

Dániel Darvas (CERN / BME)

PLCverif: Model checking PLC programs

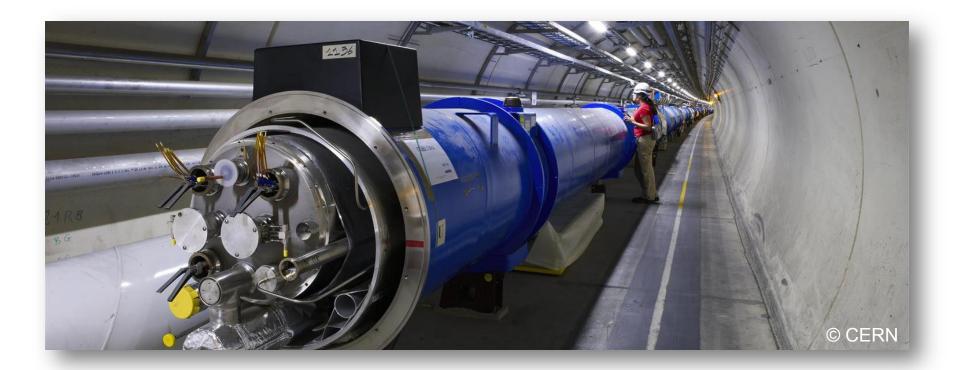
Formal Methods course, BME 22/02/2017

Contains joint work with B. Fernández Adiego, E. Blanco Viñuela, S. Bliudze, J.O. Blech, J-C. Tournier, T. Bartha, A. Vörös, R. Speroni, I. Majzik



CERN European Org. for Nuclear Research

- Largest particle physics laboratory
- Accelerator complex, incl. Large Hadron Collider (LHC)
 - Proton beams with high energies





PLCs

- Programmable Logic Controllers: robust industrial computers, specially designed for process control tasks
- 1000+ PLCs at CERN
 - Including many critical systems



Vacuum







© Siemens AG 2014, All rights reserved

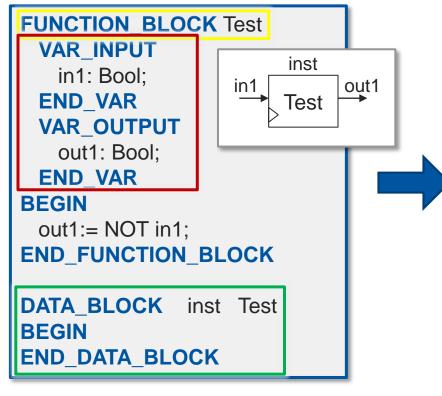
Cryogenics



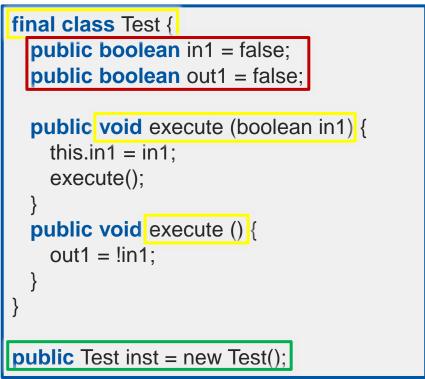
PLC programming

- 5 standard PLC programming languages
 - Base building block: *function block*

Siemens SCL language



"Equivalent" Java code





Motivation for formal verification

- PLCs are often not safety-critical

but

- **Expensive equipment** is operated by PLCs
- Update of PLC programs difficult
- The cost of downtime is high



Using formal methods

 Formal verification (model checking) may complement testing to find more complex faults

but

- Model checking has to be accessible to the PLC developers
- Required **effort** has to be in balance with the **benefits**
 - The method has to be **adapted to the available knowledge**
 - Formal details should be hidden
 - Recurring tasks should be automated or facilitated



Model checking of PLC programs



Challenges

Formal models

Creation of formal models require lots of effort and knowledge

- Formal requirements

• Formalizing requirements in e.g. CTL/LTL is difficult, they are inconvenient and ambiguous without strong knowledge

Model size and model checking performance

- "Naïve modelling" often leads to complex, large models requiring excessive resources to verify
- Optimization of models is difficult and tedious

- Model checker development

• CERN is not a computer science research centre, development of a custom model checker would need too much effort



Can we use external tools?

- General-purpose formal modelling and verification tools (e.g. UPPAAL, NuSMV)
 - Usage is **difficult** for control engineers
 - Too much repetitive tasks in modelling
- Software model checkers (e.g. CBMC)
 - PLCs use special programming languages and execution scheme

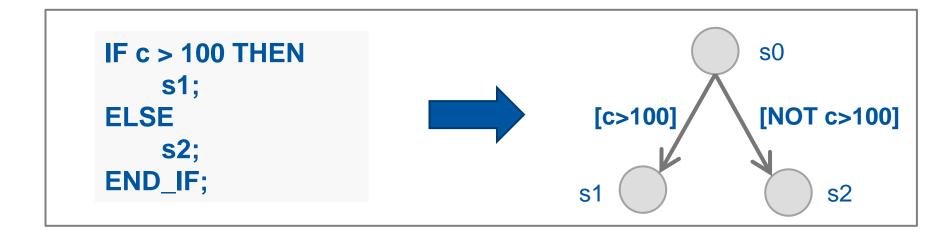
PLC-specific model checkers

- No industrial solution yet
- Some academic tools (e.g. Arcade.PLC)



Formal modelling

 Formal models (~automata) automatically generated from the source code of the PLC programs (via AST)





Formalizing the requirements

- Use of **CTL/LTL** is too difficult for most control engineers
- Typical requirements were captured as textual requirement patterns
 - **Placeholders** to be filled by the users (using simple expressions)

If α and β are true, then α shall stay true until β becomes true.

$$AG((\alpha \wedge \beta) \to A[\alpha \ U \neg \beta])$$



Model size and performance

- Size of the generated formal model is often huge, verification often impossible (memory bottleneck)
- Automated reductions reduce the resource needs
 - General-purpose, structural reductions
 - Domain-specific reductions
 - Exploit the extra knowledge about the domain, the execution schema, etc.
 - Requirement-specific reductions
 - Removes the parts of the model which **do not influence the** satisfaction of the current requirement



External model checkers

- Development of a custom model checker would need excessive effort
- Instead, we reuse (wrap) existing general-purpose
 model checkers as generic verification engines
 - UPPAAL
 - NuSMV / nuXmv
 - ITS
 - ...
- Input (model+requirement) mapping +
 Output (counterexample) mapping needed



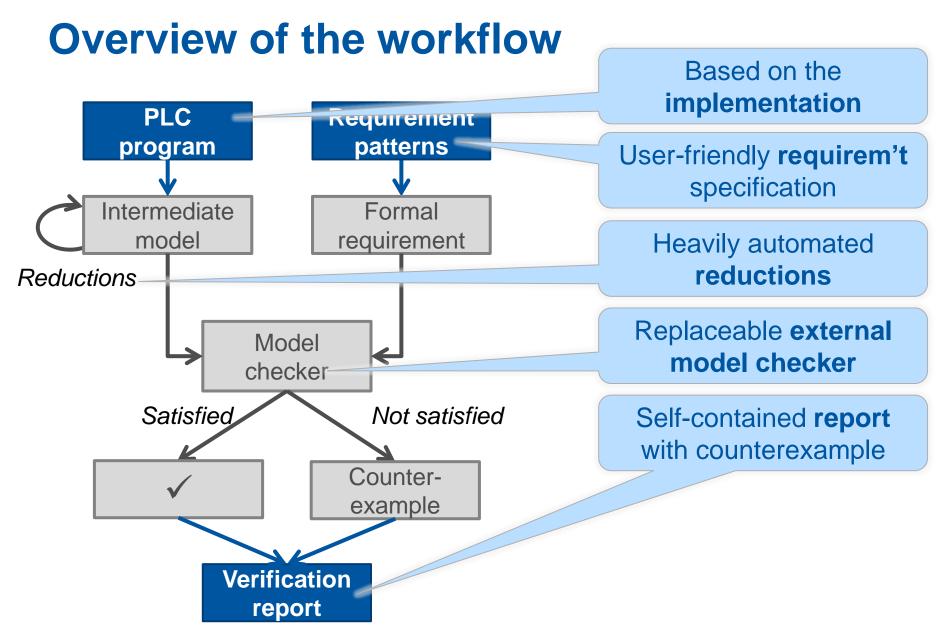
Intermediate model

- Simple, automata-based formalism
- Describes the **behaviour** of the PLC program

- Advantages:

- Helps to use **model reductions** (on the IM)
- Helps to use various model checkers with different syntaxes
- Simplifies (decouples) the PLC program → Model checker model transformation, thus reduces the risk of faults







More info: B. Fernández et al. Bringing automated model checking to PLC program development - A CERN case study. In Proc. WODES 2014, pp. 394-399. IFAC, 2014. doi: 10.3182/20140514-3-FR-4046.00051

Overview of the workflow

attings Help b Project Explore DemoSource.scl Verification Case (Demo001) (S) C b DemoSource.scl Verification case Variables b DemoSource.scl General General General information about the current verification case. Describe here the name of the case and explain its motivation. Variables ID: Demo001 Instance.a	
Project Explore Origination Case OpernoSource.scl DemoProject DemoVerification case Variables Variable Coneral General General General ID: Demo001 Demo001	
▶ ♥ DemoProject Verification case Variable ▶ DemoSourcescl ♥ General Filter: ▶ DemoVriefCase.vc General information about the current verification case. Describe here the name of the case and explain its motivation. Filter: ▶ UNICOS_base.bt ID: Demo001	
Verification case Variable DemoSource.scl De	s
Constant of the case and explain its motivation. UNICOS, base.bt ID: Demo001 Demo001 Demo001 Demo001 Demo001	
DemoVerifCase.vc General information about the current verification case. Describe here the name of the case and explain its motivation. UNICOS_base.bt ID: Demo001 Instance.a	
instance.a	me
Name: If A is false, C cannot be true. instance.c	
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.	
Description: The requirement is based on the documentation of the function block and the following Jira case: https://icecontrols.its.cem.ch/jira/browse/UCPC-1111	
Source code: DemoSource.scl Refresh variables	
► Requirement	
Advanced configuration	
Verification	
The verification can be started in this section. Also, the result can be seen here. Tool: NuSMV	
R Progress Generation Log Execution Output 🕃 Problems 😒	
0 items	
Description Resource Path Location Type	

Based on the implementation

Jser-friendly requirem't specification

Heavily automated reductions

Replaceable external model checker

Self-contained report with counterexample

> **Tool** hiding the formal details





More info: B. Fernández et al. Bringing automated model checking to PLC program development - A CERN case study. In Proc. WODES 2014, pp. 394-399. IFAC, 2014. doi: 10.3182/20140514-3-FR-4046.00051

The PLCverif tool

 DemoProject DemoSource.scl DemoVerifCase.vc UNICOS_base.bt 	a : BOOL; b : BOOL; END_VAR	no, a bug! This is	an "AND-gate", th	us it should be AND	D here!	 □ Variables □ Outline ○ □ DemoSource △ □ □ DemoSource △ □ □ [function_block] AndQ △ □ □ (function_block] AndQ □ □ Variable declara □ □ Variable declara □ □ Statement list
 DemoProject DemoSource.scl DemoVerifCase.vc UNICOS_base.bt 	<pre>● FUNCTION_BLOCK AndGate ● VAR_INPUT a : BOOL; b : BOOL; END_VAR ● VAR_OUTPUT c : BOOL; END_VAR BEGIN c := a OR b; // Oh</pre>	no, a bug! This is	an "AND-gate", th	us it should be AND		Hide non-structural elements General ElemoSource Function_block] AndG Elements Elements Elements Elements Elements Elements Elements Hide non-structural elements Figure 1 Elements Figure 1 Figure 1 Fig
	۲				*	
0 item	Arogress E Generation Log E	Execution Output	Problems 😒			
	scription	Re	source Path	Location	Туре	



Г

The PLCverif tool

PV PLCverif				
Settings Help				
- G 4. 🗈 🗲 🖻				
Project Explorer 🛛 🖓 📄 🗸	DemoSource			Variables
DemoSource.scl	▼ General			Filter:
DemoVerifCase.vc	General inform	nation about the current verification case. Describe here the name of the case and explai	in its motivation.	
UNICOS_base.txt	ID:	Demo001		Variable name instance.a
	Name:	If A is false, C cannot be true.		instance.b
		If A is false, C cannot be true. As this function block models an AND-gate, if any of the false, the output should be false too. The requirement is based on the documentation of the function block and the followin https://icecontrols.its.cern.ch/jira/browse/UCPC-1111		instance.c
	Source code:	DemoSource.scl 🔹	Refresh variables	
	▶ Requireme	nt		
	Advanced	configuration		
	Verification The verificatio Tool: Nus	on can be started in this section. Also, the result can be seen here.	•	
		Generation Log 🗖 Execution Output 💽 Problems 😒		∇

Defining verification cases (requirement, fine-tuning, etc.) No model checker-related things or temporal logic expressions



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. <u>A = false & C = true</u> 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	с	TRUE

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



Example verification metrics

Each line represents the verification of a PLC program with a specific requirement.

	Source code lines	Unreduced model	Reduced model	Verification time (NuSMV)
(1)	12	24	24	0.04 s
(2)	1000	3.8 × 10 ²⁴²	2.2 × 10 ⁸	0.24 s
(3)	1000	3.8 × 10 ²⁴²	5.8 × 10 ⁶	0.23 s
(4)	17,700	10 ³²⁴⁴⁶	7.9 × 10 ³⁵	21.7 s
(5)	10,000	10 ⁹⁷⁸	1.6 × 10 ⁸⁴	~7 min



Verification times measured on:

Intel i7-3770, 8 GB RAM, Win 7 x64, Java 8 NuSMV 2.6.0 (physical PC)

Scaling

- Providing acceptable performance is a continuous challenge
- However, many successful industrial applications, e.g.:
 - **Module library** of CERN's in-house PLC framework (UNICOS)
 - ~1000 lines of code
 - Unreduced potential state space: up to ~10²⁵⁰
 - *Verification time:* typically in the range of seconds
 - Safety logic of magnet testing facility (see later)
 - ~10,000 lines of code
 - Unreduced potential state space: up to ~10¹⁰⁰⁰
 - *Verification time:* in the range of 1..10 minutes



Case study: SM18 magnet testing facility



SM18 PLCSE safety controllers



Goal: ensuring safety by allowing/forbiddin Core: selected test switch statuses current voltages cryo conditions Safety-critical, can be dangerous: 14 kA, liquid He, -271°C, vacuum test allowed



More info: D. Darvas, I. Majzik, E. Blanco. Formal verification of safety PLC based control software. In Integrated Formal Methods, LNCS 9681, pp. 508-522. Springer, 2016. doi: 10.1007/978-3-319-33693-0_32

Challenges in the verification

- Complex, semi-formal (ambiguous) requirements



Semi-formal specification

- Allowed tests described in a tabular form

	Selected test	1	2
out	Voltage	>100 V	>50 V
lnp	Overheating	FALSE	don't care
	Cryo OK	TRUE	TRUE
utput	TestEnabled	TRUE	TRUE
Out	SpecialTest	TRUE	FALSE

 If SelTest=1 and Voltage>100 and not Overh and CryoOk, then TestEnabled shall be true, SpecialTest shall be true.

Not bad, but ambiguous

- Colours have undefined additional meanings
- Some ambiguous values in cells, e.g. "1 / NA / NA / 0"



<u> </u>							TYPE OF TEST	for X1		9 [.]						TYPE OF TES	T for X2			
			Power All	Power Main Magnet	Power Aux Magnet CD	Power Aux	IAP	IAP @	RRR, AC TE	Lyre, MM warm	HV Tests	Power All	Power Main Magnet	Power Aux	Power Aux	LAP	IAP @	RRR, AC TF	Lyre, MM warm	HV Tests
0			1	2	Magnet CD 3	Magnet EF 4	@Warm Initial 5	Cold & Warm Final 6	7	8	9	1	2	Magnet CD 3	Magnet EF 4	@Warm Initial 5	Cold & Warm Final 6	7	8	9
Ψ		TBC ACTIVE BENCH 1																		
<u></u>	Rs I	TBC POLARITY MAIN 3			_	-	-	-	-	-					_	-	-	-	-	
TEST CONFIG.	PARAMETERS	TEC SWITCH CD 4 TEC SWITCH EF 5			-															
ES S	RAM	TBC HV TEST 6 TBC SWITCH QH 7		-	-					-		-		-	12	-	-		-	
н	PA	TEC SWITCH OH 7 TEC MAGNET PHASE 8			_		_					-		_	_	_				
		THE FLASHBOX NOL POWER NO																		
Π		TEC_V_OH1 11 TEC_V_OH2 12 TEC_V_OH2 13 TEC_V_OH4 14 TEC_V_LEAD_A 15 TEC_V_LEAD_B 16 TEC_V_LEAD_C 17																		
		TBC V QH3 13		-													-			
	101)	TBC_V_LEAD_A 15 TBC_V_LEAD_B 16			- 10 - 1	-		- 12		_	10				_	- 14	-	- 14	_	- 10
	00	TBC_V_LEAD_B 16 TBC_V_LEAD_C 17	- 11		- 24-	- 8-						- 55-	- 12	- 10-				- 10		
	In I	TBC_V_LEAD_C 17 TBC_V_LEAD_D 18 TBC_V_LEAD_E 19		_	- 12	-2-			- 3-						- 2			- 11-1		
	0 IN	TBC_V_LEAD_F 20		_	_	-24-	_	_				-22-		_	- 24-					
	13 ANALOG INPUTS (0-																			
	3 AN	TBC_I_MAIN 21																		
	1																			
		TBC_I_CD 22 TBC_I_EF 23	-		And Persons in		_	_	100	_	50	and the second second	- 10	Concession of the local division of the loca		- 10	_			- 29
		15 OF ESWITCHEMAIN 24			-	-	-	-		-		10000	1	-	-	-			-	-
		TBC1_CABLE_TEMP 25 TBC1_CABLE_WATER 26			- 2 - 1	- 2 -	- 8 -			- 2 -			- 8 -		- 3 -	- 8 -		- 2 -		
		TBC1_INTERC_QH_CONN 27	and the second	1000 C	and in such		Contraction of	100	and the second	and the second	1.1	100	the second second	and the second	100	100	Contract Street	100	and the second	
		TBC1_SWITCH_CD 28 TBC1_SWITCH_EF 29																	_	
INPUT VALUES TO BE CHECKED	0	TBC2_SWITCH_MAIN 80 TBC2_CABLE_TEMP 31			-	-				-				_	_	_				
Ô	22 DIGITAL INPUTS	TBC2_CABLE_TEMP 31 TBC2_CABLE_WATER 32 TBC2_INTERC_GH_CONN 33			- 1	- 1	_			_		_		- 10-	- 1	_			- 1	10
X	L IN	TBC2_SMTCH_CD 34			_	-	-					_						_		
ш	GITA	TEC2_SWITCH_EF 35 TECESWITCH_MAIN_CC 36																		
B	22 DI	THE SWITCH CD CC 37																		
2	1.	TBC POWER QH 39																		
ŝ		TBC POWER OH 39 TBC SWITCH OH HF 40 TBC SWITCH OH HF 40 TBC STATUS PC MAIN 42 TBC STATUS PC AUX 43																		
2		TBC_STATUS_PC_MAIN 42 TBC_STATUS_PC_AUX 43			- 10	- 10		_	- 10 -		- 10		-					- 10		
A		TBC POL MAIN A 44				- 2	-		- 11-				1.1	_		-		1.1		
5		TBC_POL_MAIN_B 45 TBC_WATCHDOG TBC1_FT_LEAD_A 46			-	-	-	-						-	_			_	-	-
đ		TRC1 ET LEAD B 47				- 3-												- 31		
=		TBC1_LEAD_AUX 48 TBC1_T_MAG 49		- 25			- 2-		- 2 -						- 3 -			- 10-		
		TBC1_ANTICRYO 50					-	1.1	1.16		1.744							- 12 -		12
		1BC1_CRY0_4_SK 51 1BC1_CRY0_4_SK 52						1000	and the second second				-							
	1000	TBC1 ORYO HV 53 TBC1 ORYO 20K 54			_	_	_	- Aller	- 2					_	_	_		-		
	H	TBCI_CRYO_300K 55				- 1	-			1.1	-	_		_					_	
		TBC2_FT_LEAD_A 57 TBC2_FT_LEAD_B 58	_			- 11	_				100	and the second second	and the second second						_	
	INPUTS FROM	TBC2_LEAD_AUX 59	_							-		and party in	-							
	Ind.	TBC2_LEAD_AUX 59 TBC2_T_MAG 60 TBC2_ANTICRYO 61							- 3-						- 37					
	=	TBC2 CRYO 1 9K 62										-	111				100	100		
		TBC2_CRYO_HV 64				- 1		-	1 2 -			12	32		100			and the second second		
		TBC2_CRYO_20K 65 TBC2_CRYO_300K 66							-			-								
		TBC2_CRYO_300KAIR 67 TBC1_CRYO_W			_	_	-	_		_			10		_	_		_	10.0	
		TBC1_CRYO_W TBC2_CRYO_W TBC1_CRYO_AUX_W													_					
		TBC1_CRYO_AUX_W TBC2_CRYO_AUX_W	-		_	_			-			_		-					_	-
	NOC	TECLINTERC POWER 88																		
	6 DO INTERC	TESS, BILLER 70																		
S	9 INI O	TEC INTERC CC 72																		
M	- PP	TBC_WATCHDOG		_	_		_			_				_	_				_	
SIGNALS	26F	IBC_WATCHDOG IBC_CRYO_I_BELOW_2KA 74				-				-					-					
S	200	TBC2_CRYO_ACTIVE_BENCH 76				_	_							_		_				
OUTPUT	s≩	TBC1_HV_OK_300KAIR 77 TBC1_HV_OK_COLD 78										_								-
Ë	145	TBC2_HV_OK_S00KAIR 79				_	_			_	-								_	10
5		TBC OK CD POWER 81	_			_														1
	OUTPUTS FOR OK	TBC OK CD FOWER 81 TBC OK EF FOWER 82 TBC OK MAIN POWER 83 TBC OK MAIN POWER 83 TBC1 OK FOR TEST 84 TBC2 OK FOR TEST 85	-																	
	58	TBC1 OK FOR TEST 84												_						
	-	IBUZ_UK_FUK_IEST 85			× 1			· ·	T V				7 2			1	1 2	T 7 3	2 7	4

From M. Charrondiere

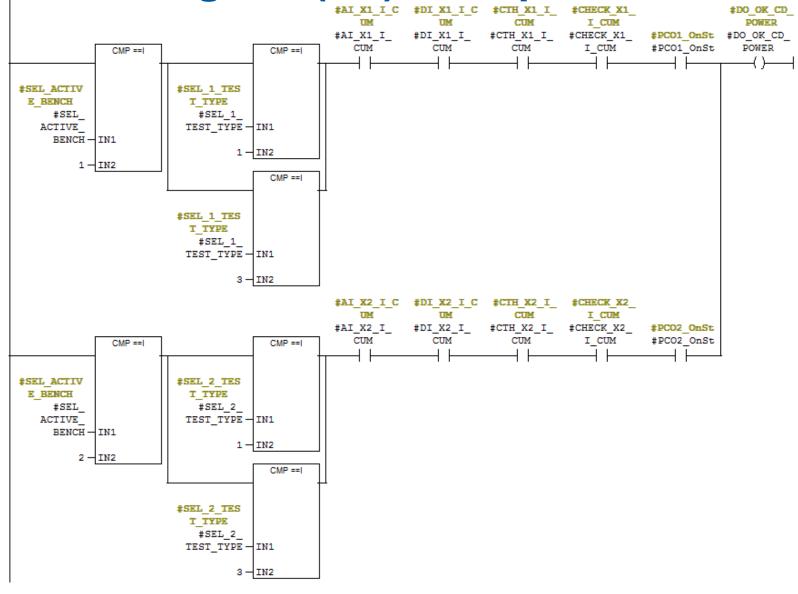
Challenges in the verification

- Complex, semi-formal (ambiguous) requirements

- 'LD' programming language
 - Due to development restrictions for safety PLC programs
 - Has to be exported to 'STL' language first
 - Semantics of 'STL' is not precisely defined



Ladder Diagram (LD) example





Excerpt from the work of R. Speroni

Siemens Statement List (STL) example

NETWORK		0		;
TITLE =POW	ER CD	А	(
		L	•	#SEL_ACTIVE_BENCH;
Α(; ;	L		2;
L	#SEL_ACTIVE_BENCH;	==	=I	; ;
L	1;)		• •
==I	;	A	(; ;
)	;	0	(; ;
Α(;	L		#SEL_TYPE_TEST_X2;
0(;	L		1;
L	#SEL_TYPE_TEST_X1;	==	=I	; ;
L	1;			; ;
==I	;	0	(; ;
)	;	L		#SEL_TYPE_TEST_X2;
0(;	L		3;
L	#SEL_TYPE_TEST_X1;	==	=I	; ;
L	3;)		; ;
==I	;)		;
)	;	Α		#AI_X2_I_CUM;
)	;	Α		#DI_X2_I_CUM;
Α	#AI_X1_I_CUM;	Α		<pre>#CTH_X2_I_CUM;</pre>
Α	<pre>#DI_X1_I_CUM;</pre>	=		#DO_OK_CD_POWER;
Α	#CTH_X1_I_CUM;			



Challenges in the verification

- Complex, semi-formal (ambiguous) requirements

- 'LD' programming language

- Due to development restrictions for safety PLC programs
- Has to be exported to 'STL' language first
- Semantics of 'STL' is not precisely defined

- Complex safety logic

Many inputs and outputs



TBC_ACTIVE_BENCH		
TBC_POLARITY_MAIN>		
TBC_SWITCH_CD>		
TBC_SWITCH_EF		
TBC_MAGNET_PHASE		
TBC_FLASHBOX_ADJ_POWER		
TBC_V_QH1		
TBC V QH2		
TBC V OH3 →		
TBC_V_QH4>		
TBC_V_LEAD_A>		
TBC_V_LEAD_B		
TBC_V_LEAD_C		
TBC_V_LEAD_E		
TBC_I_MAIN		
TBC I CD		TBC1_INTERC
TBC_I_EF		TBC1_INTERC_POWER
TBC1 SWITCH MAIN>		
TBC1_CABLE_TEMP>		→ TBC2_INTERC
TBC1_CABLE_WATER>		TBC2_INTERC_POWER
TBC1_INTERC_QH_CONN		→ TBC_INTERC_CC
TBC1_SWITCH_CD		
TBC1_SWITCH_EF		TBC_FLASHBOX_ADJ_ON
TBC2_CABLE_TEMP		TBC_CRYO_I_BELOW_2KA
TBC2_CABLE_WATER		TBC1_CRYO_ACTIVE_BENCH
TBC2 INTERC OF CONN>	SM18 PLCSE	
	SITIOFLOSE	TBC2_CRYO_ACTIVE_BENCH
TBC2_SWITCH_CD>		
TBC2_SWITCH_CD	safety logic	→ TBC1_HV_OK_300KAIR
TBC2_SWITCH_EF	safety logic	TBC1_HV_OK_300KAIR
TBC2_SWITCH_EF	safety logic	TBC1_HV_OK_300KAIR TBC1_HV_OK_COLD
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC	safety logic	TBC1_HV_OK_300KAIR
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC TBC_POWER_QH	safety logic	TBC1_HV_OK_300KAIR TBC1_HV_OK_COLD
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC TBC_POWER_QH TBC_SWITCH_QH_HF	safety logic	TBC1_HV_OK_300KAIR TBC1_HV_OK_COLD TBC2_HV_OK_300KAIR TBC2_HV_OK_COLD
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_IF TBC_SWITCH_QH_IF TBC_STATUS_PC_MAIN	safety logic	TBC1_HV_OK_300KAIR TBC1_HV_OK_COLD TBC2_HV_OK_300KAIR TBC2_HV_OK_COLD TBC2_OK_CD_POWER
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	safety logic	TBC1_HV_OK_300KAIR TBC1_HV_OK_COLD TBC2_HV_OK_300KAIR TBC2_HV_OK_COLD
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_AUX TBC_STATUS_PC_AUX TBC_POL_MAIN_A	safety logic	TBC1_HV_OK_300KAIR TBC1_HV_OK_COLD TBC2_HV_OK_300KAIR TBC2_HV_OK_COLD TBC2_OK_CD_POWER
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC TBC_POWER_QH TBC_SWITCH_OH_HF TBC_SWITCH_QH_HF TBC_STATUS_PC_MAIN TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_B	safety logic	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
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC TBC_POWER_QH TBC_SWITCH_QH_HF TBC_SWITCH_QH_HF TBC_STATUS_PC_MAIN TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC_POL_MAIN_A TBC_I_FT_LEAD_A	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_OH TBC_SWITCH_OH_HF TBC_SWITCH_OH_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	safety logic	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
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_AUX TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_B TBC1_FT_LEAD_A TBC1_FT_LEAD_AUX	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_SWITCH_OP_HF TBC_SWITCH_OH_HF TBC_STATUS_PC_MAIN TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_LEAD_AUX TBC1_T_MAG TBC1_ANTICRYO	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_QH TBC_SWITCH_QH_HF TBC_SWITCH_QH_HF TBC_STATUS_PC_MAIN TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_T_MAG TBC1_CRYO_1_9K	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_QH TBC_SWITCH_QH_HF TBC_SWITCH_QH_LF TBC_STATUS_PC_AUX TBC_STATUS_PC_AUX TBC_POL_MAIN_B TBC1_FT_LEAD_A TBC1_FT_LEAD_B TBC1_CAD_AUX TBC1_CRYO_19K TBC1_CRYO_19K	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC TBC_POWER_QH TBC_SWITCH_QH_LF TBC_STATUS_PC_AUX TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_B TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_CFT_LEAD_A TBC1_CRYO_1_9K TBC1_CRYO_4_5K TBC1_CRYO_HV	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC TBC_POWER_QH TBC_SWITCH_0H_HF TBC_STATUS_PC_MAIN TBC_STATUS_PC_MAIN TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_CRYO_19K TBC1_CRYO_4_5K TBC1_CRYO_20K	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_OH TBC_SWITCH_OH_IF TBC_SWITCH_OH_IF TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_B TBC1_FT_LEAD_A TBC1_FT_LEAD_B TBC1_FT_LEAD_A TBC1_CRYO_1_9K TBC1_CRYO_1_9K TBC1_CRYO_4_5K TBC1_CRYO_20K TBC1_CRYO_300K	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_QH TBC_SWITCH_QH_IF TBC_SWITCH_QH_IF TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC_POL_MAIN_B TBC1_FT_LEAD_A TBC1_FT_LEAD_B TBC1_EAD_AUX TBC1_CRYO_1_9K TBC1_CRYO_1_9K TBC1_CRYO_20K TBC1_CRYO_300KAIR	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_OH TBC_SWITCH_OH_IF TBC_SWITCH_OH_IF TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_B TBC1_FT_LEAD_A TBC1_FT_LEAD_B TBC1_FT_LEAD_A TBC1_CRYO_1_9K TBC1_CRYO_1_9K TBC1_CRYO_4_5K TBC1_CRYO_20K TBC1_CRYO_300K	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_SWITCH_QH_EF_CC TBC_SWITCH_QH_HF TBC_SWITCH_QH_IF TBC_STATUS_PC_MAIN TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_10K TBC1_CRYO_20K TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC2_FT_LEAD_A	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_QH TBC_SWITCH_QH_IF TBC_SWITCH_QH_IF TBC_STATUS_PC_AUX TBC_OD_MAIN_A TBC_POL_MAIN_A TBC_POL_MAIN_B TBC1_FT_LEAD_A TBC1_FT_LEAD_B TBC1_CRYO_1_9K TBC1_CRYO_1_9K TBC1_CRYO_19K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_T_MAG	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_QH TBC_SWITCH_QH_LF TBC_SWITCH_QH_LF TBC_STATUS_PC_AUX TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_B TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_45K TBC1_CRYO_300K TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_B TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_T_MAG TBC2_T_MAG TBC2_T_MAG TBC2_T_MAG TBC2_T_MAG TBC2_T_MAG TBC2_ANTICRYO	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_SWITCH_EF_CC TBC_SWITCH_OH_HF TBC_SWITCH_OH_HF TBC_STATUS_PC_MAIN TBC_STATUS_PC_MAIN TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC2_FT_LEAD_B TBC2_FT_LEAD_B TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_B TBC2_FT_LEAD_B TBC2_FT_LEAD_B TBC2_FT_LEAD_B TBC2_FT_LEAD_B TBC2_FT_LEAD_B TBC2_FT_LEAD_A	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_OH TBC_SWITCH_OH_HF TBC_SWITCH_OH_HF TBC_SWITCH_OH_HF TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_B TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_20K TBC1_CRYO_20K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_20K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_300K TBC1_CRYO_19K TBC2_CRYO_1_9K TBC1_CRYO_1_9K TBC1_	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_OH TBC_SWITCH_OH_IF TBC_SWITCH_OH_IF TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_QH TBC_SWITCH_QH_FF TBC_SWITCH_QH_FF TBC_STATUS_PC_MAIN TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_19K TBC2_CRYO_10K TBC2_CRYO_20K	safety logic	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_FOR_TEST
TBC2_SWITCH_EF TBC_SWITCH_MAIN_CC TBC_SWITCH_CD_CC TBC_SWITCH_CD_CC TBC_POWER_OH TBC_SWITCH_OH_IF TBC_SWITCH_OH_IF TBC_STATUS_PC_AUX TBC_POL_MAIN_A TBC_POL_MAIN_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_FT_LEAD_A TBC1_CRYO_19K TBC1_CRYO_19K TBC1_CRYO_300KAIR TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC1_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_300KAIR TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_FT_LEAD_A TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K TBC2_CRYO_4_5K	safety logic	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_FOR_TEST

CERN

Problems found (before putting in production!)

Requirement misunderstanding

- Recognised while specifying requirements formally

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 misunderstandings

6 problems could not be found using our typical testing methods



Summary

Where are we now?

- Model checking: more and more used for real cases
 - Sometimes non-expert users use PLCverif **autonomously**
 - Integration into the development process is in progress
- Several successful case studies
 - Model checking revealed interesting and potentially critical problems
 - **Counterexample** is a huge advantage
- Improvements are always possible
 - New reduction methods
 - Support for new model checkers
 - Support for additional PLC languages





www.cern.ch

For more information...

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



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, pp. 911-914, JaCoW, 2015. <u>http://doi.org/10.18429/JACoW-ICALEPCS2015-WEPGF092</u>
- B. Fernández et al. Applying model checking to industrial-sized PLC programs. IEEE Transactions on Industrial Informatics, 11(6):1400-1410, 2015. <u>http://doi.org/10.1109/TII.2015.2489184</u>
- D. Darvas et al. Formal verification of safety PLC based control software. Integrated Formal Methods (LNCS 9681), pp. 508-522, Springer, 2016. <u>http://doi.org/10.1007/978-3-319-33693-0_32</u>



Formal specification at CERN

- D. Darvas et al. Requirements towards a formal specification language for PLCs. 2014. <u>http://doi.org/10.5281/zenodo.14907</u>
- 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, pp. 907-910, JaCoW, 2015. <u>http://dx.doi.org/10.18429/JACoW-ICALEPCS2015-WEPGF091</u>
- D. Darvas et al. Syntax and semantics of PLCspecif. CERN Report, EDMS 1523877, 2015. <u>https://edms.cern.ch/document/1523877</u>
- D. Darvas et al. Formal verification of safety PLC based control software. Integrated Formal Methods (LNCS 9681), pp. 508-522, Springer, 2016. <u>http://doi.org/10.1007/978-3-319-33693-0_32</u>

