Final Review
Brussels, December 12th, 2008

Achievements and Perspectives :

Testing and Verification

Cluster leader : Kim Guldstrand Larsen

CISS, Aalborg University, DENMARK

Core Partners of the Cluster

- **CISS, Aalborg University**
  (real-time verification and testing, controller synthesis, security)
- **EPFL**
  (models and tools for quantitative aspects of embedded systems)
- **CFV / Centre Fédéré de Verification**
  (model checking and robustness of hybrid and real-time systems)
- **INRIA / Rennes**
  (symbolic testing, security, controller synthesis)
- **LSV / CNRS**
  (model checking, security protocols and logics)
- **OFFIS, Oldenborg**
  (UML-based verification and testing)
- **University of Twente**
  (verification and testing of hybrid and stochastic systems, security)
- **Uppsala University**
  (real-time verification, testing and schedulability)
- **Verimag**
  (real-time verification and testing, security protocols analysis)

Affiliated partners:
5 industrial
6 academic

Cluster Activities

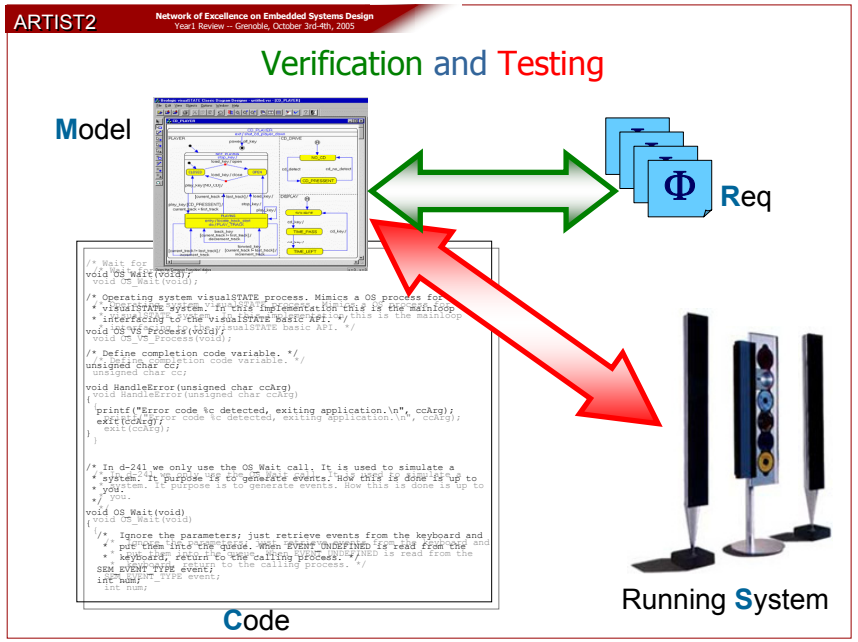
- JPRA-Cluster Integration
  Quantitative Testing and Verification
  (Ed Brinksma)

- JPIA-Platform:
  Testing and Verification Platform
  (Kim G. Larsen)

- JPRA-Cluster Integration
  Verification of Security Properties

Vision & Long Term Goals

- 30-70% of production time is currently spend on elaborate, ad-hoc testing
- Gap between industrial practice and academic state-of-the-art
- Time-to-market may be shortened considerable by verification and performance analyses of early design models
- Models must deal with quantitative information (real-time, memory, bandwidth, energy).



Vision & Long Term Goals

Improve current industrial practice for validating embedded systems applications by continuous dissemination and improvement of existing powerful testing and verification techniques and tools.

Effort on making state-of-the-art verification and testing technology *visible* and *easily accessible* for industry with long term vision of integration in tool chains applied in industry.

Quantitative Testing and Verification:

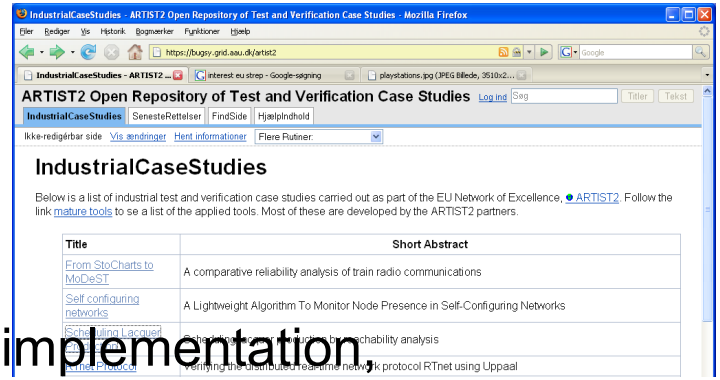
High Level Objectives Y4

- controller synthesis, robustness and implementability
- property-preserving code generation,
- generic frameworks using abstraction and compositionality
- combinations of testing and verification techniques.
- optimal scheduling,
- monitoring and fault diagnosis,
- analysis of hybrid models, stochastic and timed models

Testing and Verification Platform

High Level Objectives Y4

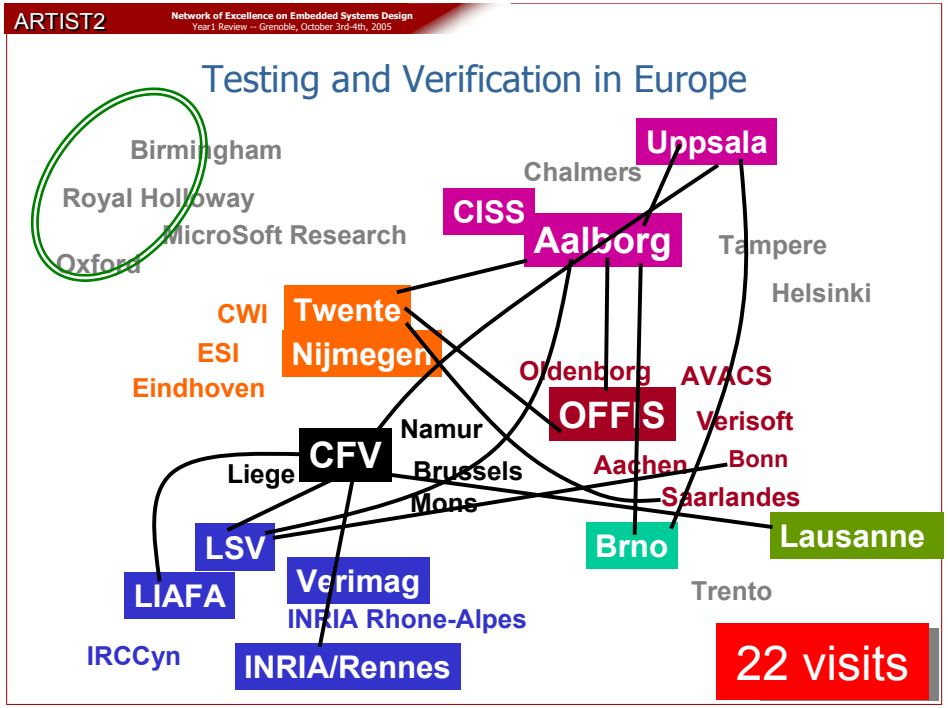
- continued improvement related to the individual tools
- dissemination as well as application on industrial case studies (https://bugsy.grid.aau.dk/artist2)



- high performance tools server (64 bit architecture and distributed implementation, common web-interface)

State of Integration in Europe

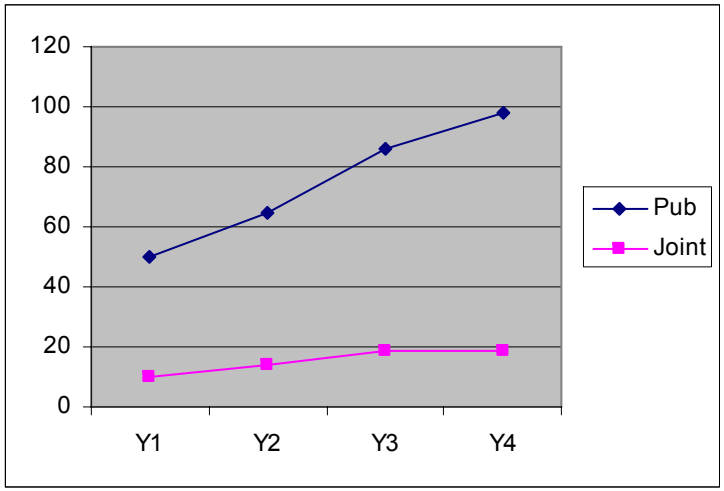
- **Extensive collaboration** between partners of the cluster
- **Extensive collaboration** with leading research teams outside Europe.
- **Extensive interaction** with other communities
- **National Centers and projects**
  - CISS, ESI, ..
  - CREDO, DaNES, DOTS, Testec, SAVE++, ..
- **New FP7/ARTEMIS/ESF Projects**
  - ARTIST Design (Modeling and Validation)
  - QUASIMODO (STREP)
  - MULTIFORM (STREP)
  - COMBEST (STREP)
  - GASICS
  - CESAR



Information Society

Building Excellence

- **98 publications Y4**
  (ARTIST2 total: 299)
- **19 joint publications Y4**
  (ARTIST2 total: 62)
- High level of **dissemination** through PhD schools and industrial seminars (>30 keynote presentations).
- **Strong impact** on a number of important international **conferences** (CAV, TACAS, FORMATS, EMSOFT, CONCUR, ETAPS, HSCC,..)
- **ARTIST2 PhD schools** (Autrans, Shanghai).
- **Transfer to industry** through long-term collaboration performed by individual partners. National centers and laboratories.



Building Excellence

- **Workshops organized**
  - INFINITY08
  - TIME'08
  - PDMC'08
  - Dagstuhl Seminar on Distributed and GRID computing
  - RTSS'08 Track on Design and Verification
  - FIT'08
  - NWPT'08
  - MOVEP
  - **CAV'09**
- **TURING AWARD 2007**

  Ed Clarke, Allen Emerson, Joseph Sifakis

Grand Officier de l'Ordre national du Merite

Overall Assessment at the end of the NoE

- *Quantitative Testing and Verification*
  - Verification for new quantitative models
    (priced TA, probabilistic TA, priced HA, stochastic games,..)
  - CEGAR for quantitative models
    (timed, hybrid, stochastic,..)
  - Compositional Verification Frameworks
  - Controller Synthesis
    (1-clock PTA, budget constraints, Part. Obs., ATL)
  - Generation of predictable code not pursued

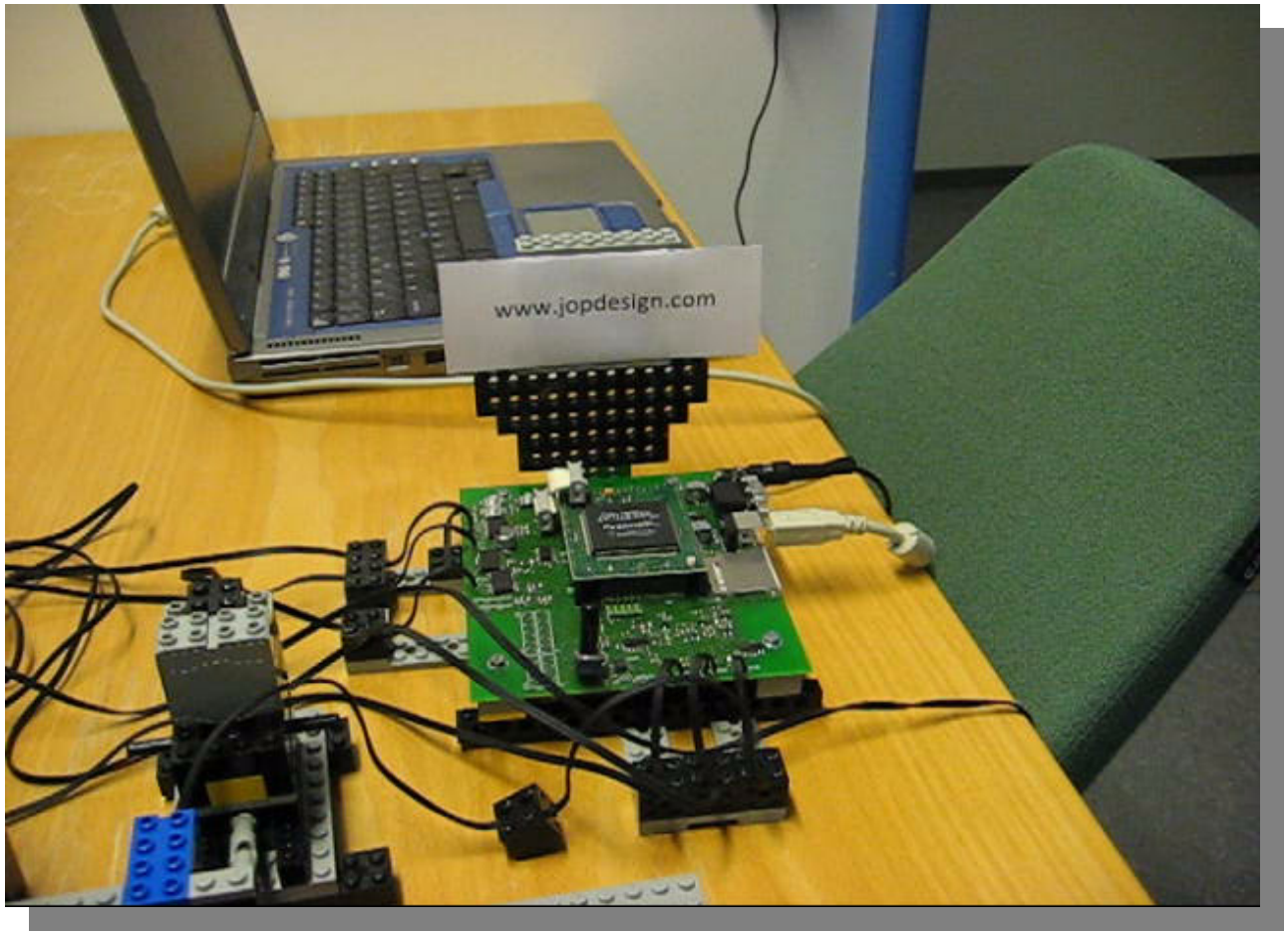
Overall Assessment at the end of the NoE

- *Testing and Verification Platform*
  - Individual tools mature, with industrial applications
    (AMT, BIP, DeVINE,SPIN,TIMES, UPPAAL,..)
  - High-performance Verification Server has been achieved.
  - Joint infra-structure for European Verification Grid not pursued.

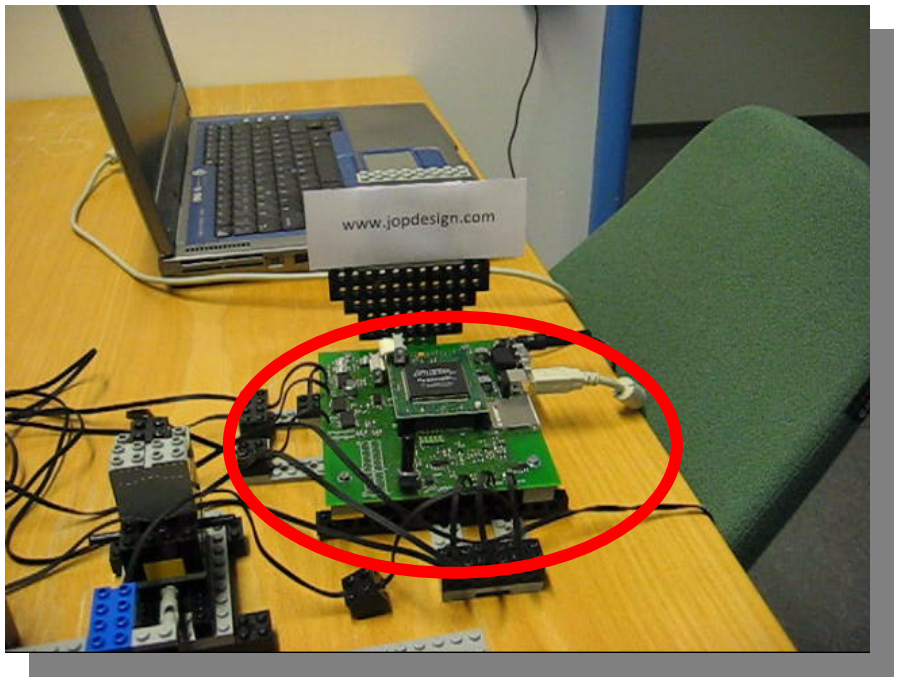
Overall Assessment at the end of the NoE

- Extensive list of publications, invited and keynote lectures, etc witnesses *true excellence* within the area.
- Substantial effort has been put by individual partners in *dissemination* to research and industry.
- A large number of new collaborative projects has been initiated.

Highlight 1: A Safety Critical System



Hardware

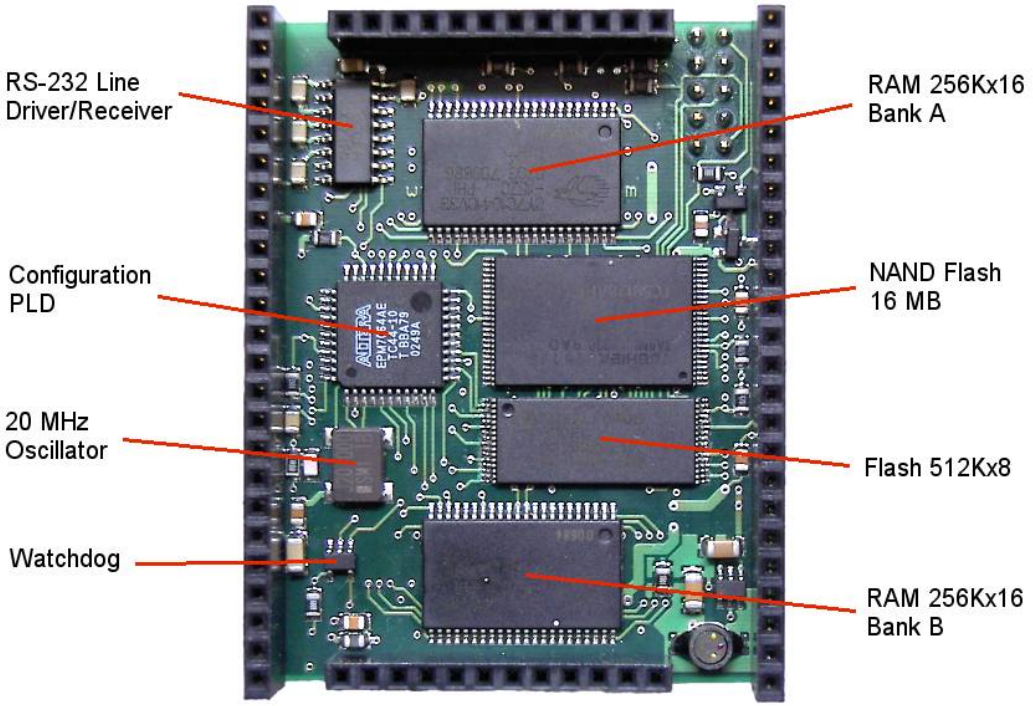


- JOP (Java Optimized Processor)
- Native execution of Java Bytecode
- Bytecode implemented in Microcode
- Avoid unpredictable data-cache
- Time predictable
- Developed new method and stack cache
- Implemented in FPGA

Java Optimizing Processor

Martin Schöberl
University of Tech., Vienna

FPGA



SARTS –Safety Critical Java

```
public static void main(String[] args) {
        new SporadicPushMotor(
                new SporadicParameters(4, 4000, 60), 0);
        new SporadicPushMotor(
                new SporadicP
        PeriodicMotorSpooler mo
                new PeriodicM
                        new
        new PeriodicReadSensor(
                new PeriodicPa
        RealtimeSystem.start();
}
```

TASKS

```
private void handleBrick() {
private void handleBrick() {
private void handleBrick() {
private void handleBrick() {
private void handleBrick() {
Sensors.synchronizedReadSensors();
int input = (Sensors.getBufferedSensor(0) + Sensors
                .getBufferedSensor(1)) >> 1;

if (awaitingBrick) {
        if (input > lastRead) {
                lastRead = input;
        } else if ((lastRead - input) >= TRESHOLD) {
                awaitingBrick = false;
                if (lastRead > BRICK_DETECTED) {
                        brickFound(lastRead);
                }
        }
```

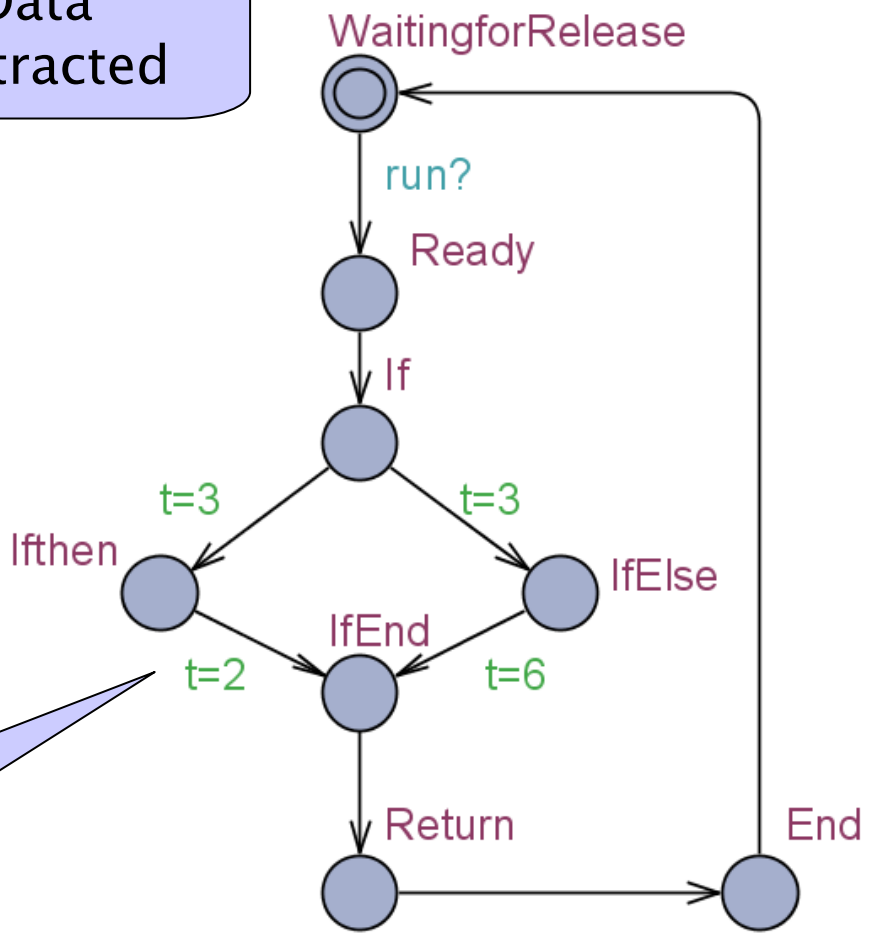
METHODS

Byte code – Timed Automata

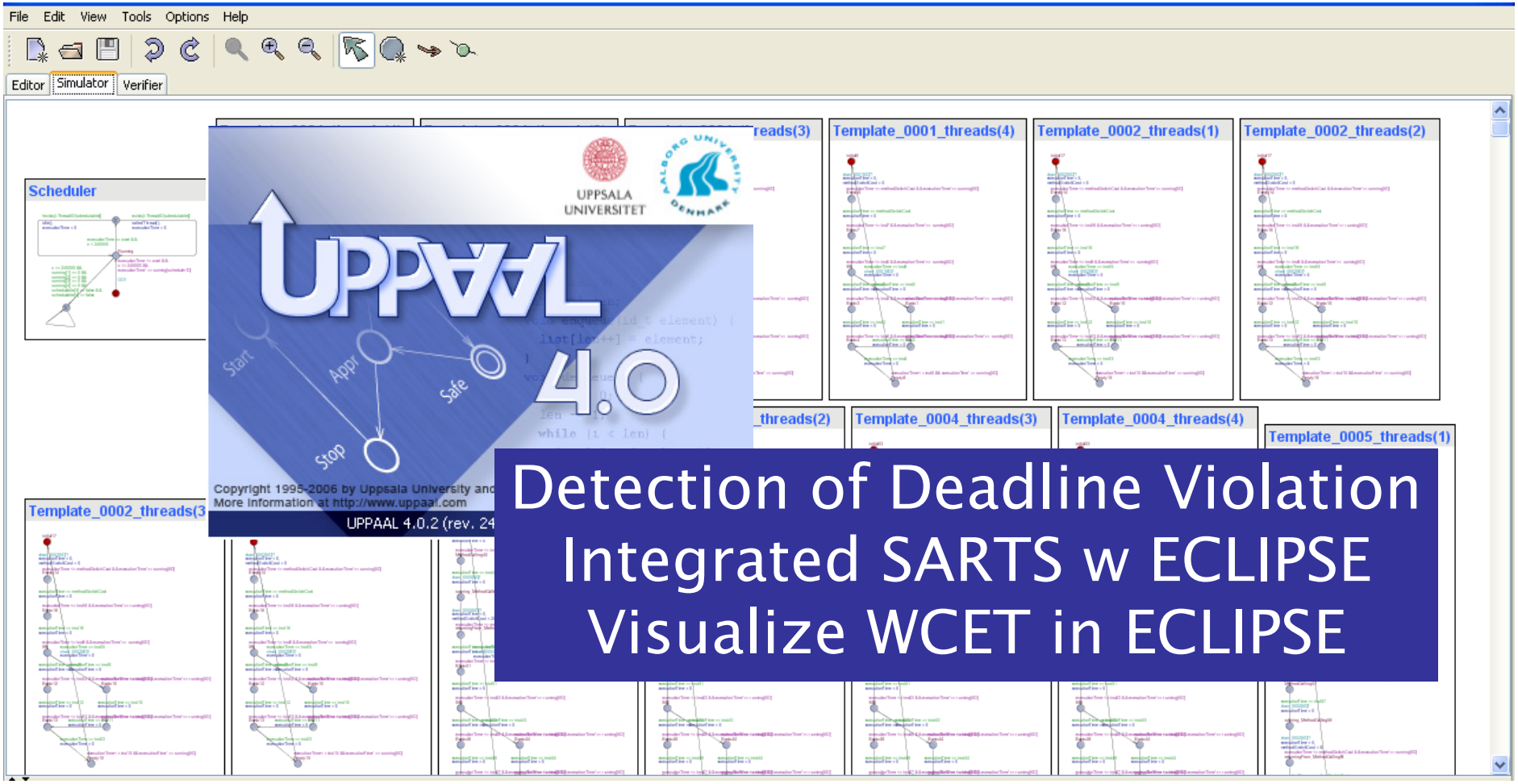
```
protected boolean run()
    if i<5 {
        i = i + 4;
    } else {
        i = i * 4;
    }
    return true;
}
```

Data abstracted

Timing = WCET from microcode

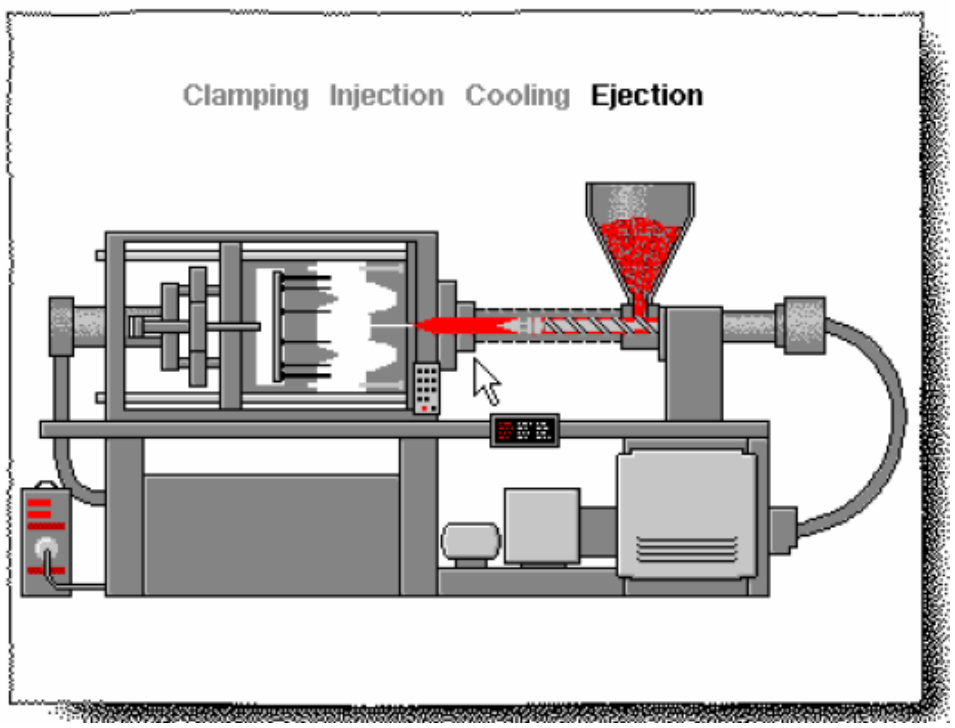


SARTS – to Timed Automata



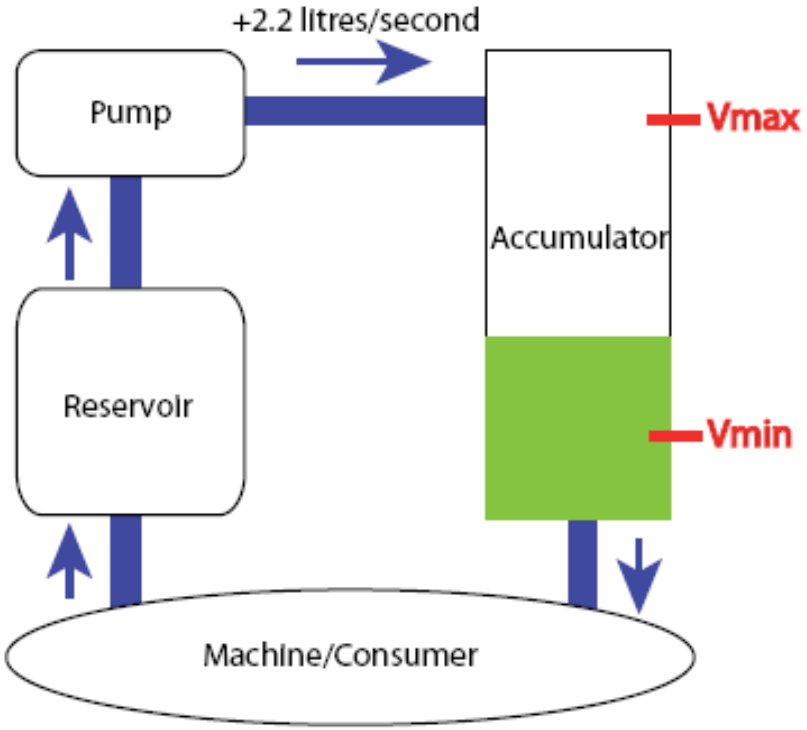
18 methods + 4 tasks = 76 components

Highlight 2: Plastic Injection Molding Machine



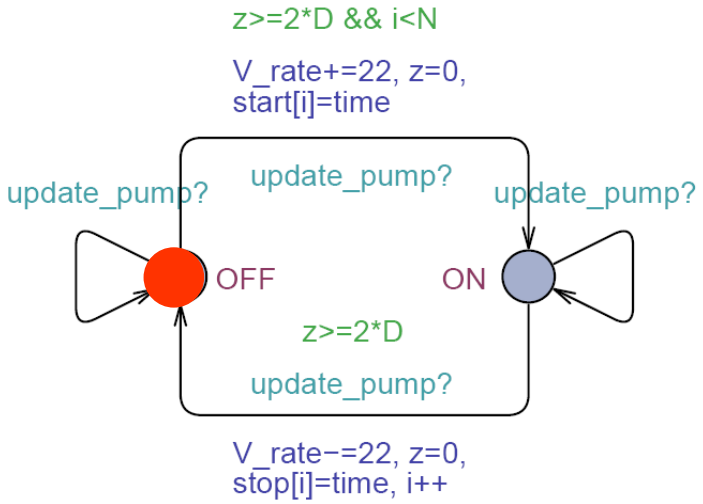
- Robust and optimal control
- Tool Chain
  - Synthesis: **UPPAAL TIGA**
  - Verification: **PHAVer**
  - Performance: **SIMULINK**
- 40% improvement of existing solutions..

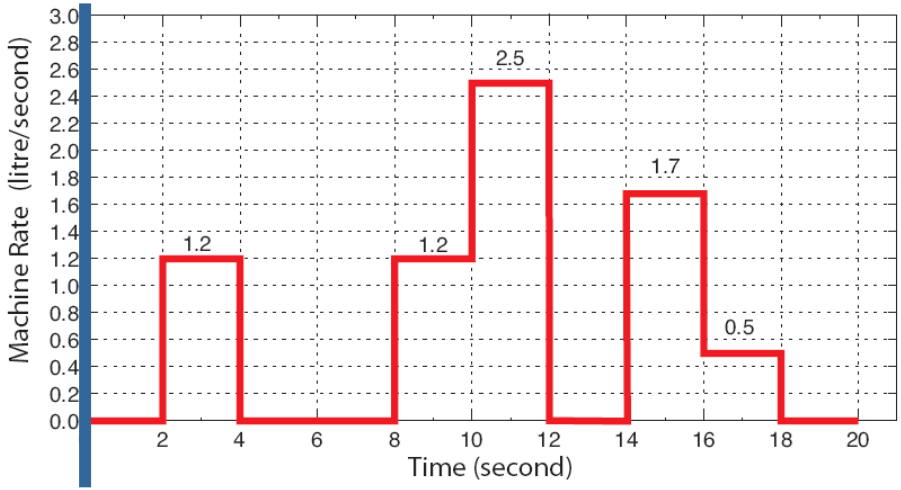
Oil Pump Control Problem

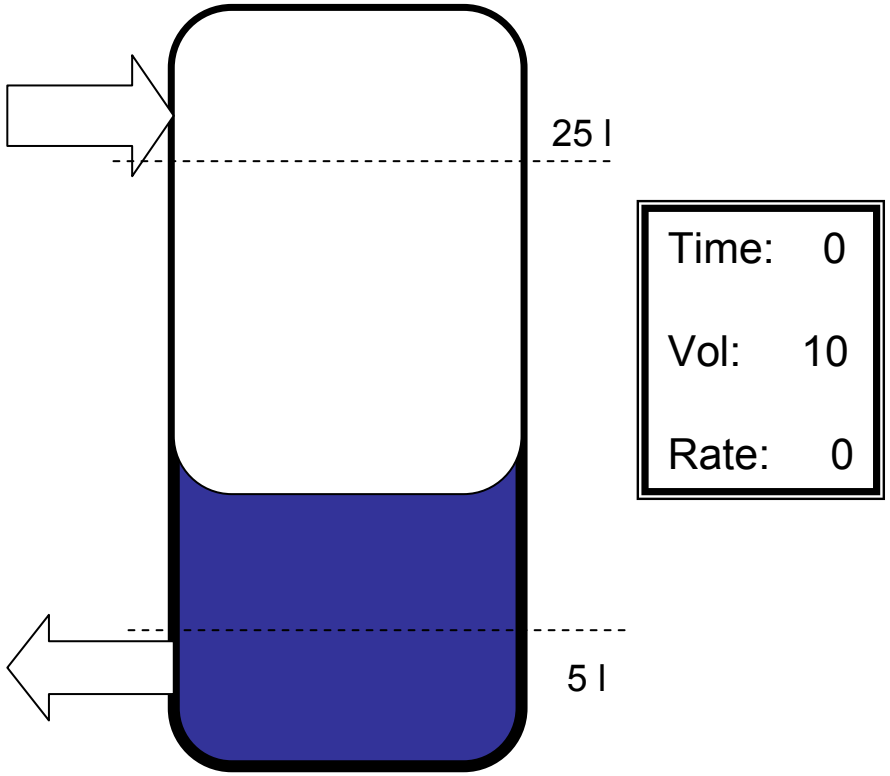


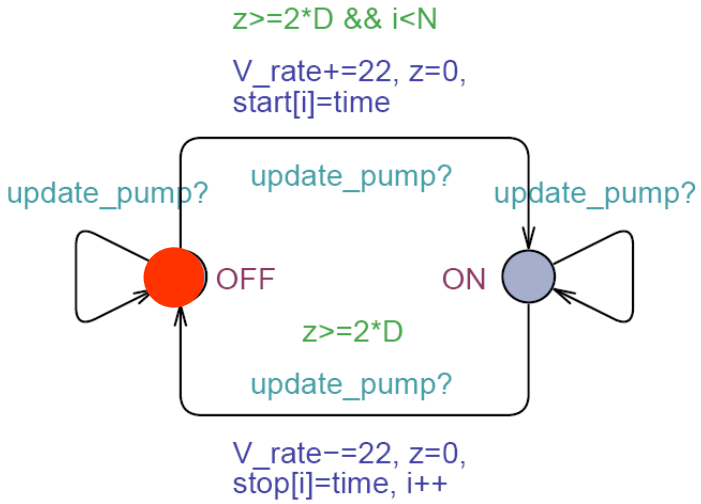
- R1: stay within safe interval [5 , 25]
- R2: minimize average/overall oil volume

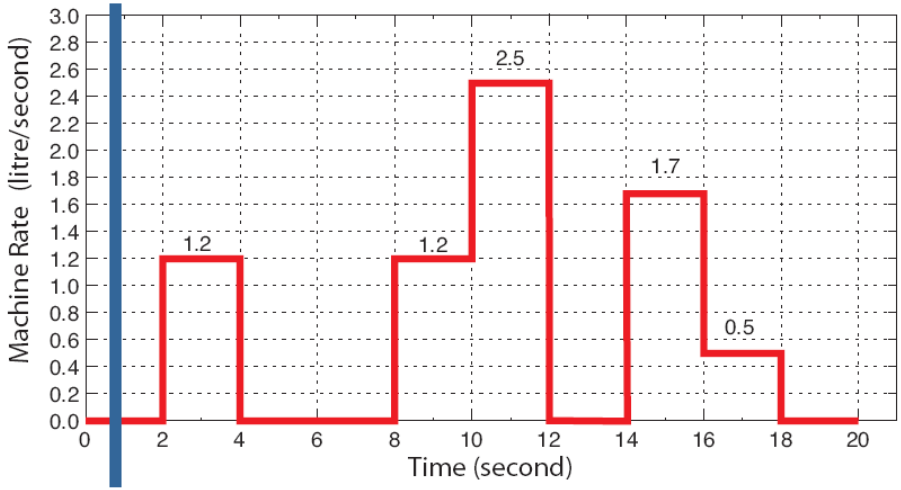
$$\int_{t=0}^{t=T} v(t)dt \,/\, T$$

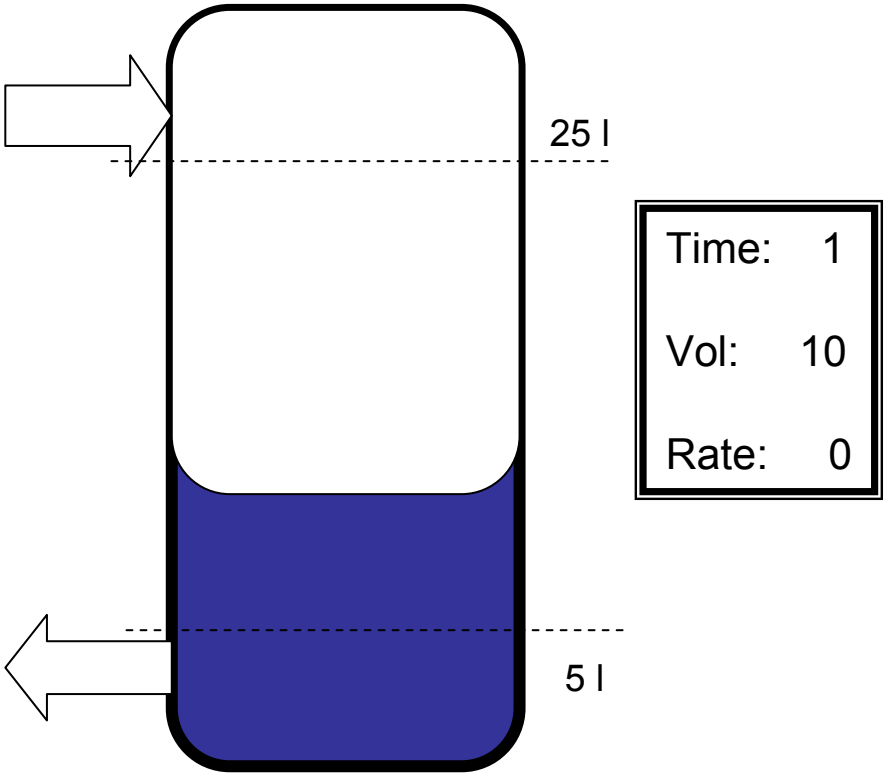

z>=2*D && i<N
V_rate+=22, z=0,
start[i]=time
update_pump?
update_pump?
update_pump?
OFF
ON
z>=2*D
update_pump?
V_rate−=22, z=0,
stop[i]=time, i++

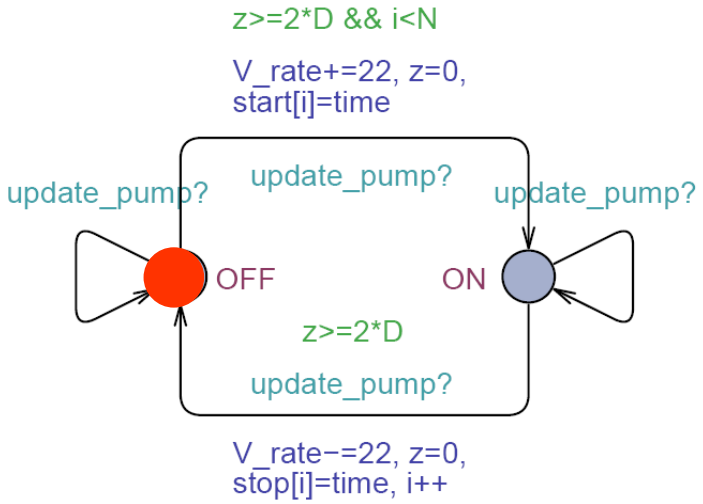

Machine Rate (litre/second)
Time (second)
1.2
1.2
2.5
1.7
0.5

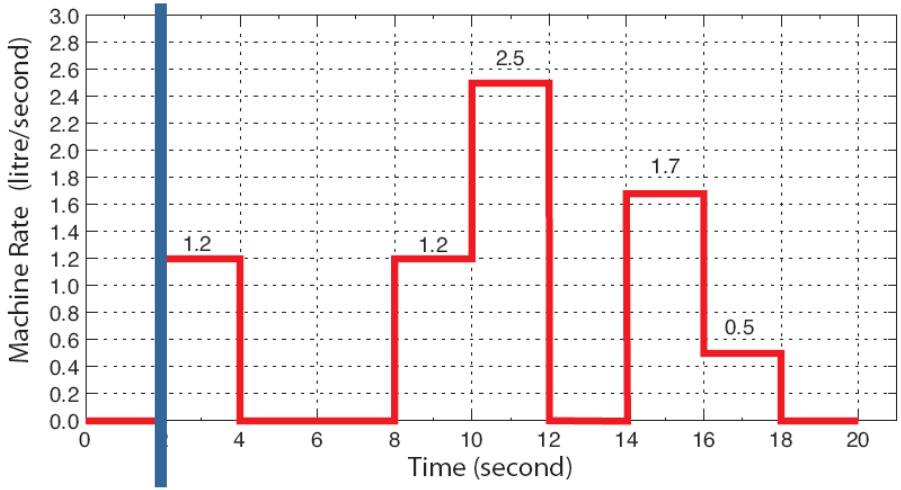

25 l
5 l
Time: 0
Vol: 10
Rate: 0

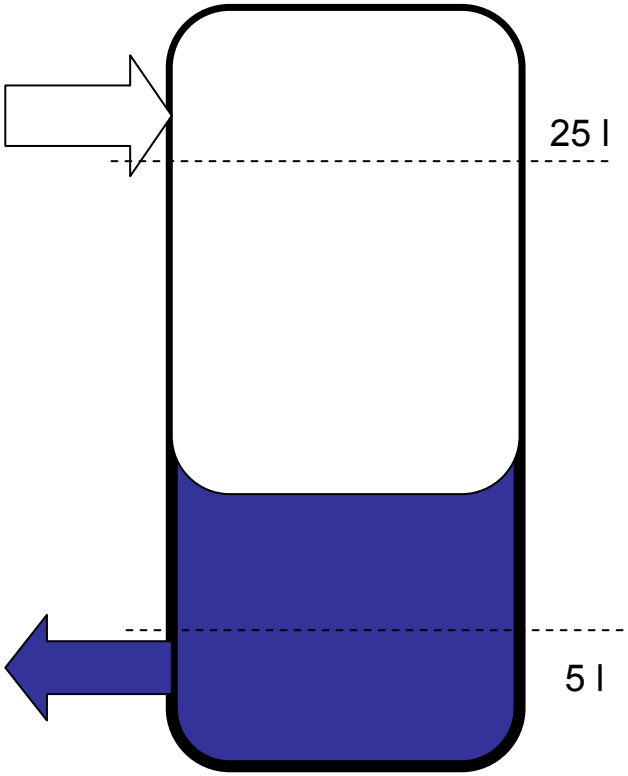

z>=2*D && i<N
V_rate+=22, z=0,
start[i]=time
update_pump?
update_pump?
update_pump?
OFF
ON
z>=2*D
update_pump?
V_rate−=22, z=0,
stop[i]=time, i++


Machine Rate (litre/second)
Time (second)
1.2
1.2
2.5
1.7
0.5


25 l
5 l
Time: 1
Vol: 10
Rate: 0



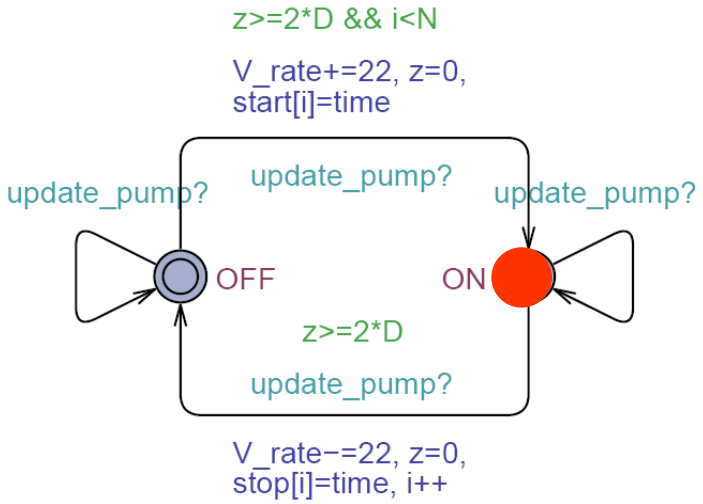


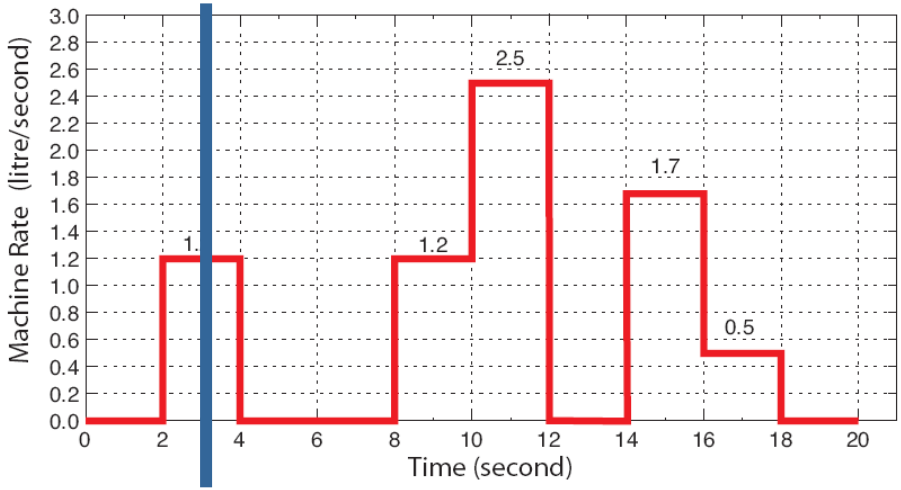


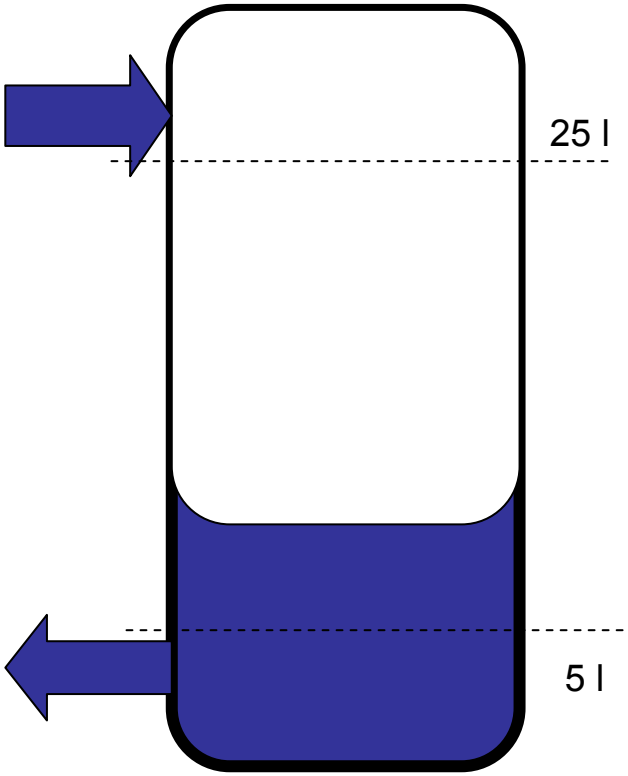
Time: 2

Vol: 10

Rate: -1.2



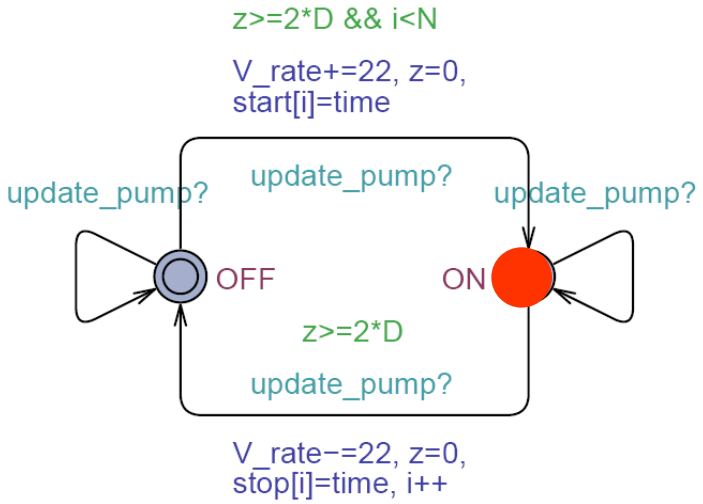


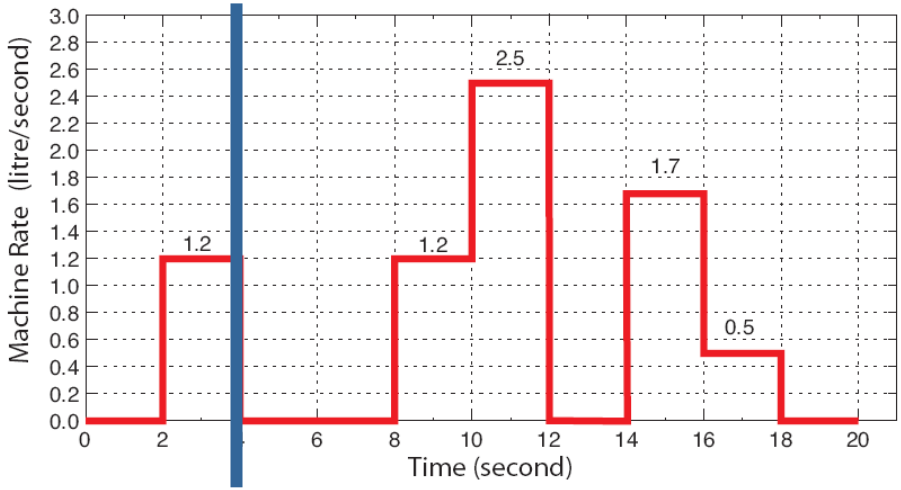


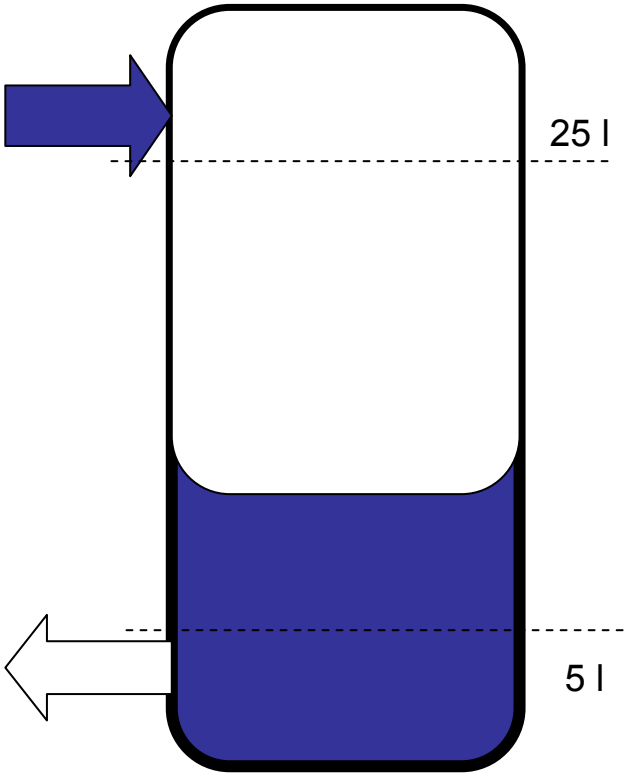
Time: 3

Vol: 8.8

Rate: +1.0



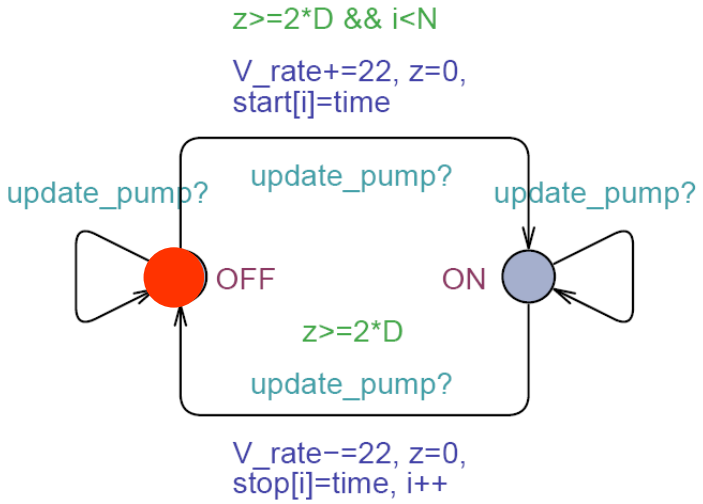


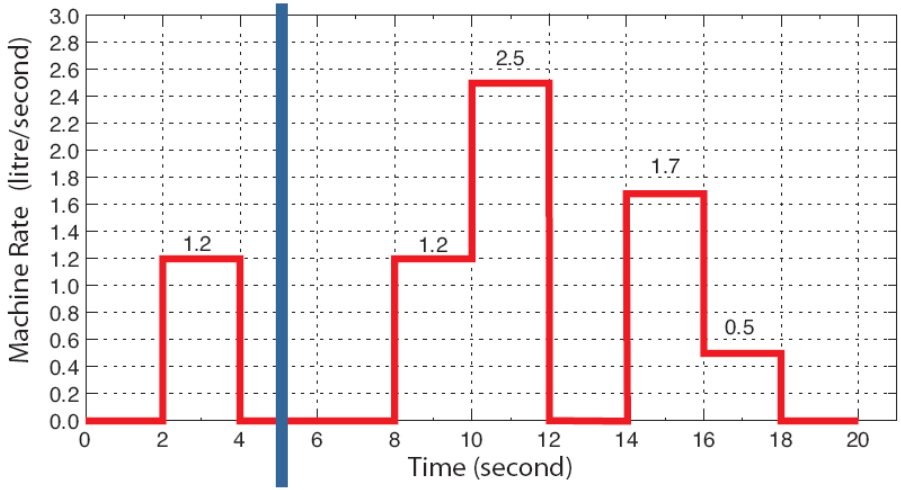


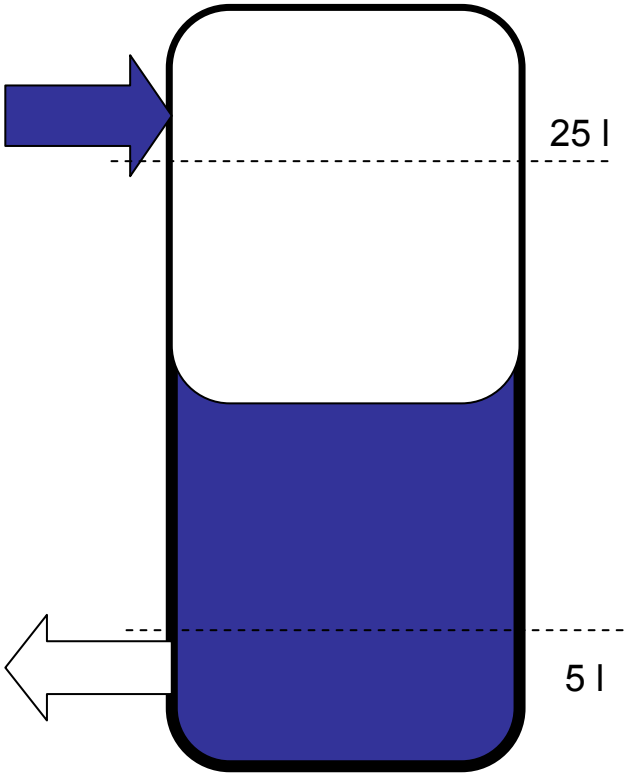
Time: 4

Vol: 9.8

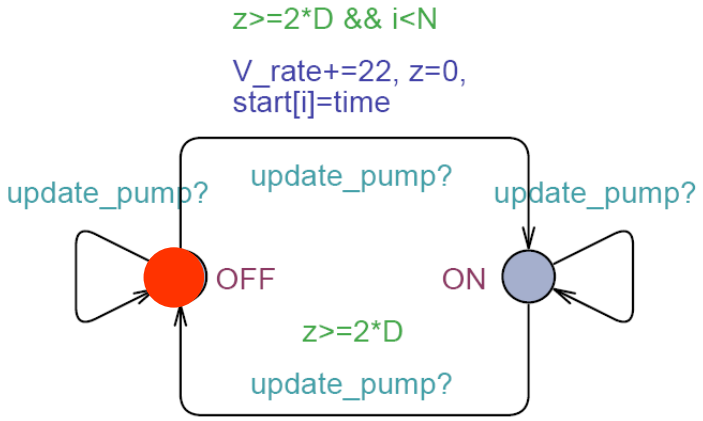
Rate: +2.2

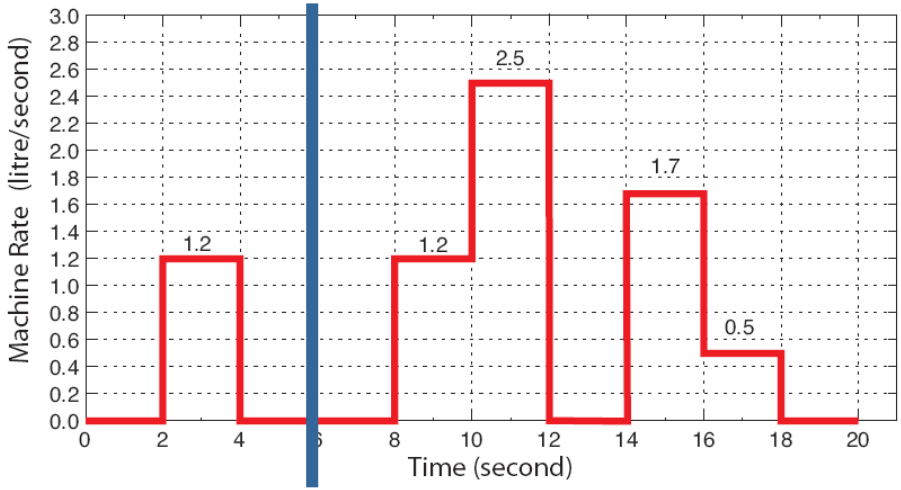


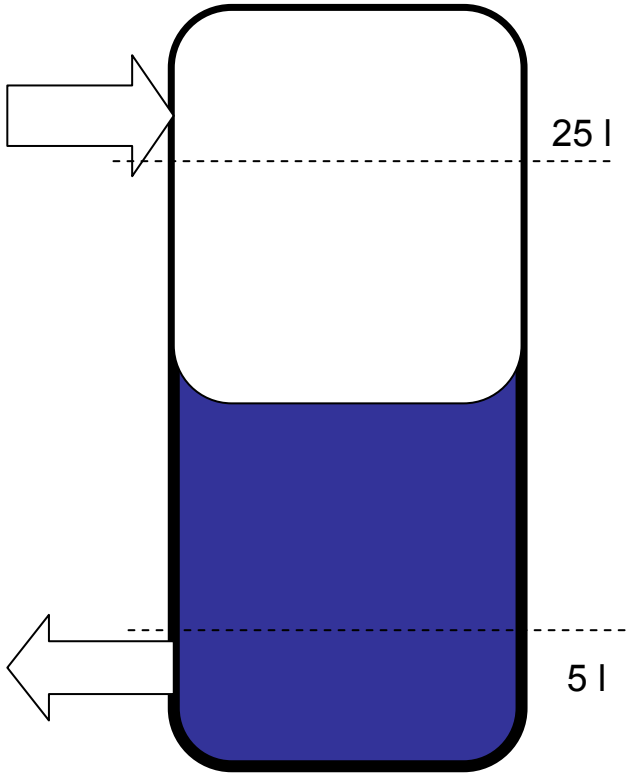




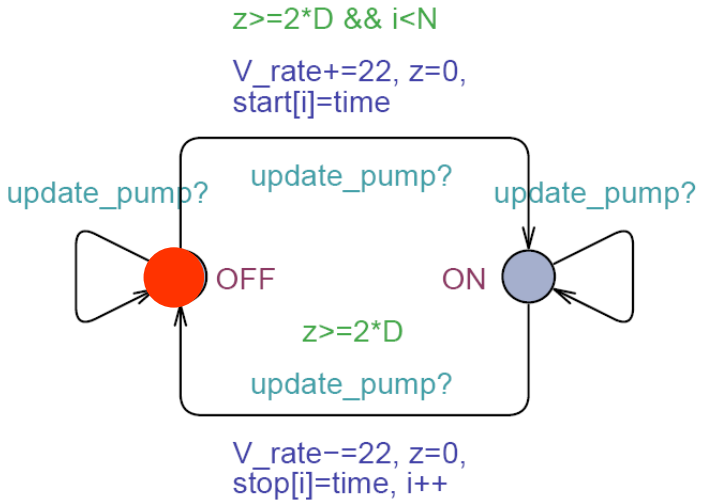
Time:	5
Vol:	12
Rate:	0

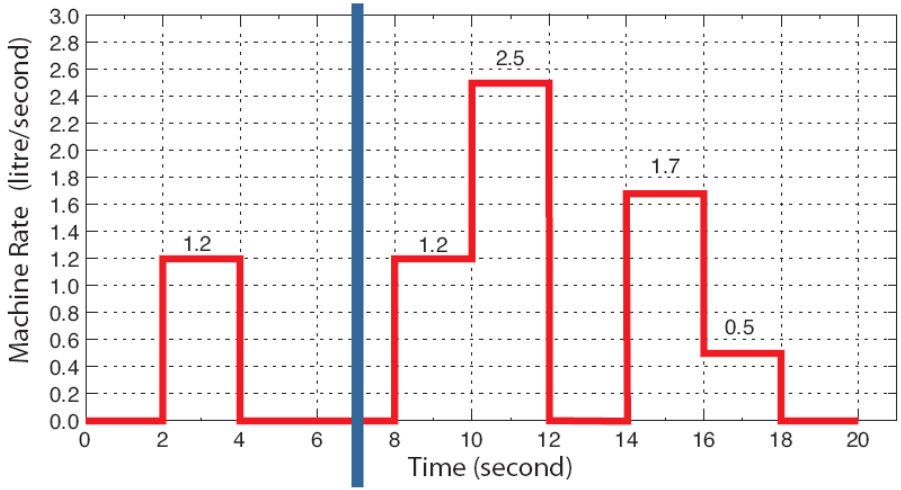


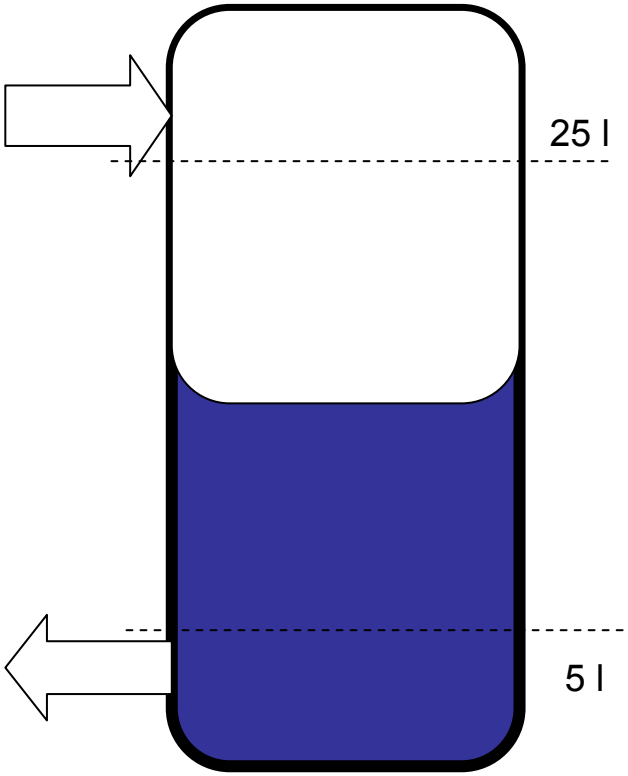




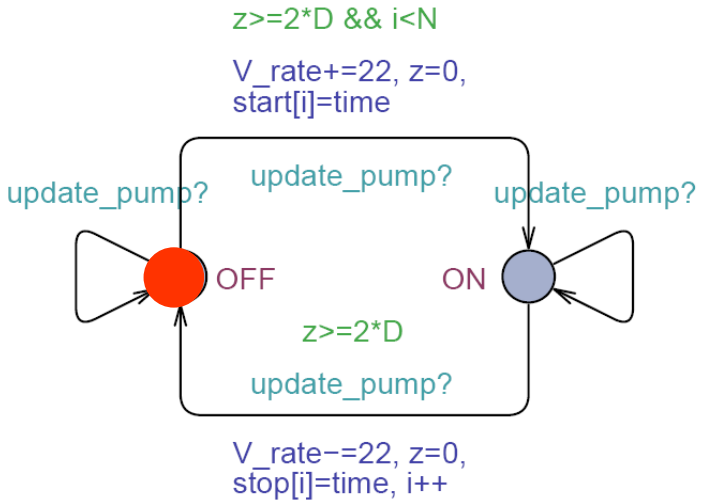
Time:	6
Vol:	12
Rate:	0

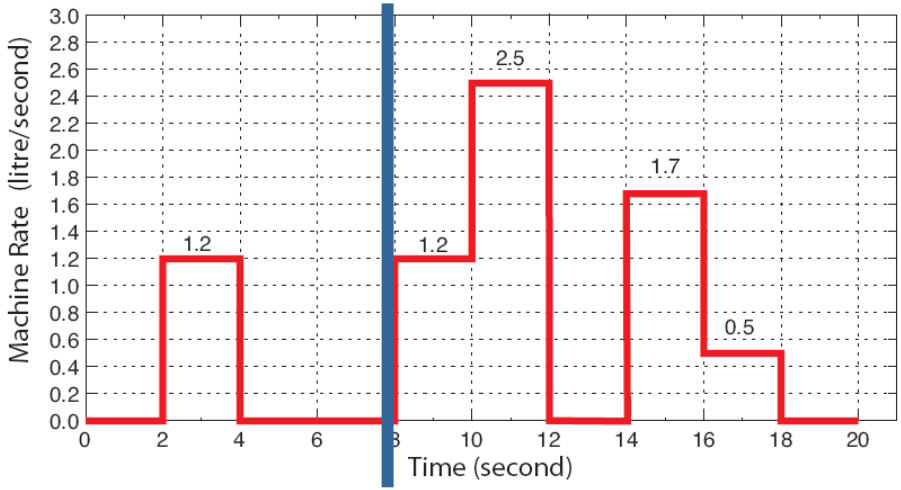


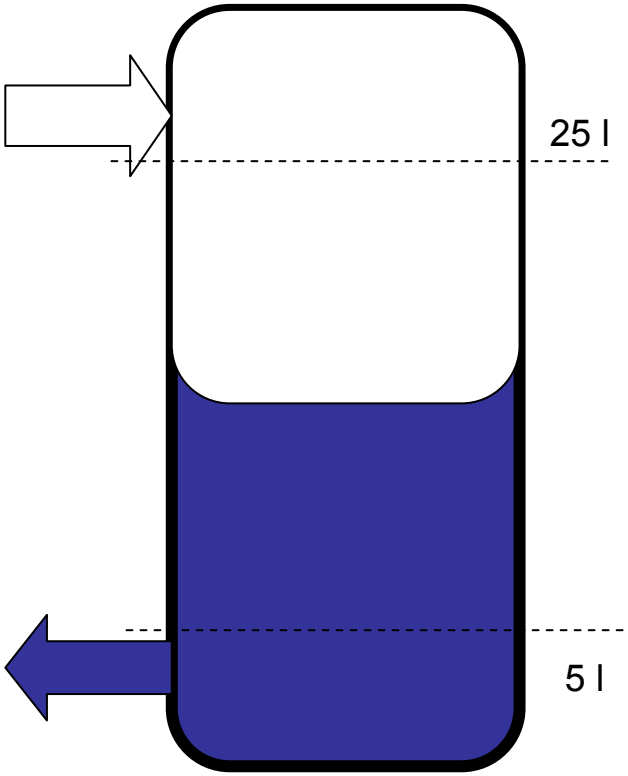




Time:	7
Vol:	12
Rate:	0



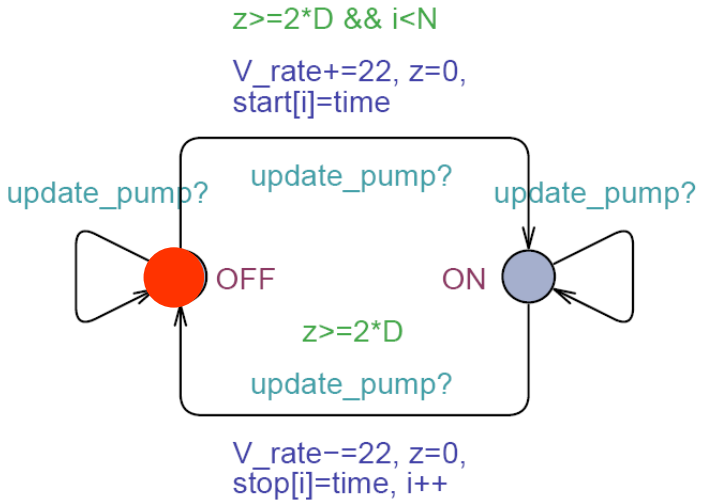


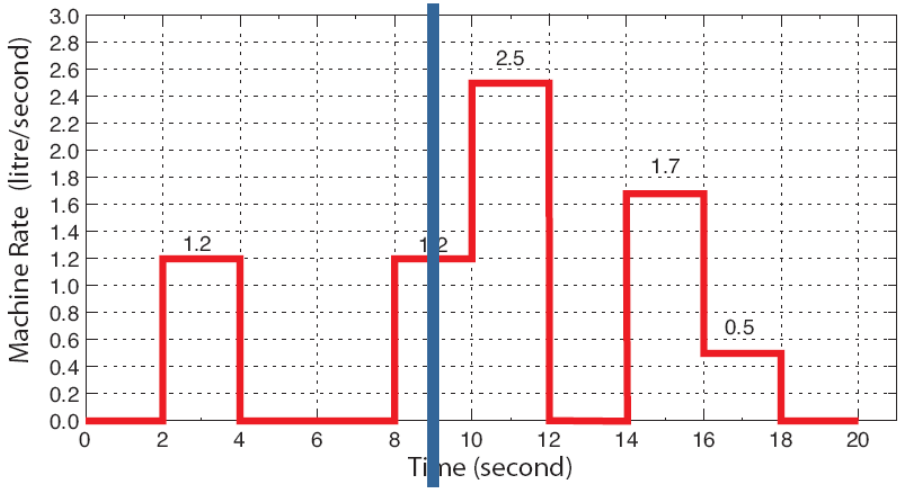


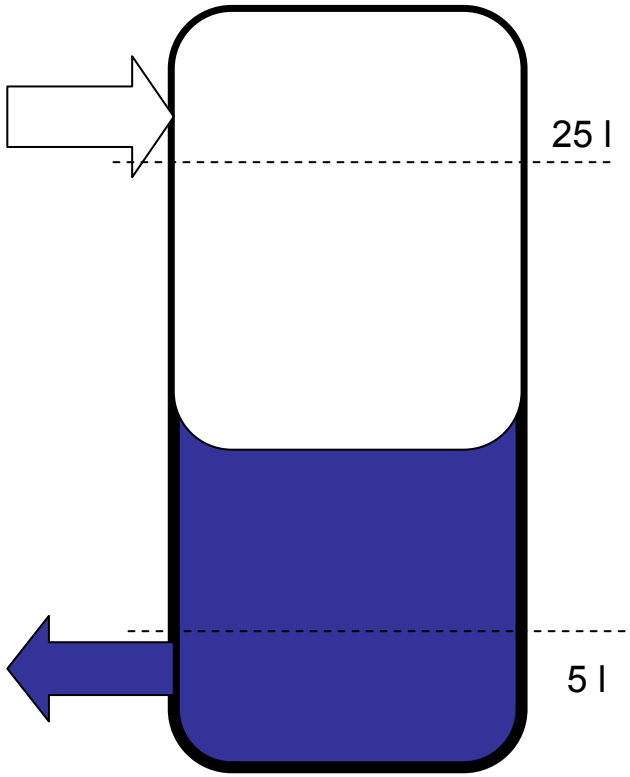
Time: 8

Vol: 12

Rate: -1.2



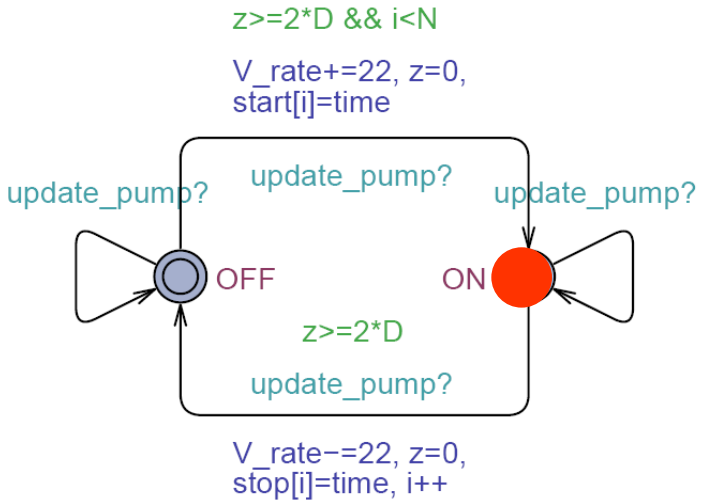


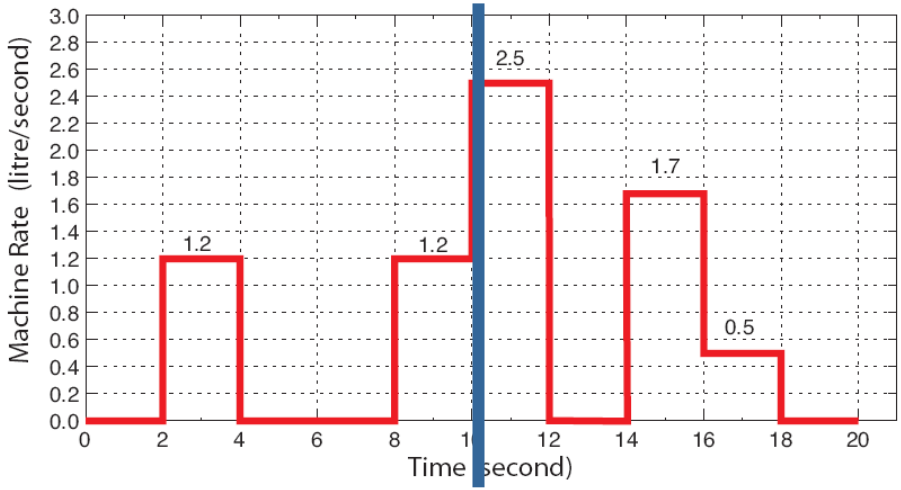


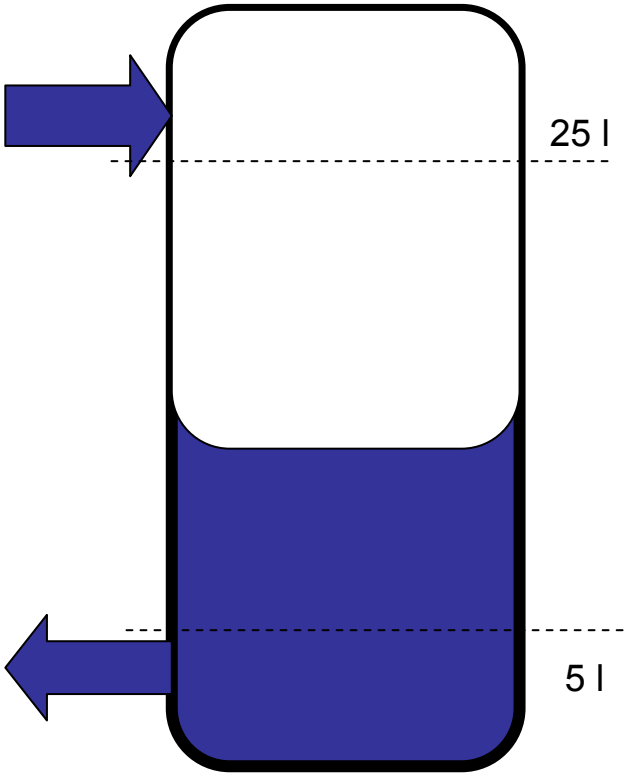
Time: 9

Vol: 10.8

Rate: -1.2



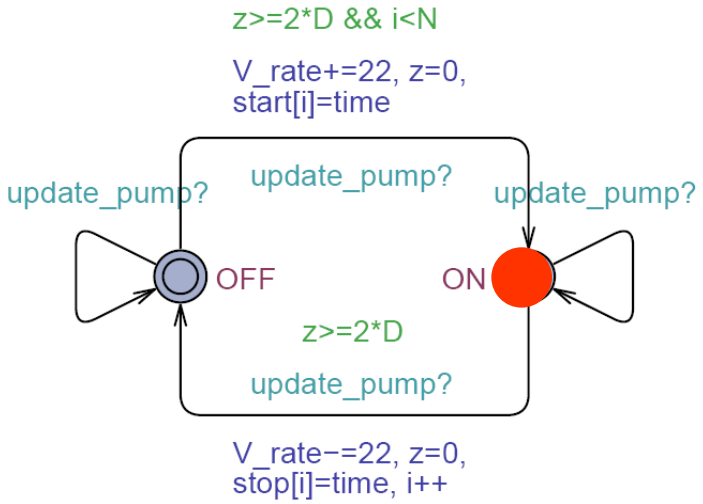


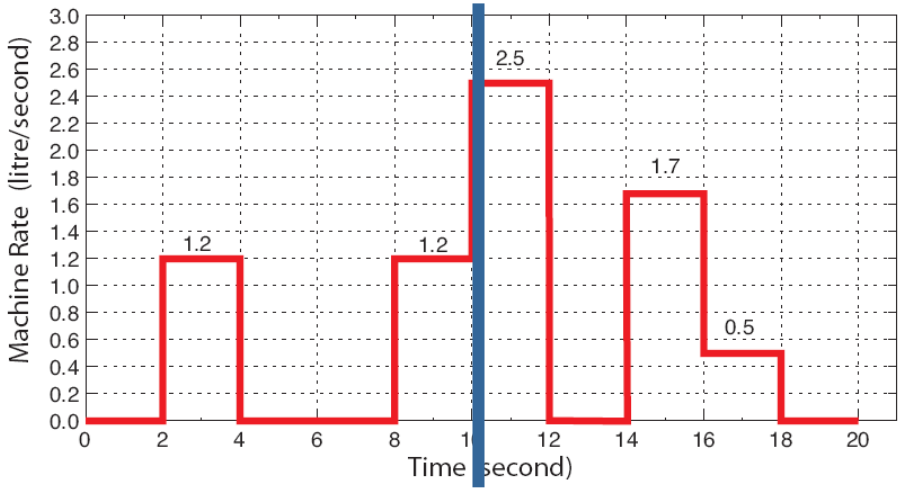


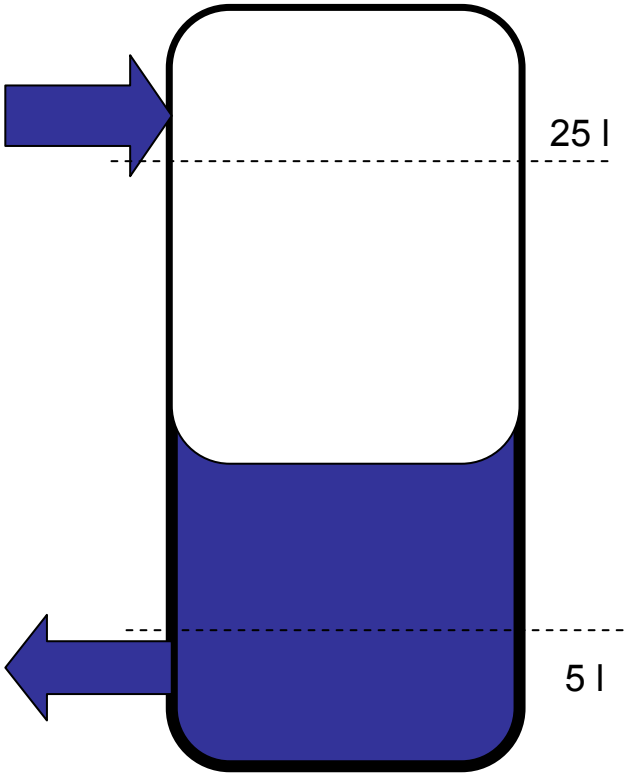
Time: 10

Vol: 9.6

Rate: -0.3



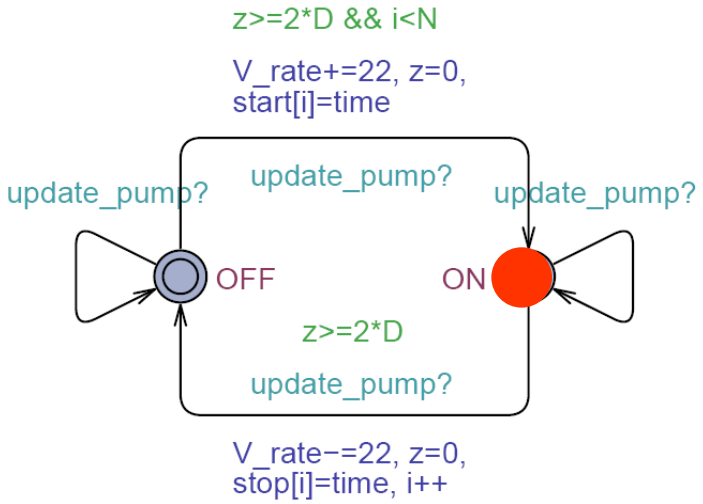


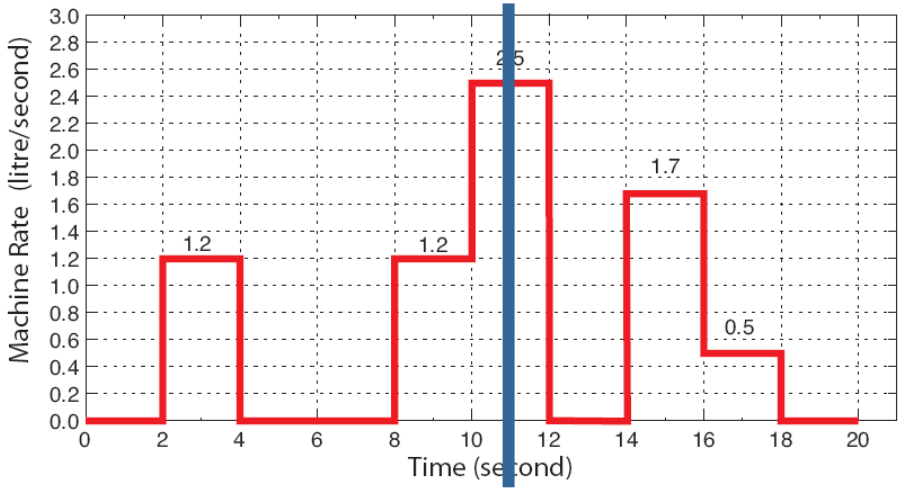


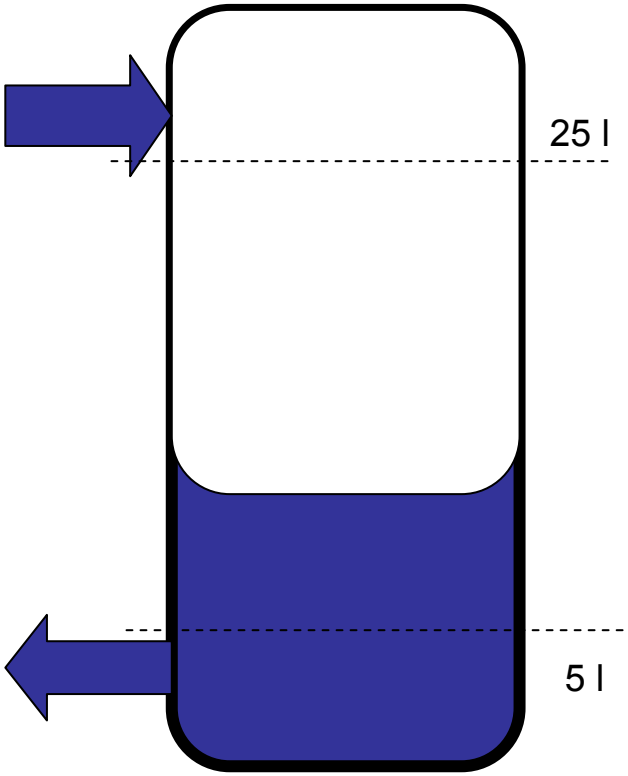
Time: 10

Vol: 9.6

Rate: -0.3



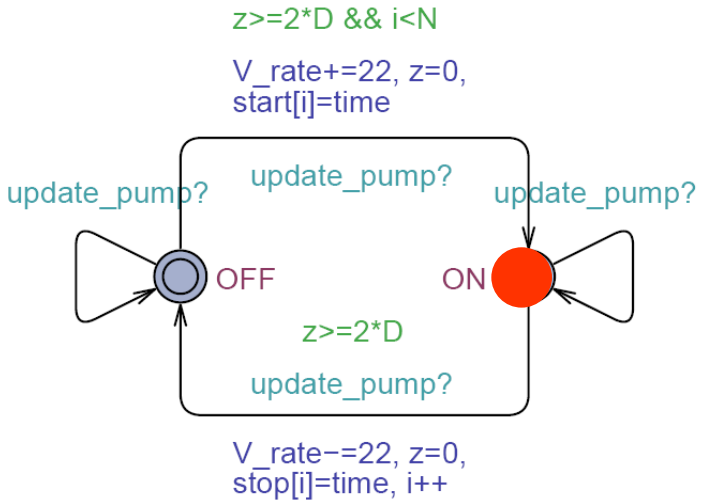


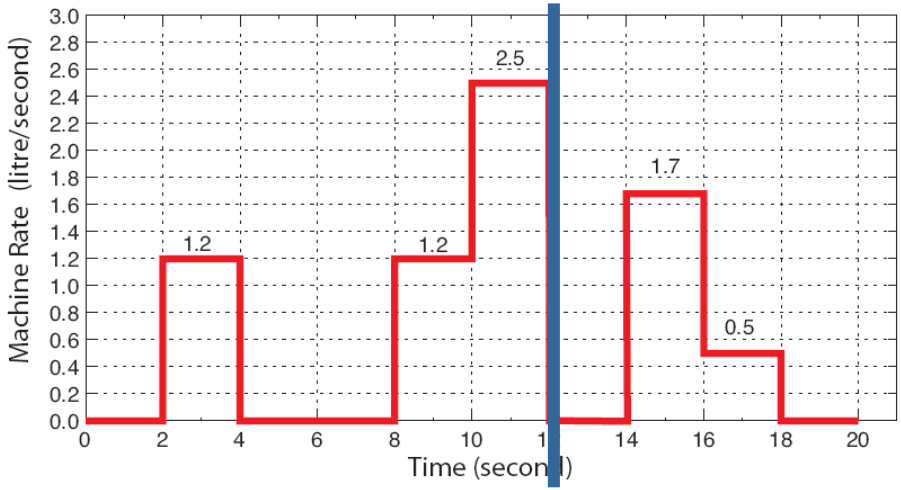


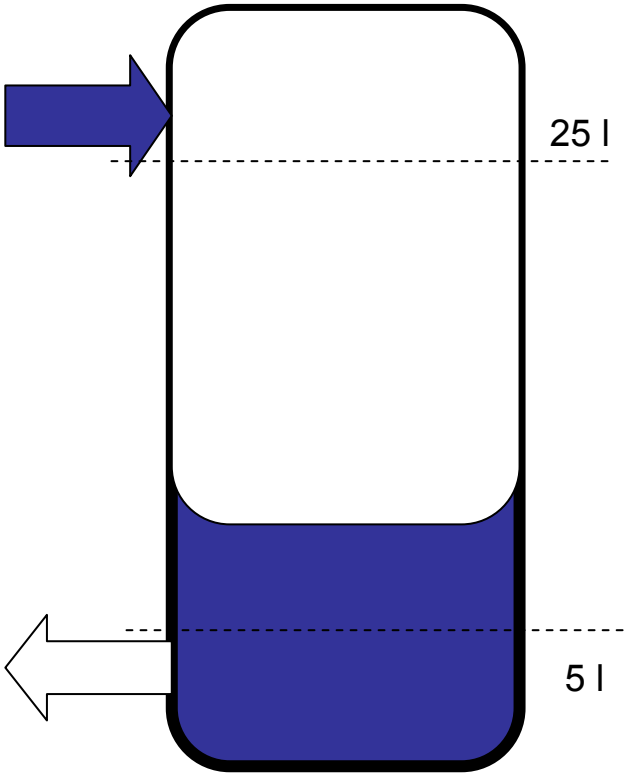
Time: 11

Vol: 9.3

Rate: -0.3



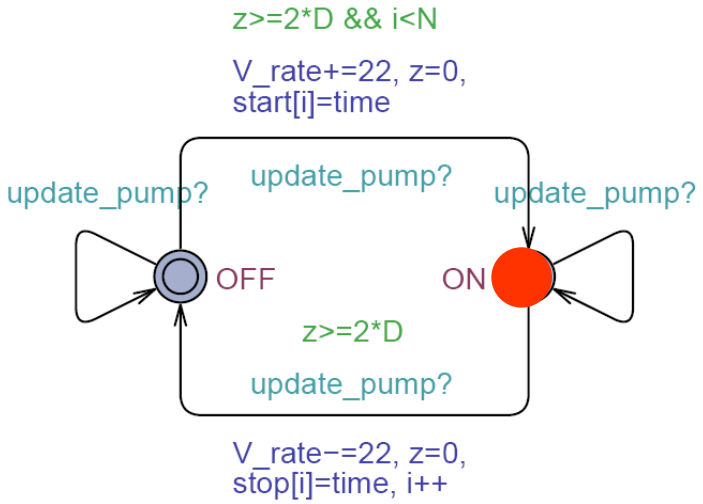


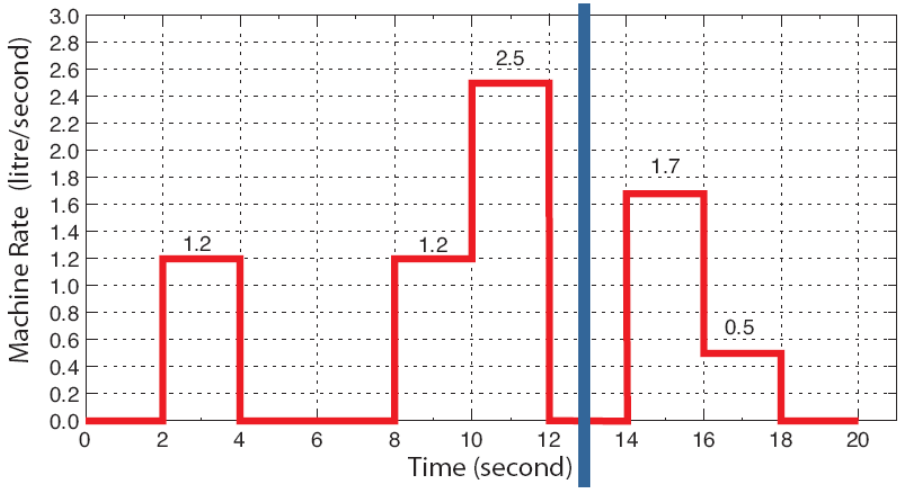


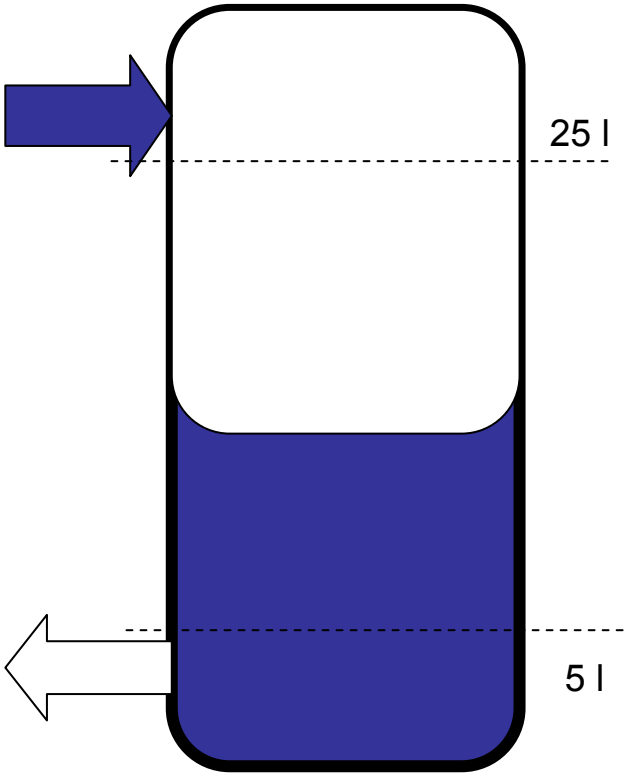
Time: 12

Vol: 9.3

Rate: +2.2



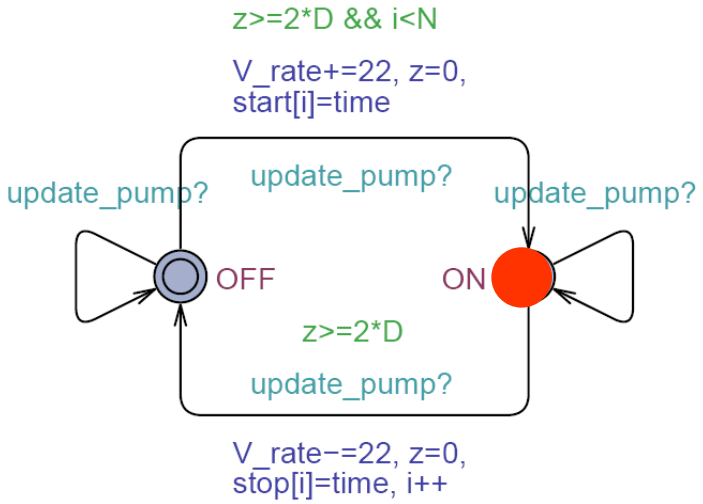


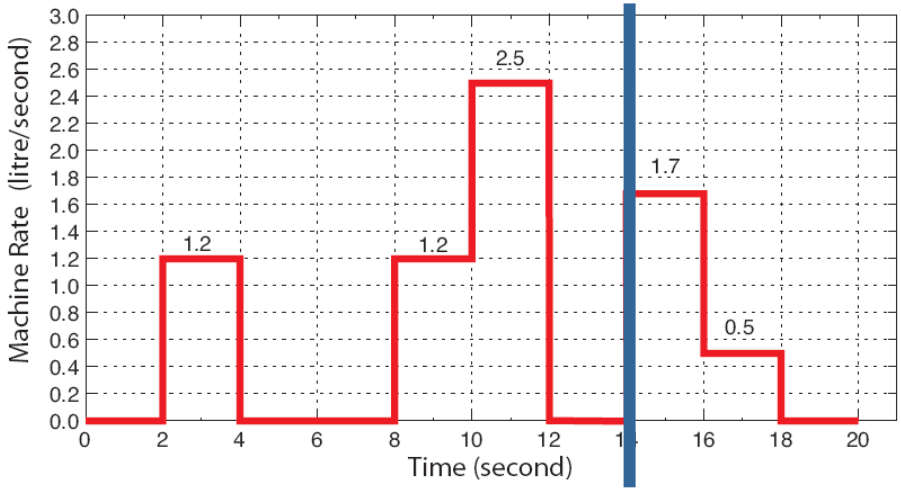


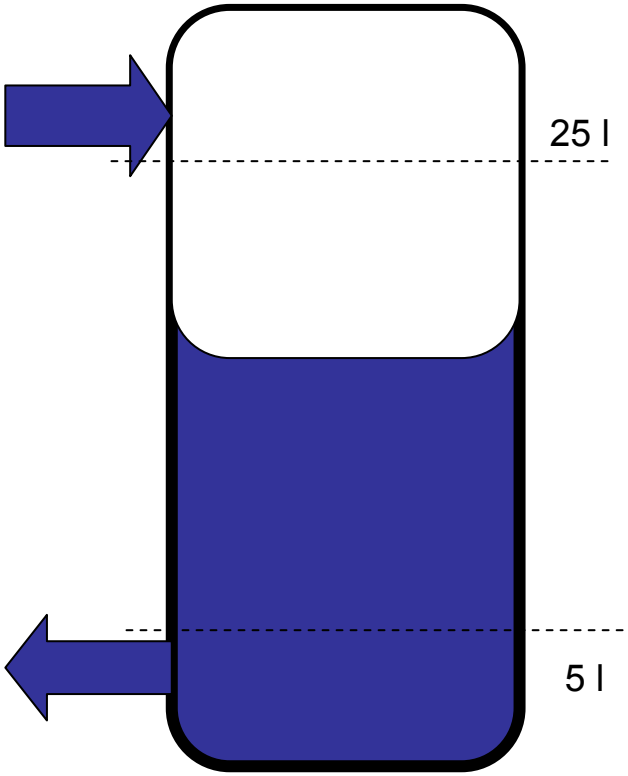
Time: 13

Vol: 11.5

Rate: +2.2



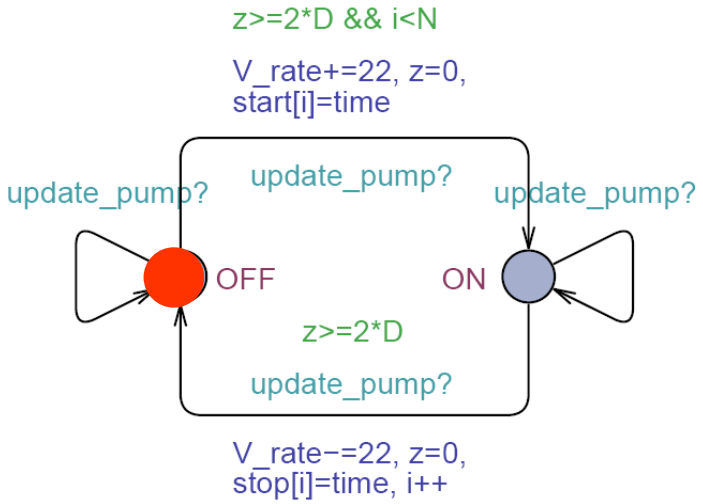


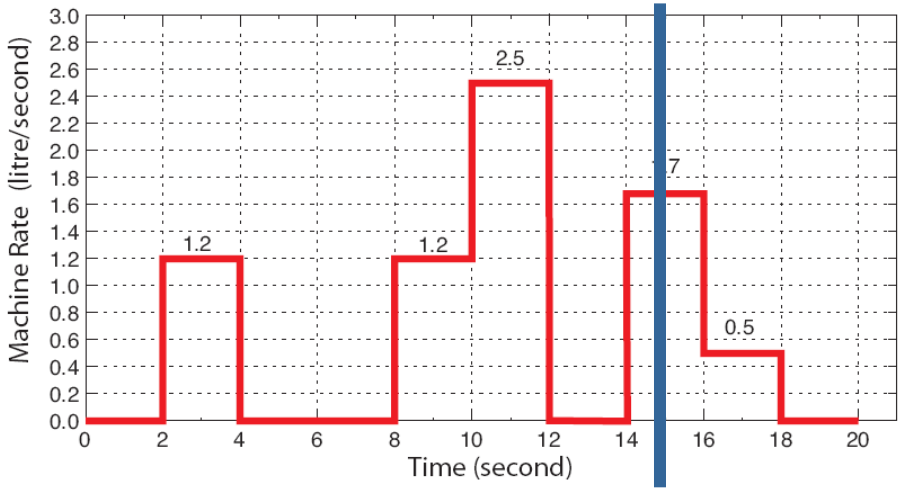


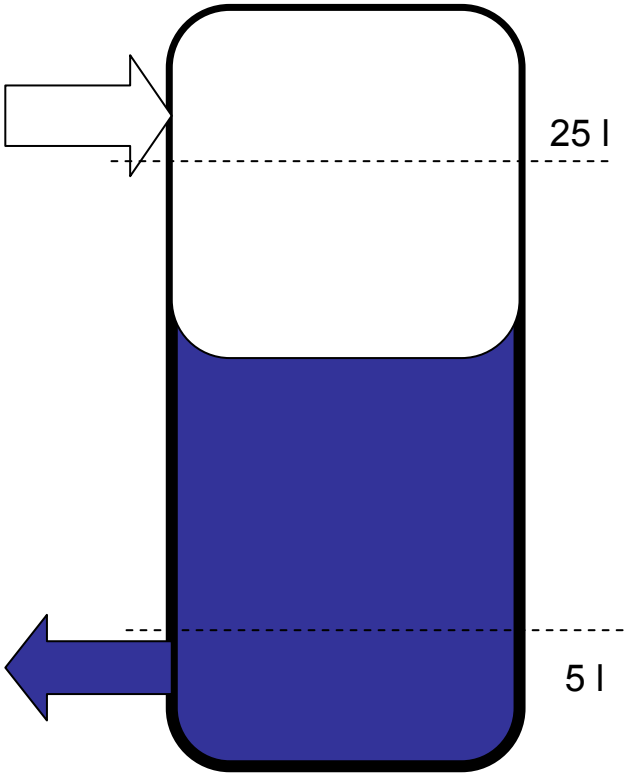
Time: 14

Vol: 13.7

Rate: +0.5



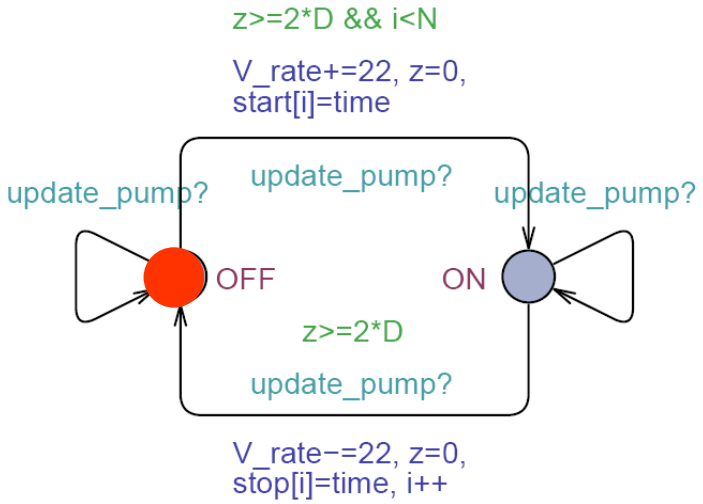


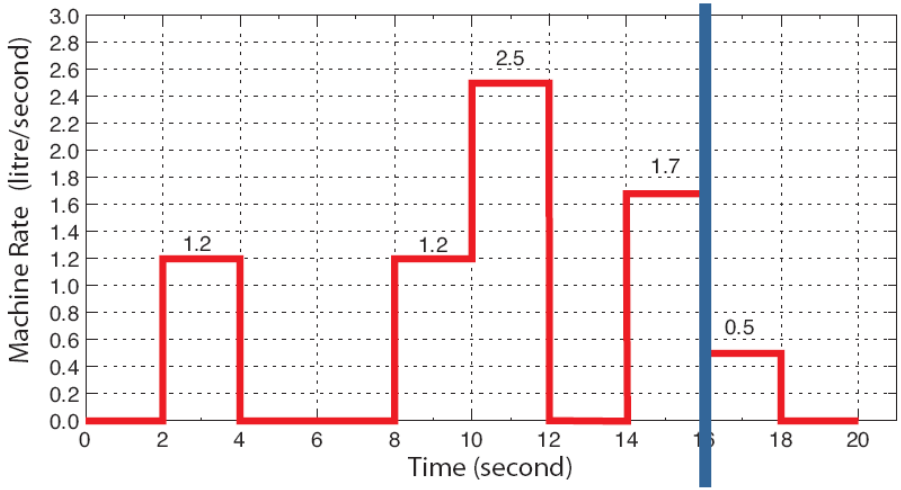


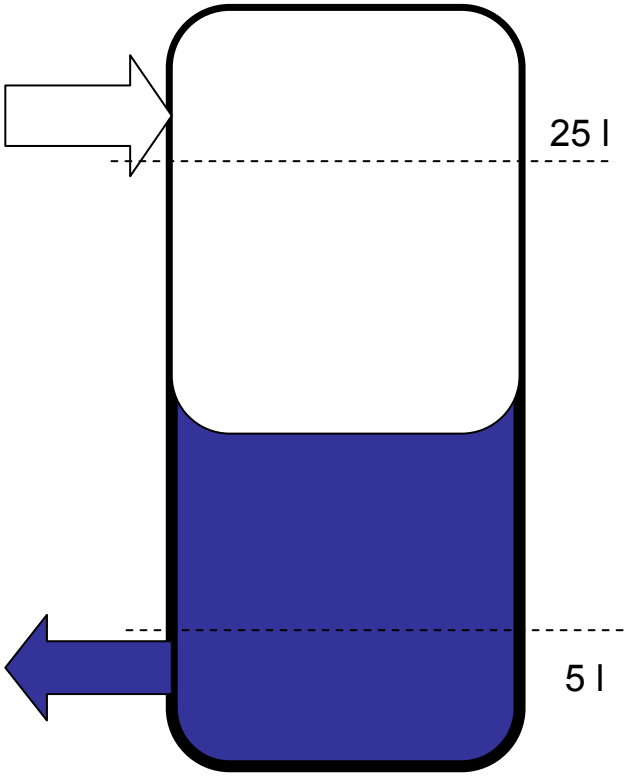
Time: 15

Vol: 14.2

Rate: -1.7



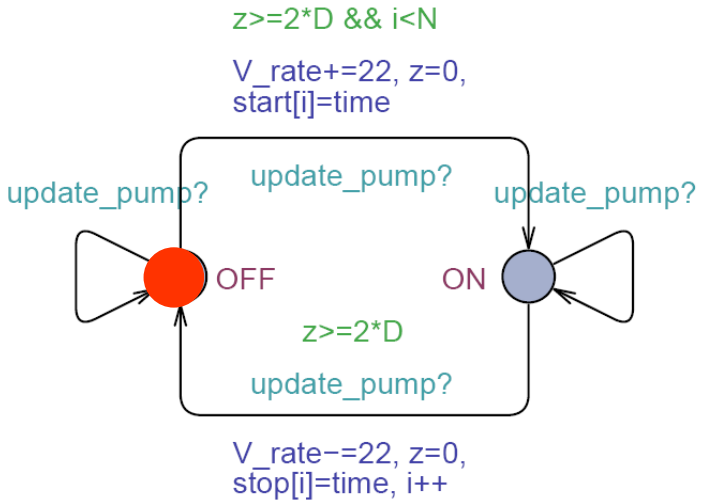


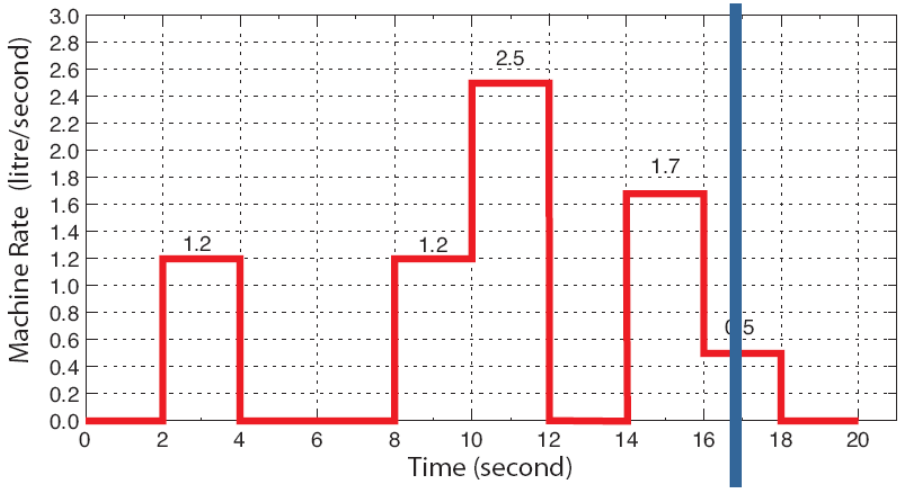


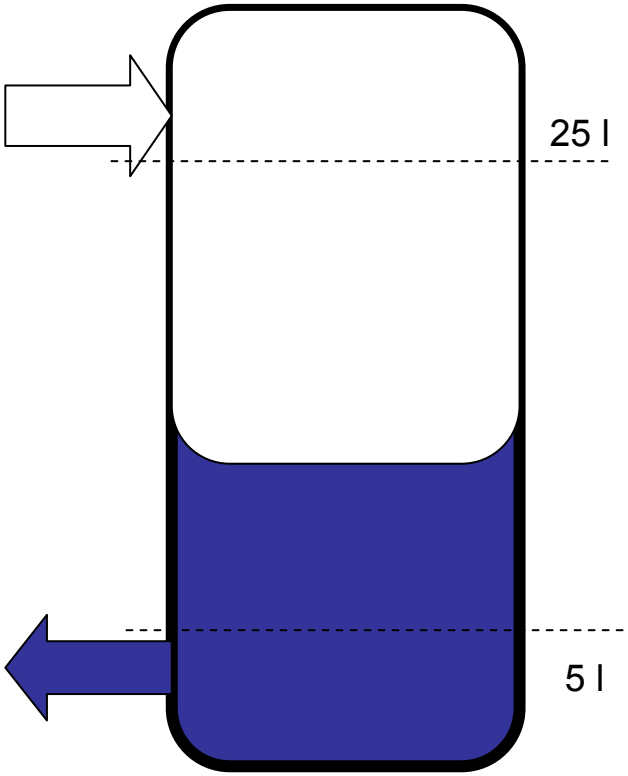
Time: 16

Vol: 12.5

Rate: -0.5



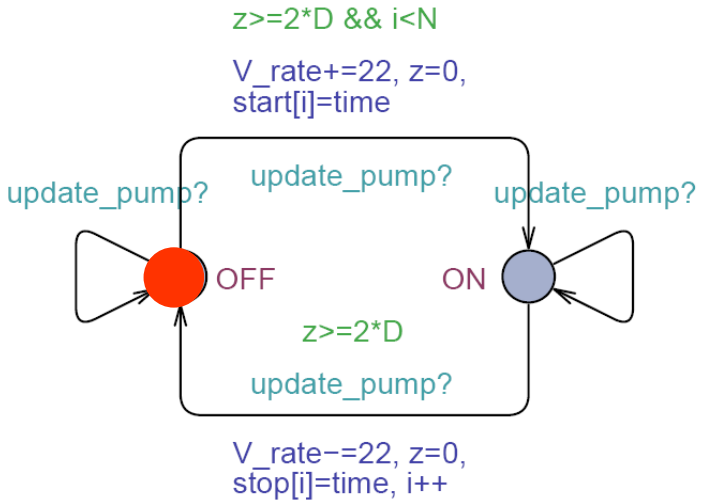


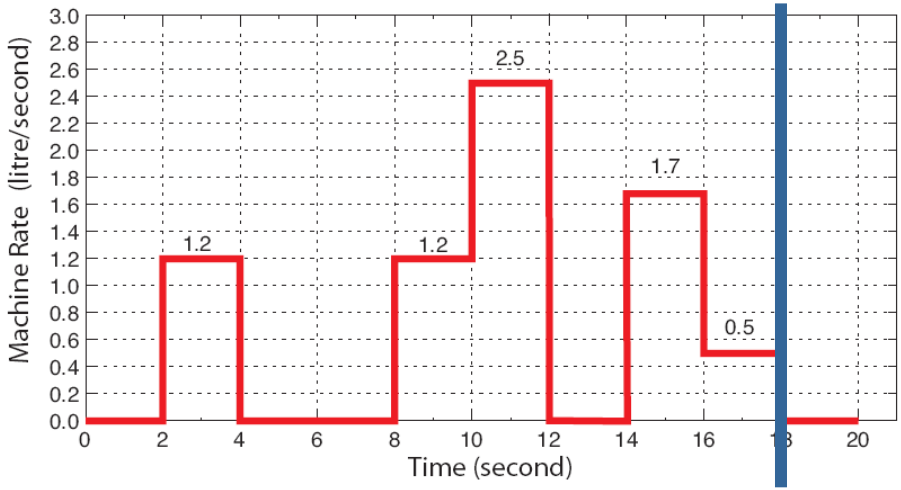


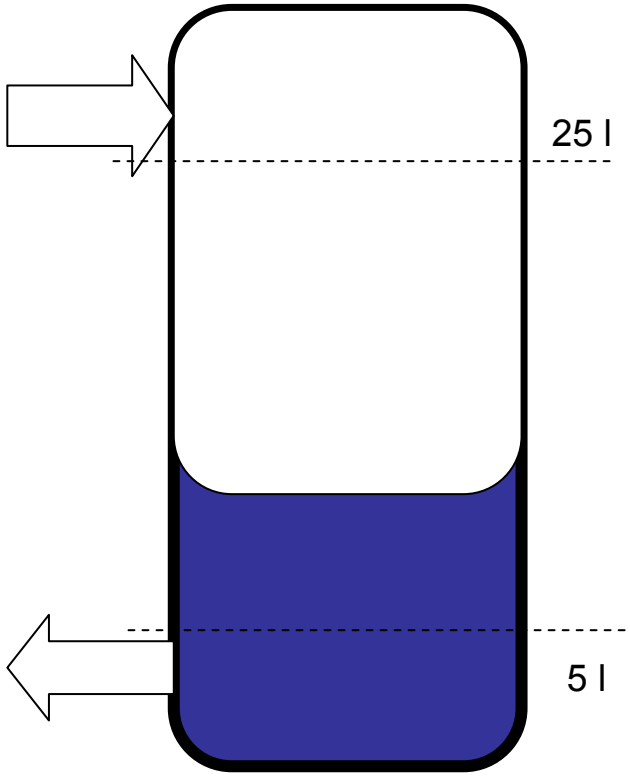
Time: 17

Vol: 12.0

Rate: -0.5



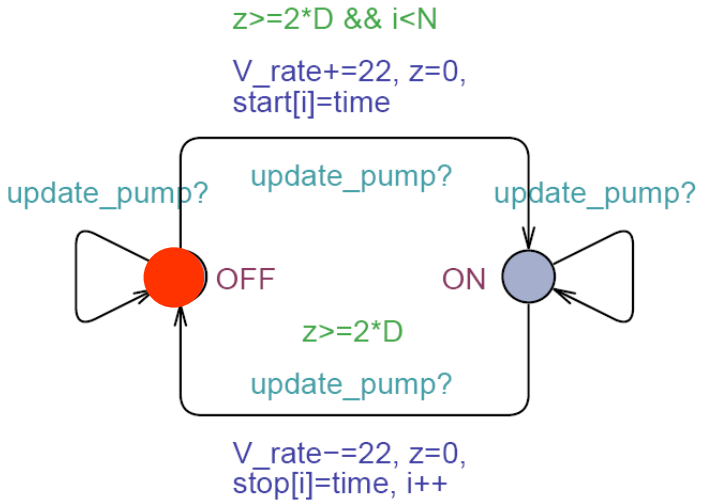


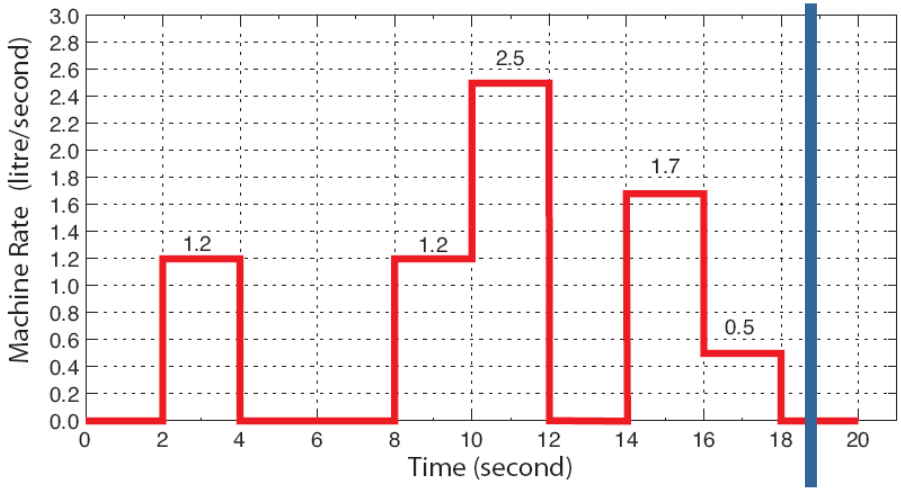


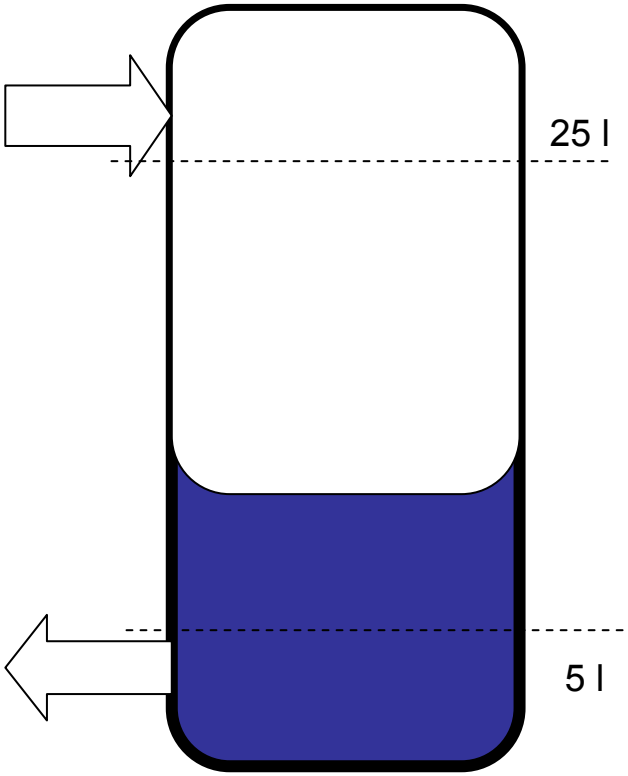
Time: 18

Vol: 11.5

Rate: 0



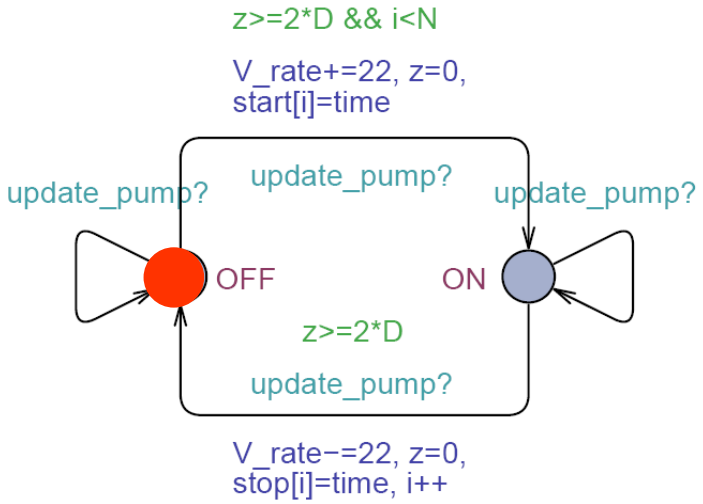


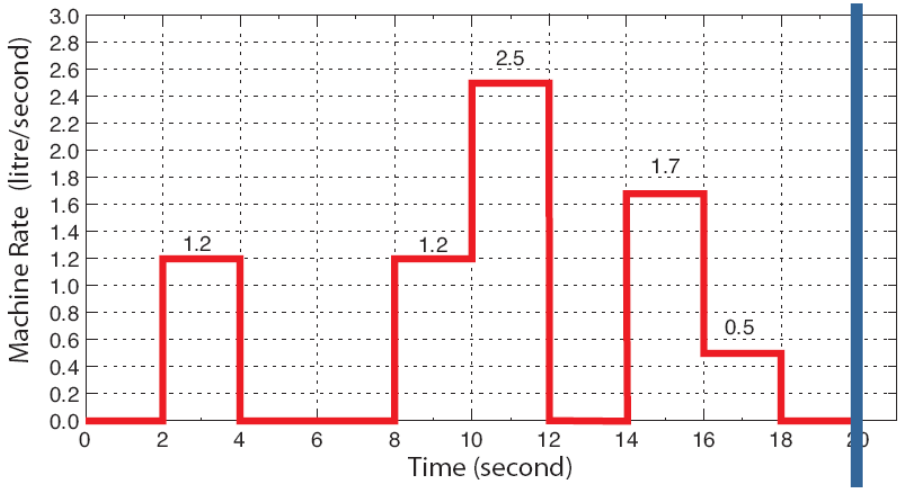


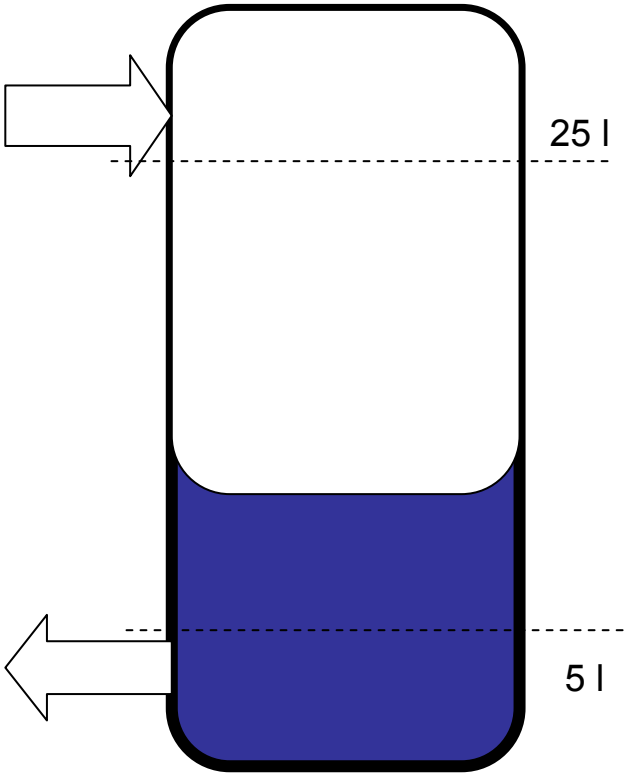
Time: 19

Vol: 11.5

Rate: 0







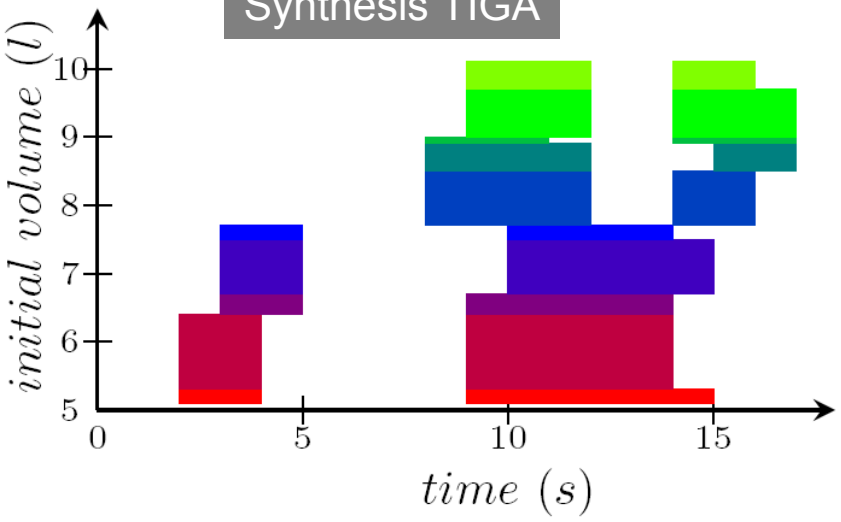
Time: 20

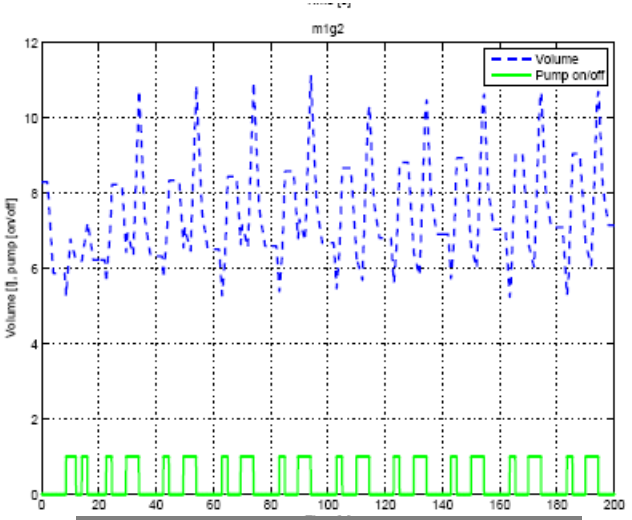
Vol: 11.5

Rate: 0

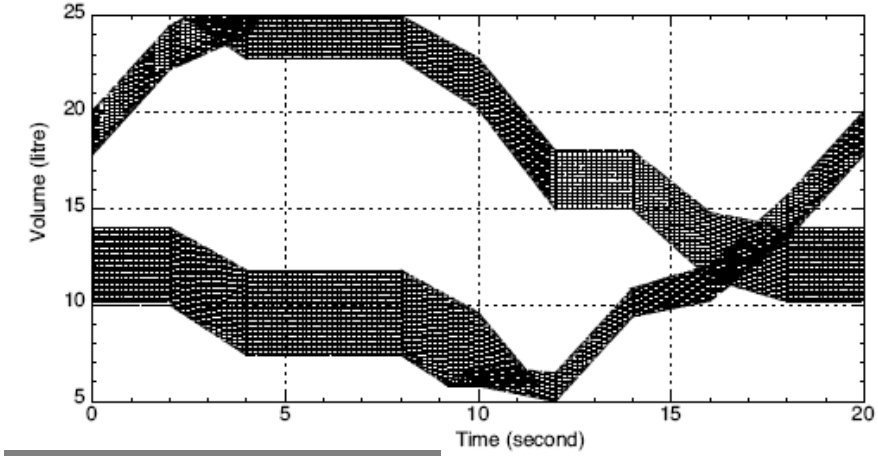
Tool Chain

Synthesis TIGA





Performance Evaluation
SIMULINK



Verification PHAVER

Guaranteed

Correctness

Robustness

with

40% improvement

To be continued in

ARTIST DESIGN

(Modeling & Validation)

Quasimodo

Multiform

Gasics

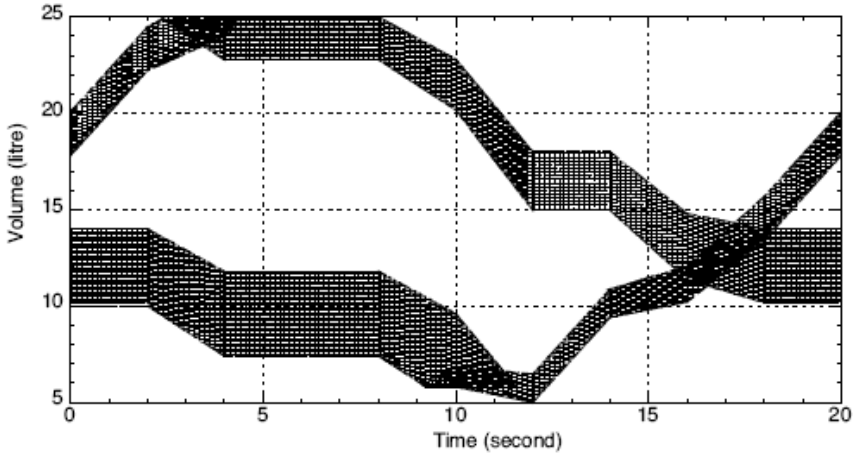
DaNES

DOTS

..

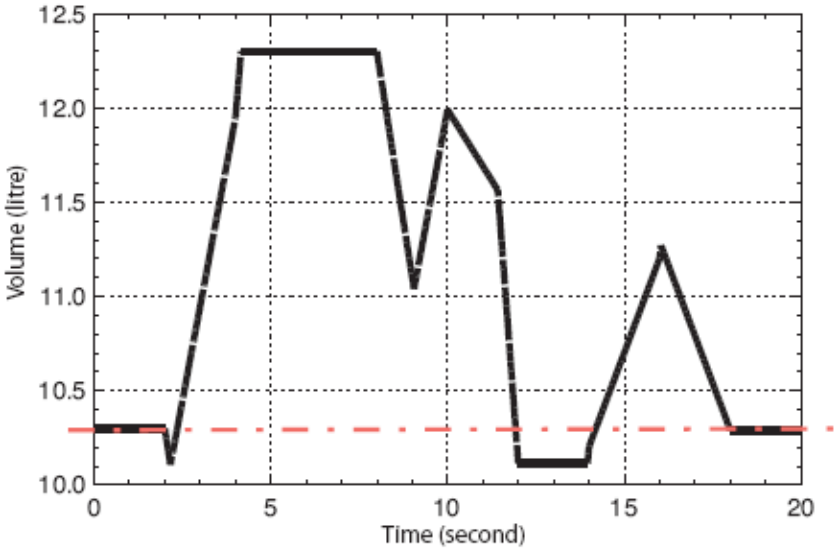
!

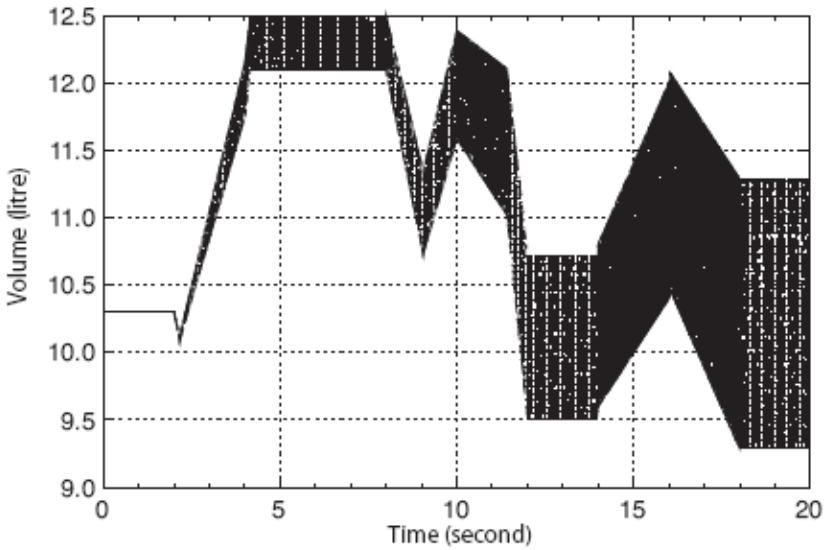
Verification Using PHAVER



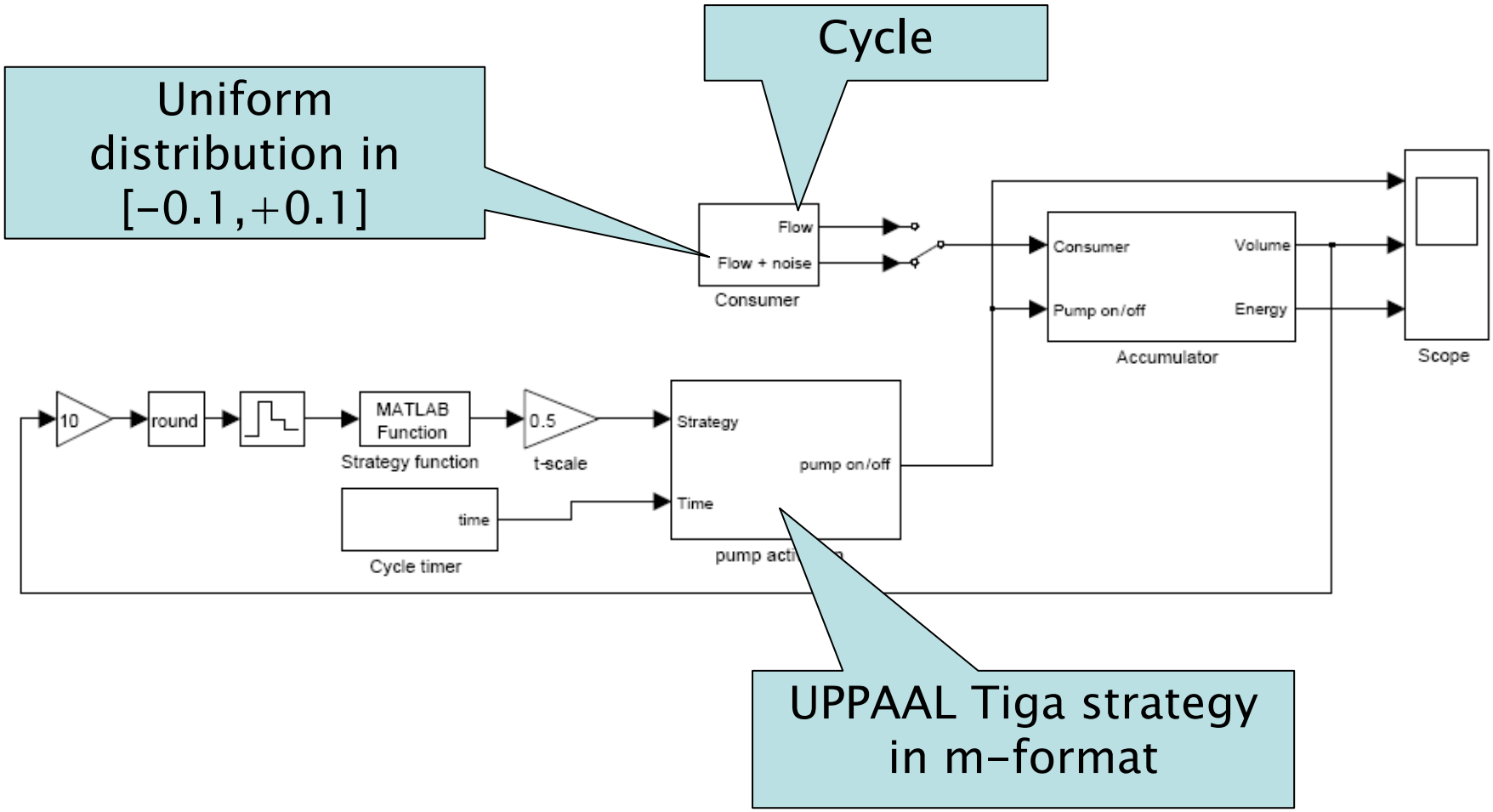
Bang-Bang safe and robust

HyDAC optimized
possibly unsafe under fluctuation

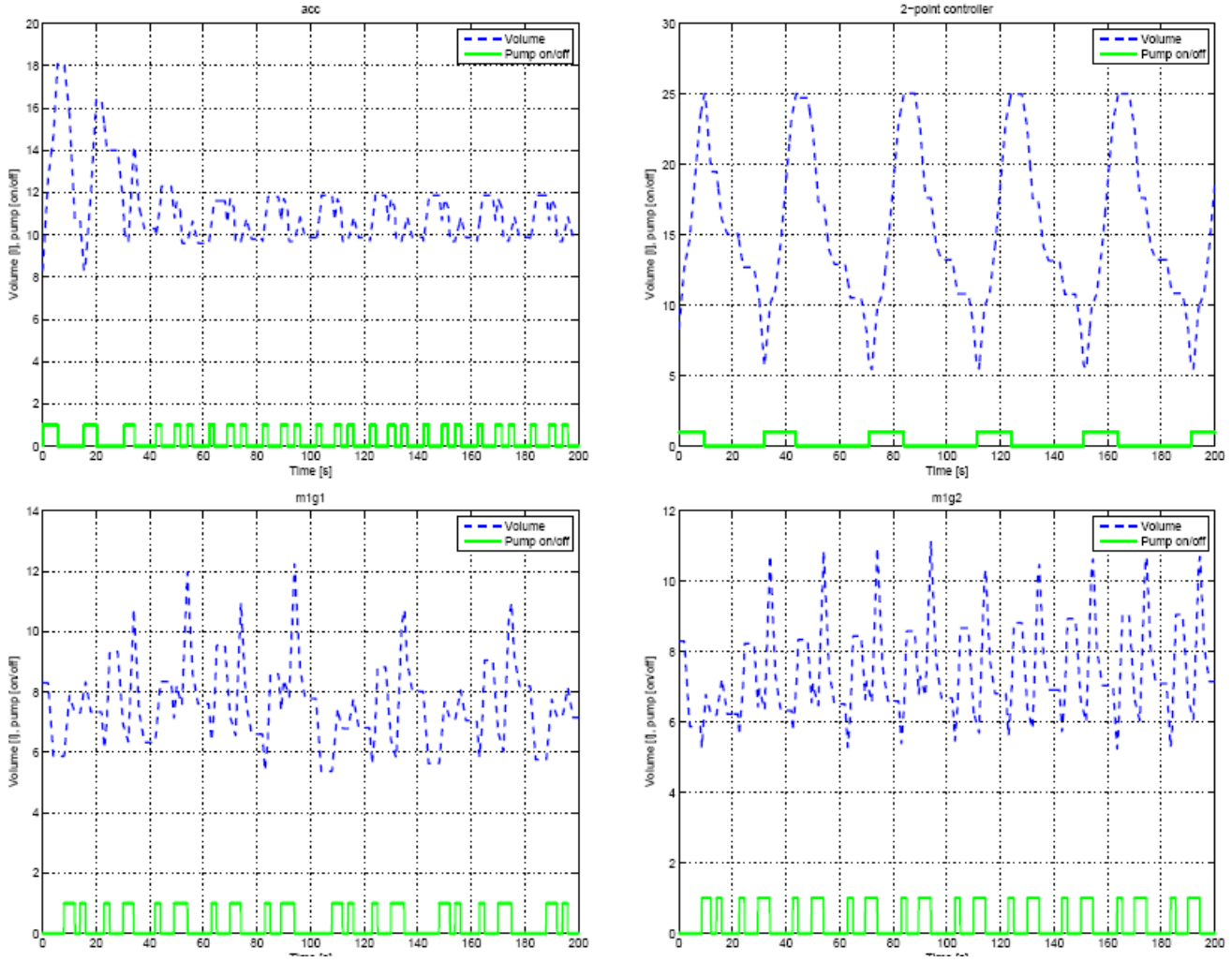




Performance SIMULINK



Results


acc
2−point controller
m1g1
m1g2
Volume
Pump on/off
Volume [l], pump [on/off]
Time [s]

Results

Controller	Acc. volume	Mean volume	Mean volume (TIGA)
Bang-Bang	2689	13.45	
Hy			
G1			
G1			
G1			
G1			
G2			
G2			
G2			
G2M1	1489		

Guaranteed

Correctness

Robustness

with

40% improvement in performance

HSCC09:
Franck Cassez, Jan J Jessen, Kim G. Larsen,
Jean-Francois Raskin, Pierre-Alain Reynier