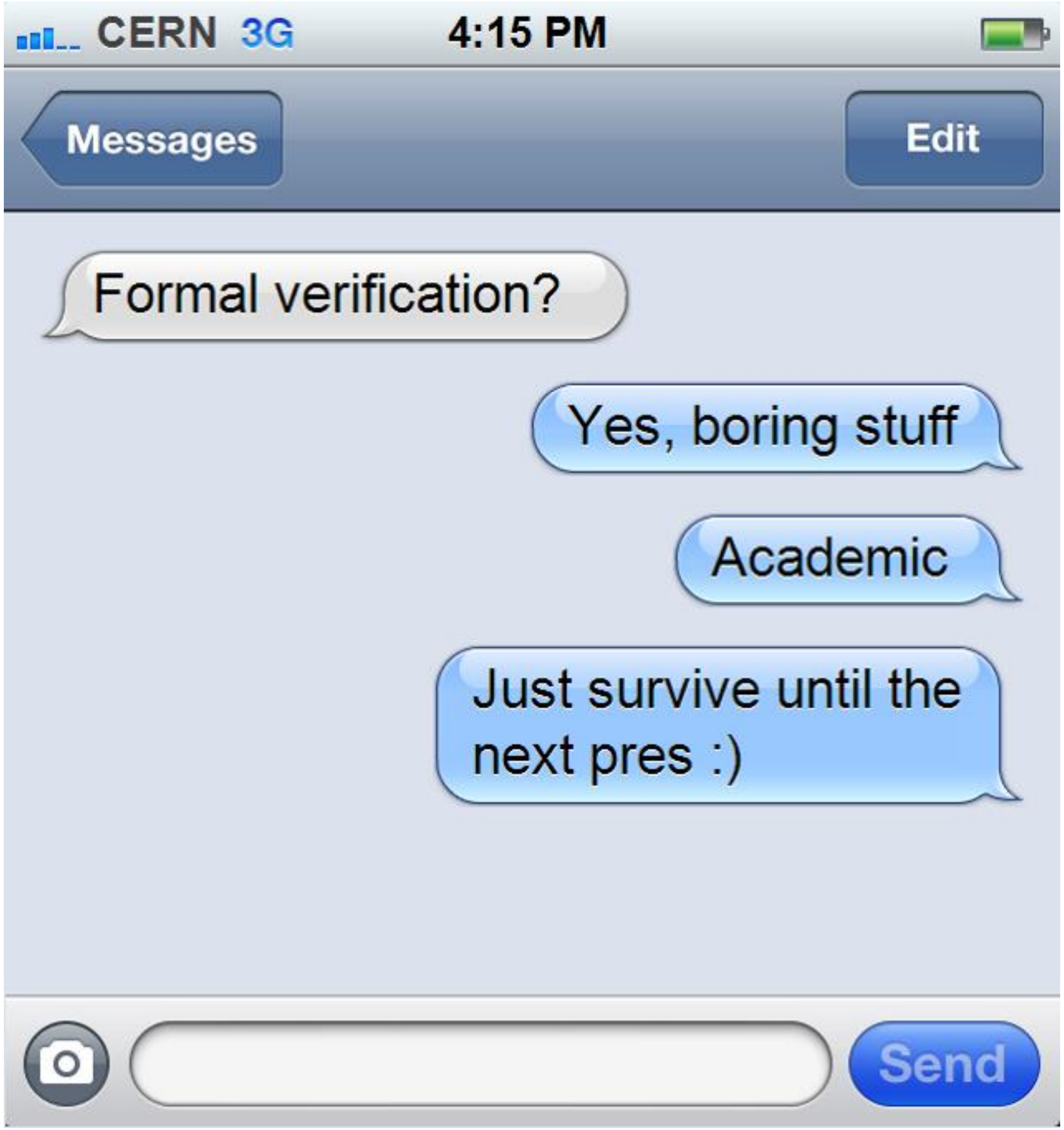
CERN

Dániel Darvas (BE-ICS-PCS)

Formal verification of industrial control systems

3th Workshop on PLC/COTS-based Interlock and Protection Systems
02/02/2016, CERN

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



Formal verification?

Yes, boring stuff

Academic

Just survive until the next pres :)

Source: http://www.iphonetextgenerator.com/

Context – CERN

- PLCs for controlling **vacuum**, **cryogenics, CV**, etc. systems + **safety** systems
- Failures might have *negative impact*
- **Increasing complexity** without **decreasing quality**?

© CERN

Context – PLCs at CERN

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

Goal

- To **improve the quality** by eliminating bugs
  - Complementing automated and manual testing

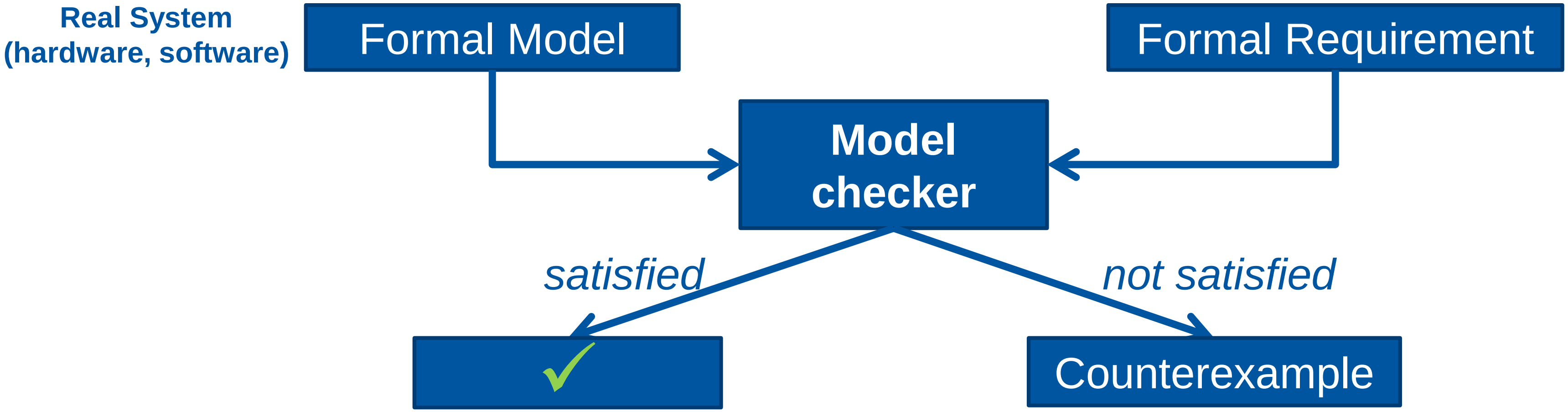
- **Model checking** to find **“high quality” bugs**

- **Integrating** formal verification to the development process

What is formal verification?

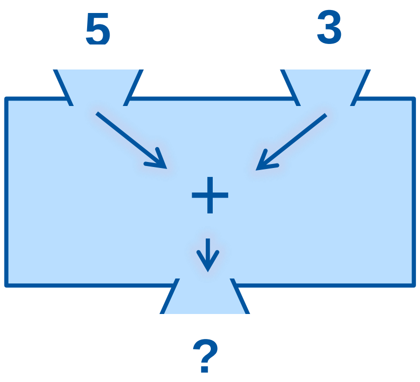
- **Formal verification**: mathematically sound methods to check properties of specifications / implementations / …

- **Model checking**
  - **Automated** formal verification method
  - Checks **all possible executions** (contrarily to testing)
  - Goal: prove correctness OR **find hidden/rare problems**



Testing vs. model checking

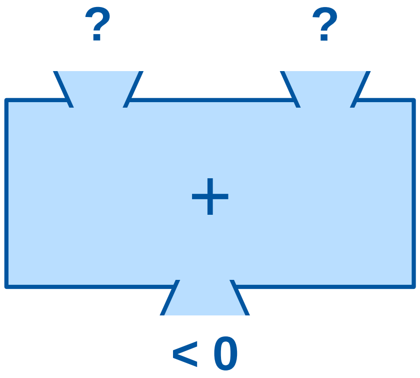
Testing



`add(5,3)=8 ?`

- **Inputs are known**, outputs are checked

Model checking



`add(…,…)<0 ?`

- E.g. the possibility of an **output combination** is checked.
- **Temporal expressions** are possible

Usage of formal verification

- Used both in **industry** and **academia**
  - Typically when the *cost of failure is high*

- Formal verification for **PLCs**
  - Mostly in academic environment
  - Not widely spread yet in industry – **too difficult**!

The presented logos are trademarks of the corresponding companies and their usage is nominative fair use. None of the companies endorse or support the presented work.

Main challenges of model checking

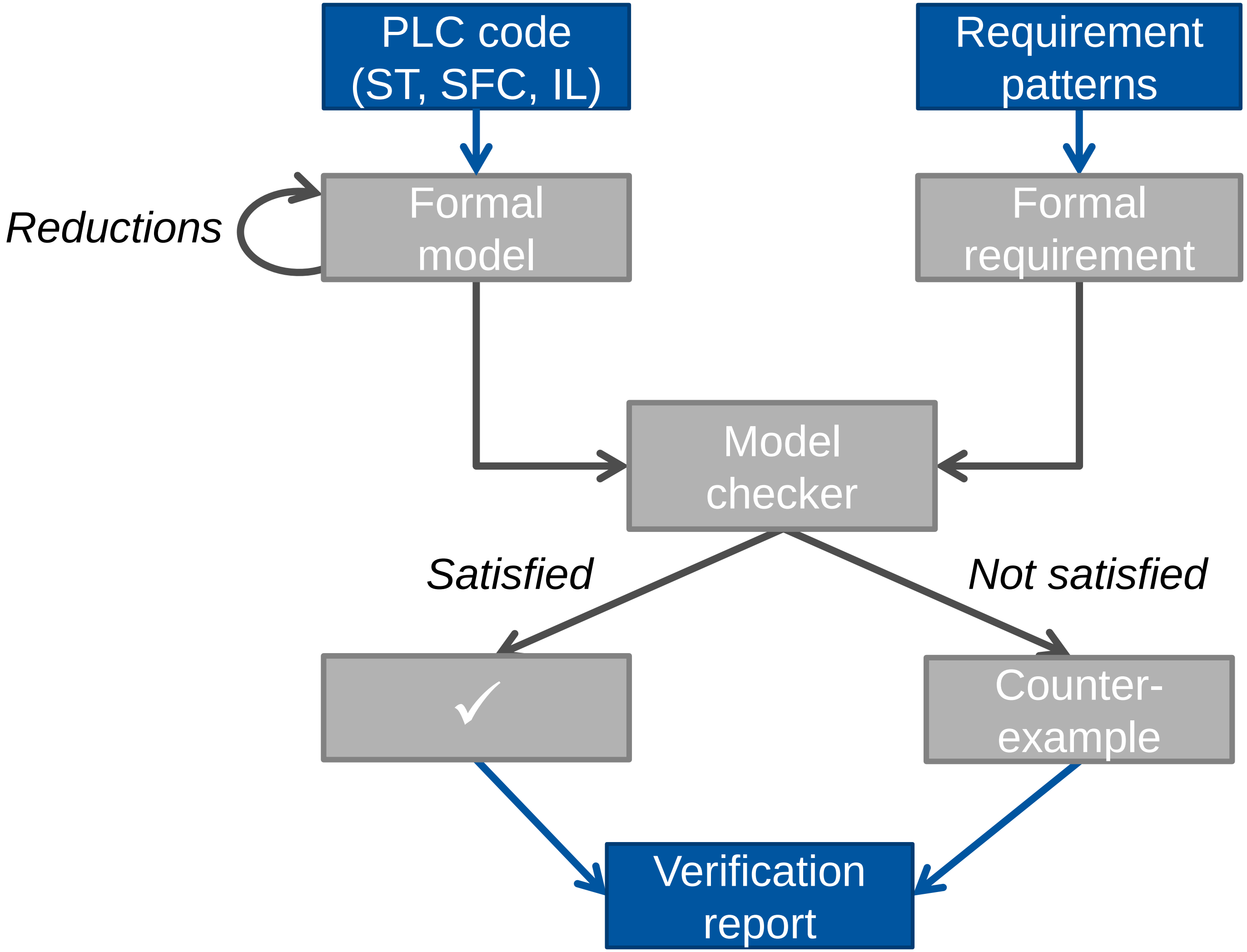
- **Formalization**
  - … of source code
  - … of requirements

- **Performance**

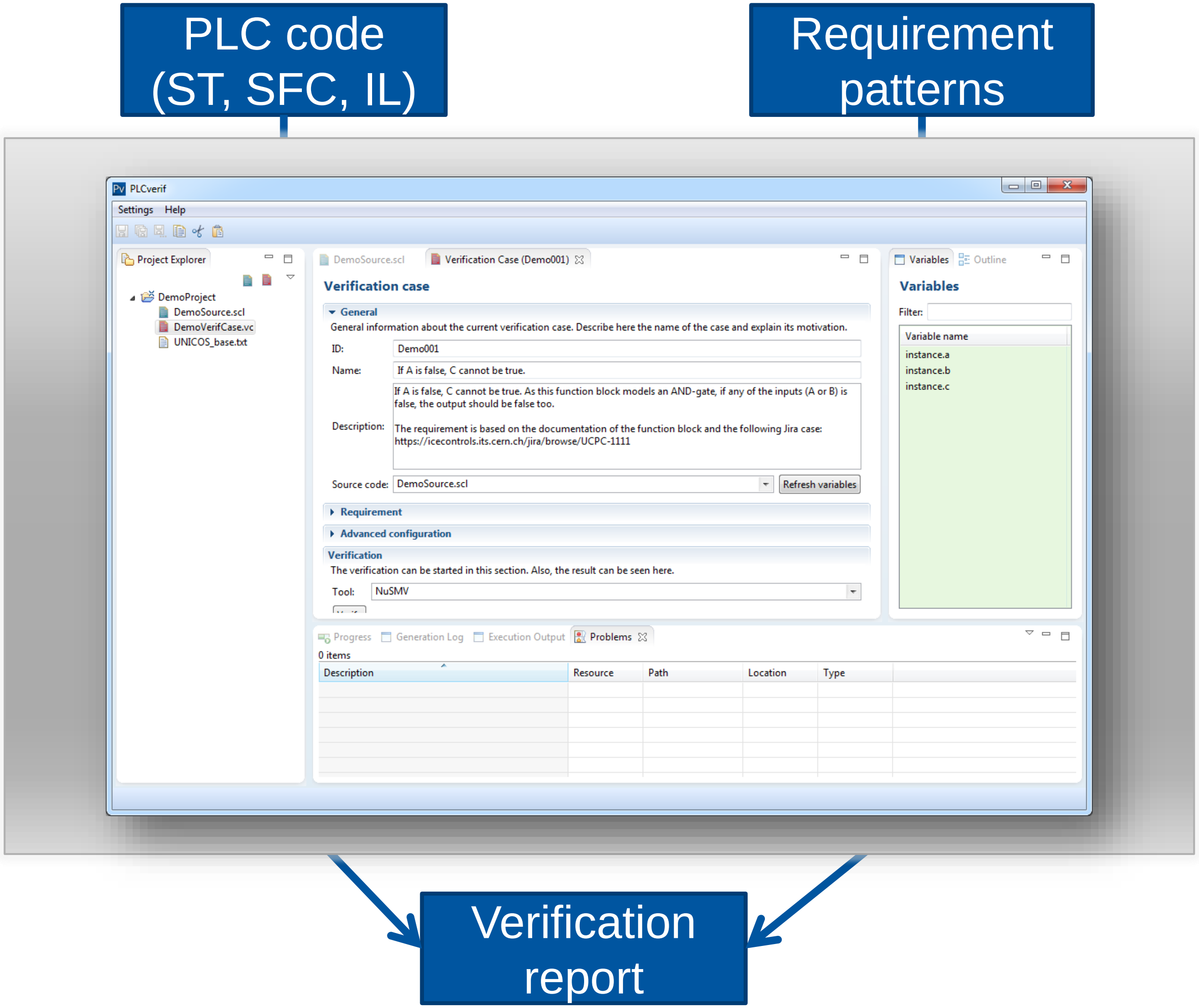
- Making it **accessible to the developers**

(No general solution to date.)

Model checking (extended workflow for PLCs)



Model checking (extended workflow for PLCs)



PLC code (ST, SFC, IL)

Requirement patterns

Verification report

Verification case

General

General information about the current verification case. Describe here the name of the case and explain its motivation.

ID: Demo001

Name: If A is false, C cannot be true.

Description: If A is false, C cannot be true. As this function block models an AND-gate, if any of the inputs (A or B) is false, the output should be false too.

The requirement is based on the documentation of the function block and the following Jira case: https://icecontrols.its.cern.ch/jira/browse/UCPC-1111

Source code: DemoSource.scl

Requirement

Advanced configuration

Verification

The verification can be started in this section. Also, the result can be seen here.

Tool: NuSMV

Variables

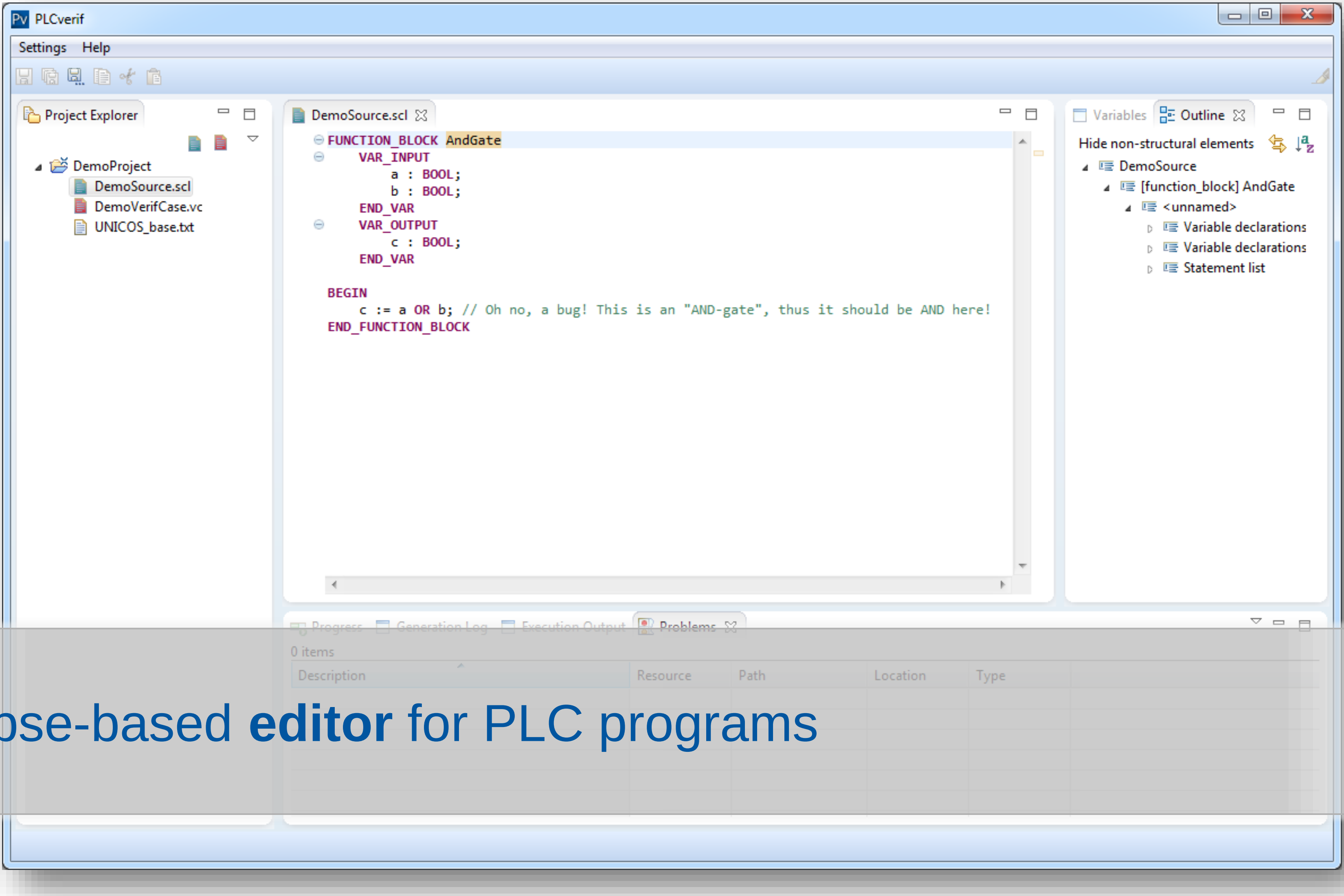
Filter:

Variable name
instance.a
instance.b
instance.c

0 items

Description	Resource	Path	Location	Type

The PLCverif tool

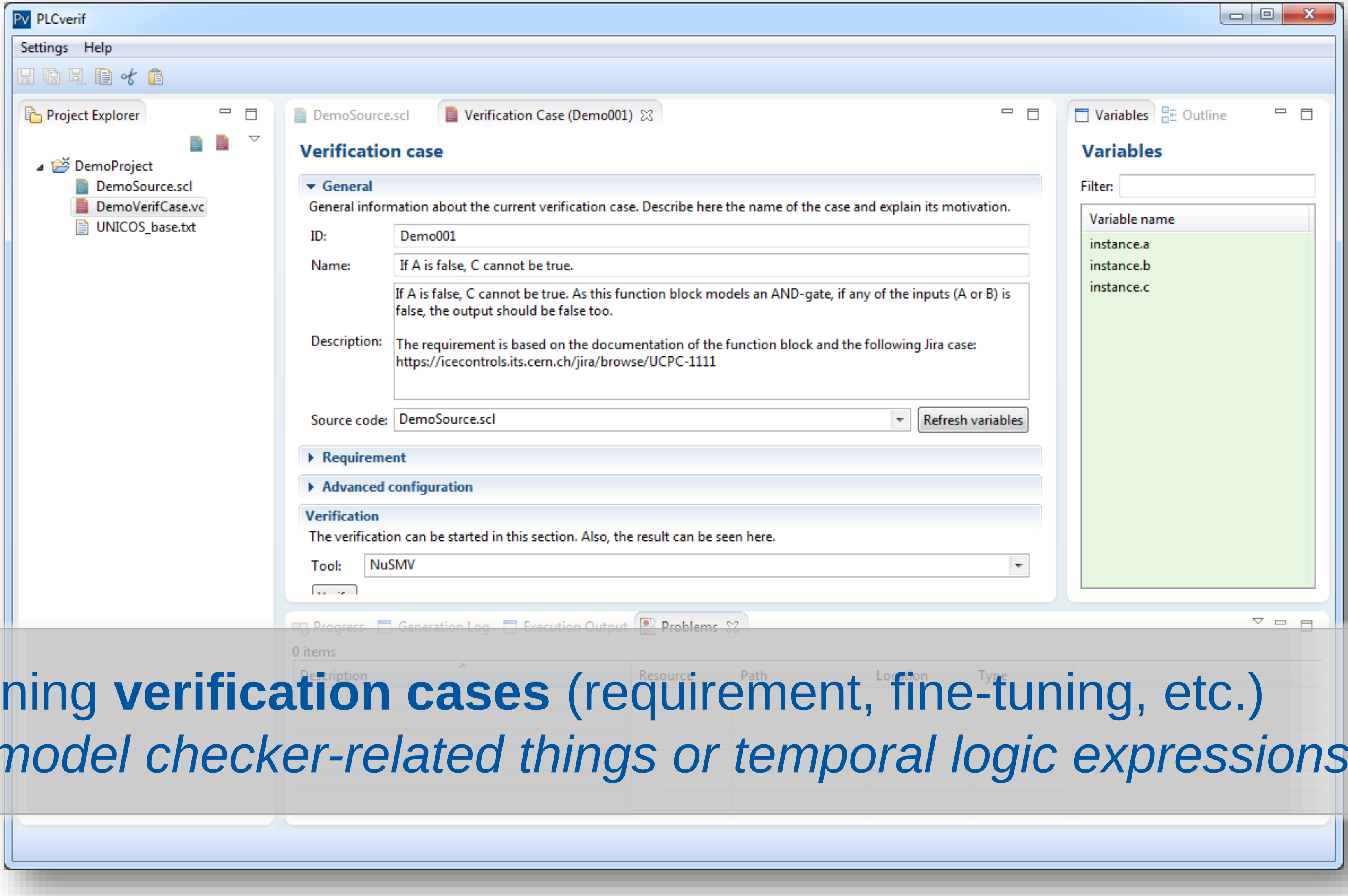


```
FUNCTION_BLOCK AndGate
    VAR_INPUT
        a : BOOL;
        b : BOOL;
    END_VAR
    VAR_OUTPUT
        c : BOOL;
    END_VAR

BEGIN
    c := a OR b; // Oh no, a bug! This is an "AND-gate", thus it should be AND here!
END_FUNCTION_BLOCK
```

Eclipse-based **editor** for PLC programs

The PLCverif tool



Verification case

General

General information about the current verification case. Describe here the name of the case and explain its motivation.

ID: Demo001

Name: If A is false, C cannot be true.

Description: If A is false, C cannot be true. As this function block models an AND-gate, if any of the inputs (A or B) is false, the output should be false too.

The requirement is based on the documentation of the function block and the following Jira case: https://icecontrols.its.cern.ch/jira/browse/UCPC-1111

Source code: DemoSource.scl

Requirement

Advanced configuration

Verification

The verification can be started in this section. Also, the result can be seen here.

Tool: NuSMV

Variables

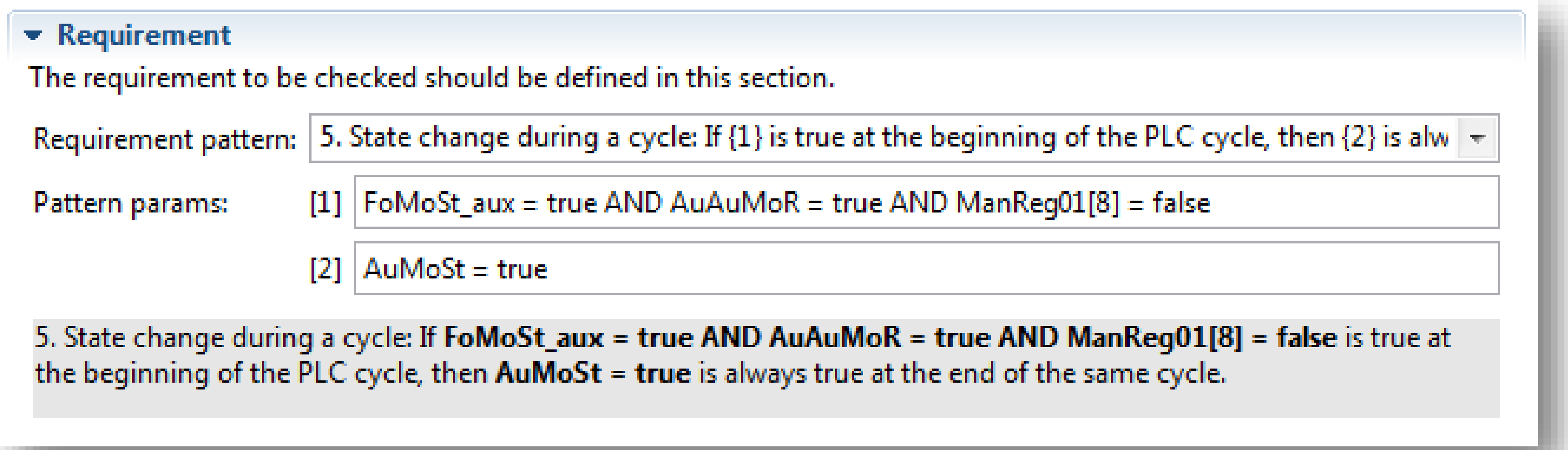
Filter:

Variable name
instance.a
instance.b
instance.c

Defining **verification cases** (requirement, fine-tuning, etc.)

No model checker-related things or temporal logic expressions

The PLCverif tool



Requirement

The requirement to be checked should be defined in this section.

Requirement pattern: 5. State change during a cycle: If {1} is true at the beginning of the PLC cycle, then {2} is alw

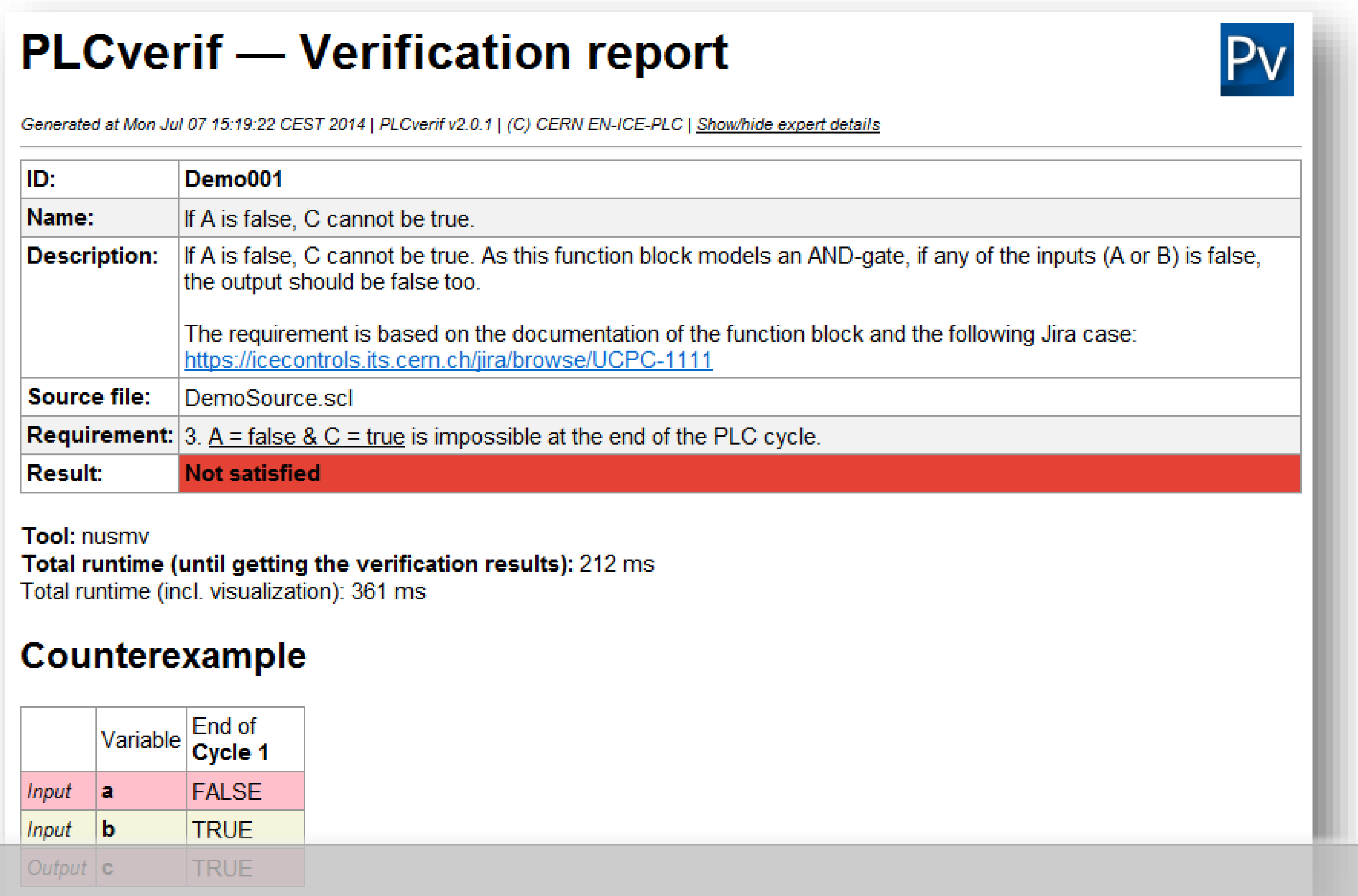
Pattern params: [1] FoMoSt_aux = true AND AuAuMoR = true AND ManReg01[8] = false

[2] AuMoSt = true

5. State change during a cycle: If **FoMoSt_aux = true AND AuAuMoR = true AND ManReg01[8] = false** is true at the beginning of the PLC cycle, then **AuMoSt = true** is always true at the end of the same cycle.

Requirement patterns

The PLCverif tool



PLCverif — Verification report

Generated at Mon Jul 07 15:19:22 CEST 2014 | PLCverif v2.0.1 | (C) CERN EN-ICE-PLC | Show/hide expert details

ID:	**Demo001**
Name:	If A is false, C cannot be true.
Description:	If A is false, C cannot be true. As this function block models an AND-gate, if any of the inputs (A or B) is false, the output should be false too. The requirement is based on the documentation of the function block and the following Jira case: https://icecontrols.its.cern.ch/jira/browse/UCPC-1111
Source file:	DemoSource.scl
Requirement:	3. A = false & C = true is impossible at the end of the PLC cycle.
Result:	**Not satisfied**

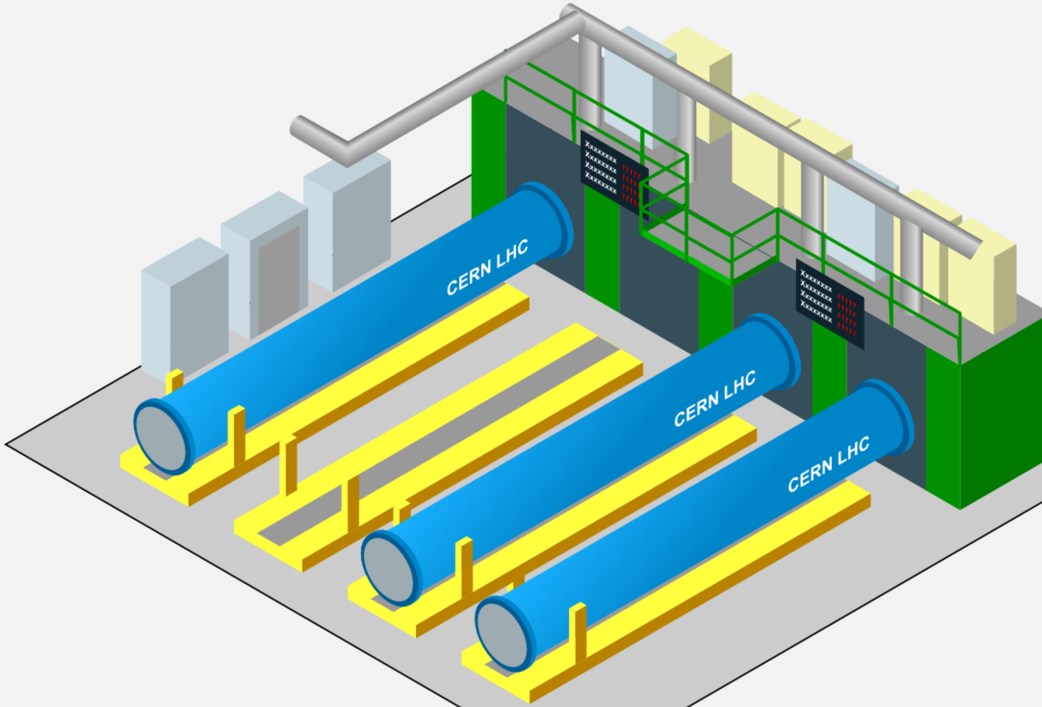
Tool: nusmv
Total runtime (until getting the verification results): 212 ms
Total runtime (incl. visualization): 361 ms

Counterexample

	Variable	End of **Cycle 1**
Input	**a**	FALSE
Input	**b**	TRUE
Output	**c**	TRUE

Click-button verification,
verification **report** with the analysed **counterexample**

Example – SMTP safety system

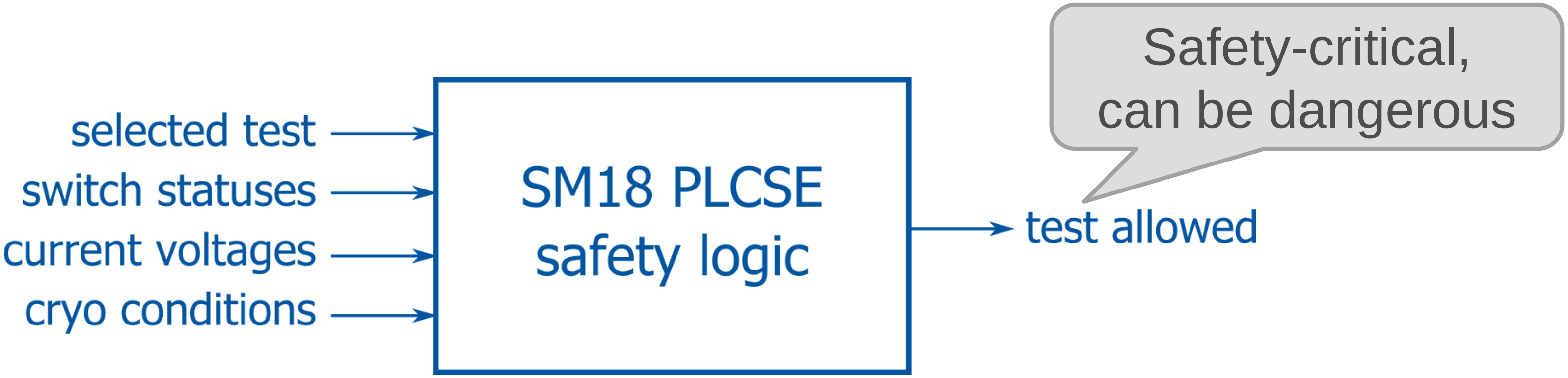


Sc Magnet Test Plant safety system

© CERN

Goal: ensuring **safety** by allowing/forbidding tests

Core:


selected test

switch statuses

current voltages

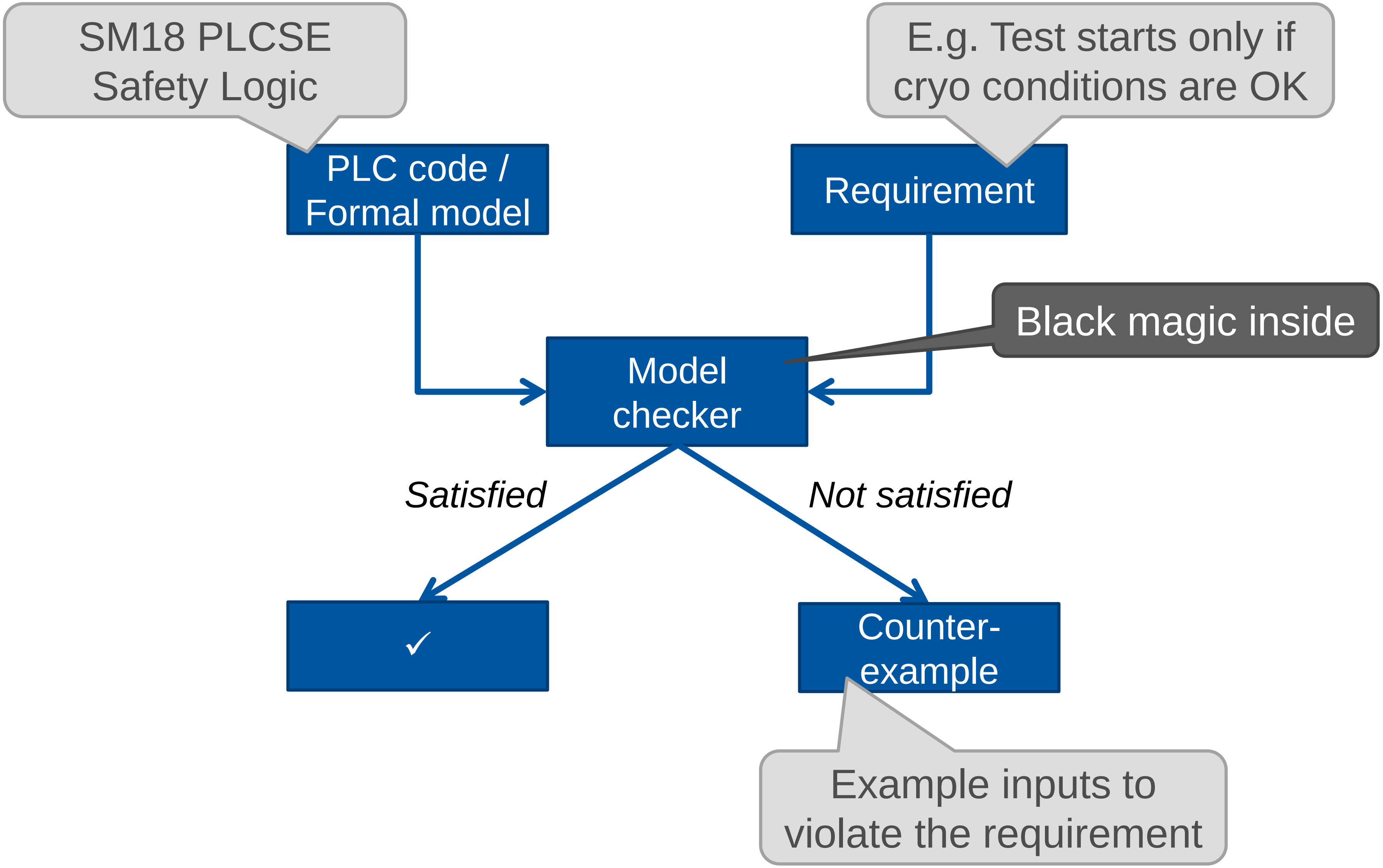
cryo conditions

SM18 PLCSE safety logic

test allowed

Safety-critical, can be dangerous

Model checking workflow for this case



SM18 PLCSE Safety Logic

E.g. Test starts only if cryo conditions are OK

PLC code / Formal model

Requirement

Black magic inside

Model checker

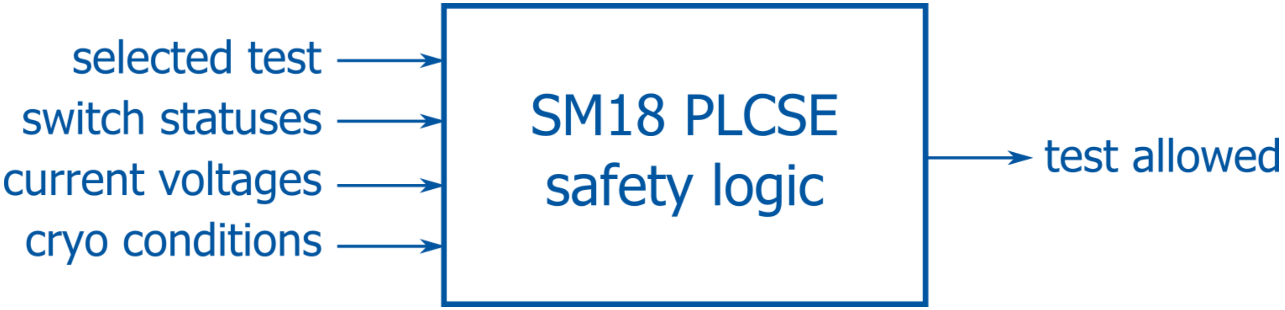
Satisfied

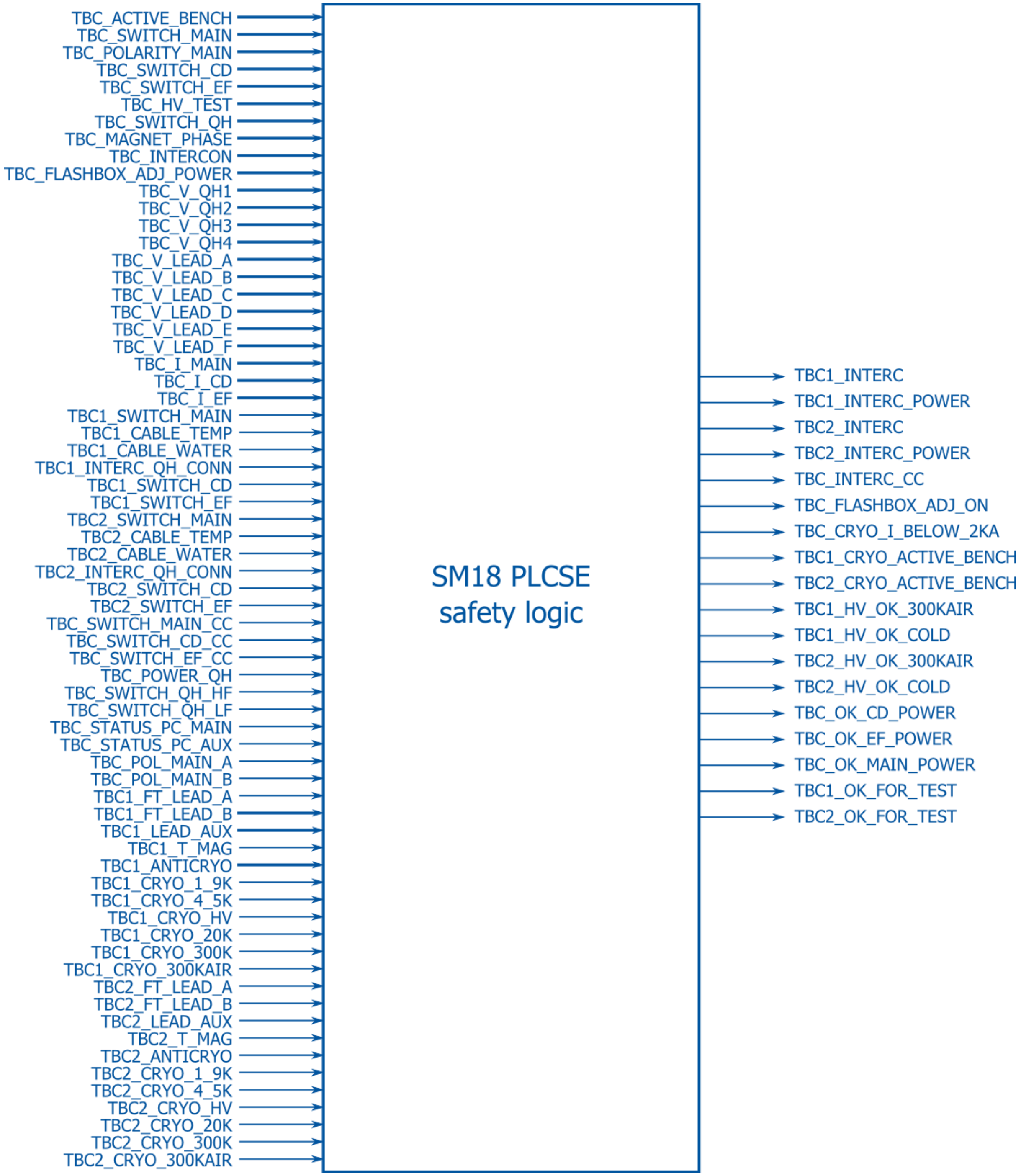
Not satisfied

✓

Counter-example

Example inputs to violate the requirement


selected test
switch statuses
current voltages
cryo conditions
SM18 PLCSE
safety logic
test allowed

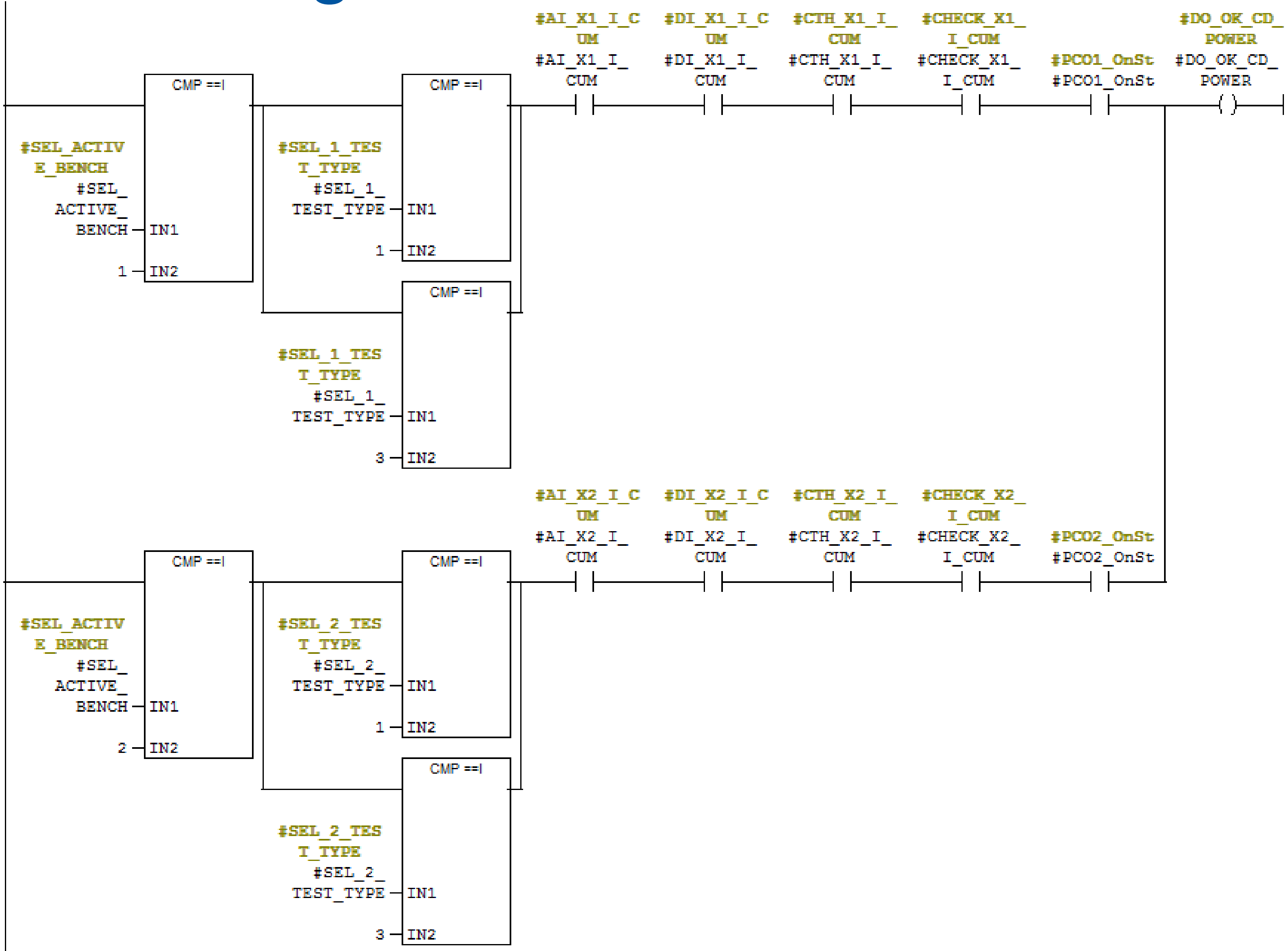


SM18 PLCSE safety logic

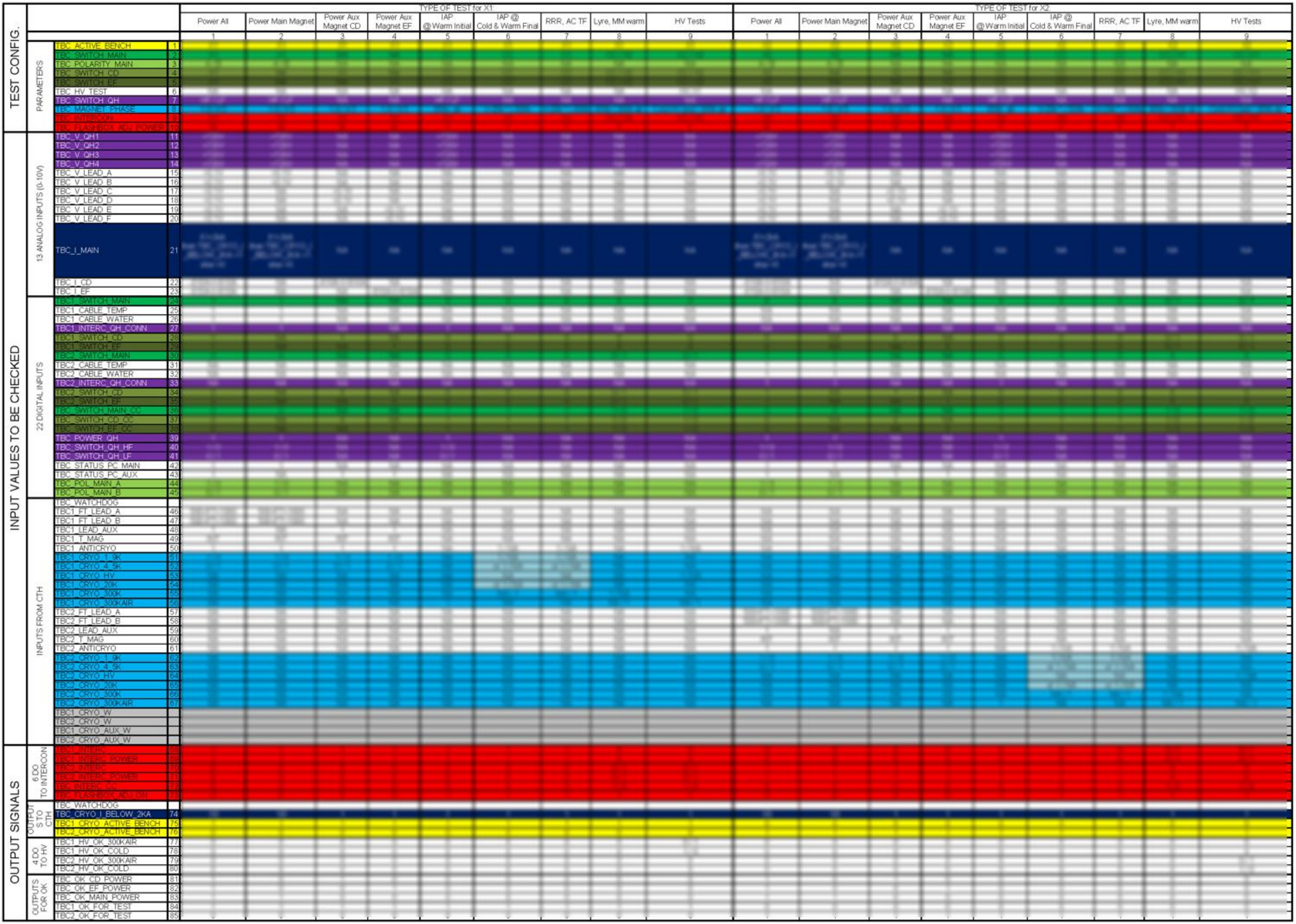
TBC_ACTIVE_BENCH
TBC_SWITCH_MAIN
TBC_POLARITY_MAIN
TBC_SWITCH_CD
TBC_SWITCH_EF
TBC_HV_TEST
TBC_SWITCH_QH
TBC_MAGNET_PHASE
TBC_INTERCON
TBC_FLASHBOX_ADJ_POWER
TBC_V_QH1
TBC_V_QH2
TBC_V_QH3
TBC_V_QH4
TBC_V_LEAD_A
TBC_V_LEAD_B
TBC_V_LEAD_C
TBC_V_LEAD_D
TBC_V_LEAD_E
TBC_V_LEAD_F
TBC_I_MAIN
TBC_I_CD
TBC_I_EF
TBC1_SWITCH_MAIN
TBC1_CABLE_TEMP
TBC1_CABLE_WATER
TBC1_INTERC_QH_CONN
TBC1_SWITCH_CD
TBC1_SWITCH_EF
TBC2_SWITCH_MAIN
TBC2_CABLE_TEMP
TBC2_CABLE_WATER
TBC2_INTERC_QH_CONN
TBC2_SWITCH_CD
TBC2_SWITCH_EF
TBC_SWITCH_MAIN_CC
TBC_SWITCH_CD_CC
TBC_SWITCH_EF_CC
TBC_POWER_QH
TBC_SWITCH_QH_HF
TBC_SWITCH_QH_LF
TBC_STATUS_PC_MAIN
TBC_STATUS_PC_AUX
TBC_POL_MAIN_A
TBC_POL_MAIN_B
TBC1_FT_LEAD_A
TBC1_FT_LEAD_B
TBC1_LEAD_AUX
TBC1_T_MAG
TBC1_ANTICRYO
TBC1_CRYO_1_9K
TBC1_CRYO_4_5K
TBC1_CRYO_HV
TBC1_CRYO_20K
TBC1_CRYO_300K
TBC1_CRYO_300KAIR
TBC2_FT_LEAD_A
TBC2_FT_LEAD_B
TBC2_LEAD_AUX
TBC2_T_MAG
TBC2_ANTICRYO
TBC2_CRYO_1_9K
TBC2_CRYO_4_5K
TBC2_CRYO_HV
TBC2_CRYO_20K
TBC2_CRYO_300K
TBC2_CRYO_300KAIR

TBC1_INTERC
TBC1_INTERC_POWER
TBC2_INTERC
TBC2_INTERC_POWER
TBC_INTERC_CC
TBC_FLASHBOX_ADJ_ON
TBC_CRYO_I_BELOW_2KA
TBC1_CRYO_ACTIVE_BENCH
TBC2_CRYO_ACTIVE_BENCH
TBC1_HV_OK_300KAIR
TBC1_HV_OK_COLD
TBC2_HV_OK_300KAIR
TBC2_HV_OK_COLD
TBC_OK_CD_POWER
TBC_OK_EF_POWER
TBC_OK_MAIN_POWER
TBC1_OK_FOR_TEST
TBC2_OK_FOR_TEST

Ladder Diagram



Excerpt from the work of R. Speroni



				TYPE OF TEST for X1:									TYPE OF TEST for X2:								
				Power All	Power Main Magnet	Power Aux Magnet CD	Power Aux Magnet EF	IAP @ Warm Initial	IAP @ Cold & Warm Final	RRR, AC TF	Lyre, MM warm	HV Tests	Power All	Power Main Magnet	Power Aux Magnet CD	Power Aux Magnet EF	IAP @ Warm Initial	IAP @ Cold & Warm Final	RRR, AC TF	Lyre, MM warm	HV Tests
				1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9
TEST CONFIG.	PARAMETERS	TBC_ACTIVE_BENCH	1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_MAIN	2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_POLARITY_MAIN	3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_CD	4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_EF	5	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_HV_TEST	6	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_QH	7	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_MAGNET_PHASE	8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_INTERCON	9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_FLASHBOX_ADJ_POWER	10	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
INPUT VALUES TO BE CHECKED	13 ANALOG INPUTS (0-10V)	TBC_V_QH1	11	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_QH2	12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_QH3	13	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_QH4	14	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_LEAD_A	15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_LEAD_B	16	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_LEAD_C	17	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_LEAD_D	18	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_LEAD_E	19	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_V_LEAD_F	20	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_I_MAIN	21	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_I_CD	22	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_I_EF	23	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	22 DIGITAL INPUTS	TBC1_SWITCH_MAIN	24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CABLE_TEMP	25	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CABLE_WATER	26	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_INTERC_QH_CONN	27	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_SWITCH_CD	28	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_SWITCH_EF	29	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_SWITCH_MAIN	30	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CABLE_TEMP	31	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CABLE_WATER	32	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_INTERC_QH_CONN	33	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_SWITCH_CD	34	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_SWITCH_EF	35	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_MAIN_CC	36	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_CD_CC	37	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_EF_CC	38	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_POWER_QH	39	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_QH_HF	40	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_SWITCH_QH_LF	41	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_STATUS_PC_MAIN	42	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_STATUS_PC_AUX	43	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_POL_MAIN_A	44	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_POL_MAIN_B	45	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	INPUTS FROM CTH	TBC_WATCHDOG		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_FT_LEAD_A	46	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_FT_LEAD_B	47	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_LEAD_AUX	48	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_T_MAG	49	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_ANTICRYO	50	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_1_9K	51	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_4_5K	52	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_HV	53	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_20K	54	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_300K	55	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_300KAIR	56	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_FT_LEAD_A	57	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_FT_LEAD_B	58	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_LEAD_AUX	59	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_T_MAG	60	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_ANTICRYO	61	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_1_9K	62	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_4_5K	63	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_HV	64	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_20K	65	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_300K	66	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_300KAIR	67	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_W		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_W		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_AUX_W		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_AUX_W		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
OUTPUT SIGNALS	6 DO TO INTERCON	TBC1_INTERC	68	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_INTERC_POWER	69	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_INTERC	70	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_INTERC_POWER	71	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_INTERC_CC	72	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_FLASHBOX_ADJ_ON	73	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	OUTPUTS TO CTH	TBC_WATCHDOG		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_CRYO_I_BELOW_2KA	74	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_CRYO_ACTIVE_BENCH	75	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_CRYO_ACTIVE_BENCH	76	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	4 DO TO HV	TBC1_HV_OK_300KAIR	77	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_HV_OK_COLD	78	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_HV_OK_300KAIR	79	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_HV_OK_COLD	80	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	OUTPUTS FOR OK	TBC_OK_CD_POWER	81	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_OK_EF_POWER	82	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC_OK_MAIN_POWER	83	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC1_OK_FOR_TEST	84	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		TBC2_OK_FOR_TEST	85	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

From M. Charrondiere

Problems found *(before putting in production!)*

Requirement misunderstanding

- Recognised while specifying requirements

Functionality problems

- “The [magnet] test should start, but it doesn’t.”

Safety problems

- “The [magnet] test **should NOT start**, but it does.”

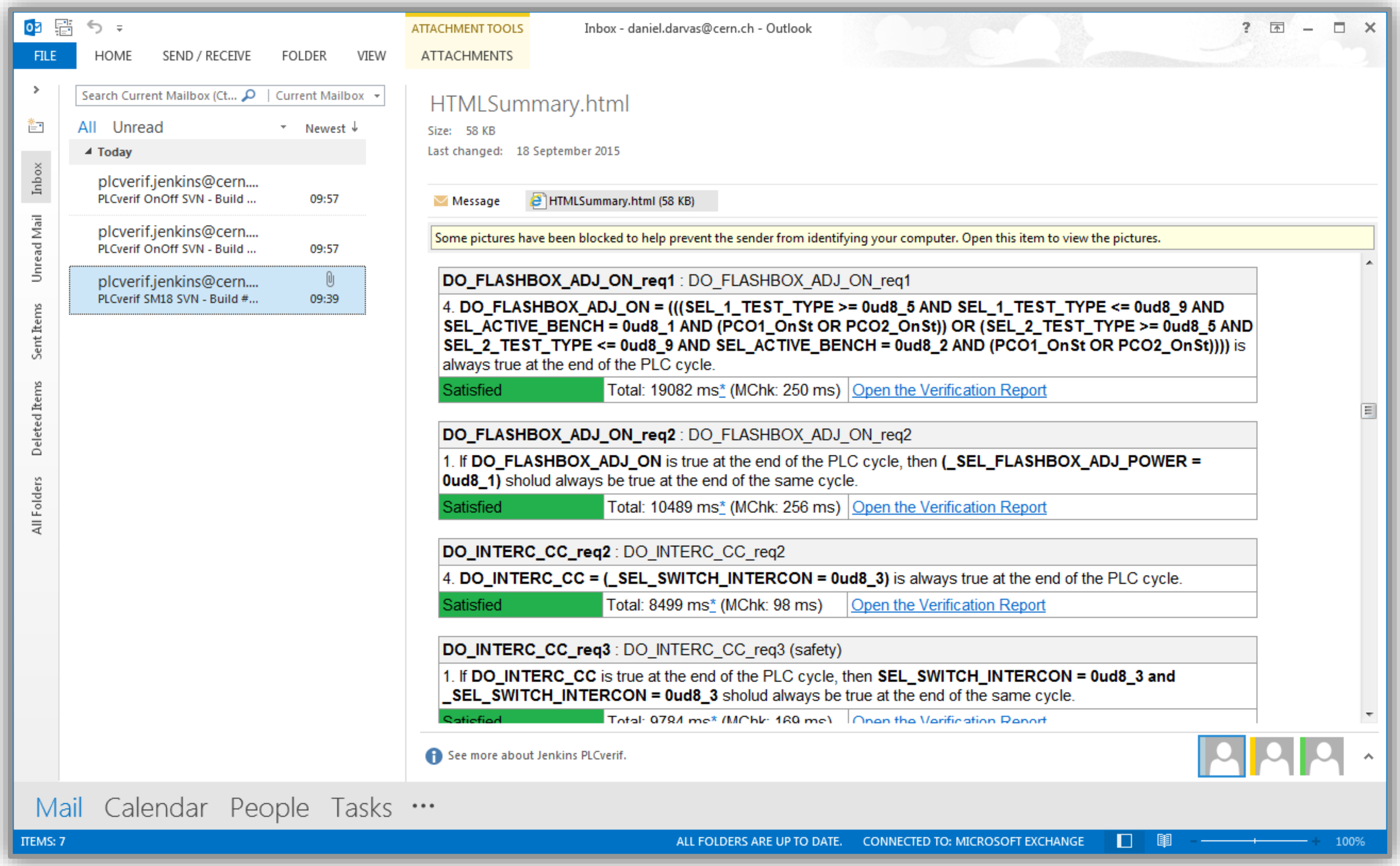
Problems found

In total **14 issues** found

4 requirement misunderstanding

6 problems could not be found using our testing

Continuous verification



plcverif.jenkins@cern....
PLCverif OnOff SVN - Build ... 09:57

plcverif.jenkins@cern....
PLCverif OnOff SVN - Build ... 09:57

plcverif.jenkins@cern....
PLCverif SM18 SVN - Build #... 09:39

HTMLSummary.html

Size: 58 KB
Last changed: 18 September 2015

Some pictures have been blocked to help prevent the sender from identifying your computer. Open this item to view the pictures.

DO_FLASHBOX_ADJ_ON_req1 : DO_FLASHBOX_ADJ_ON_req1

4. **DO_FLASHBOX_ADJ_ON = (((SEL_1_TEST_TYPE >= 0ud8_5 AND SEL_1_TEST_TYPE <= 0ud8_9 AND SEL_ACTIVE_BENCH = 0ud8_1 AND (PCO1_OnSt OR PCO2_OnSt)) OR (SEL_2_TEST_TYPE >= 0ud8_5 AND SEL_2_TEST_TYPE <= 0ud8_9 AND SEL_ACTIVE_BENCH = 0ud8_2 AND (PCO1_OnSt OR PCO2_OnSt))))** is always true at the end of the PLC cycle.

Satisfied	Total: 19082 ms* (MChk: 250 ms)	Open the Verification Report

DO_FLASHBOX_ADJ_ON_req2 : DO_FLASHBOX_ADJ_ON_req2

1. If **DO_FLASHBOX_ADJ_ON** is true at the end of the PLC cycle, then **(_SEL_FLASHBOX_ADJ_POWER = 0ud8_1)** sholud always be true at the end of the same cycle.

Satisfied	Total: 10489 ms* (MChk: 256 ms)	Open the Verification Report

DO_INTERC_CC_req2 : DO_INTERC_CC_req2

4. **DO_INTERC_CC = (_SEL_SWITCH_INTERCON = 0ud8_3)** is always true at the end of the PLC cycle.

Satisfied	Total: 8499 ms* (MChk: 98 ms)	Open the Verification Report

DO_INTERC_CC_req3 : DO_INTERC_CC_req3 (safety)

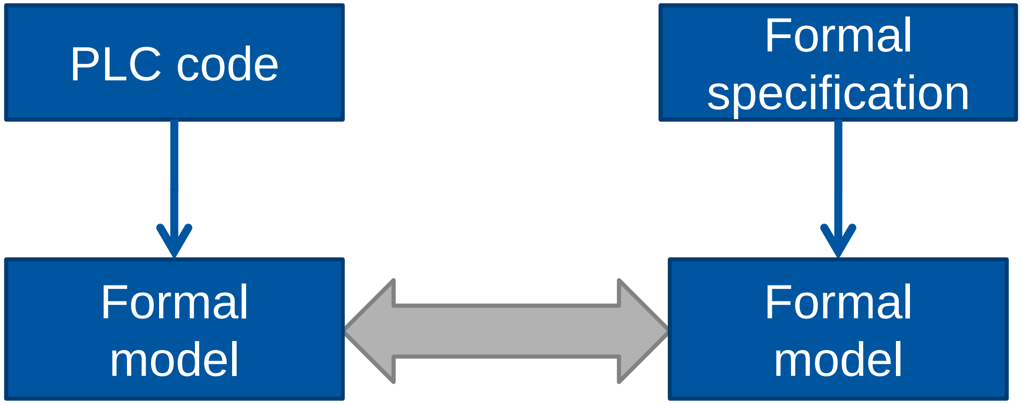
1. If **DO_INTERC_CC** is true at the end of the PLC cycle, then **SEL_SWITCH_INTERCON = 0ud8_3 and _SEL_SWITCH_INTERCON = 0ud8_3** sholud always be true at the end of the same cycle.

Satisfied	Total: 9784 ms* (MChk: 169 ms)	Open the Verification Report

See more about Jenkins PLCverif.

Alternative method *(side note)*

Formal specification +
Behaviour **equivalence checking**



- Formal specification is needed
- Computationally difficult
- Complete
- No need for requirement extraction

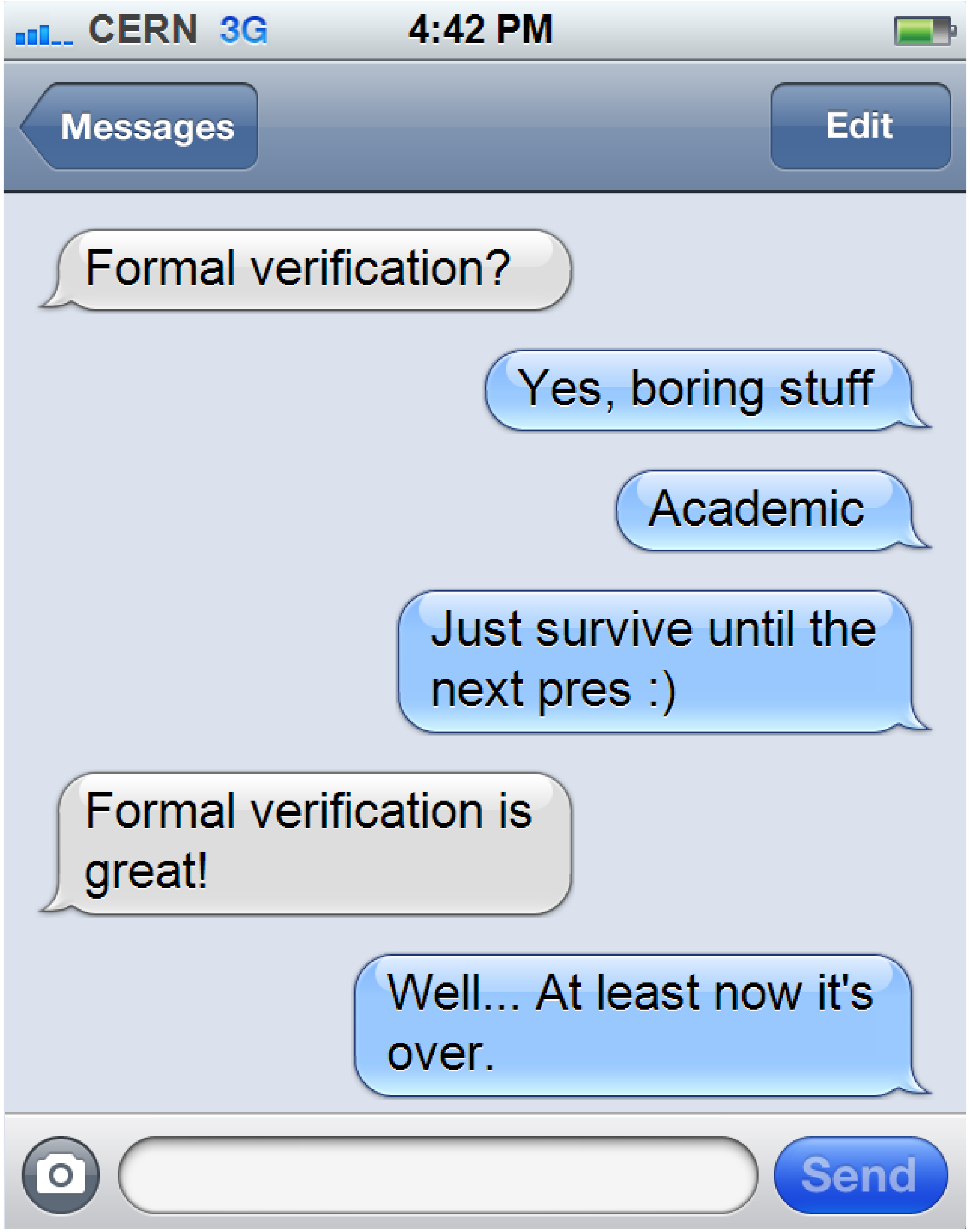
Summary

- “Formal verification is not relevant to industry.” **FALSE**!

- First steps to **apply formal verification** to PLCs
  - **Interesting bugs** found (*with joint effort*)
  - **Critical parts** can be checked
  - **Complementary** to testing

- Still long way to go
  - Improving the **performance**
  - **Formal specification**

http://cern.ch/**plcverif**



Formal verification?

Yes, boring stuff

Academic

Just survive until the next pres :)

Formal verification is great!

Well... At least now it's over.

Source: http://www.iphonetextgenerator.com/

CERN

www.cern.ch