Conformance test of logic controllers of critical systems from industrial specifications

Julien PROVOST, Jean-Marc FAURE
(LURPA, ENS Cachan)
François CHERIAUX, Laurence PICCI
(EDF R&D)

Works funded by the French Research Agency (TESTEC project)

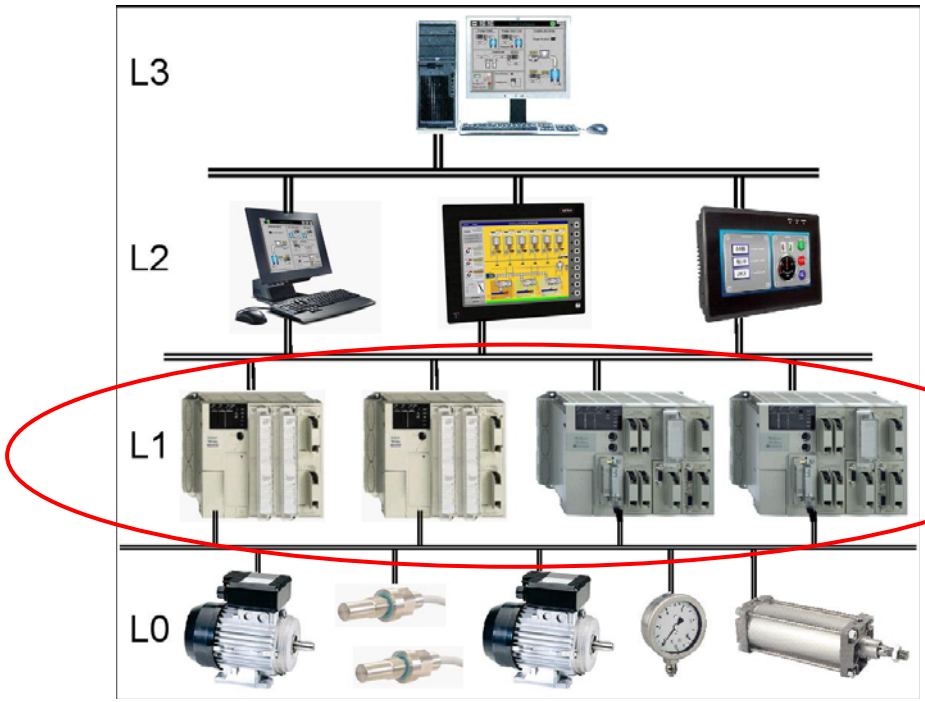
ESREL 2010

Outline

- **Background**
  - Process safety and controllers' correctness
  - Conformance test
- **Motivations of the work**
- **First contribution: avoiding combinatory explosion by preliminary verification of structural properties**
  - Method principle
  - Illustration on an example
- **Second contribution: building automatically test sequences from Grafcet specifications**
  - Method principle
  - Illustration on an example
- **Conclusion and prospects**

Process safety and controllers' correctness

Process safety relies strongly on logic controllers' correctness



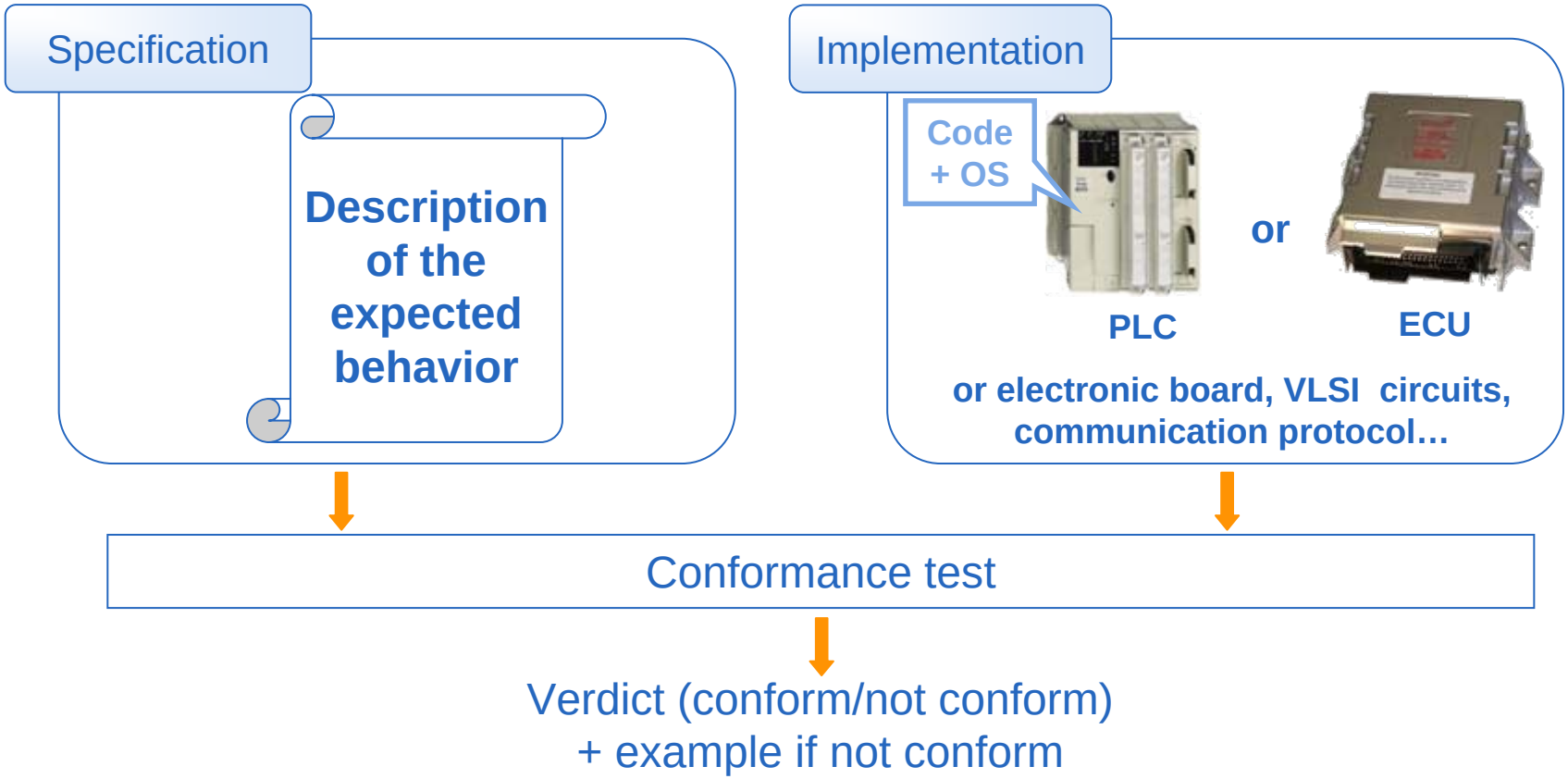
Control system architecture

Control algorithms developed from specifications in tailor-made languages (Logic Functional Diagram, Grafcet (IEC 60848))

Conformance test - 1

Overall objective

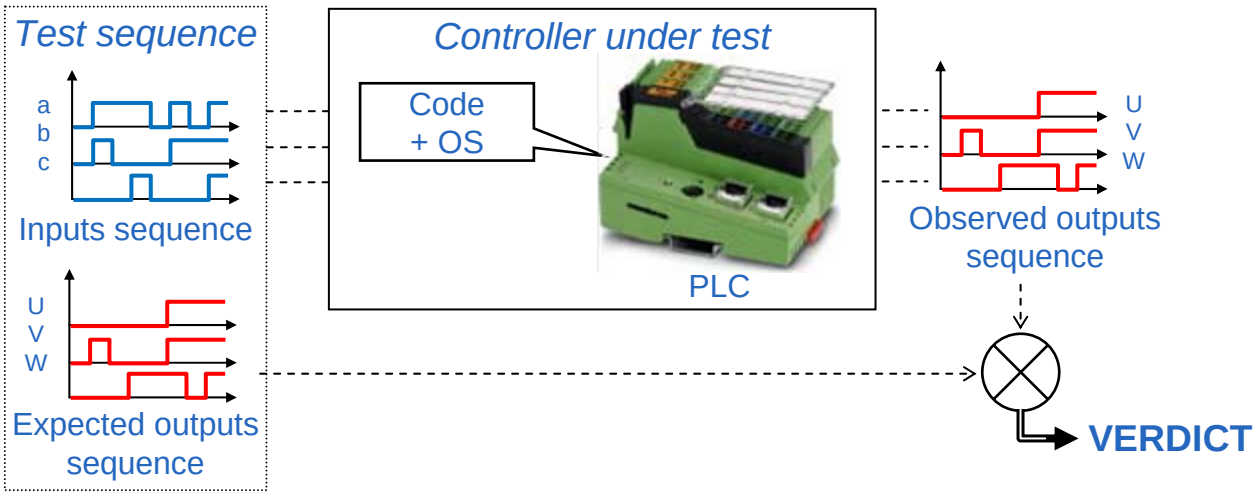
Check whether an implementation, seen as a black-box with inputs-outputs, behaves correctly with respect to its specification



Conformance test - 2

Execution of the test

- The implementation under test is connected to a test-bench which generates an inputs sequence.
- The observed outputs sequence is compared to the expected one.

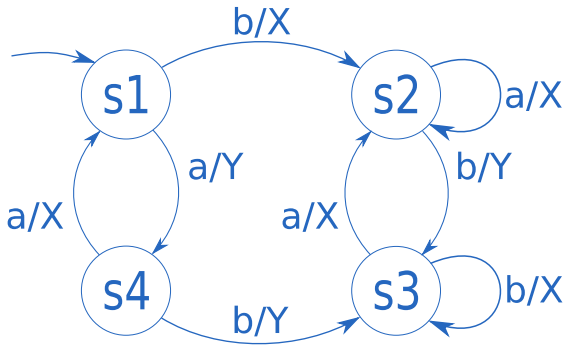


How to build automatically the test sequence from the specification?

Conformance test - 3

Many works have answered this question when the specification is a formal model for DES (Discrete Event Systems)

- Mealy machine (Lee-Yannakakis, 1996)
- Transition system (Tretmans, 2008)



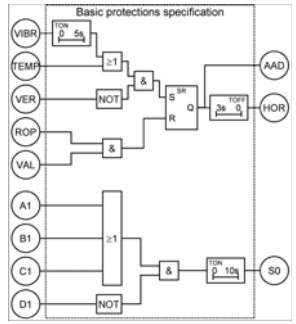
Unfortunately, two significant drawbacks

- Combinatory explosion often occurs when dealing with non-trivial examples
  - **Too long test sequence leads to non-acceptable test duration**
- Industrial specifications are not written in formal languages!

Motivations of the work

To tackle out these two issues

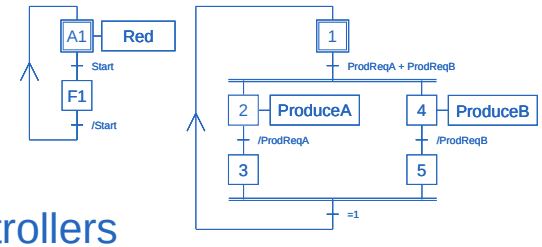
- To limit the size of the test sequence by preliminary verification of structural properties



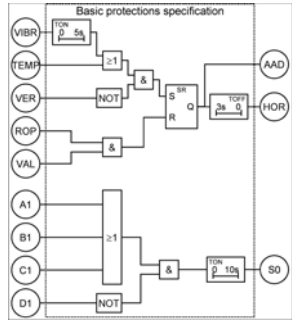
➡ Work performed for specifications in LFD

- To endow the industrial specification languages with a formal semantics so as to take benefit from the results on conformance test based on formal specification models

➡ Work performed for the IEC 60848 language (Grafcet)



Method principle



1 – Verification of structural properties of the implementation

Analyze the dependency relations between the outputs and the inputs

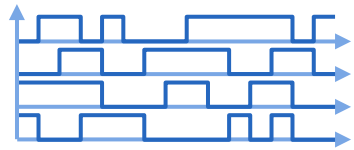
Property 1	OK
Property 2	OK
Property 3	OK
Property 4	OK
Property 5	OK
Property 6	OK

2 – Construction of a size-reduced test sequence

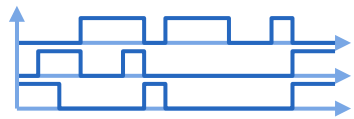
Build test steps from the dependency relations

Work developed for specifications of non-timed and timed systems

Test step	1	2	3	4	5	...
Inputs values combination	$\bar{a}.\bar{b}.\bar{c}$	a.b.c	$a.\bar{b}.\bar{c}$	$\bar{a}$.b.c	$\bar{a}.b.\bar{c}$	...
Expected outputs values combination	$\bar{U}.V.W$	$\bar{U}.V.W$	$\bar{U}.V.W$	$\bar{U}.V.W$	$\bar{U}.V.W$	...

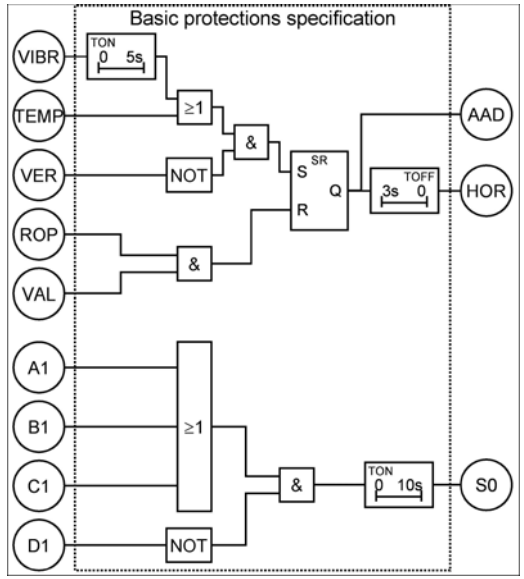


Inputs sequence



Expected outputs sequence

Example - 1



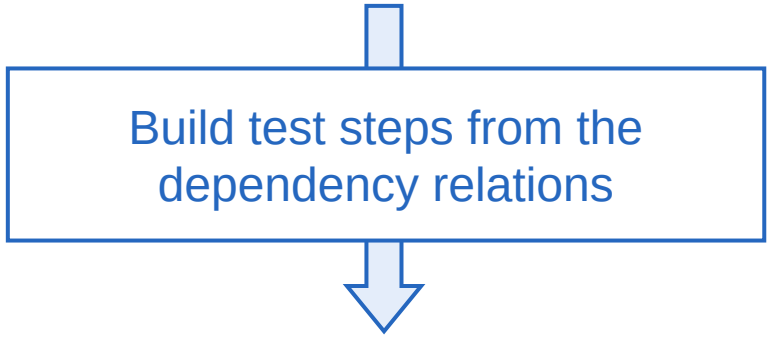
Dependency relations analysis

AAD = SR(AND(OR(TON 5S(VIBR),TEMP),NOT(VER)),AND(ROP,VAL))
HOR = TOFF 3S(SR(AND(OR(TON 5S(VIBR),TEMP),NOT(VER)),AND(ROP,VAL)))
S0 = TON 10S(AND(OR(A1,B1,C1),NOT(D1)))

Are these relations satisfied by the implementation?

Example - 2

AAD = SR(AND(OR(TON 5S(VIBR),TEMP),NOT(VER)),AND(ROP,VAL))
HOR = TOFF 3S(SR(AND(OR(TON 5S(VIBR),TEMP),NOT(VER)),AND(ROP,VAL)))
S0 = TON 10S(AND(OR(A1,B1,C1),NOT(D1)))

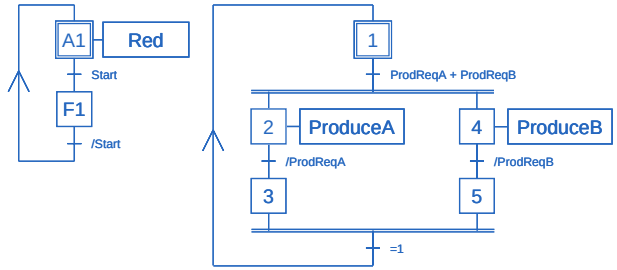


The test sequence for conformance test of AAD will include only 5 inputs sequence.

Timers and memories are observable and controllable;
then it is possible to perform separately the tests
of the non-timed and timed parts of the specification.

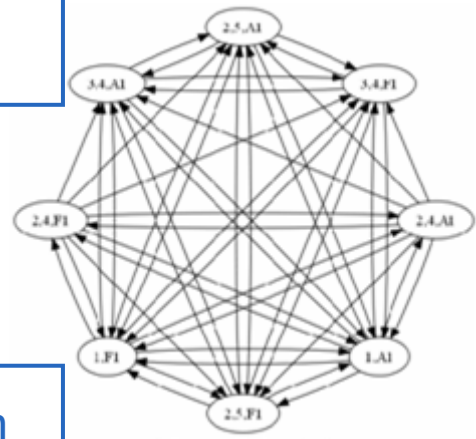
Reduction of the overall test sequence length
by one order of magnitude
and the test duration by more than two orders.

Method principle (Provost, 2009)



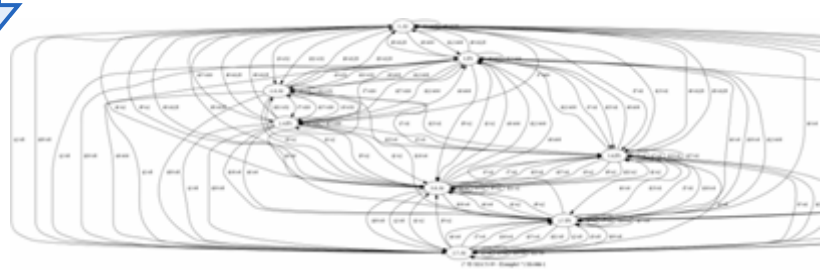
1 – Construction of the Stable Locations Automaton (SLA)

Determine the state space of the specified behavior



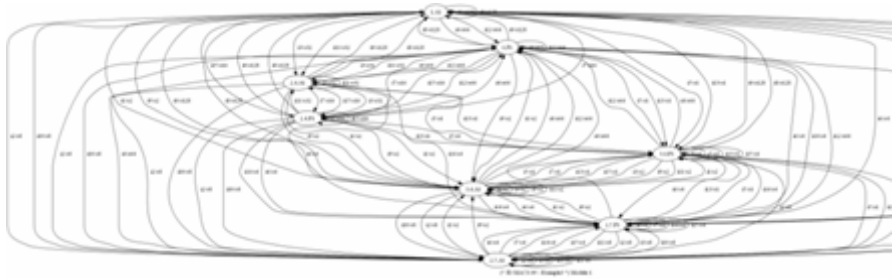
2 – Translation into a Mealy machine

Represent transitions between states by set enumeration



Work developed for specifications of non-timed logical systems

Method principle

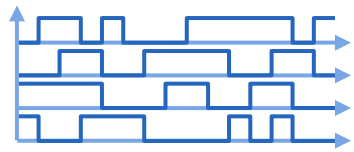


3 – Construction of a test sequence

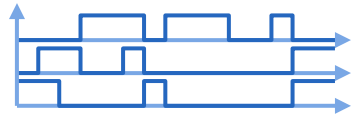
[Mei-Ko 62], [Naito 81]

Determine a sequence enabling exhaustive test

Test step	1	2	3	4	5	…
Inputs values combination	$\bar{a}.\bar{b}.\bar{c}$	a.b.c	$a.\bar{b}.\bar{c}$	$\bar{a}.b.c$	$\bar{a}.b.\bar{c}$	…
Expected outputs values combination	$\bar{U}.V.W$	$\bar{U}.V.W$	$\bar{U}.V.W$	$\bar{U}.V.W$	$\bar{U}.V.W$	…



Inputs sequence



Expected outputs sequence

Size of the Mealy machine

- The input (output) alphabet of the machine contains $2^{n_{IV}}$ ($2^{n_{OV}}$) elements, where n_{IV} (n_{OV}) is the number of input (output) variables of the SLA (Grafcet).

- Number of states of the Mealy machine = Number of locations of the SLA

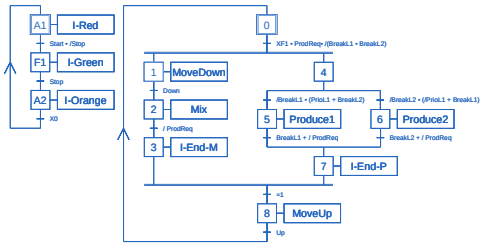
$$n_{states} = n_{LSLA}$$

- Number of transitions of the Mealy machine = f(Number of locations of the SLA, Number of input variables of the SLA (Grafcet) n_{IV})

$$n_{transitions} = n_{LSLA} \cdot 2^{n_{IV}}$$

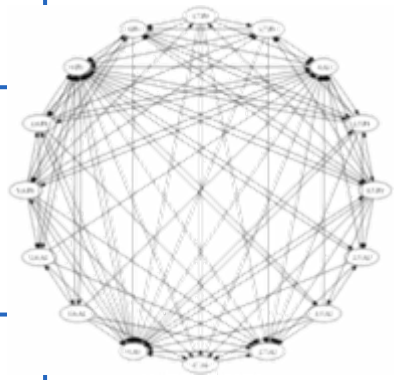
- The number of transitions of the SLA has no influence on the size of the Mealy machine.

Example



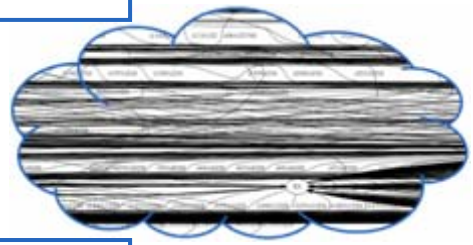
Determine all states of the specified behavior

200ms



Represent transitions between states by set enumeration

400ms



Determine a test sequence enabling exhaustive test

500ms

Test step	1	2	3	4	5	...
Inputs values combination	$\bar{a}.\bar{b}.\bar{c}$	a.b.c	a.$\bar{b}$.$\bar{c}$	$\bar{a}$.b.c	$\bar{a}$.b.$\bar{c}$	...
Expected outputs values combination	$\bar{U}$.V.W	$\bar{U}$.V.W	$\bar{U}$.V.W	$\bar{U}$.V.W	$\bar{U}$.V.W	...

Initial Grafcet

- 8 inputs, 10 outputs, 12 steps
- 2 connected graphs
- Several active steps at every date

Stable Locations Automaton

- 8 inputs, 10 outputs
- 16 locations, 102 transitions
- Single graph
- Boolean transition conditions

Mealy machine

- 256 inputs, 1024 outputs
- 16 states, 4096 directed arcs

Test sequence

- 7438 test steps

Conclusion

- **Preliminary verification of structural properties can reduce the length of test sequences built from LFDs.**
- **A formal semantics of IEC 60848 Grafcet is available and test sequences for conformance test from Grafcet specifications can be built automatically.**

- **On-going works to implement these results into an existing tool for controllers' specification, design and implementation**
  - ControlBuild – Dassault Systems

Prospects

- **To remove some limitations of the works**
  - To address LFDs with backwards loops
  - To propose a formal semantics of Grafcet including physical time modeling primitives
- **To couple the results of these two studies**
  - Formal semantics of LFD

Conformance test of logic controllers of critical systems from industrial specifications

Julien PROVOST, Jean-Marc FAURE
(LURPA, ENS Cachan)
François CHERIAUX, Laurence PICCI
(EDF R&D)

Works funded by the French Research Agency (TESTEC project)

ESREL 2010