
CERN

Dániel Darvas (CERN / TU Budapest)

Quantitative and formal methods for the industrial control systems at CERN: dreams and reality

Formal Evaluation of Critical Infrastructures Seminar
06-09/12/2015, Dagstuhl

Contains joint work of B. Fernández, E. Blanco, S. Bliudze, J.O. Blech, J-C. Tournier, T. Bartha, A. Vörös, I. Majzik, R. Speroni, M. Lettrich, B. Bradu, Ph. Gayet

This presentation does not necessarily reflect the views of the CERN management.

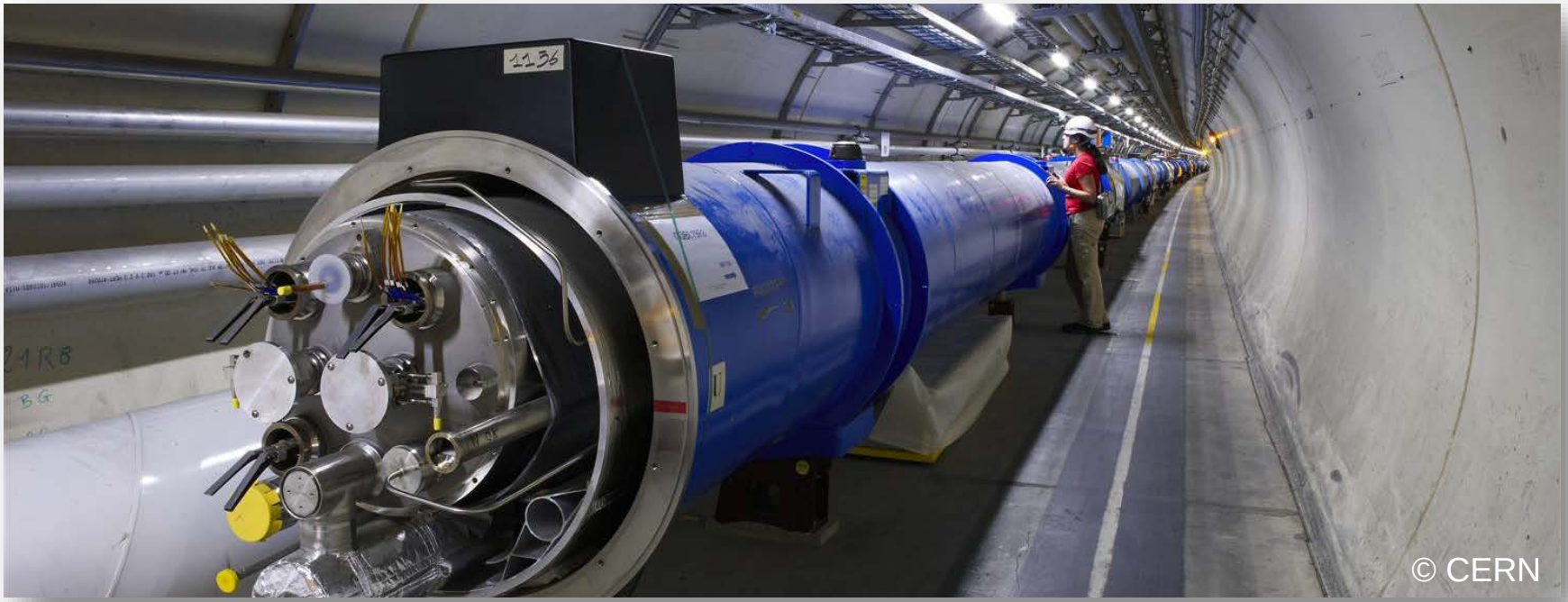
CERN

MŰEGYETEM 1782

http://go.cern.ch/**xt8F**

CERN *European Org. for Nuclear Research*

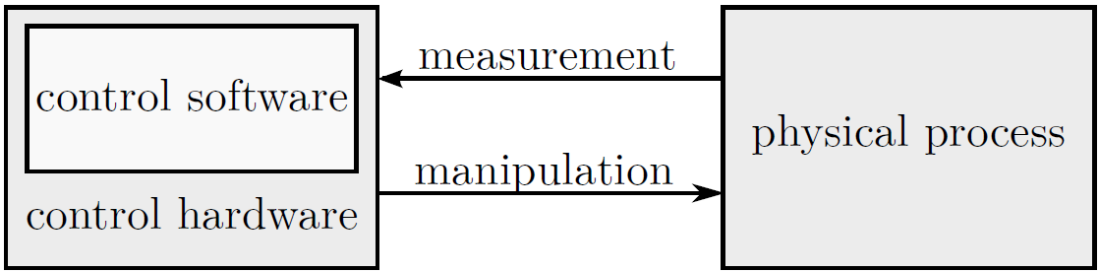
- Largest **particle physics laboratory**
- Large Hadron Collider (LHC)
  - Proton* beams with high energies



CERN

MŰEGYETEM 1782

Industrial control systems at CERN



- Wide **variety of systems** to control
  - Cooling and ventilation
  - Cryogenics (temperatures <100K) – superconducting magnets
  - Vacuum
  - Gas mixture

Implementation of industrial controls

- Programmable Logic Controllers
  - ***robust industrial computers***
  - Small computing capacity, **special programming languages**
- **Special, isolated domain**
- **1000+ PLCs** at CERN

Quantitative formal methods at CERN?

- We use **quantitative methods**
  - **Simulation** of dynamic models
  - → Correct functionality, optimal operation
- We (start to) use **formal methods**
  - **Model checking**, **formal specification**
  - → Correct functionality, safe operation
- **Quantitative formal methods**
  - Not (yet?)

Quantitative methods
for industrial control systems at CERN

*Contents courtesy of **B. Bradu** et al.*

Quantitative methods (QM)

Our way:

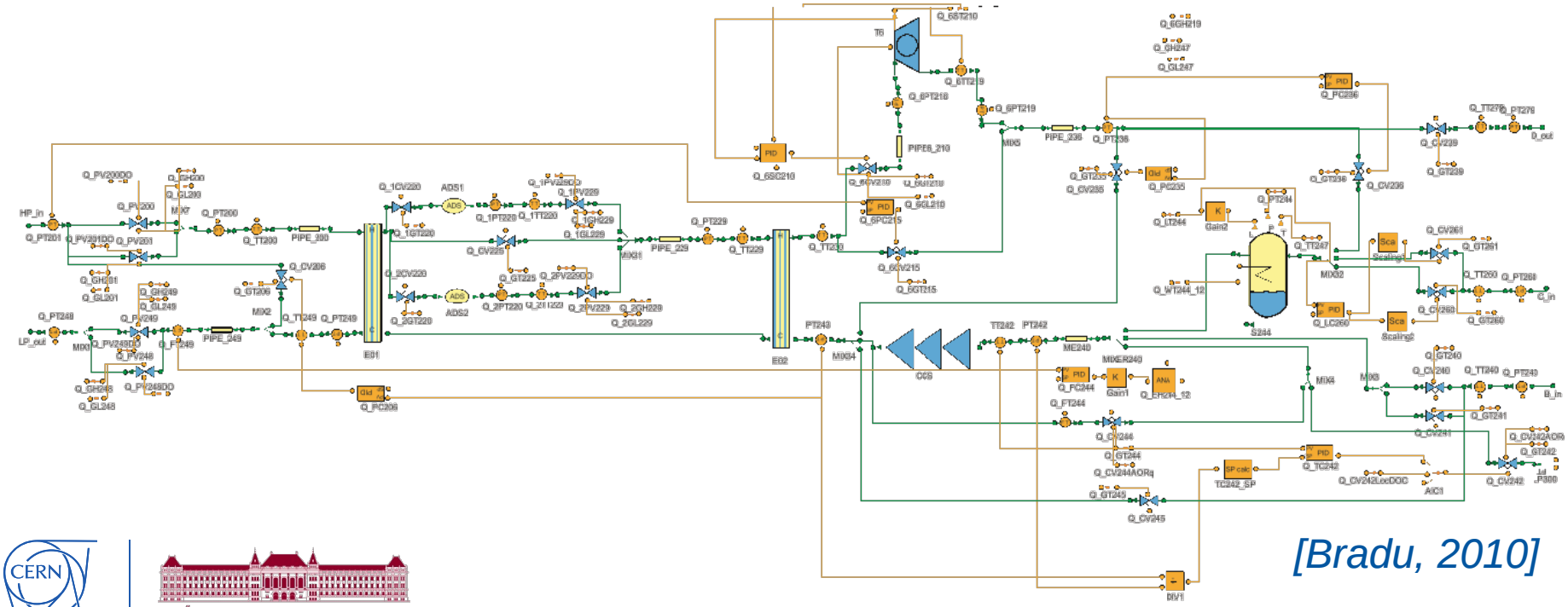
1. **Build a model** (plant + controller)
   With certain *speed*, *precision* and *validity range*

2. **Simulate the behaviour**
   For a certain scenario

QM: Plant modelling

- **Bottom-up** models based on **components**
  - The **structure of the plant** is known
  - The **behaviour of components** is known*

- **Amazingly accurate** results *(looking from IT world)*



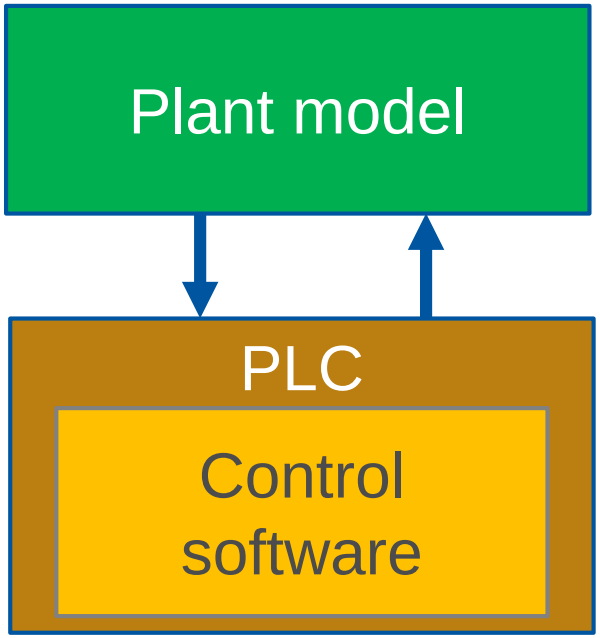
[Bradu, 2010]

QM: Controller modelling

Method A: **Simplified regulation loop** included in the model

Method B: **Reusing the real implementation**

- Also to **test the implementation**, train operators, …



QM: Simulation

- = Solving thousands of differential equations

- **Difficult task**
  - ~1..10× speed for cryogenics
  - ~10..100× speed for ventillation

Usage of **quantitative formal methods:** could be **AWESOME**, but **extremely challenging**.

- *Can the temperature be always kept under 2.5 K assuming certain conditions/range?*
- No solution yet.

Formal methods
for industrial control systems at CERN

V&V-related methods for ICS at CERN

Non-formal verification:

- Integration/acceptance testing – in use
- Virtual commissioning – in use
- Static code analysis – missing, to do!
- Unit testing – missing

Formal methods (work in progress)**:**

- **Model checking**
- **Formal specification**

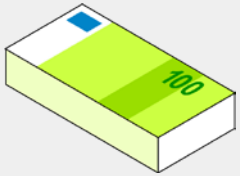
Not widely used in industry yet.

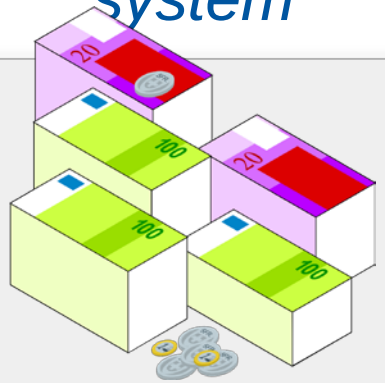
Our systems vs. “famous success stories”

LHC cryogenics control

Flight control system

“Cost of failure”





V&V

?

modelling

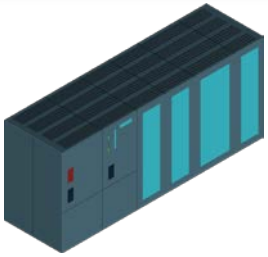
generators

certified code

(semi-)formal specification

theorem proving

model checking

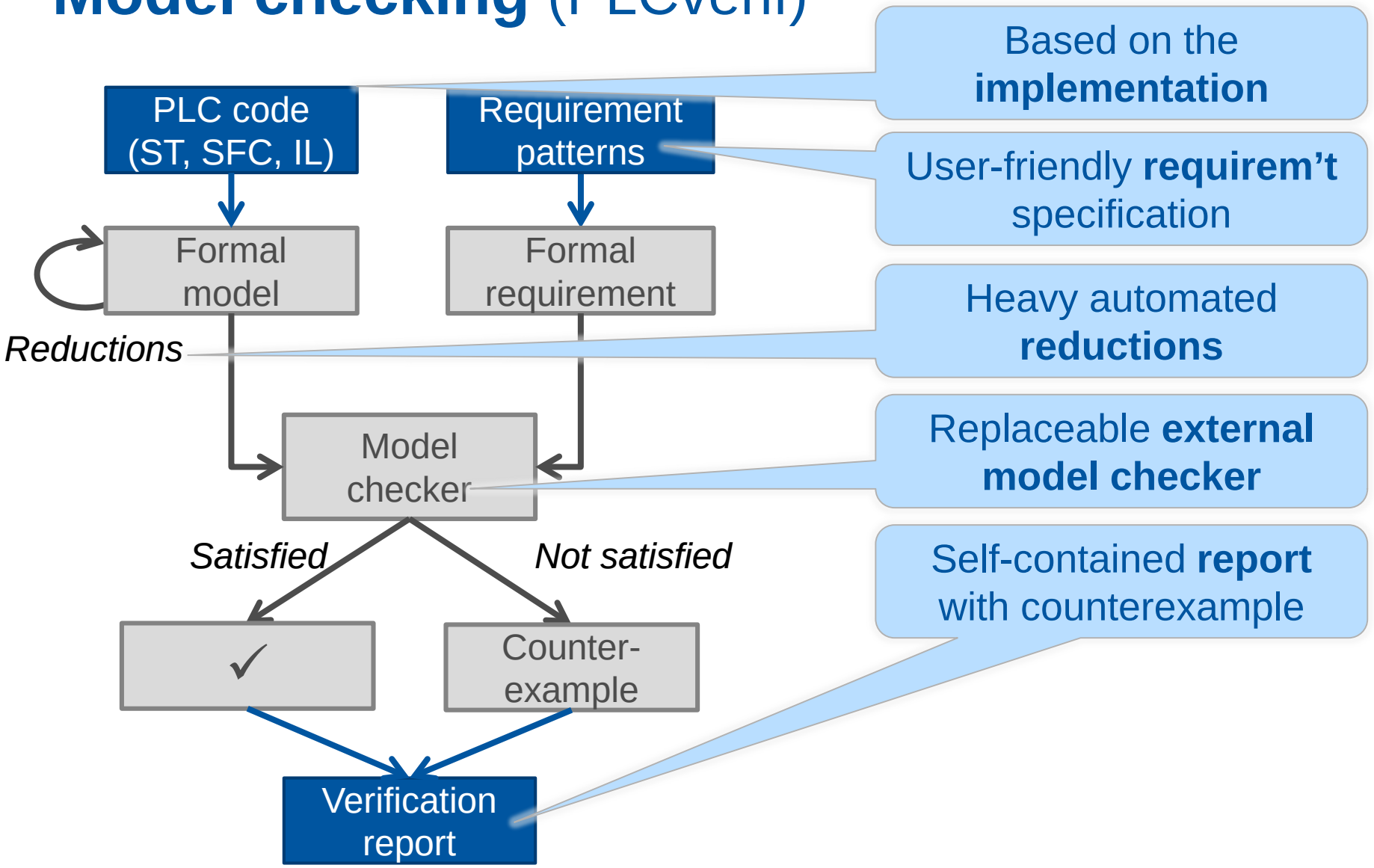


Lightweight
methods are needed.

This possibly implies
domain-specific methods.

Tool support is crucial.

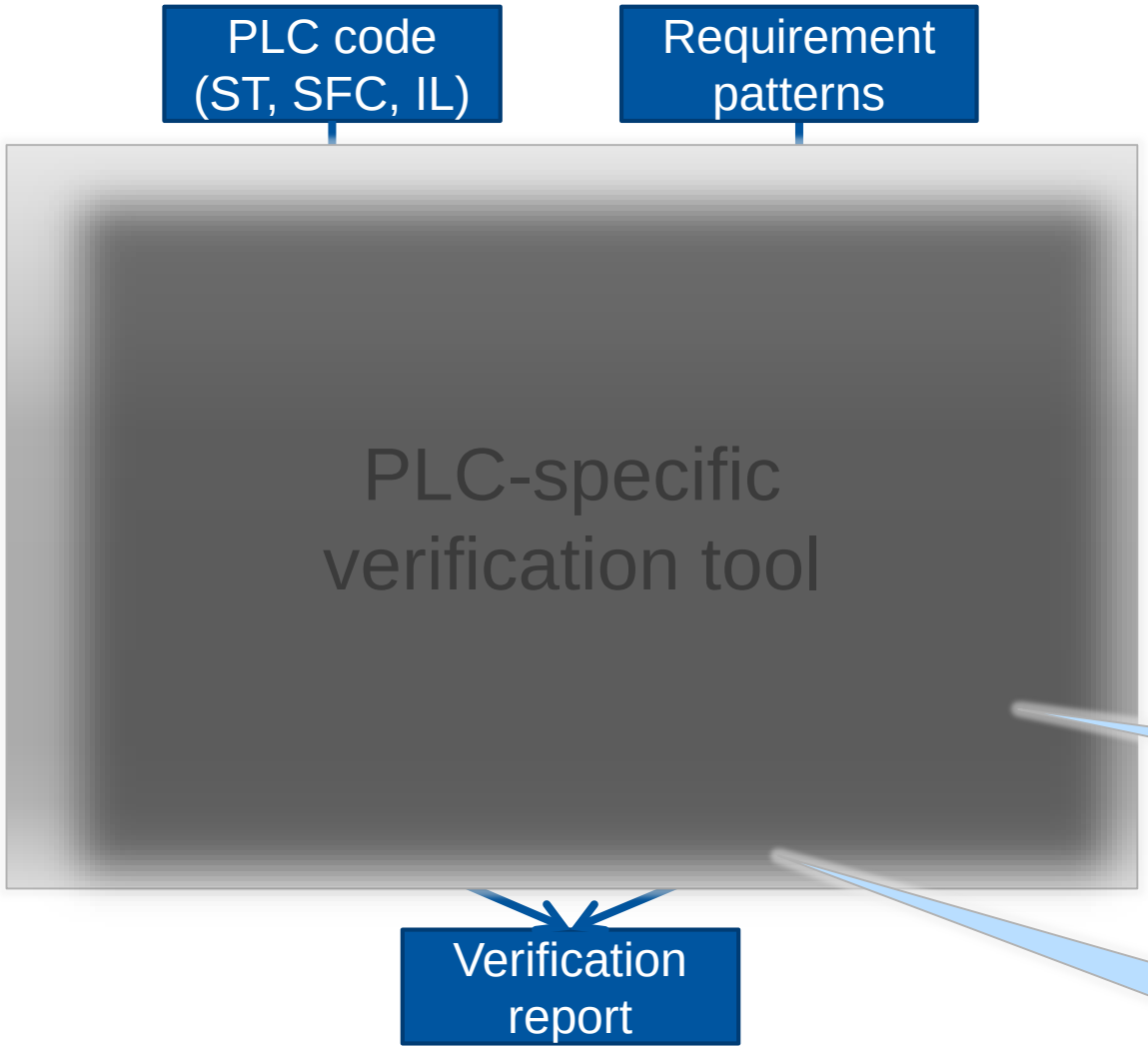
Model checking (PLCverif)



CERN

MŰEGYETEM 1782

Model checking (PLCverif)



Based on the **implementation**

User-friendly **requirem't** specification

Heavy automated **reductions**

Replaceable **external model checker**

Self-contained **report** with counterexample

Tool hiding the formal details

Jenkins-based continuous verification

CERN

MŰEGYETEM 1782

Formal specification

- **Goals**:
  - Provide **unambiguous**, **consistent** requirements
  - Help the **formal verification** and **re-engineering**

- **Lightweight** method: easy to introduce, adapted to the available **knowledge**

- **Domain-specific**

PLCspecif: example

ExampleModule

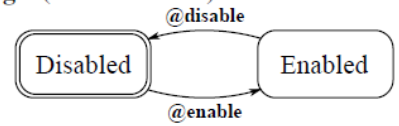
Assigned inputs:
- ValueReq : INT16
- EnableReq_fromLogic : BOOL
- EnableReq_fromScada : BOOL
- EnableReq_fromField : BOOL
- DisableReq : BOOL
- PMin : INT16 param
- PMax : INT16 param

Assigned outputs:
- Value : INT16
- Status : BOOL

Input definitions: — (none)

Event definitions:
- @disable ⇐ `rising_edge`(DisableReq) (`pri`=1)
- @enable ⇐ EnableReq_fromLogic OR EnableReq_fromScada OR EnableReq_fromField (`pri`=2)

Core logic (state machine)



Output definitions:
- _Value =

`ValueReq` < `PMin`	`ValueReq` > `PMax`	result
T	·	`PMin`
F	T	`PMax`
F	F	`ValueReq`

- Value =

`in_state`(Enabled)	result
T	`_Value`
F	0

- Status = `in_state`(Enabled)

Invariant properties:
- ALWAYS *PMin* ≤ *Value* ≤ *PMax* ASSUMING *PMin* ≤ *PMax*

Detailed behaviour specification

Structured, **hierarchical**

Separation of concerns

Domain-specific semantics

Unifies different semi-formal formalisms

Supports **verification**

CERN

MŰEGYETEM 1782

PLCspecif: expected benefits

- Helps **understanding**, thus the development
- **Code generation**
- Base for **verification**
- Conformance checking: helps **verification, re-engineering**, …
  - Specification-specification
  - Specification-code (legacy / manually modified / …)

Summary

- **Quantitative methods** regularly applied, but challenging
- **Formal methods** successfully applied to some industrial control systems
  - **Complements** simulation and testing
  - Successful applications – E.g. safety system of the cryogenics testing hall
- **No quantitative formal** methods (yet)

Main principles for formal methods:

- **Lightweight**
- **Domain-specific**
- Adapted to CERN's special needs to some extent

CERN

MŰEGYETEM 1782

http://go.cern.ch/**xt8F**

For more information…

- Project website (with publication list)
  http://cern.ch/project-plc-formalmethods/
- PLCverif tool's website
  http://cern.ch/plcverif
- PLCspecif's website
  http://cern.ch/plcspecif
- CERN website – http://home.cern

- **Contact me**
  daniel.darvas@cern.ch
  http://cern.ch/ddarvas

Simulation at CERN

- B. Bradu et al. **A process and control simulator for large scale cryogenic plants.** Control Engineering Practice, 17(12), pp. 1388-1397, 2009. https://hal-supelec.archives-ouvertes.fr/hal-00446033/document
- B. Bradu et al. **Modeling of the very low pressure helium flow in the LHC Cryogenic Distribution Line after a quench.** Cryogenics, 50, pp. 71-77, 2010. https://hal-supelec.archives-ouvertes.fr/hal-00452782/document
- B. Bradu et al. **CRYOLIB: a commercial library for modelling and simulation of cryogenic processes with EcosimPro.** Proc. of 24th Int. Cryogenic Engineering Conf., 2012. http://bbradu.web.cern.ch/bbradu/pdf/ICEC24_Bradu_Cryogenic_library2.pdf
- B. Bradu et al. **Example of cryogenic process simulation using EcosimPro: LHC beam screen cooling circuits.** Cryogenics, 53, pp. 45-50, 2013. http://bbradu.web.cern.ch/bbradu/pdf/Beam_screens_simulation.pdf
- Homepage of B. Bradu: http://bbradu.web.cern.ch/bbradu/cv.php

Model checking at CERN

- D. Darvas et al. **Formal verification of complex properties on PLC programs**. Formal Techniques for Distributed Objects, Components, and Systems (LNCS 8461), pp. 284-299, Springer, 2014.
- B. Fernández et al. **Bringing automated model checking to PLC program development – A CERN case study**. Proc. of the 12th Int. Workshop on Discrete Event Systems, pp. 394-399, 2014.
- D. Darvas et al. **PLCverif: A tool to verify PLC programs based on model checking techniques.** Proc. of the 15th Int. Conf. on Accelerator & Large Experimental Physics Control Systems, 2015. In press. http://icalepcs.synchrotron.org.au/papers/wepgf092.pdf
- B. Fernández et al. **Applying model checking to industrial-sized PLC programs.** IEEE Transactions on Industrial Informatics, 2015. In press, available on-line. http://dx.doi.org/10.1109/TII.2015.2489184

Formal specification at CERN

- D. Darvas et al. **Requirements towards a formal specification language for PLCs.** 2014. DOI: 10.5281/zenodo.14907
- D. Darvas et al. **A formal specification method for PLC-based applications.** Proc. of the 15th Int. Conf. on Accelerator & Large Experimental Physics Control Systems, 2015. In press. http://icalepcs.synchrotron.org.au/papers/wepgf091.pdf
- D. Darvas et al. **Syntax and semantics of PLCspecif.** CERN Report, EDMS 1523877, 2015. https://edms.cern.ch/document/1523877

www.cern.ch