A conformance relation for model-based testing of PLC

Anaïs Guignard

LURPA, ENS Cachan

Summary

I / Introduction

II / Test sequence construction and execution

III / A conformance relation for MIC test sequences

IV / Conclusions and perspectives

Summary

I / Introduction

- Reminder on conformance testing
- Claim
- Assumptions
- Notations
- Treated example

II / Test sequence construction and execution

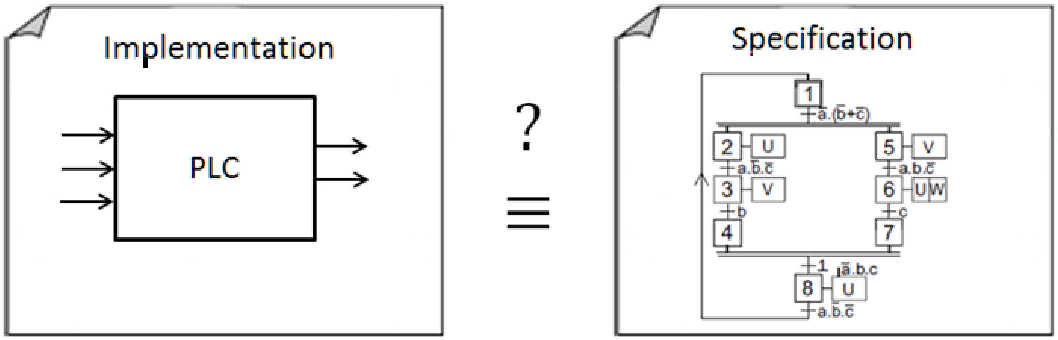
III / A conformance relation for MIC test sequences

IV / Conclusions and perspectives

Reminder – Validation

Validation of an implementation [Boehm,79]:

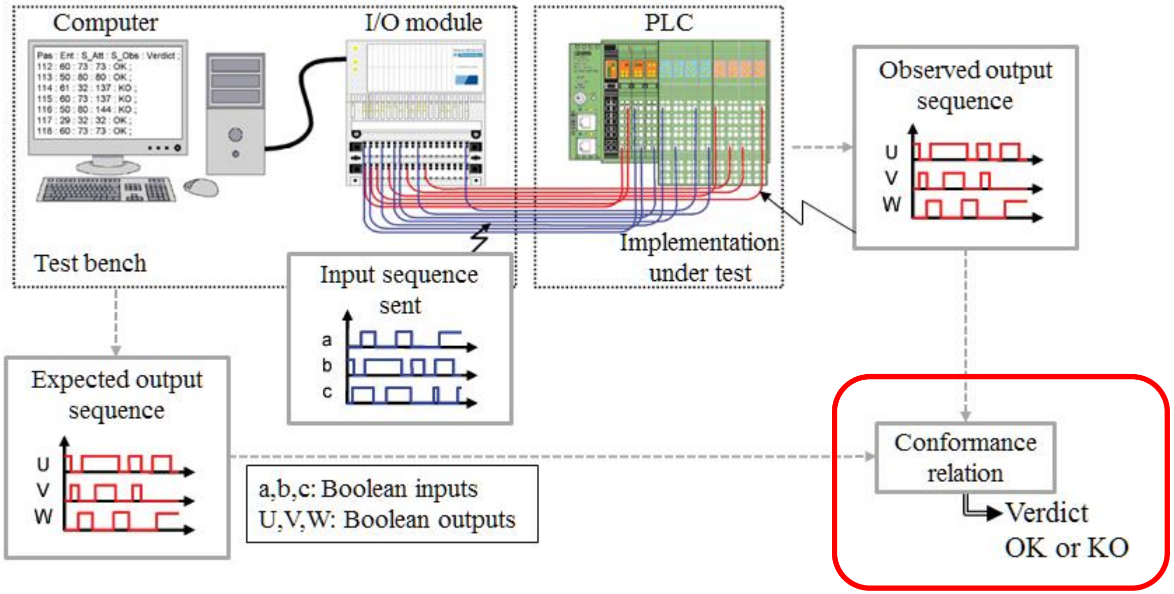
- Are we doing the right product?



Focus on conformance test

Reminder – Conformance test

Conformance test:



Based on:

- Knowledge of the formalized specification
- Generation of a test sequence depending on a given test objective
- Verdict for the whole test sequence depending on the conformance relation
- No knowledge about the plant

Relations to verify

Test objective, usually given as coverage criterion:

- Path coverage, … (Software)
- Output, logic gates coverage, … (logic circuits)
- States, Input combinations, transitions, … (functional test)

Conformance relation (also called implementation relation):

- A formal relation between implementation and specification model
- Expresses the correctness of the implementation with respect to specifications

Conformance relation

Example of conformance relations:

- **For labeled transition system: [Tretmans,96]**
  - I $ioco$ S $= \forall\sigma \in Straces(S): out(I\ after\ \sigma) \subseteq out(S\ after\ \sigma)$

- **For timed automata: [Styp,10], [Nunez,02]**
  - Timed LTS: I t$ioco$ S $= \forall\sigma \in Straces(S): out_t(I\ after_t\ \sigma) \subseteq out_t(S\ after_t\ \sigma)$
  - Timed FSM : I $conf_a$ S $iff\ I\ conf_{nt}\ S\ and\ \forall e \in NTEvol(I) \cap NTEvol(S), \forall t,$

    $$(e,t) \in TEvol(I) \Rightarrow (e,t) \in TEvol(S)$$

- **For Mealy machine:**
  - I $conf$ S $iff\ \forall et \in \sigma_{test},\ the\ observed\ (I_{obs}, O_{obs})\ is\ such\ as$

    $$\delta(s_u, I_{obs}) = s_d\ and\ \lambda(s_u, I_{obs}) = O_{obs}$$

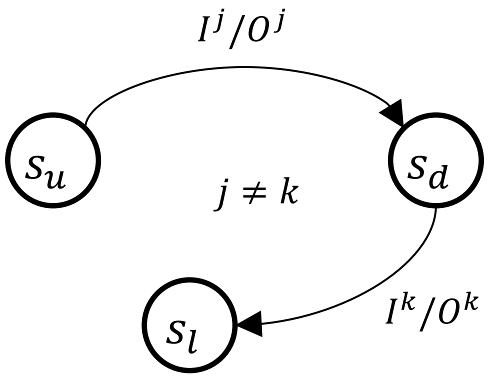
Claim

- Usual conformance relations are based on models of the implementation
- Conformance test is performed on a Programmable Logic Controllers (PLC)
- We claim to propose a conformance relation that takes in count the features of the PLC as the cyclic reading of the inputs values

Assumptions

On the specification model:

- **Non timed**
- **Mealy machine**
- **Complete and deterministic**
- **Without transient evolution (two following transitions that are not self-loop with the same input condition)**
- **States distinguishable by the output emission**



On the observation:

- **All Input/Output changes are detected**

Notations

V_I Set of input variables

V_O Set of output variables

A Mealy machine is a $6-tuple\ (\mathcal{I}_M, \mathcal{O}_M, S, s_{init}, \delta, \lambda)$ where:

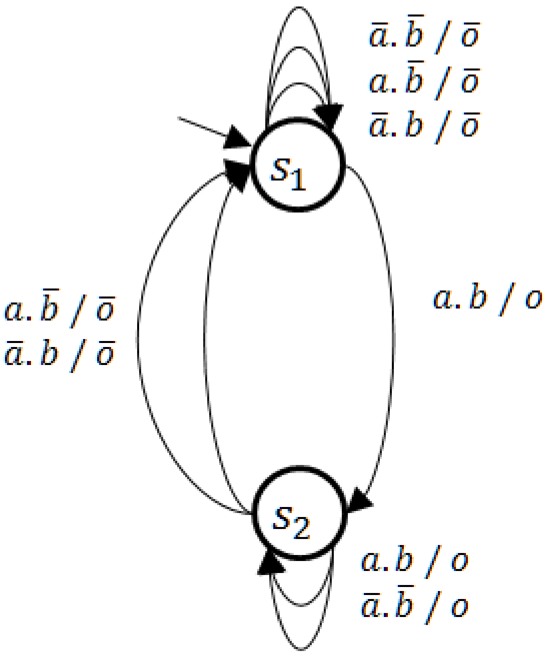
- $\mathcal{I}_M$ is the input alphabet
- $\mathcal{O}_M$ is the output alphabet
- S is the set of states
- s_{init} is the initial state
- $\delta: S \times \mathcal{I}_M \rightarrow S$ is the transition function
- $\lambda: S \times \mathcal{I}_M \rightarrow \mathcal{O}_M$ is the output function

$\sigma = (\ldots, (I_{obs}, O_{obs}), \ldots)$ Observation sequence with $I_{obs} \in \mathcal{I}_M$ and $O_{obs} \in \mathcal{O}_M$

Example of specification model

2 inputs : $\mathbf{V_I} = \{a, b\}$

1 output : $\mathbf{V_O} = \{o\}$



Summary

I / Introduction

II / Test sequence construction and execution

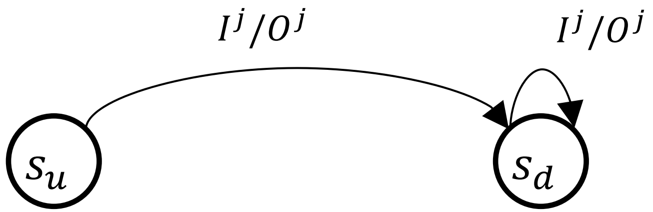
- MIC test sequence
- Desynchronization phenomenon and consequences
- SIC test sequence
- SIC/MIC test sequence

III / A conformance relation for MIC test sequences

IV / Conclusions and perspectives

Test step

Transition to test :

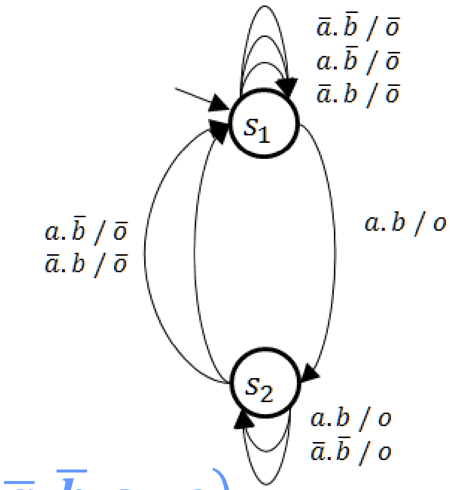


Elementary test step : $et = (s_u, I^j, s_d, O^j)$

- Remark: One test step test both the transition and the self-loop

Test sequence : $TS = (et_1, \dots, et_n)$

Test sequence



Test sequence with :

- Minimal-length test sequence

$$TS_{MIC} = \big((s_1, \bar{a}.\bar{b}, s_1, \bar{o}), (s_1, a.b, s_2, o), (s_2, \bar{a}.\bar{b}, s_2, o), (s_2, a.\bar{b}, s_1, \bar{o}), (s_1, a.b, s_2, o), (s_2, \bar{a}.b, s_1, \bar{o})\big)$$

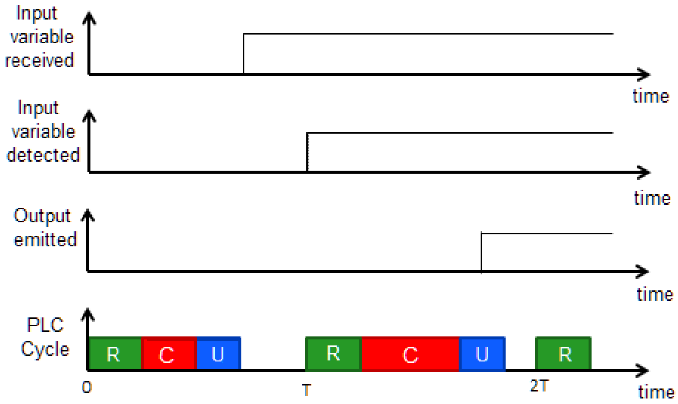
There are some Multiple – Input – Change (MIC) test steps.

- For example: $(s_1, \bar{a}.\bar{b}, s_1, \bar{o}), (s_1, a.b, s_2, o)$ need a and b to synchronously change to True

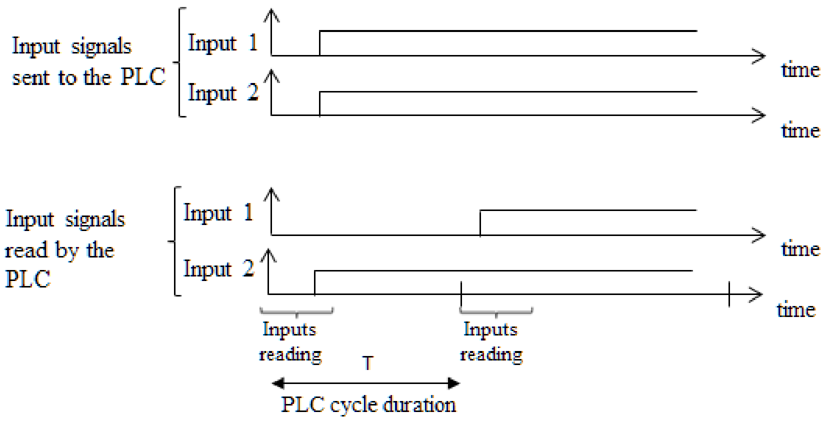
This may be wrongly treated by the PLC.

Desychronization phenomenon

Due to the Cyclic I/O scanning of the PLC



Synchronous changes of inputs can be read on different PLC cycles



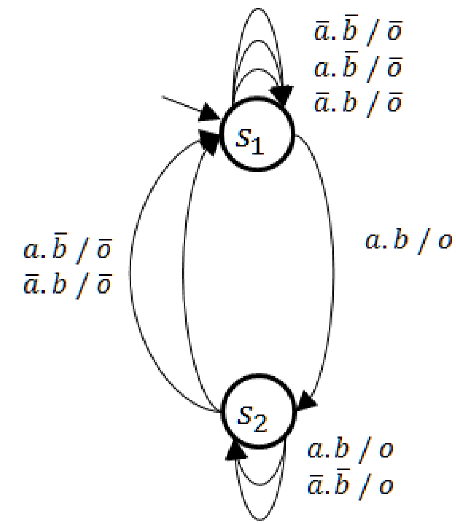
Frequency on test execution

Experiment [Provost,10]:

- 8 simultaneous input changes from False to True then True to False
- Inputs allocated on two I/O modules
- 20 000 drawings

Input changes \ PLC period		10 ms	20 ms
On main module	True to False	0,022 %	0,014 %
	False to True	0,886 %	0,455 %
On secondary module	True to False	0,040 %	0,020 %
	False to True	0,993 %	0,550 %
On both modules	True to False	39,62 %	20,23 %
	False to True	43,46 %	21,89 %

SIC test sequence



Test sequence [Provost,10]:

- Only Single – Input – Change test steps
- Minimal length

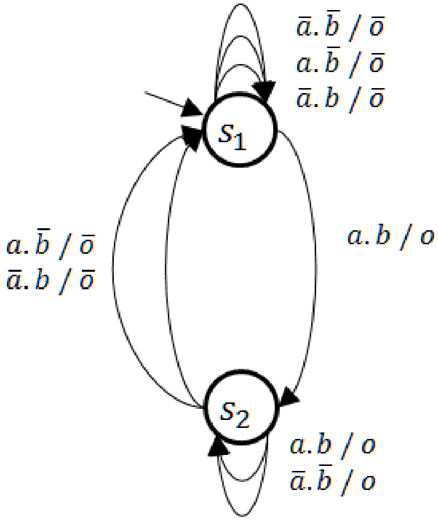
$$TS_{SIC} = ((s_1, \bar{a}.\bar{b}, s_1, \bar{o}), (s_1, a.\bar{b}, s_1, \bar{o}), (s_1, a.b, s_2, o),$$
$$(s_2, a.\bar{b}, s_1, \bar{o}), (s_1, a.b, s_2, o), (s_2, \bar{a}.b, s_1, \bar{o}))$$

Test step $(s_2, \bar{a}.\bar{b}, s_2, o)$ is missing

Conclusion:

- Not always possible to guarantee the test objective with a SIC sequence

Minimal MIC test sequence



Solution SIC – MIC [Provost,10]:

- Minimal-length SIC sequence
- Followed by non-SIC-testable test steps

$$TS_{mixed} = ((s_1, \bar{a}.\bar{b}, s_1, \bar{o}), (s_1, a.\bar{b}, s_1, \bar{o}), (s_1, a.b, s_2, o), (s_2, a.\bar{b}, s_1, \bar{o}), (s_1, a.b, s_2, o), (s_2, \bar{a}.b, s_1, \bar{o}), (s_1, a.b, s_2, o), (s_2, \bar{a}.\bar{b}, s_2, o))$$

Discussion :

- Reduces the amount of MIC test steps some can not be avoided
- The conformance relation must take them in count

Summary

I / Introduction

II / Test sequence construction and execution

III / A conformance relation for MIC test sequences

- Consequences of desynchronization on test
- Definition of a conformance relation
- Illustration
- Pursue of test execution

IV / Conclusions and perspectives

Expected behavior

Initial situation:

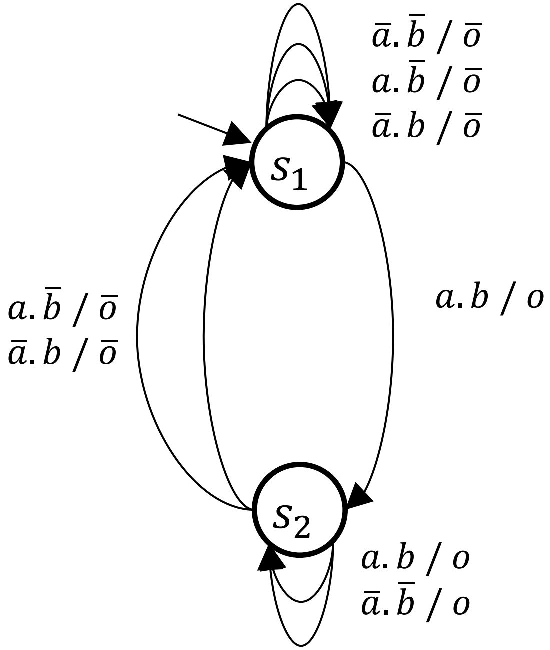
- State s_2 active
- Input combination $a.b$

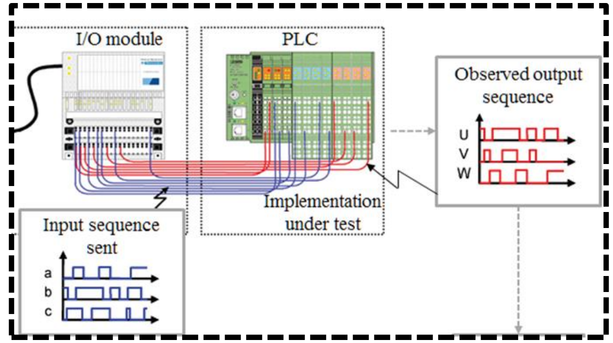
Test step:

- $et = \left(s_2, \bar{a}.\bar{b}, s_2, o\right)$

Expected sequence:

- $\sigma = \left((a.b, o)\,, (\bar{a}.\bar{b}, o), (\bar{a}.\bar{b}, o), \dots\right)$





Effective behavior

I/O observed outside the PLC

Expected sequence:

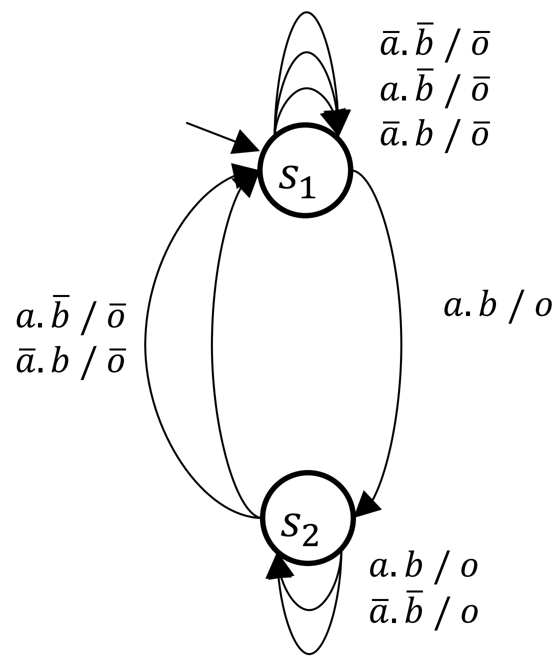
- $\sigma = \left((a.b, o), (\bar{a}.\bar{b}, o), (\bar{a}.\bar{b}, o), \dots\right)$

PLC read/updated sequence:

- $\sigma = \left((a.b, o), \underbrace{(a.\bar{b}, \bar{o})}, (\bar{a}.\bar{b}, \bar{o})\right)$

Observed sequence:

- $\sigma = \left((a.b, o), \underbrace{(\bar{a}.\bar{b}, \bar{o})}, (\bar{a}.\bar{b}, \bar{o})\right)$



Idea

The observed sequence is not the expected one

However, this implementation conforms to the specification

It should not be rejected by the conformance relation.

Conformance relation

Let $et_c = (s_b; I^j; s_c; O^j)$ be the current test step, Let $et_p = (s_a; I^i; s_b; O^i)$ be the previous test step.

The implementation conforms to the specification if for every test step there is:

Either:

- **If $s_b \neq s_c$: $\exists k \in \mathbb{N}^*$ such as $k < n$ and:**
  - If $k > 1$: $\forall l \in \mathbb{N}^*$ such as $l < k, O_{obs_l} = O^i$
  - $O_{obs_k} = O^j$
  - $\forall m \in \mathbb{N}^*$ such as $k < m \leq n, O_{obs_m} = O^j$
- **If $s_b = s_c$: $\forall k \in \mathbb{N}^*$ such as $k \leq n, O_{obs_k} = O^j$**

Test of the firing of a transition

Test of a self-loop

Or

- **$\exists k < n - 1$ such as:**
  - If $k > 1$: $\forall l \in \mathbb{N}^*$ such as $l < k, O_{obs_l} = O^i$
  - It exists $I^x \in \mathcal{I}_M$ such as:
    - $(I^x \setminus I^i \cup I^i \setminus I^x) \subset (I^j \setminus I^i \cup I^i \setminus I^j)$
    - $\lambda(s_b, I^x) = O_{obs_k}$
  - Let $s = \delta(s_b, I^x)$ be the downstream state of the transition,
  - It exists a transition such as $\lambda(s, I^j) = O_{obs_{k+1}}$
  - And $\forall m \in \mathbb{N}^*$ such as $k + 1 < m \leq n, O_{obs_m} = O_{obs_{k+1}}$

Test on which input changes are seen asynchronously:

- Checks if a transition exists from the current state associated to the observed output
- Checks if the input condition is a subset of input changes
- Checks if the next PLC cycle correctly takes in count all the input changes

Example of a correct implementation

Initial situation:

- State s_2 active
- Input combination $a.b$

Test step:

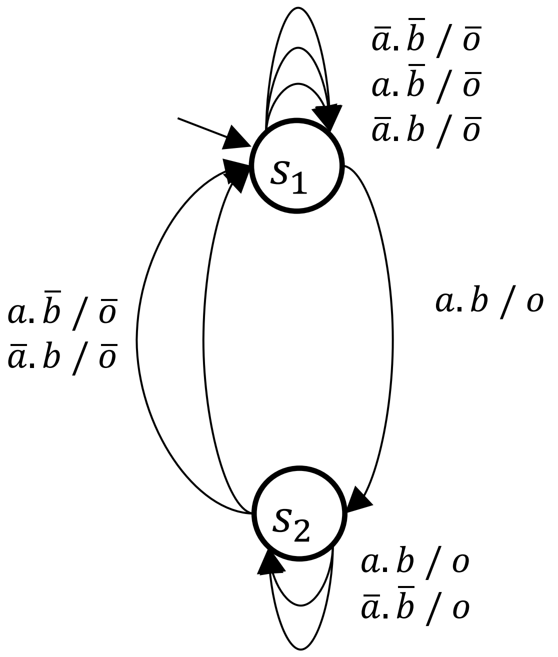
- $et = (s_2, \bar{a}.\bar{b}, s_2, o)$

Expected sequence:

- $\sigma = \left((a.b, o), (\bar{a}.\bar{b}, o), (\bar{a}.\bar{b}, o), \ldots\right)$

Observed sequence:

- $\sigma = \left(\underbrace{(a.b, o)}, \underbrace{(\bar{a}.\bar{b}, \bar{o})}, \underbrace{(\bar{a}.\bar{b}, \bar{o})}\right)$



Example of an incorrect implementation

Initial situation:

- State s_2 active
- Input combination $a.b$

Test step:

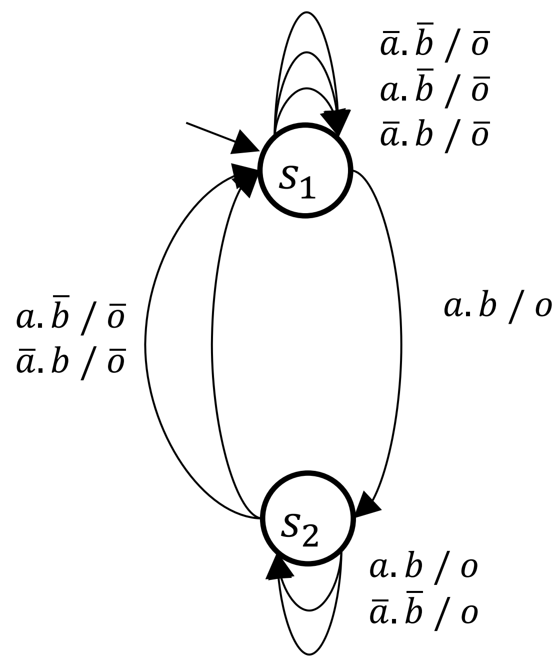
- $et = (s_2, \bar{a}.\bar{b}, s_2, o)$

Expected sequence:

- $\sigma = \left((a.b, o)\ , (\bar{a}.\bar{b}, o), (\bar{a}.\bar{b}, o), \dots \right)$

Observed sequence:

- $\sigma = \left((a.b, o)\ , (\bar{a}.\bar{b}, \bar{o}), (\bar{a}.\bar{b}, o) \right)$



Pursue of the test execution

After a desynchronization phenomenon:

- There is no guarantee that the active state is the expected state
- The active state will not correspond to the one in the next test step
- It is necessary to modify the test sequence to continue the test

Possible solutions:

- Recomputation of the whole sequence
- Finding a previous test step from which to restart the test
- Finding a SIC path to come back to the treated test step

Summary

I / Introduction

II / Test sequence construction and execution

III / A conformance relation for MIC test sequences

IV / Conclusions and perspectives

Conclusions and perspectives

Conclusion:

- **To meet the test objective, it is not always possible to prevent MIC test steps**
- **Asynchronous read of synchronous input changes cannot be ignored in the conformance relation**
- **A new conformance relation has been defined**
- **To be published in WODES'14:**
  - A. Guignard, J.M. Faure, A conformance relation for model-based testing of PLC, 12th International Workshop on Discrete Event Systems, 2014

Perspectives:

- **Choice and implementation of a method to pursue test execution**
- **Adaptation to closed-loop validation methods (to be submitted at ETFA'14)**

Bibliography

[Boehm,79]:

B. Boehm, *Software engineering: R&D trends and defense needs*, Research directions in software technology, 1979

[Tretmans,96]:

J. Tretmans: *Test Generation with Inputs, Outputs and Repetitive Quiescence*, Software concept and tool 17, 1996

[Styp,10]:

S. Styp, H. Bohnenkamp, J. Schmaltz, *A Conformance Testing Relation for Symbolic Timed Automata*, Formal Modeling and Analysis of Timed Systems, 2010

[Nunez,02]:

M. Nunez, I. Rodriguez, *Encoding PAMR into (Timed) EFSMs*, Formal Techniques for Networked and Distributed Sytems — FORTE, 2002

[Provost,10]:

J. Provost, J.M. Roussel, J.M. Faure, *SIC-testability of sequential logic controllers*, 10th International Workshop on Discrete Event Systems, 2010