Obtaining temporal and timed properties of logic controllers from fault-tree analysis

Israel BARRAGAN SANTIAGO*

Jean-Marc FAURE

Matthias ROTH

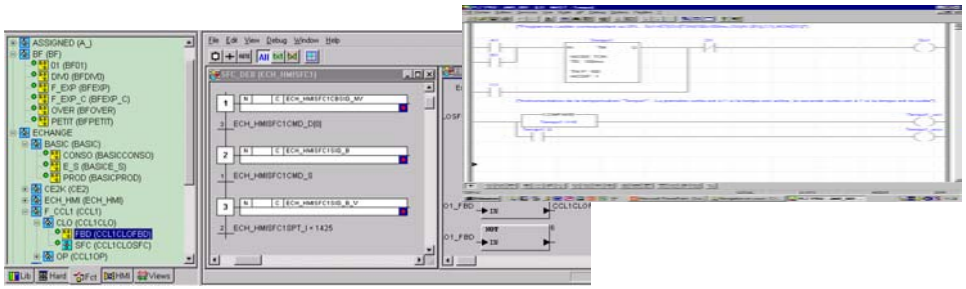
*The Mexican Council of Technology CONACYT finances Israel BARRAGAN

Outline

- Objective of the work
- Scientific challenges and proposals
- Formal models of temporal and timed gates
- Example
- Conclusion and prospects

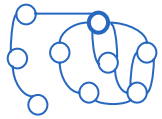
Model-Checking

Logic controller (SFC, LD, …)

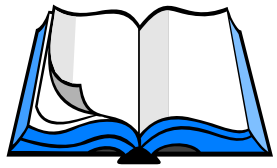


Modelling

State automaton



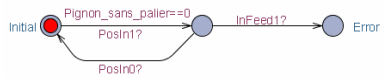
Requirements (not formal)



Significant drawback

Formalisation

AG(APB→AF ~horn)



Formal properties

Model-checking tool

Temporal MC : NuSMV

Timed MC : UPPAAL

Properties verified or counter-example

Design of formal properties

This work proposes a method to facilitate the identification and formalization of controller properties by means of Fault Tree Analysis.

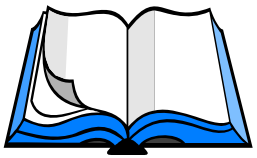
- The method shall avoid the tedious task of properties formalisation from system requirements.
- The purpose is to facilitate the use of model checking tools and techniques.

Fault tree analysis (FTA)

- **is a widespread technique for critical systems**
- shows the advantage of focusing on all the causes of an unexpected event
- is graphical
- is tool-supported (FT+, ARALIA, Hip-Hops, …)

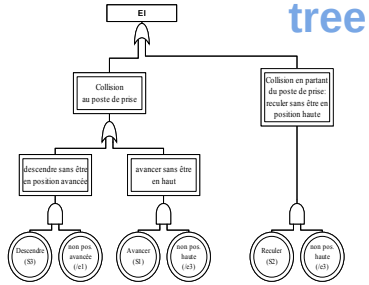
Method overview

Requirements (not formal)



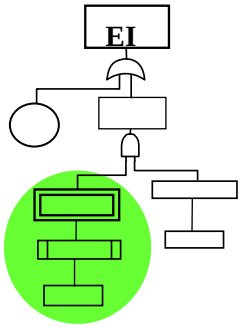
1

Resulting fault tree



2

Identifying controller faults



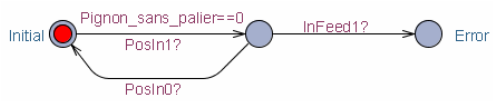
3

Steps

1. Design of the fault tree including physical component failures and controller faults.
2. Identification of sub-trees related to logic controller faults.
3. Derivation of formal properties (temporal logic, timed automata,..) stating how the controller must behave so as not to generate the fault.
4. Model-checking to verify if the properties holds or not on the controller model.

Formal properties (temporal or timed)

AG(APB→AF ~horn)



4

Model Checker

Manual activity

Automatic activity

Logic controller faults

Are systematic

- Such faults come from design flaws in the logic of the controller, either coding errors or misinterpretation of control requirements.
- They can be reproduced every time the conditions that trigger the error in the control logic are present.

Cannot be described only by combinatory expressions using Boolean connectors (AND, OR, …)

- They must be represented by DES models able of describing sequences of events and physical time.
- There is a need for gates enabling to express event ordering and physical delays (to describe faults related to physical time).

Must be written in a formalism suitable for properties construction (temporal logic, state automata)

Our proposals

New Fault-Tree general template

Definition of relevant gates to describe event ordering (temporal gates) and physical time (timed gates)

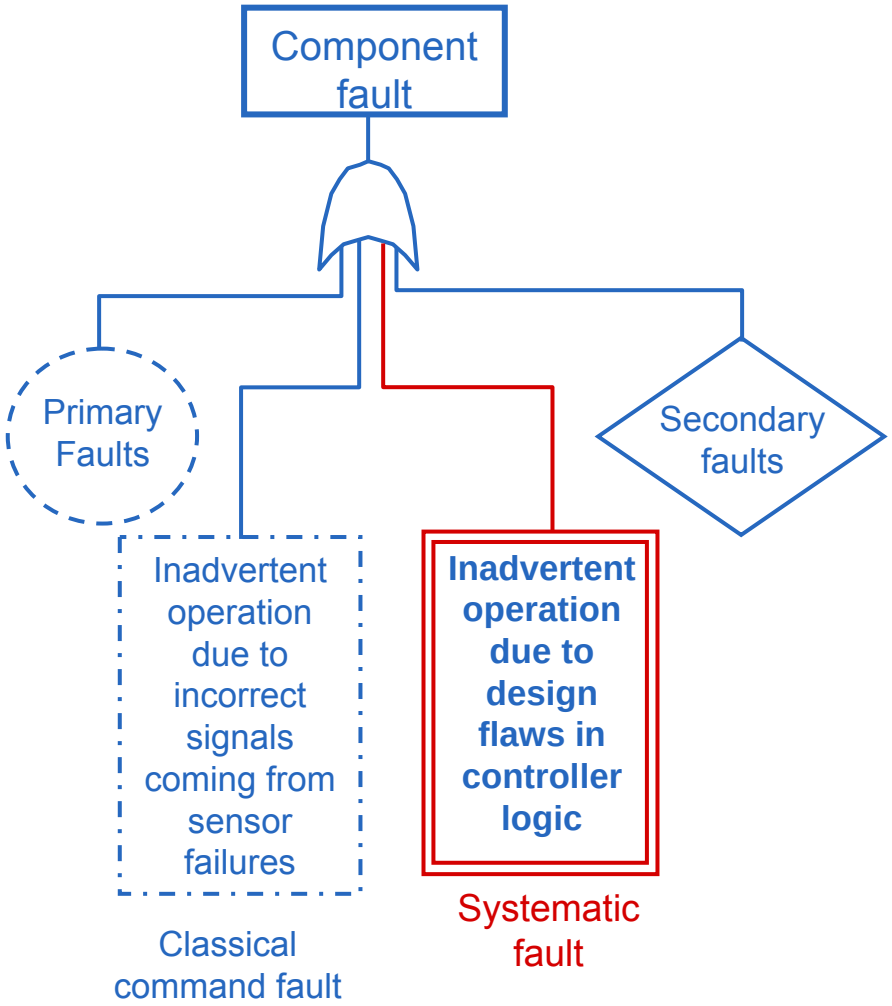
Formalization of temporal and timed gates

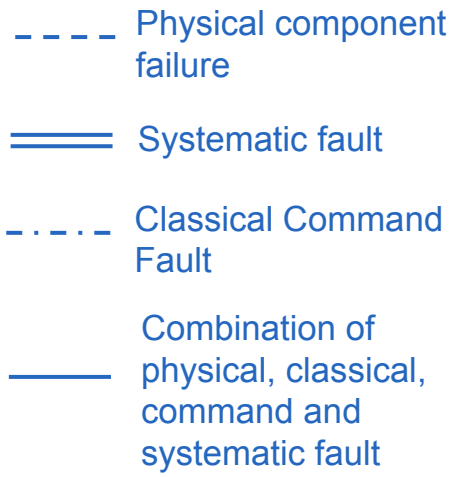
Composition rules

- To check consistency of a FT including several temporal and timed gates.
- To simplify consistent FTs by building automata equivalent to combinations of gates (use of product of automata Ac: A1|| A2).

New FT general template

[Barragan, Faure and Papadopoulos, Safeprocess 2006]

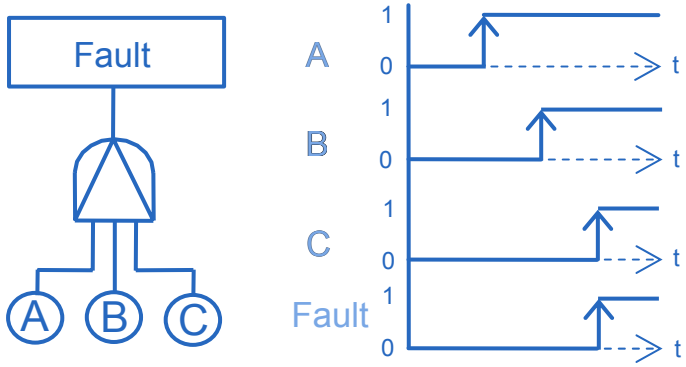




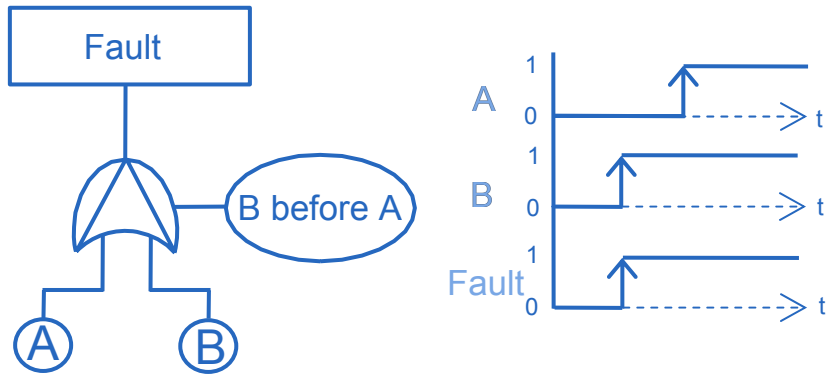
Existing temporal and timed gates

Temporal gates [FT Handbook, 1981] enable to express event ordering

Priority AND

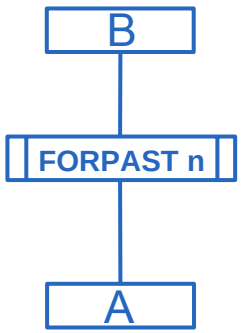


Exclusive OR with condition



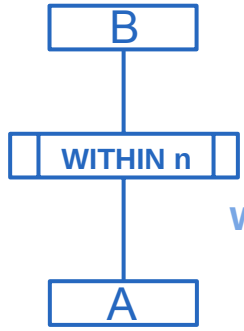
Timed gates [Palshikar, 2003], enable to express physical time

FORPAST n



A stays TRUE during n time units

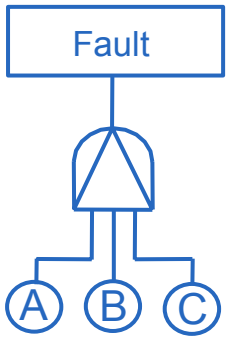
WITHIN n



A stays TRUE at least one time unit within a n time units interval

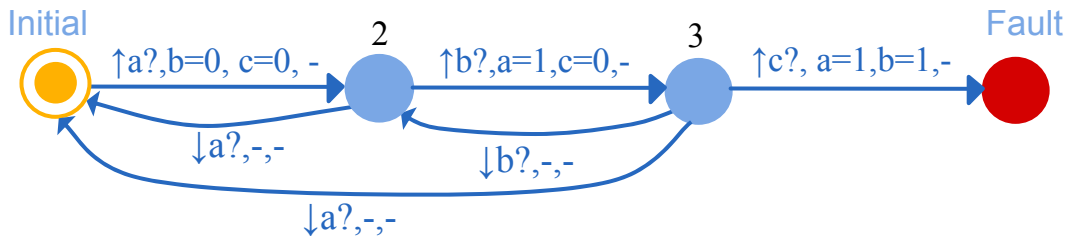
Formalizing temporal gates behaviour

Priority AND



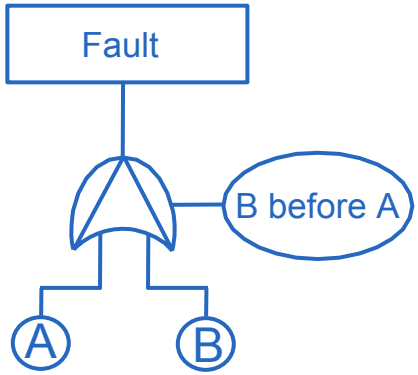
AG ¬ (A => EF (A.B => EF ABC))

In CTL



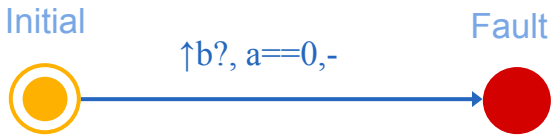
Observer automaton

Exclusive OR with condition



A (¬ B W A)

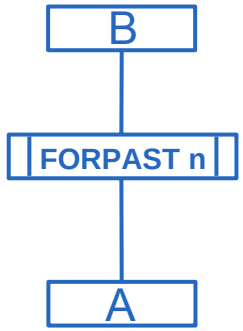
In CTL



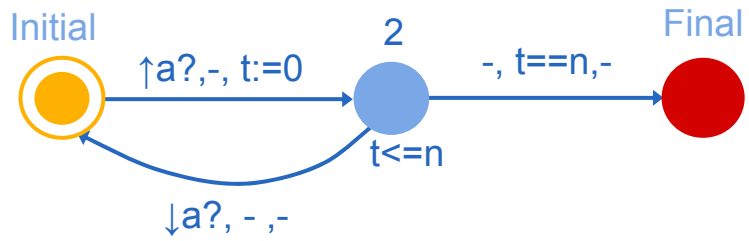
Observer automaton

Formalizing timed gates behaviour

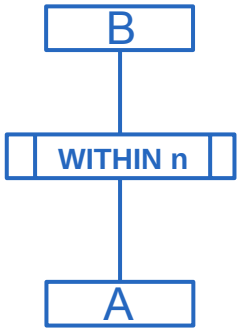
FORPAST n

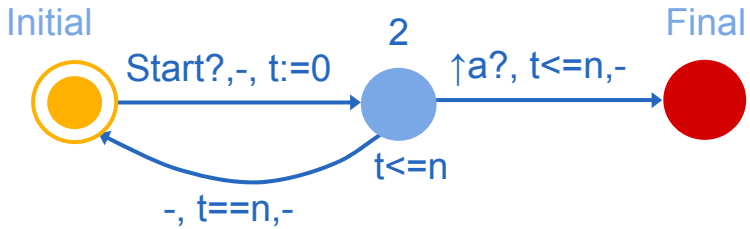


Timed Automata:



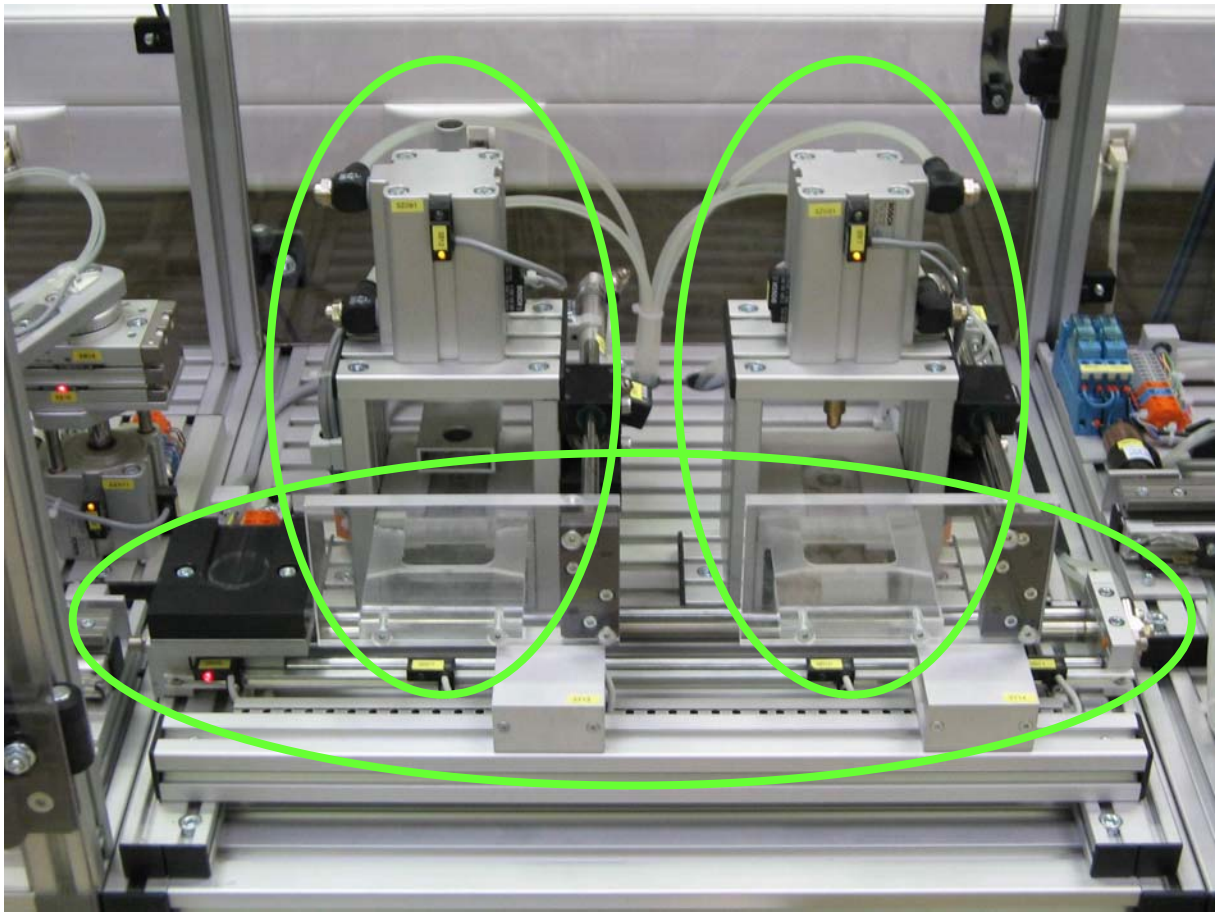
WITHIN n



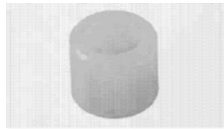


Example: Bosch Mechatronic system

Station function: To insert/remove bearings in gear wheels



Gear wheel



Bearing

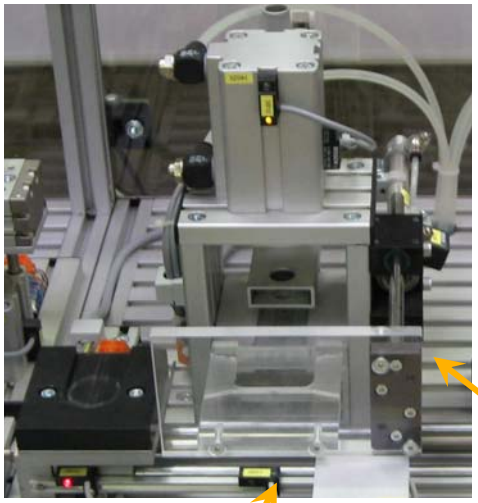
3 sub-systems:

Press to insert bearings

Press to remove bearings

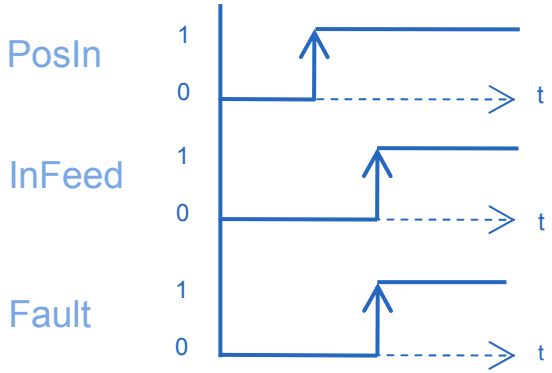
Conveyor

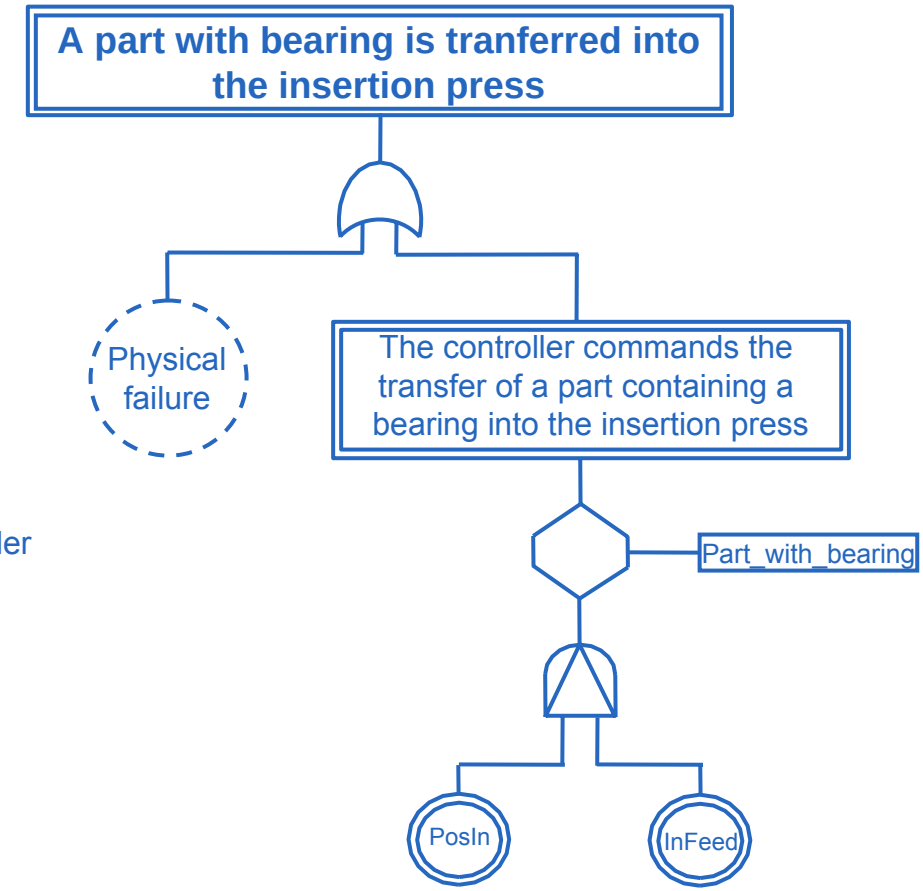
First case



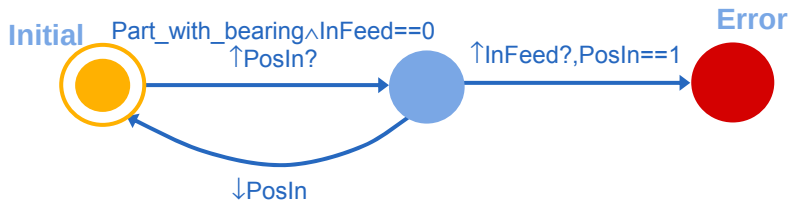
Feeder cylinder (InFeed)

Position sensor (PosIn)

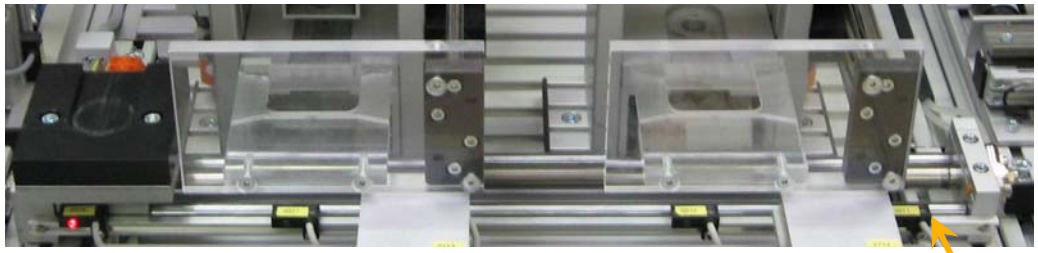




MC UPPAAL:

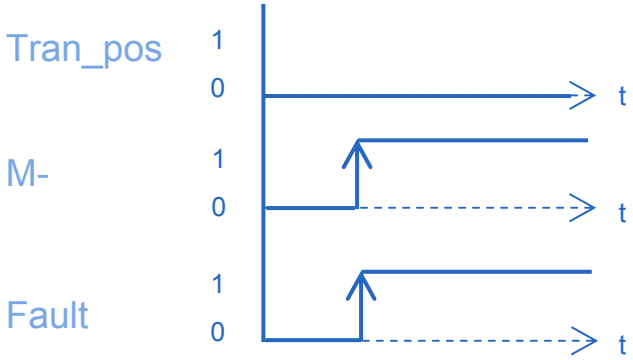


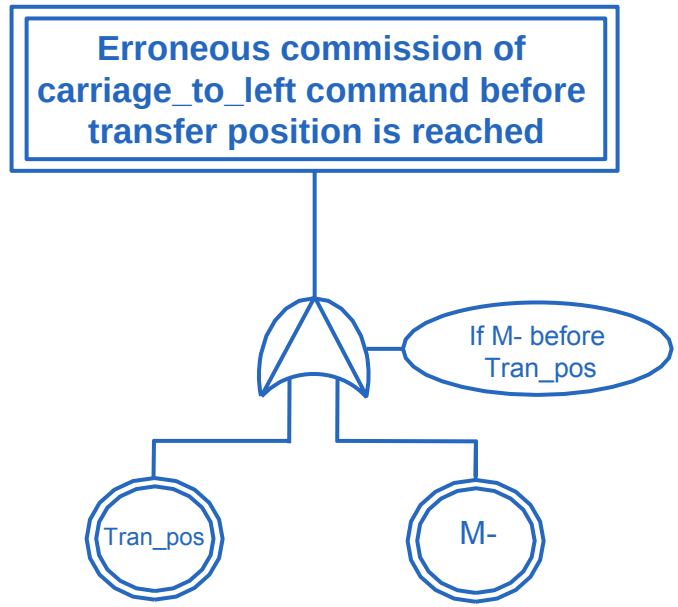
Second case



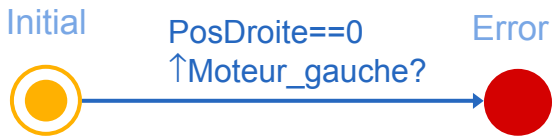
M

Transfer position
(Tran_pos)

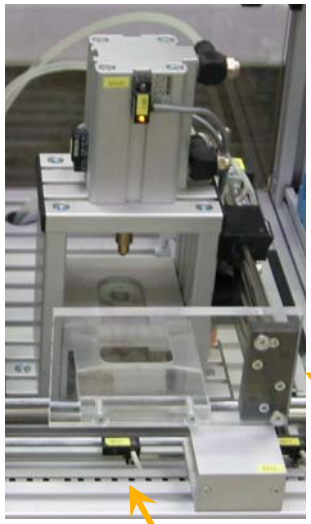




MC UPPAAL:

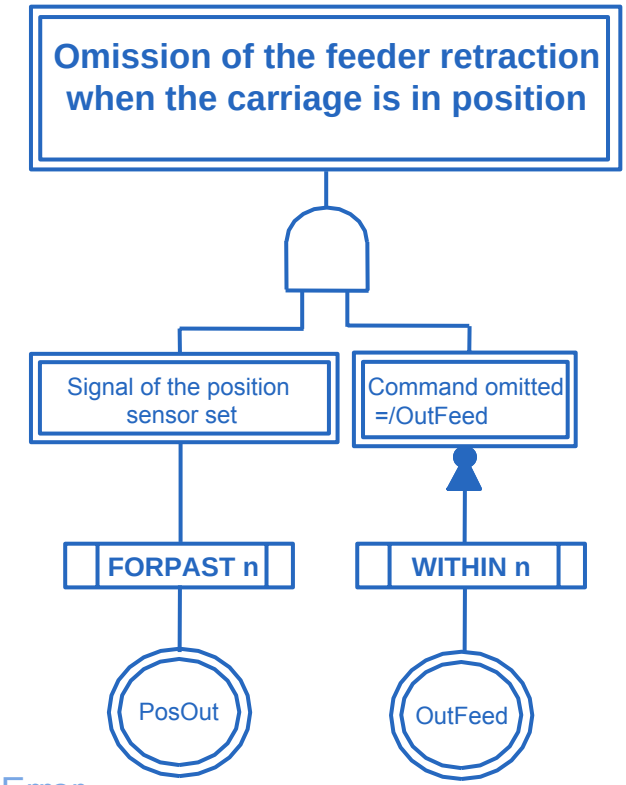


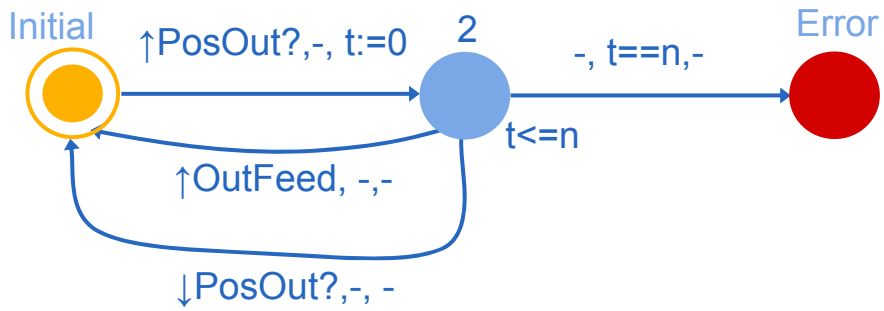
Third case: timed property



Feeder cylinder
(OutFeed)

Position sensor
(PosOut)





Conclusion and prospects

- Fault tree analysis including systematic faults of controllers can be used to simplify properties construction.
- Definition of the operational semantics of the temporal and timed gates in a model-checker compliant formalism.
- Consistency checking and FT simplification

  Rules to combine gates must be developed

  Automatic generation of minimal cut sequences
- Partial integration of the method with other works dealing with automatic generation of FT (Hip-Hops, Papadopoulos, Y. and M. Maruhn, 2001).

Obtaining temporal and timed properties of logic controllers from fault-tree analysis

Thank you for attention

Any questions ?