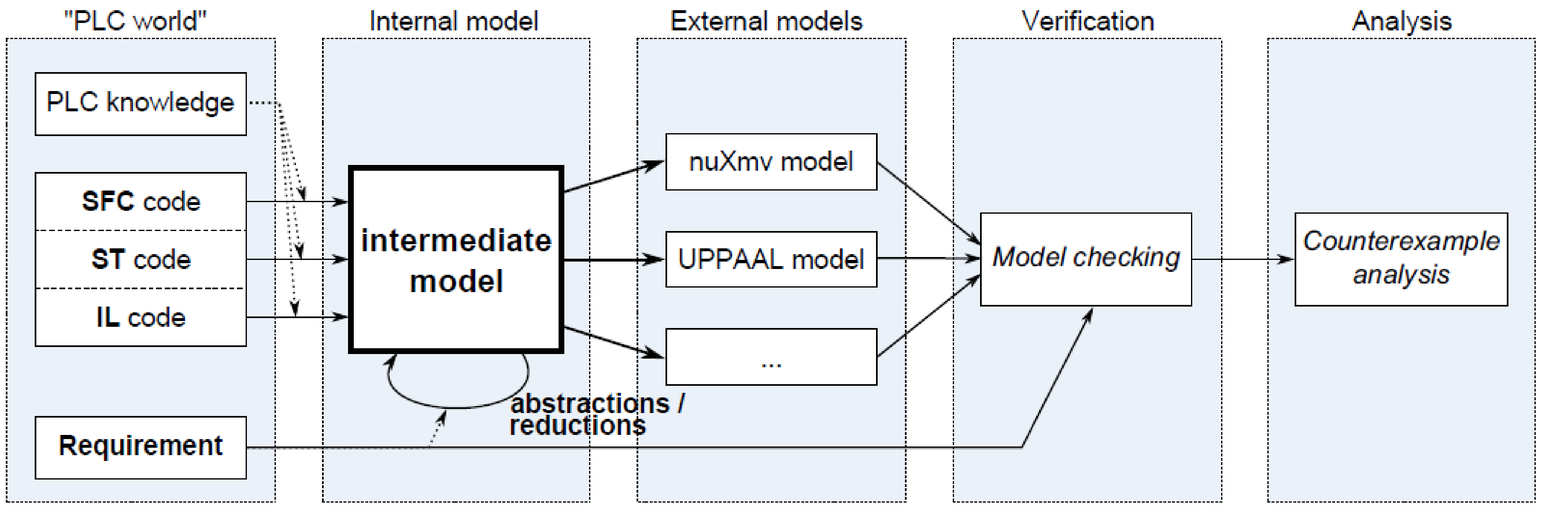
Formal Property specification:
Temporal Logic (LTL & CTL)

e.g. Real specification expressed in LTL.

G((PLC_END & FuStopI) -> ((PLC_END -> FuStopI) ***U*** (PLC_END & ! FuStopI & ((!AuOnR & !MOnR & !HOnR)-> !OutOnOV))));

Meaning:
"After falling edge on *FuStopISt*, the *OutOnOV* must remain *FALSE* if *AuOnR=FALSE* and *MOnR=FALSE*"

What are our **contributions**?



Contributions

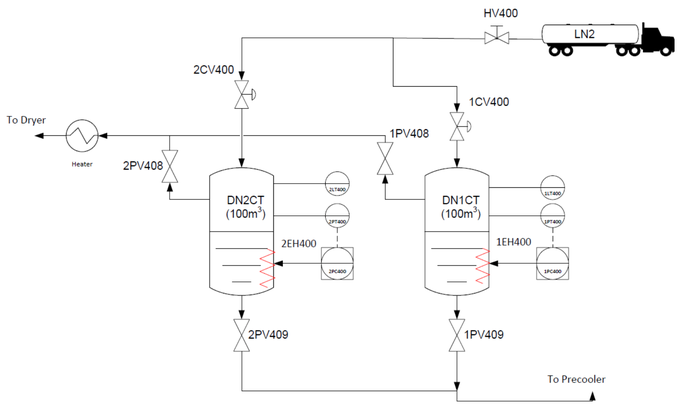
Design of a general methodology for applying automated formal verification of PLC programs.

- **Intermediate Model** based of automata.
- **Transformation rules** → Generation Tool.
- **Abstraction** techniques to reduce the state **space explosion** problem.
- Modeling the **timing aspects** of PLCs.

Results

- The methodology is applied to real control systems at CERN (e.g. **UNICOS** QSDN Cryo System).
- Bugs were found on **previously tested** systems.
- The methodology can be applied to **any PLC program** written in one of the languages defined in **IEC 61131-3** (IL, ST, etc.).
- 3 verification tools are currently integrated in the methodology: **nuXmv, UPPAAL and BIP**.

QSDN Cryogenic system



Metric	Non-reduced Model	Reduced Model	Abstract, reduced model*
PSS	10^{31985}	10^{5048}	$2.0 \cdot 10^{13}$ (RSS: $2.4 \cdot 10^{4}$)
Variables	31,402	3757	20
Generation	4.2 s	15.3 s	5.4 s
Verification	-	-	0.25 s

* Abstract reduced model obtained automatically using abstraction techniques based on a real safety requirement from the QSDN specification.

Borja Fernández Adiego
bfernand@cern.ch

Industrial Controls
Engineering Department

CERN EN Engineering Department