Rigorous Design of PLC Networks using Formal Methods

Radu Mateescu

CONVECS team
Inria Grenoble – Rhône-Alpes
Université Grenoble Alpes / LIG

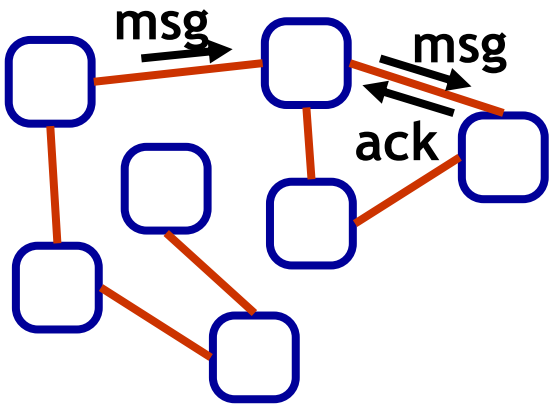
http://convecs.inria.fr

CONVECS
(Construction of Verified Concurrent Systems)
Inria – CNRS – UGA common project-team within LIG

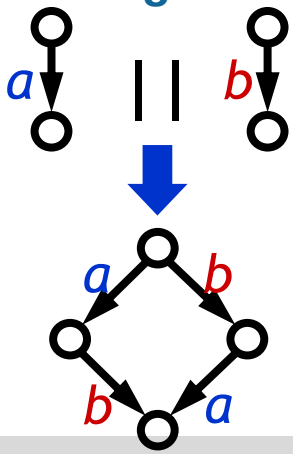
Radu Mateescu	(Inria Senior Researcher)
Hubert Garavel	(Inria Senior Researcher)
Frédéric Lang	(Inria Researcher)
Gwen Salaün	(Professor, UGA)
Wendelin Serwe	(Inria Researcher)
Gianluca Barbon	(PhD)
Lina Marsso	(PhD)
Ajay Muroor-Nadumane	(PhD)
Umar Ozeer	(PhD)
Lian Apostol	(expert engineer)

Scientific Field

Asynchronous concurrent systems



Interleaving semantics



Formal modelling of concurrent systems

- Behavioural specification languages
- Property specification languages

Compiler construction, code generation

Functional verification

- Model checking
- Equivalence checking

Quantitative analysis

- Timed, probabilistic, stochastic

Real-life case-studies and applications

Verification platform

CADP (> 50 tools + 17 libraries)
http://cadp.inria.fr

The Bluesky for I-Automation Project

Minalogic, FUI 13rd call (2012-2016)

Partners: ***Crouzet Automatismes*** (now ***InnoVista Sensors***), VM2M, Motwin, Inria, LCIS

Objectives:

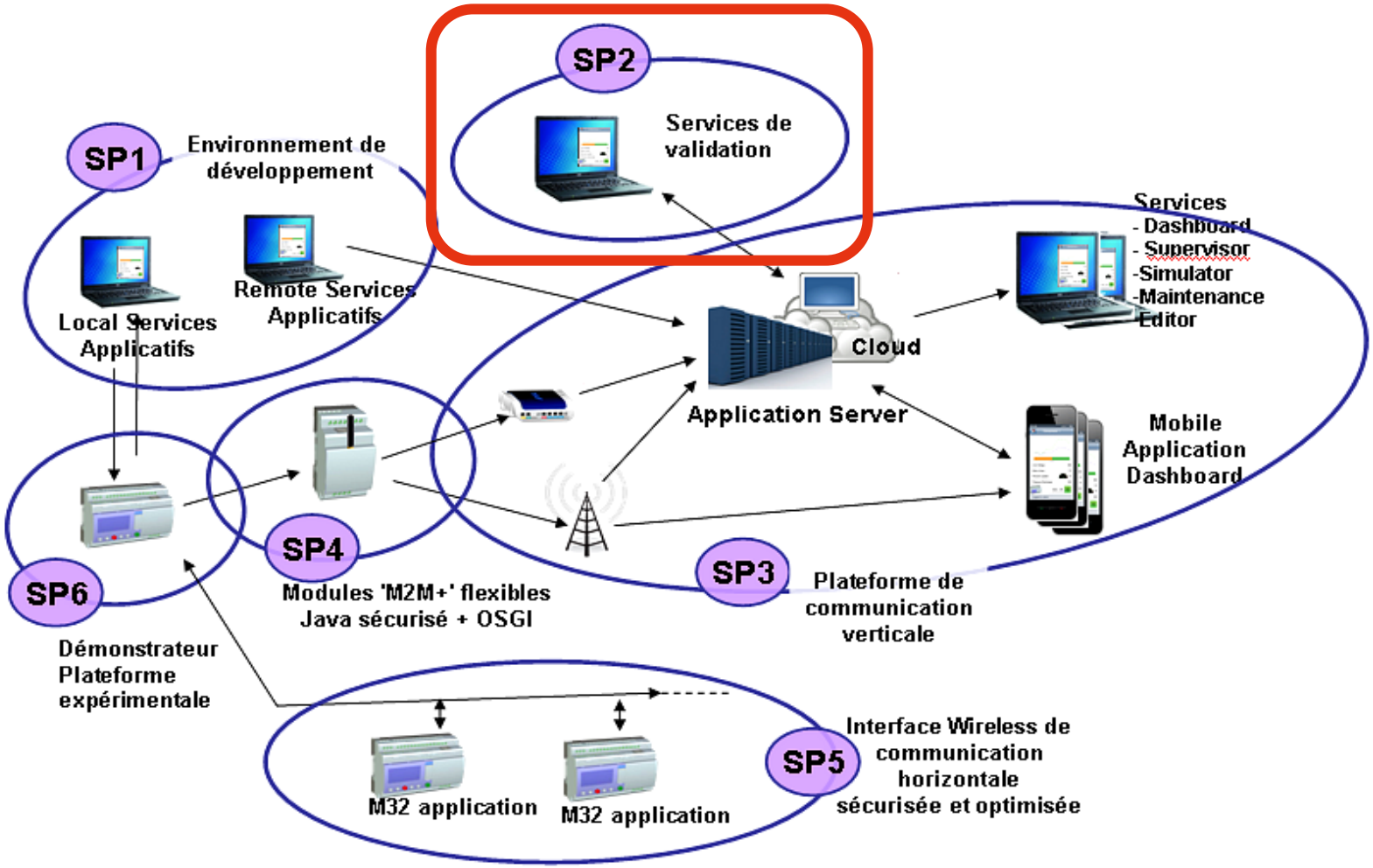
- Simple solution for distributed automation applications
- Hardware, software, communication infrastructures, and services
- New generation of ***em4*** PLCs connected to the IoT

em4 REMOTE PLC

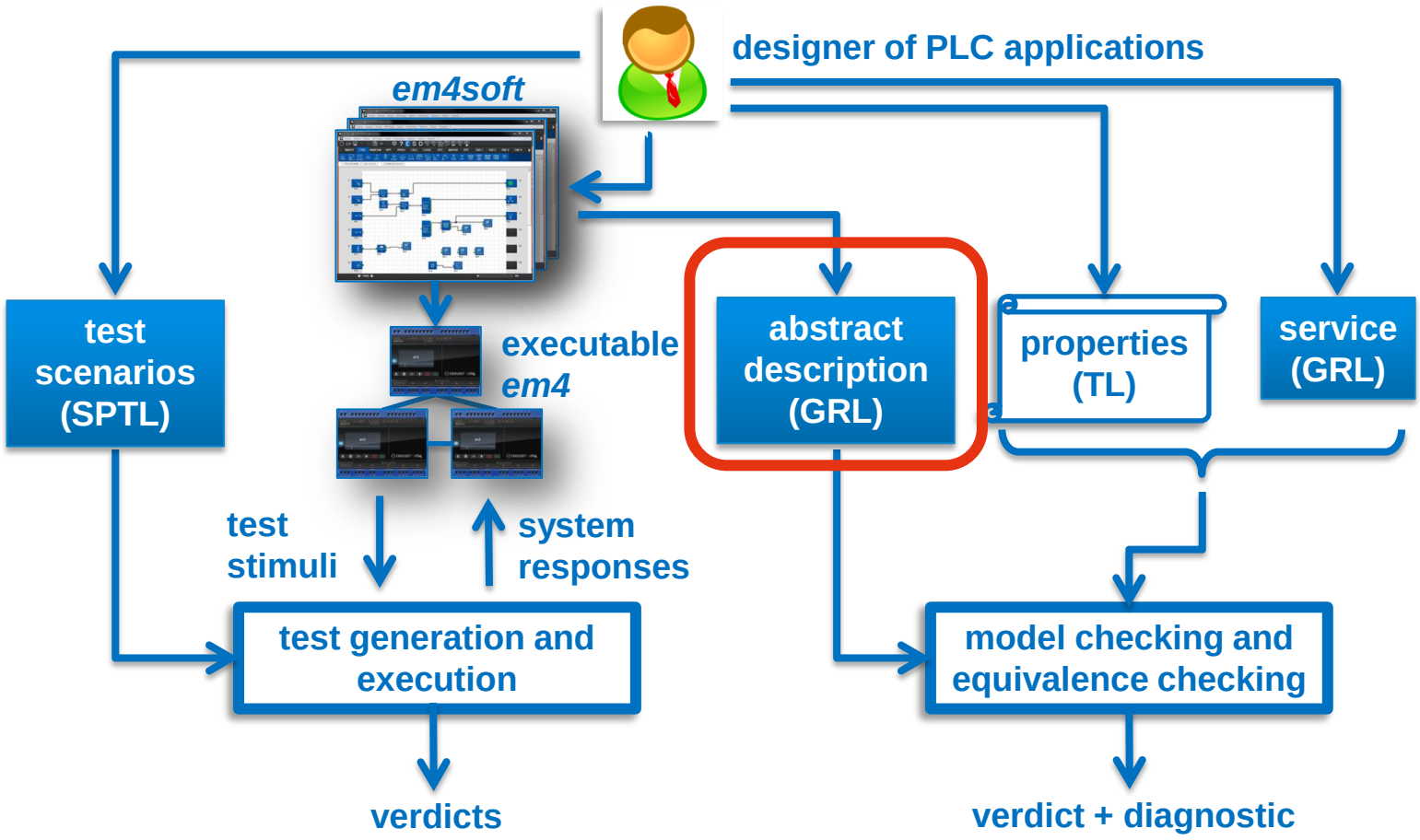
- Formal validation services for a rigorous development of distributed applications embedded on PLC networks

Inria inventeurs du monde numérique

Organization of the Project



Design Flow based on Formal Methods



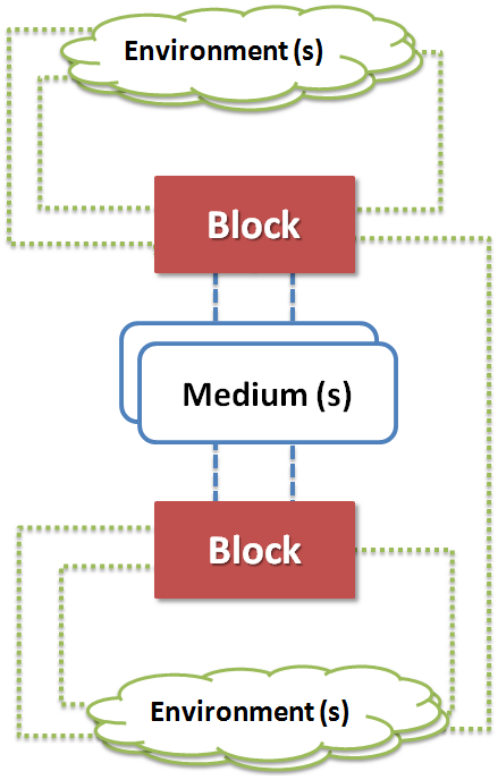
GRL: A Formal Description Language for GALS Systems

GRL (*GALS Representation Language*)

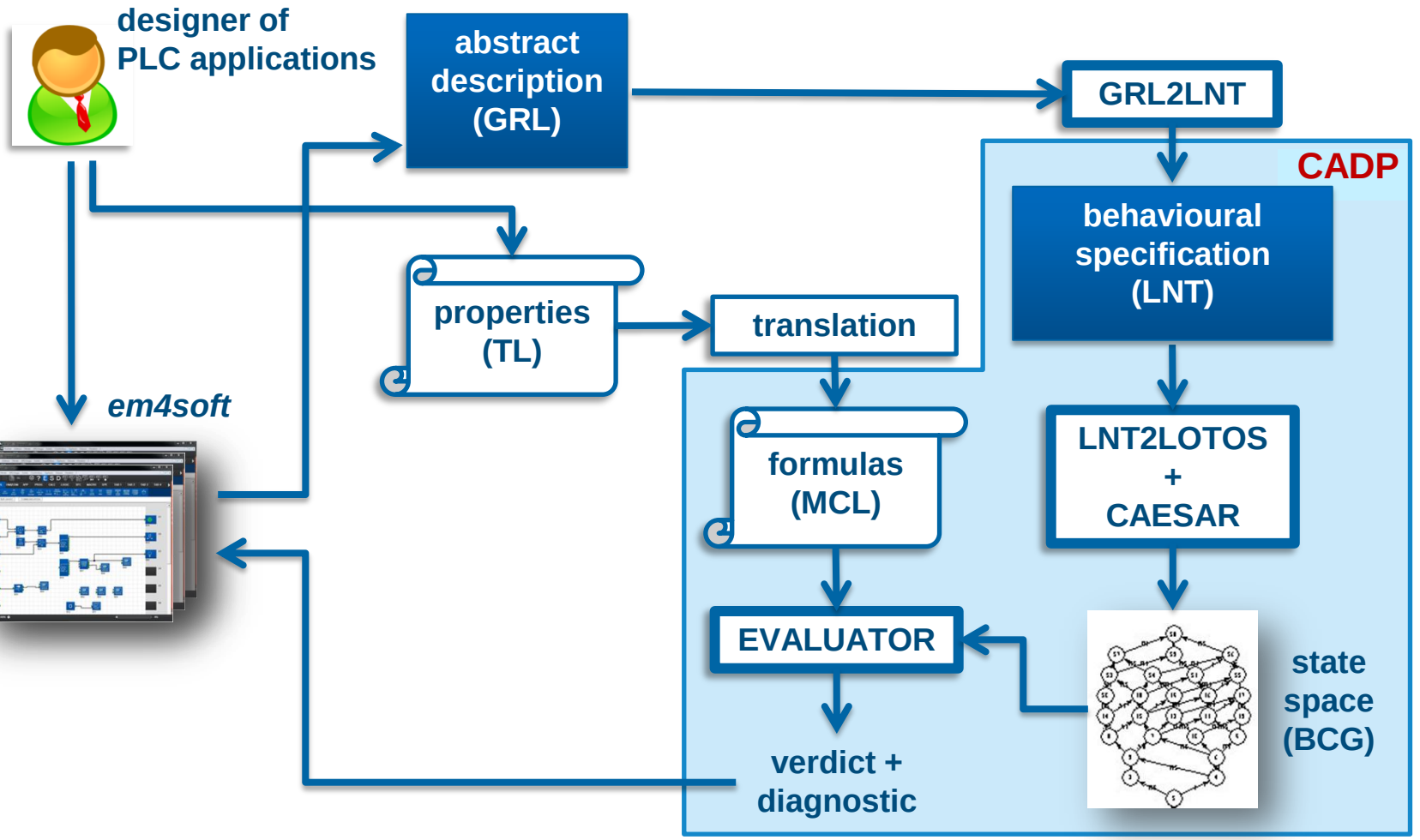
- GALS system: Globally Asynchronous and Locally Synchronous
- Principles of GRL:
  - > **Blocks**: synchronous components
  - > **Environments**: external constraints
  - > **Mediums**: asynchronous communication
  - > Formal semantics (process calculus)
- Tool support:

  translators *em4soft* → GRL → LNT

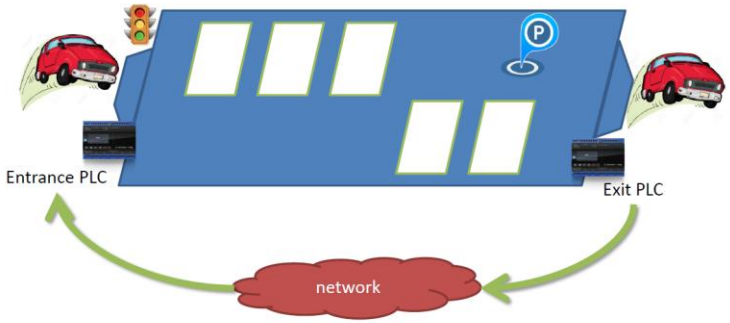
  and CADP tools

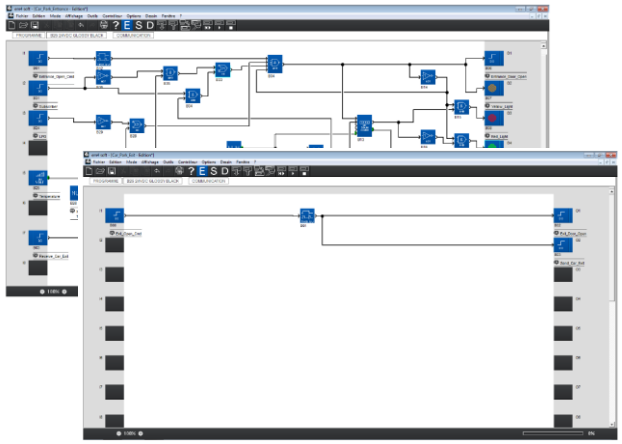


Asynchronous Validation Flow



Example:
Car Park Management





em4soft

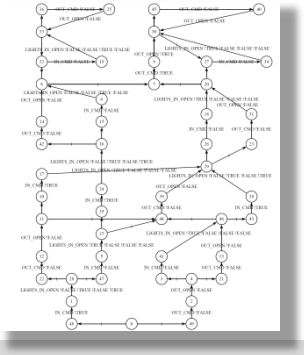
translator

```
block In_Controller (in  Open_Cmd : bool;
                     out Green_Light  : bool; …  out Door_Open : bool)

   alloc

   perm

   temp

   c2 :=
   …
   Yello
   B16 (
end bl
```

```
block Out_Controller (in  Open_Cmd  : bool;
                      out Door_Open : bool)
                     {receive Open_Distant_Cmd : bool;
                      send    Decrease_Counter : bool} is

   allocate Block_Or as B01,
            Block_Timer_BW [true, false] as B02,
            Block_Timer_AC [0, 5, Cycle] as B05

   temp c1 : bool

   B01 (Open_Cmd, Open_Distant_Cmd, ?c1);
   B02 (c1, ?Decrease_Counter);
   B05 (Decrease_Counter, _, ?Door_Open, ?_ ,?_, ?_, ?_)
end block
```

GRL

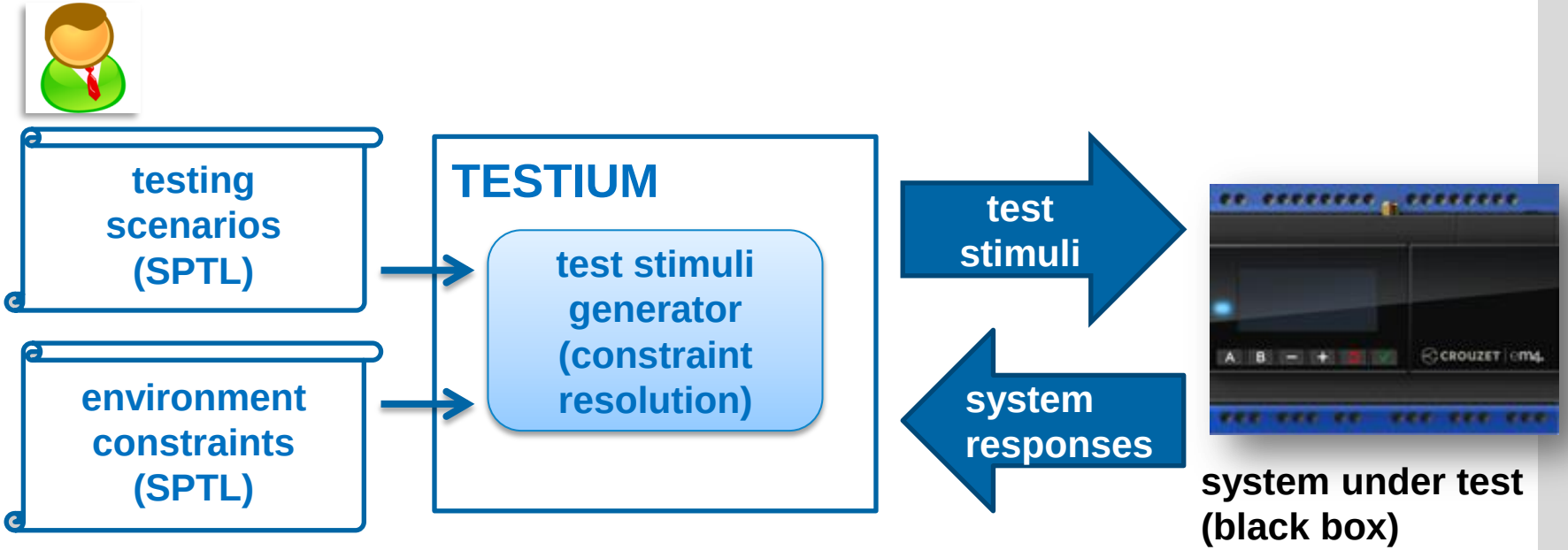
CADP + SEQ2SIM



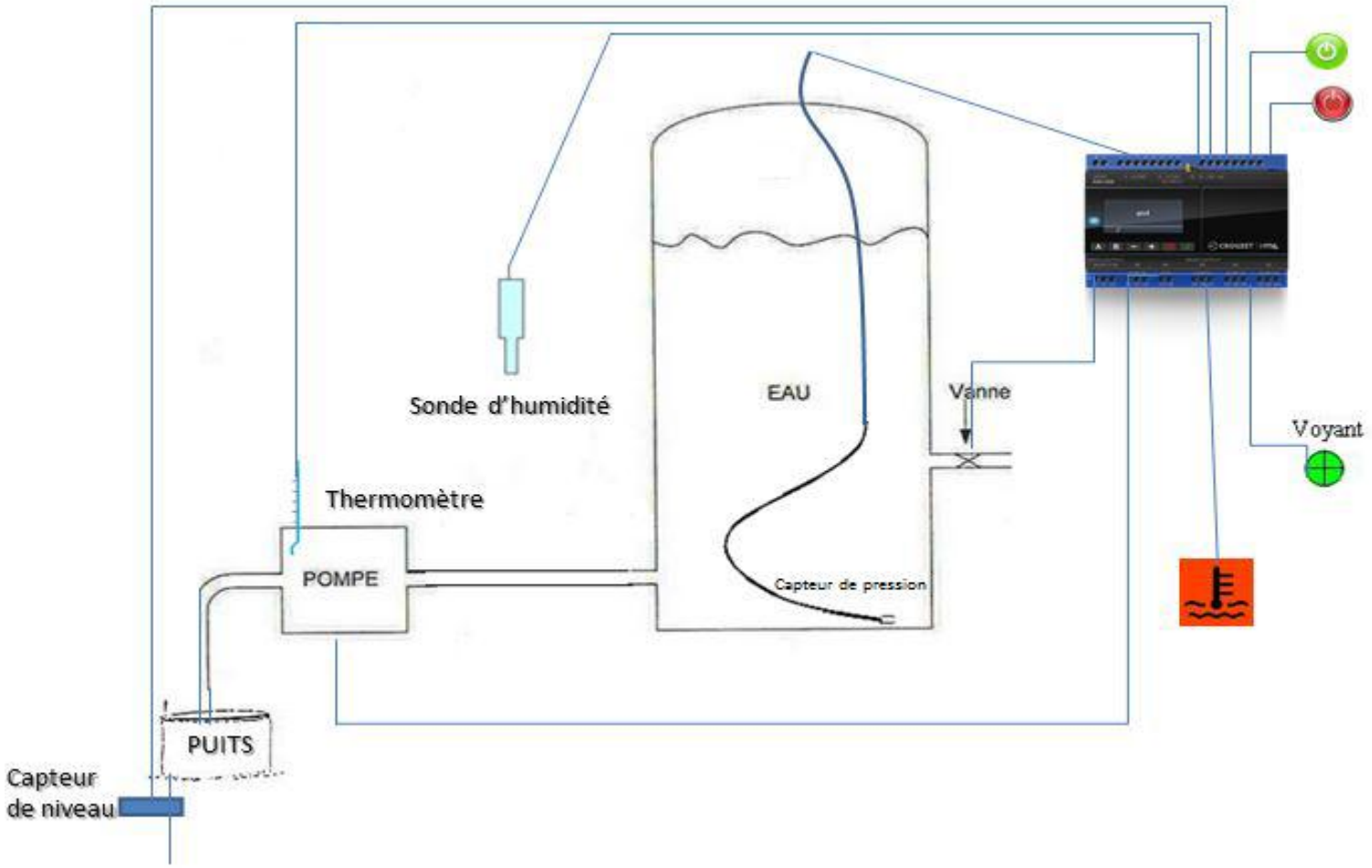
GRL2LNT + CADP

Synchronous Validation Flow

SPTL (*Synchronous Programming Testing Language*)

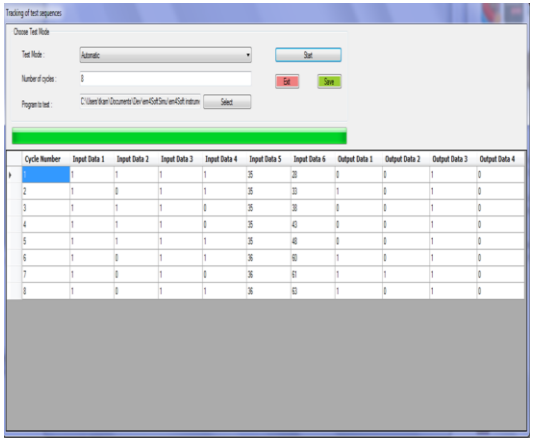


Example: Irrigation System



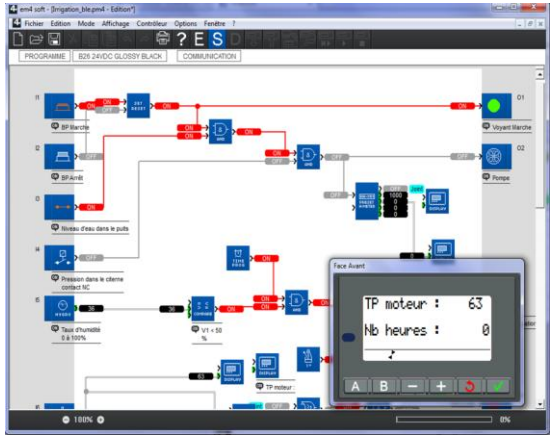
Execution of a Testing Scenario

TESTIUM



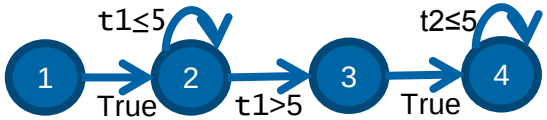
test stimuli

system responses



SPTL

```
scenario Normal
 var time t1
     time t2
begin
     {Humid = 35;Temp=28;t1.start}        |
     [Humid = 35;Temp=(pre(Temp)+5)(t1>5)]|
     {Humid=36;Temp=60;t2.start}          |
     [Humid=36;Temp>60;Temp<65(t2>5)]
end
```



- Step by step mode
- Automatic mode

Bluesky Project: Summary

Results

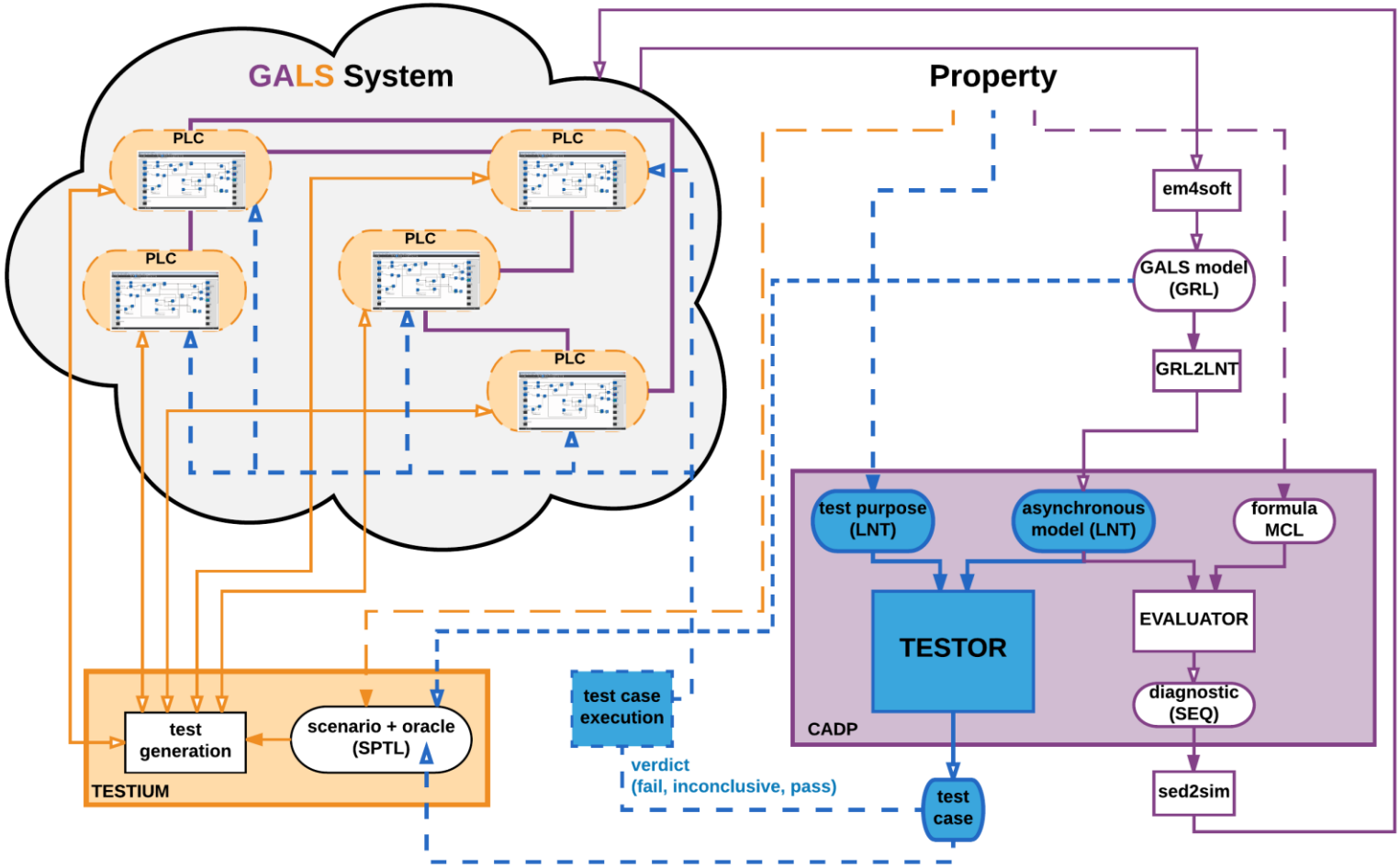
- New generation of PLCs from InnoVista Sensors
- Languages et tools for validating distributed PLC applications
  - > GRL and GRL2LNT tool: PhD of **Fatma JEBALI** (http://hal.inria.fr/tel-01511656/en)
  - > SPTL and TESTIUM tool: PhD of **Mouna TKA** (http://www.theses.fr/2016GREAM020)

Ongoing Work

- Enhancing the validation flow to automate the testing of PLC networks
- PhD of **Lina MARSSO**: *Formal Methods for Testing Networks of Controllers*

  co-supervised Inria – LCIS (ARC6 2016-2019)
  with the collaboration of Innovista Sensors

Testing Flow for GALS Systems



Thank you!

More information:

http://convecs.inria.fr

inventeurs du monde numérique