Uppaal, a toolbox for modelisation, simulation and verification of real time systems

Jamal Ben Azouze, Marien Bourguignon, Nicolas De Groote, Simon Picard, Arnaud Rosette, Gabriel Ekanga

3 juin 2015

Table of Contents

Introduction

UPPSALA
UNIVERSITET

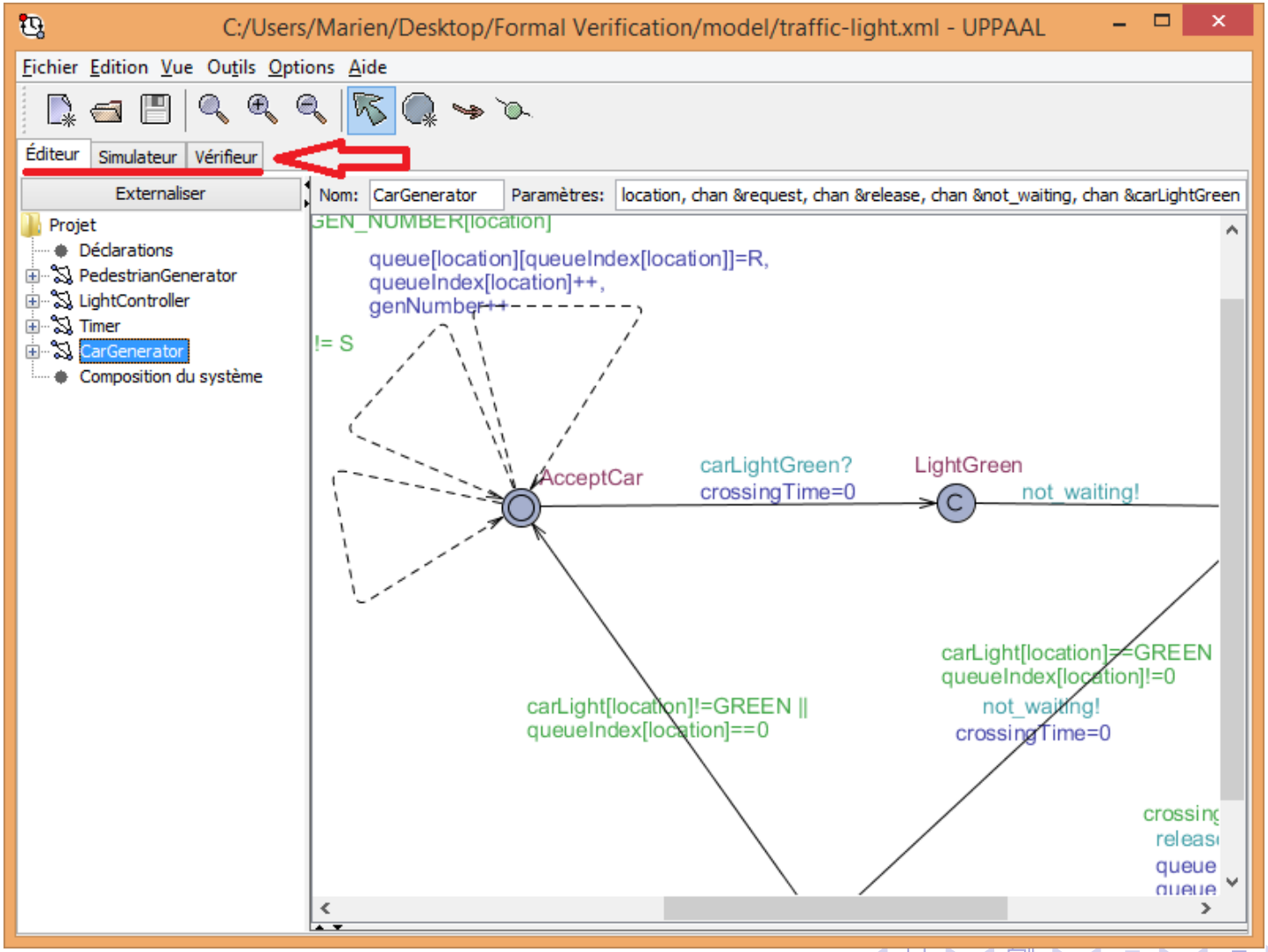
AALBORG UNIVERSITY

Features of Uppaal

Toolbox which allows

1. **Modelisation** of system through network of timed automata
2. **Simulation** through a real time simulator
3. **Model checking** through TCTL formulas

GUI


C:/Users/Marien/Desktop/Formal Verification/model/traffic-light.xml - UPPAAL
Fichier Edition Vue Outils Options Aide
Éditeur Simulateur Vérifieur
Externaliser
Projet
Déclarations
PedestrianGenerator
LightController
Timer
CarGenerator
Composition du système
Nom: CarGenerator
Paramètres: location, chan &request, chan &release, chan &not_waiting, chan &carLightGreen
queue[location][queueIndex[location]]=R,
queueIndex[location]++,
genNumber++
!= S
AcceptCar
carLightGreen?
crossingTime=0
LightGreen
not_waiting!
carLight[location]==GREEN
queueIndex[location]!=0
not_waiting!
crossingTime=0
carLight[location]!=GREEN ||
queueIndex[location]==0

Modelisation tool

Model made of

1. Extended timed automata (aka *templates*)
2. Combined into a *system* (network of timed automata)

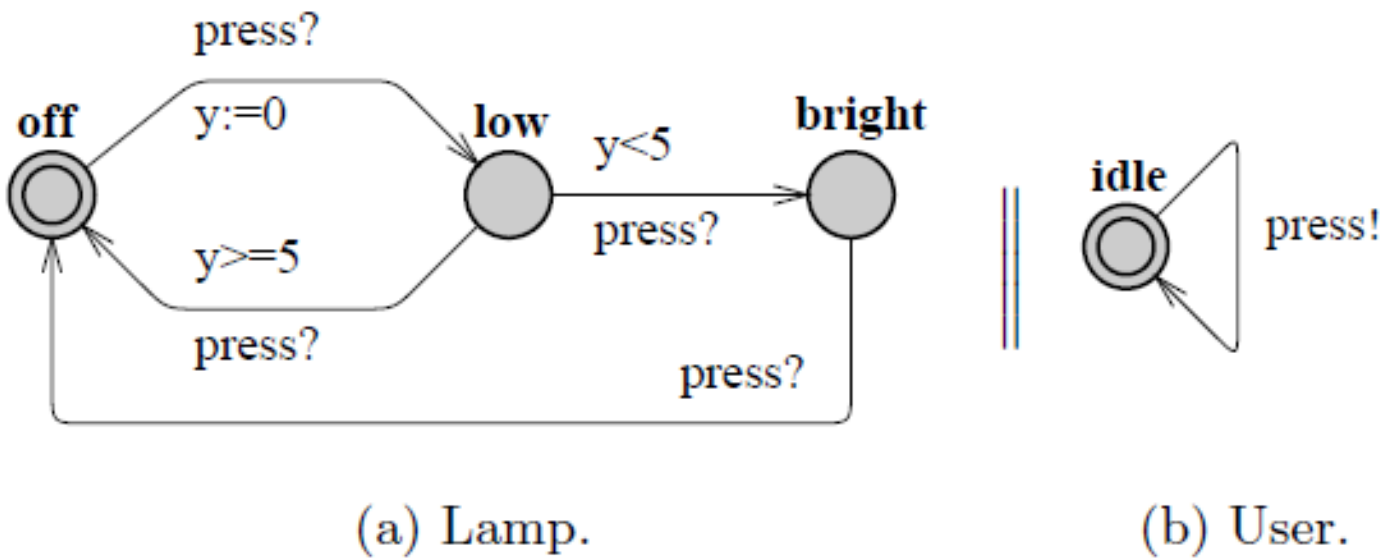


Figure: System made of ETAs. Image from *A Tutorial on Uppaal*

Extended Timed Automata (ETA)

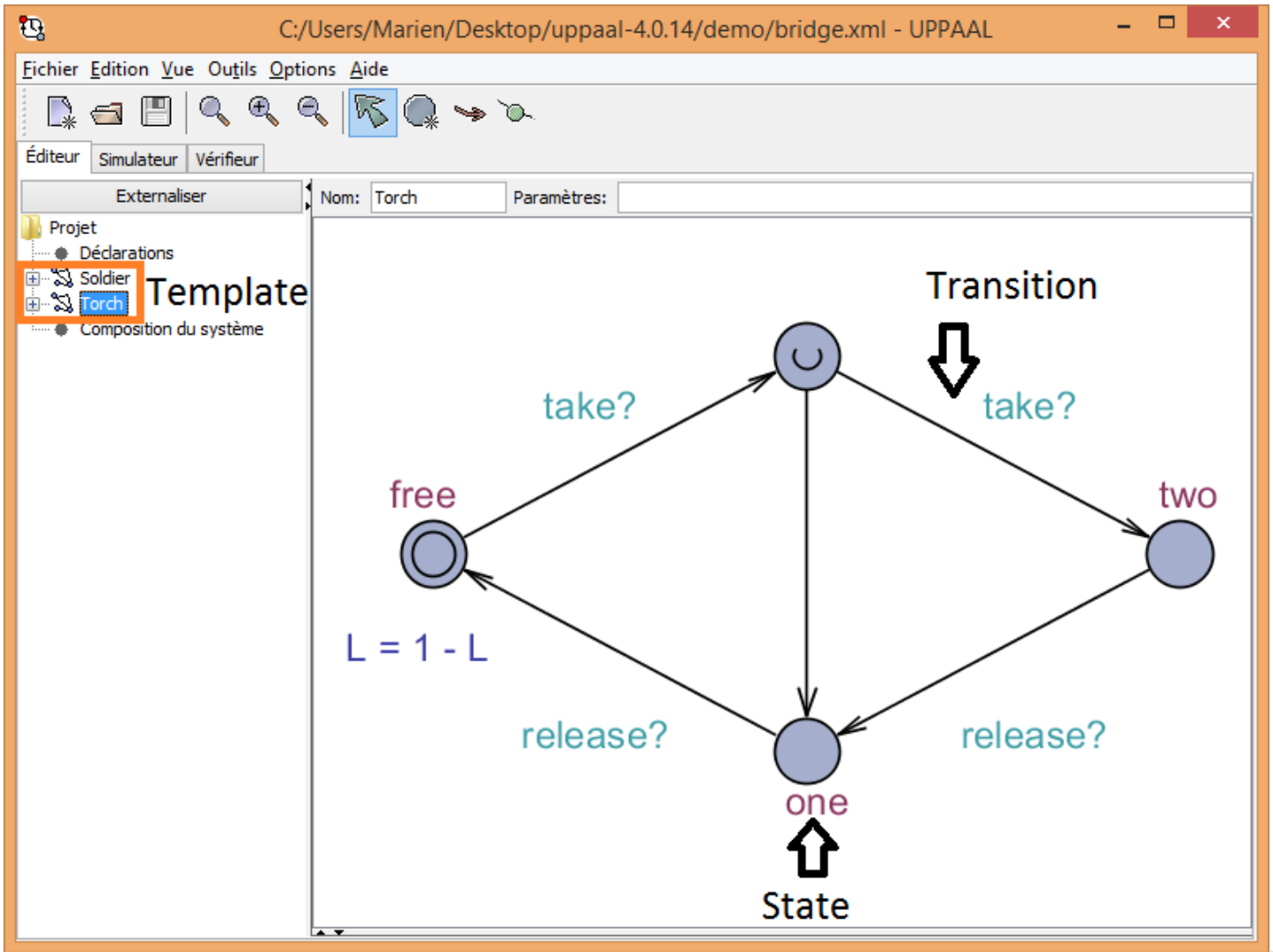
Like TA, ETA are made of

1. Vertices, called **states**
2. Edges, called **transitions**

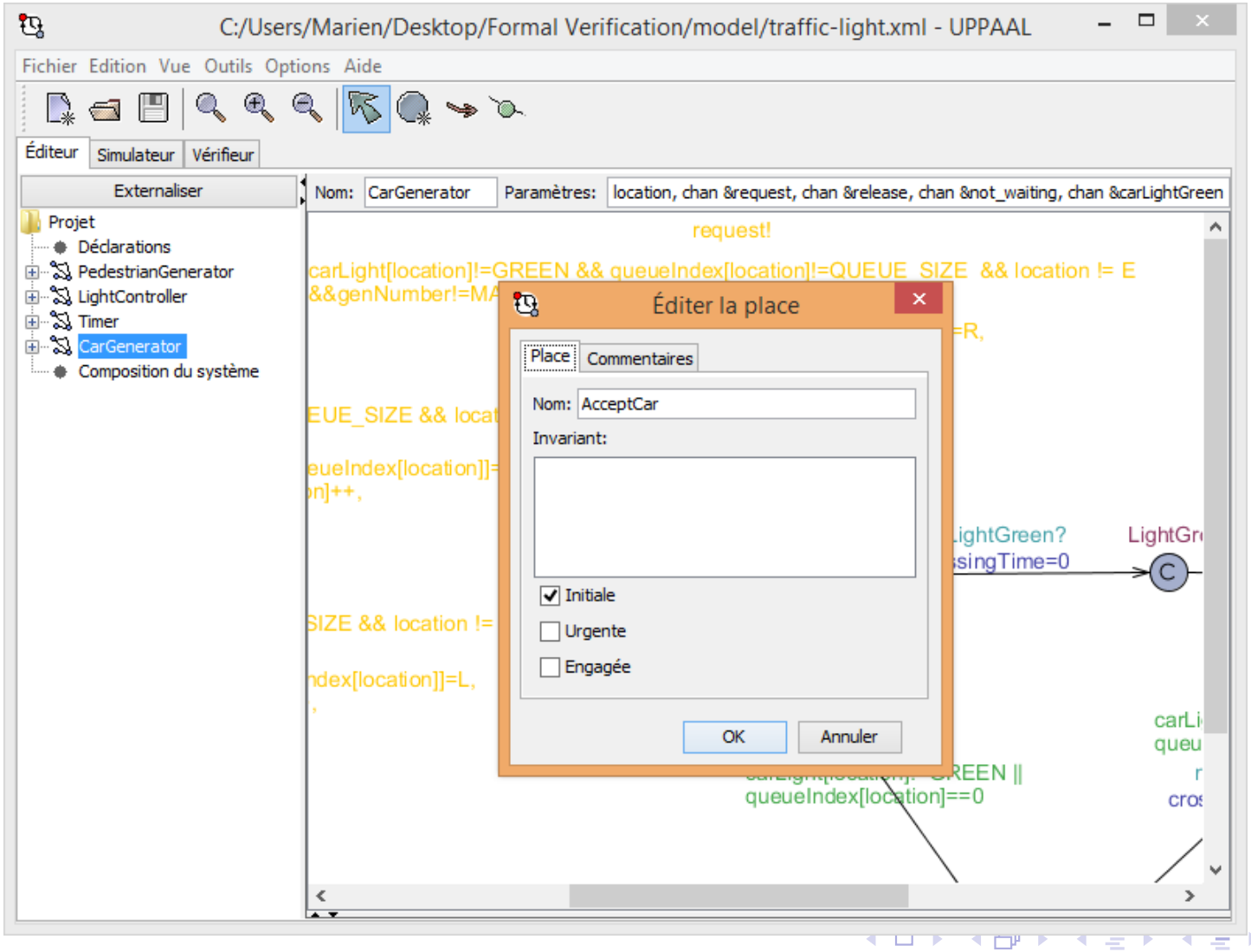
But also

1. Bounded integer variables
2. Structured data types
3. User defined functions
4. Channel synchronization

Back to the GUI (ft paint)



State (vertex)

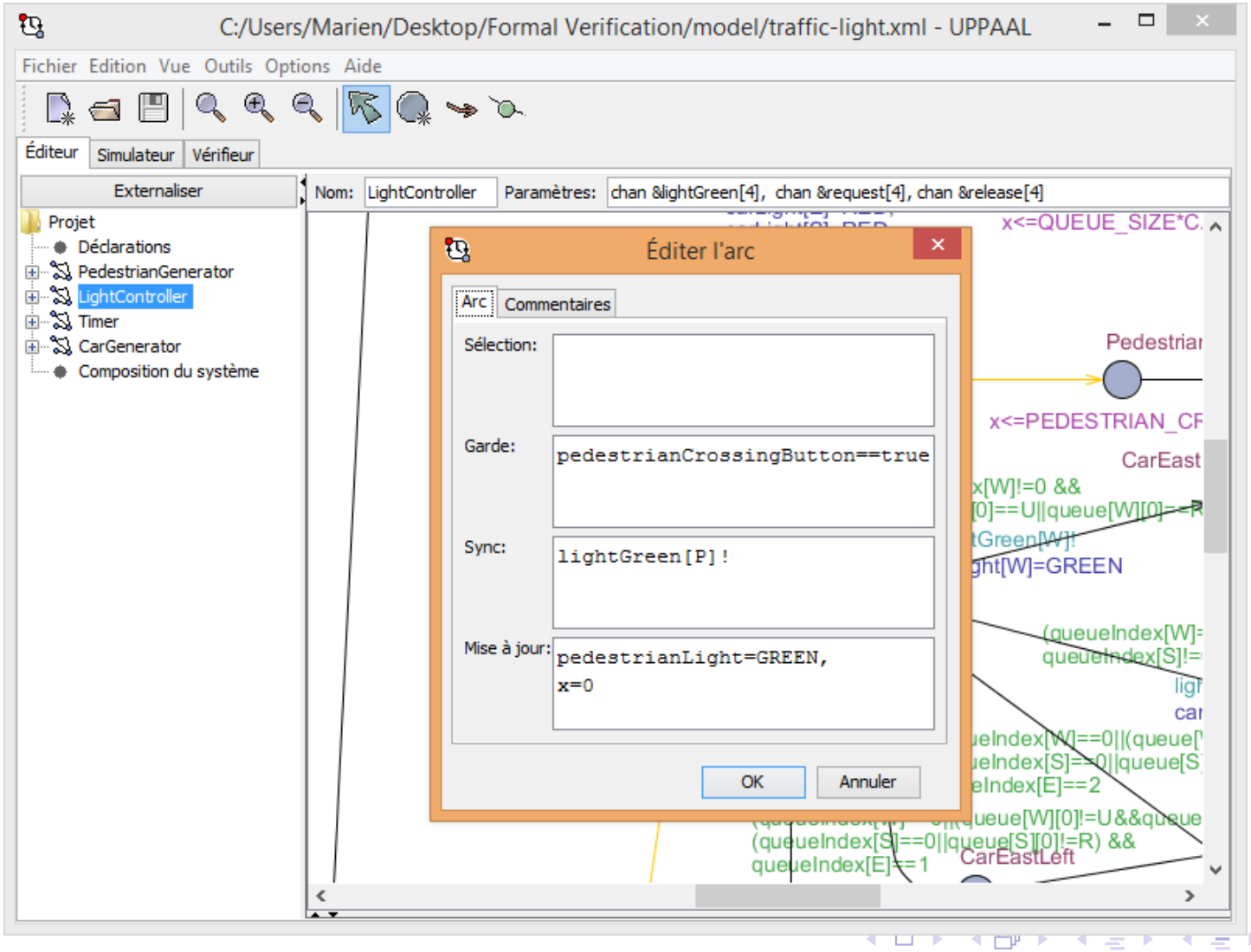


State (vertex) cont'd

Edit window :

1. **Name** : the name of the state
2. **Invariant** : free of side effect condition, only allowed to stay if it holds
3. **Initial state** : the initial state of the automaton
4. **Urgent state** : Like having the following invariant x<=0 (where x is reset in the incoming transition)
5. **Engaged state** : Like urgent (freeze time), but the next transition has to come from an urgent state

Transition (edge)



Transition (edge) cont'd

Edit window :

1. **Selection** : Nondeterministically chose a value for a variable
2. **Guard** : Invariant that has to be true to take the transition
3. **Sync** : Either *chan ?* or *chan !* Allow inter processes sync
4. **Update** : Expression with side effect. Used to alter object

Binary Synchronization (others are possible)

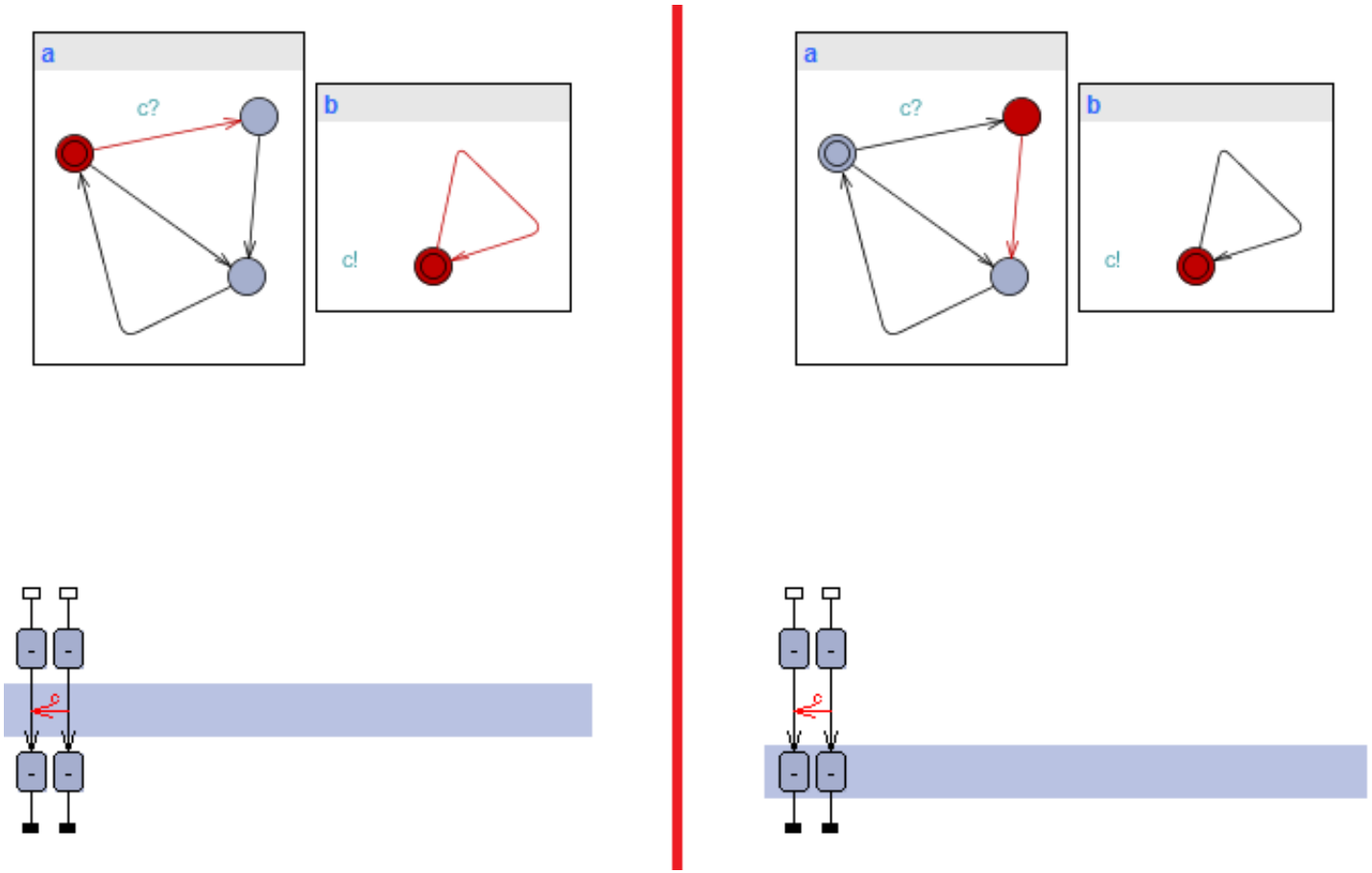
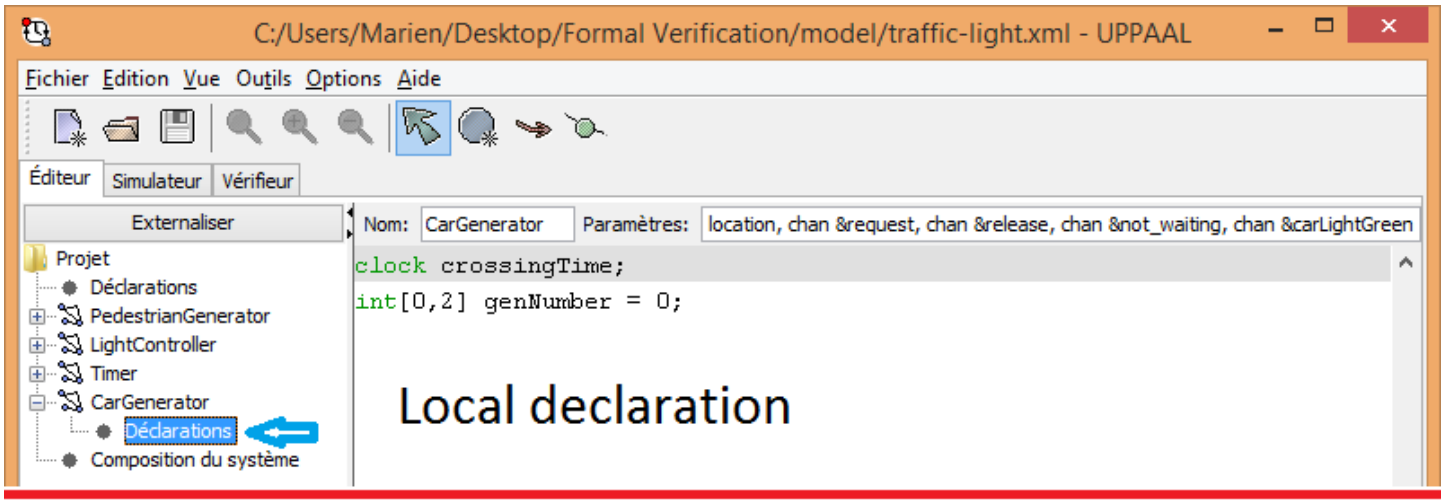
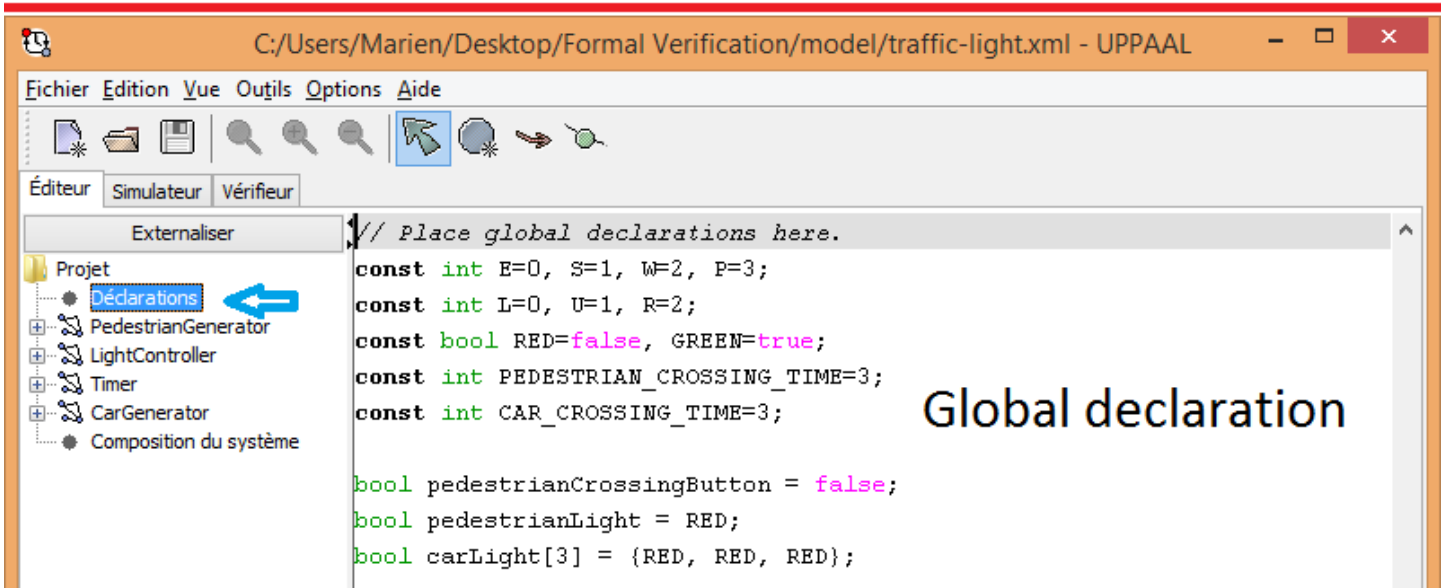


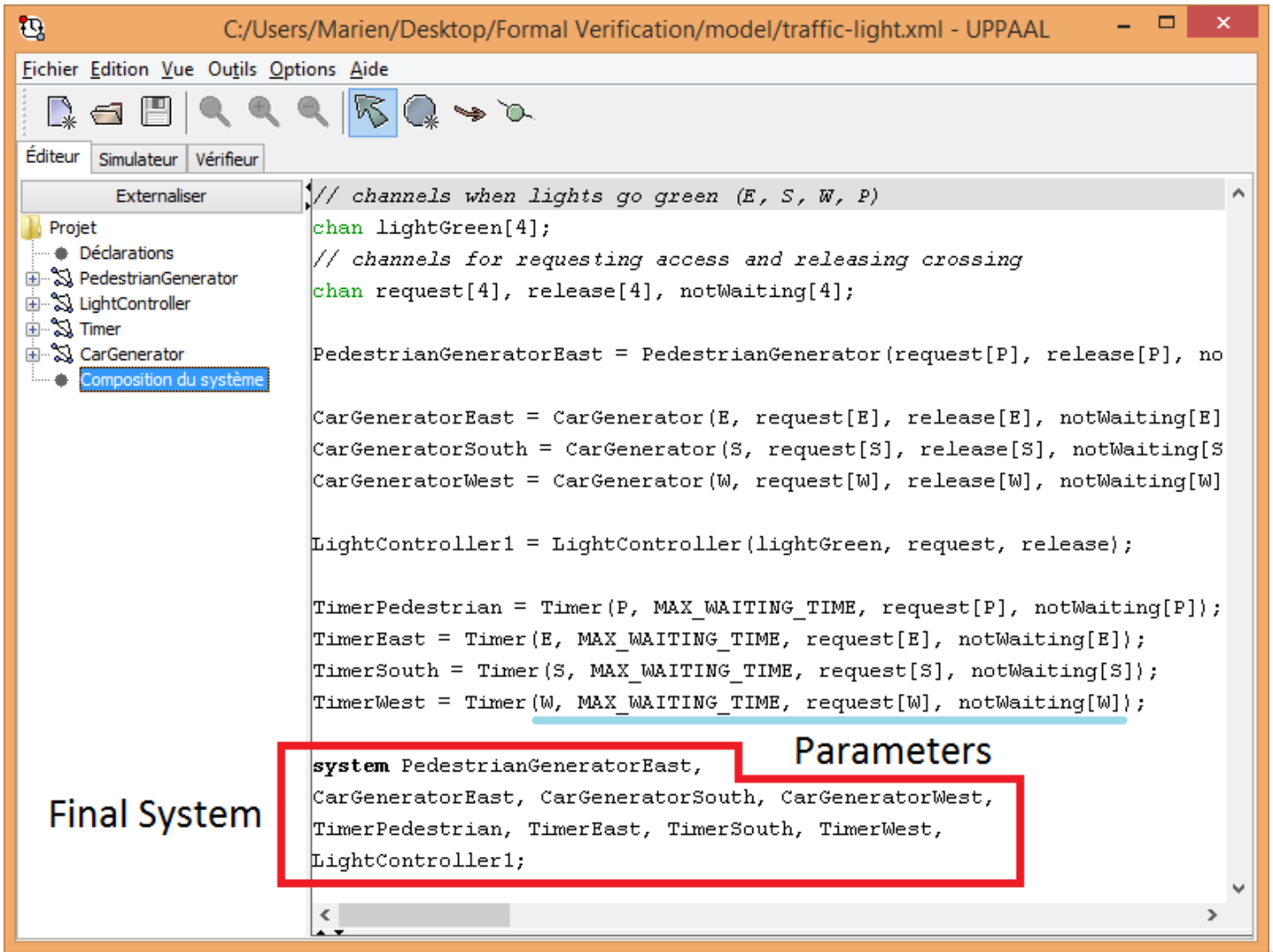
Figure: Before and after using a synchronization channel

Declaration (global or local)





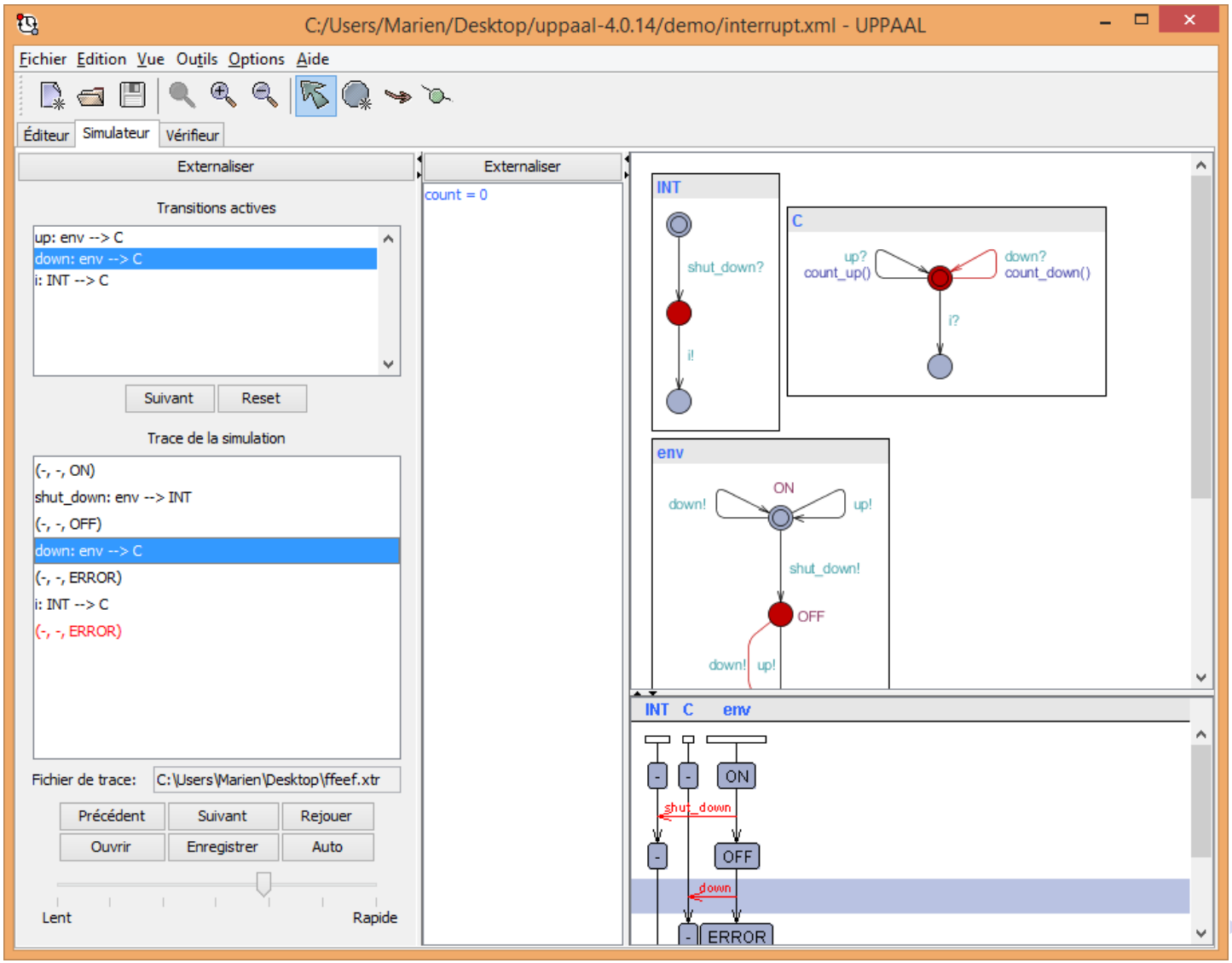
Building the system



Features

1. Manually take transitions
2. Display the state of the system (ETA and variables)
3. Output the trace (can be exported)
4. Allow replay and step by step analysis

GUI


C:/Users/Marien/Desktop/uppaal-4.0.14/demo/interrupt.xml - UPPAAL
Fichier Edition Vue Outils Options Aide
Éditeur Simulateur Vérifieur
Externaliser
Transitions actives
up: env --> C
down: env --> C
i: INT --> C
Suivant Reset
Trace de la simulation
(-, -, ON)
shut_down: env --> INT
(-, -, OFF)
down: env --> C
(-, -, ERROR)
i: INT --> C
(-, -, ERROR)
Fichier de trace: C:\Users\Marien\Desktop\ffeef.xtr
Précédent Suivant Rejouer
Ouvrir Enregistrer Auto
Lent Rapide
Externaliser
count = 0
INT
shut_down?
i!
C
up?
count_up()
down?
count_down()
i?
env
down!
ON
up!
shut_down!
OFF
down! up!
INT C env
ON
shut_down
OFF
down
ERROR

Features

Goal

1. Allow to verify a model according to a requirement specification
2. Expressed formally using simplified TCTL formulas

Kind of formulas

1. State formula : describe individual states
2. Path formula : quantify over path of the model

Formula

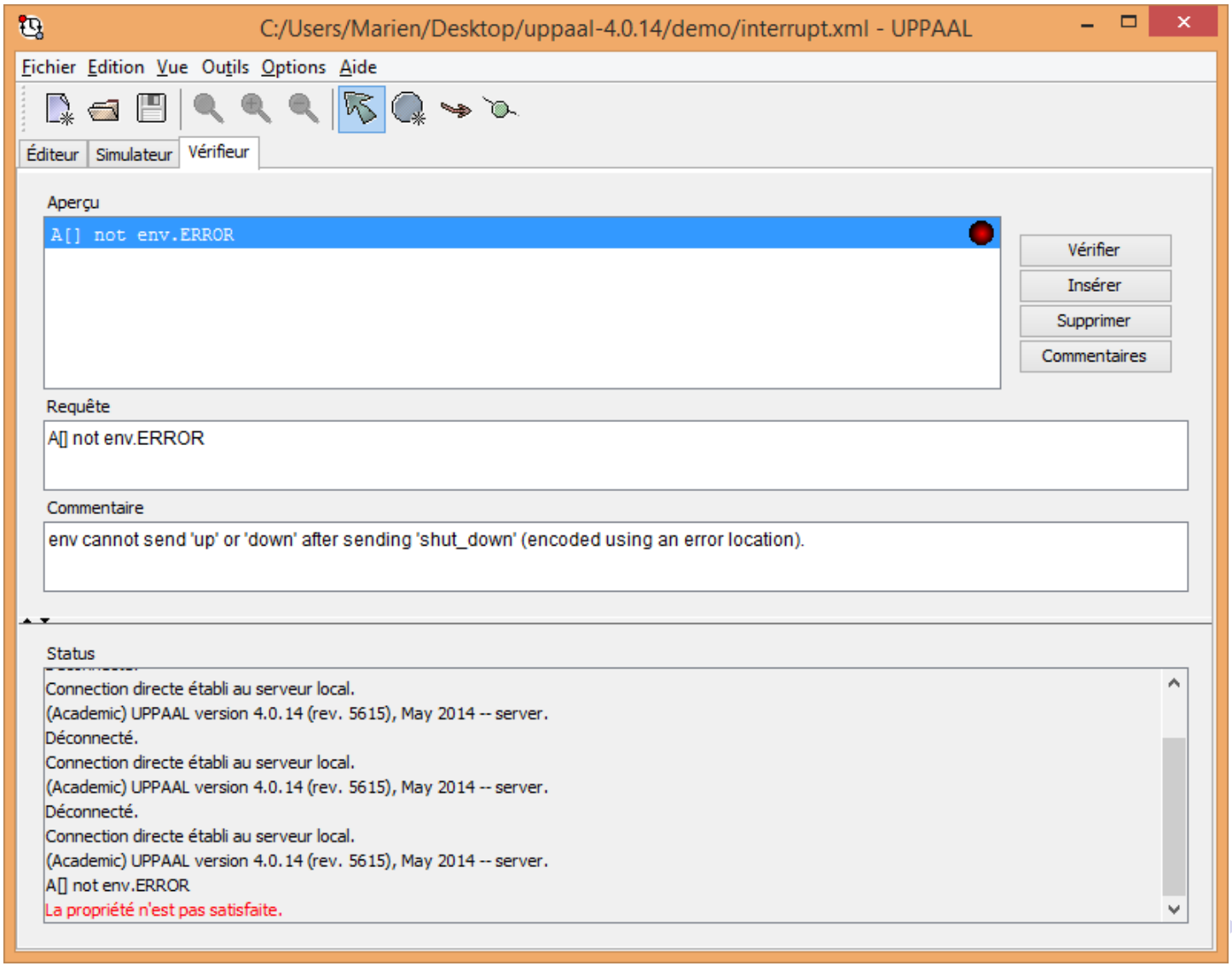
State formula

Expressions that are evaluated for a state, without looking at the behavior of the model

Path formula

1. Reachability property : can a formulae be possibly satisfied ?
2. Safety property : the system never reaches a unwanted state
3. Liveness property : the system make progress while avoiding deadlocks

GUI


C:/Users/Marien/Desktop/uppaal-4.0.14/demo/interrupt.xml - UPPAAL
Fichier Edition Vue Outils Options Aide
Éditeur Simulateur Vérifieur
Aperçu
A[] not env.ERROR
Vérifier
Insérer
Supprimer
Commentaires
Requête
A[] not env.ERROR
Commentaire
env cannot send 'up' or 'down' after sending 'shut_down' (encoded using an error location).
Status
Connection directe établi au serveur local.
(Academic) UPPAAL version 4.0.14 (rev. 5615), May 2014 -- server.
Déconnecté.
Connection directe établi au serveur local.
(Academic) UPPAAL version 4.0.14 (rev. 5615), May 2014 -- server.
Déconnecté.
Connection directe établi au serveur local.
(Academic) UPPAAL version 4.0.14 (rev. 5615), May 2014 -- server.
A[] not env.ERROR
La propriété n'est pas satisfaite.

Sources

- `http://www.uppaal.org/`
- A Tutorial on Uppaal 4.0 - Gerd Behrmann, Alexandre David, and Kim G. Larsen