A Benchmark on Dynamic Reliability An approach based on Generalized Stochastic Petri Nets (GSPN)

Andrea Bobbio
Dipartimento di Informatica, Università del Piemonte Orientale
Spalto Marengo 33, 15100 Alessandria
bobbio@mfn.unipmn.it

Daniele Codetta Raiteri
Dipartimento di Informatica, Università di Torino
Corso Svizzera 185, 10149 Torino
codetta@di.unito.it

1 The case study

The system [1] is composed by a tank containing a fluid, two pumps (P1 and P2) to fill the tank, a valve (V) to remove fluid from the tank and a controller monitoring the fluid level (H); the controller can turn ON or OFF the pumps or the valve if H is too low or too high. P1, P2 and V have the same fluid variation rate ($0.6m/h$) and can be in one of these four states: ON, OFF, stuck ON, stuck OFF. Fig. 1 [1] shows the system scheme: the system is working correctly if $HLA < H < HLB$; initially $H = 0$ with P1 and V in state ON, and P2 in state OFF; the failure of P1, P2 or V causes a variation of H: Tab. 2 indicates how H changes according to the current component states configuration; the controller orders the components to change their state depending on H according to Tab. 1. The failure conditions of the whole system are two: $H < HLV$ (dry out) or $H > HLP$ (overflow).

Boundary	P1	P2	V
$H < HLA$	ON	ON	OFF
$H > HLB$	OFF	OFF	ON

Table 1: Control laws

The failure rates of P1, P2 and V (Tab. 3) are are not dependent on the state (ON or OFF) of these components; the effect of a failure for a component consists of turning it in the state stuck ON, with probability 0.5, or in state stuck OFF, with the same probability (Fig. 2).

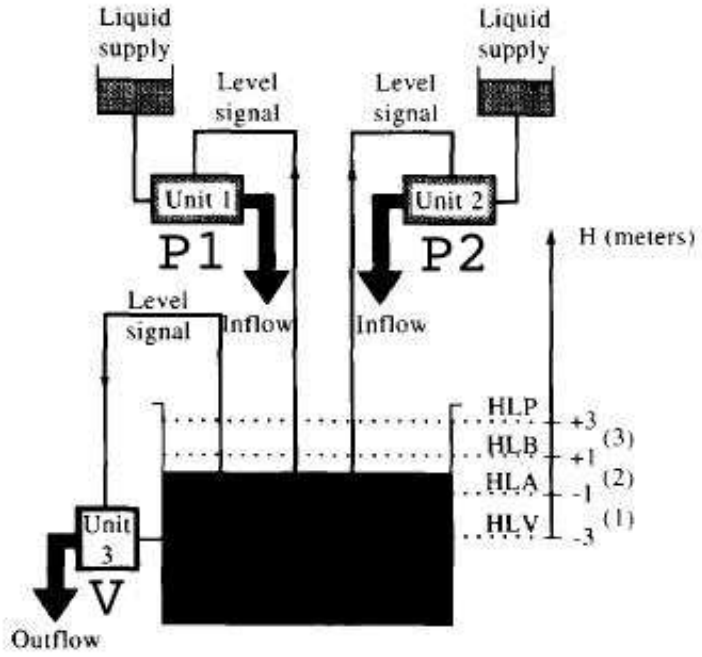


Figure 1: System scheme

P1	P2	V	effect on H
ON	OFF	OFF	$\uparrow$
ON	ON	OFF	$\uparrow\uparrow$
ON	OFF	ON	$=$
ON	ON	ON	$\uparrow$
OFF	OFF	OFF	$=$
OFF	ON	OFF	$\uparrow$
OFF	OFF	ON	$\downarrow$
OFF	ON	ON	$=$

Table 2: H variation for every system configuration

Component	failure rate
P1	0.004566
P2	0.005714
V	0.003125

Table 3: Failure rates

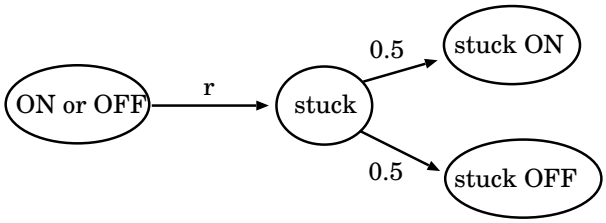


Figure 2: The states of a component; r is its failure rate

1.1 Modelling the system as a GSPN

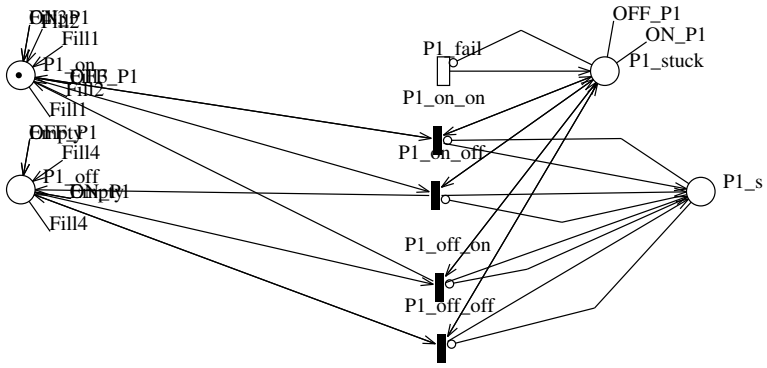
The system has been modeled as a *Generalized Stochastic Petri Net* (GSPN) [2]: we can consider three subnets concerning the component failures (Fig. 3), the controls on the pumps and the valve (Fig. 4), and the fluid level variation with the overflow or dry out conditions (Fig. 5).

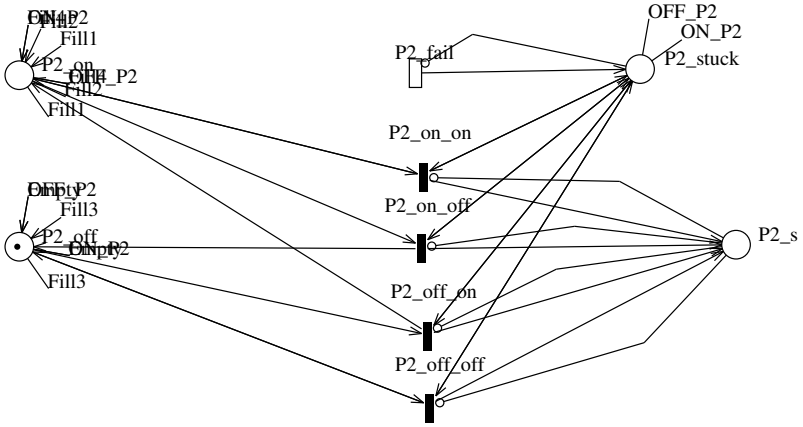
The state of a component, for instance P1, is modelled with the presence of a token in the place named P1_on or in P1_off; if P1 is even stuck, a token will appear in P1_stuck. The failure of a component is modelled as a timed transition (Fig. 3) whose firing rate is equal to the failure rate of the component; the change of the component state to stuck ON or stuck OFF is modelled with four immediate transitions: two of them are enabled if the component failed in ON state, the others are enabled if the component failed in OFF state; their aim is changing the component state to stuck ON or stuck OFF with the same probability, indipendently on the component state before its failure.

The fluid level H is modelled as the place named LEVEL (Fig. 4) whose marking (number of contained tokens) represents H as shown in Tab. 4. The immediate transition start_PUMP is enabled when $H \leq HLA$ (there are less than 4 tokens in LEVEL) and forces the pumps and the valve to change their state (if they are not stuck) according to the first control law in Tab. 1. Analogously, the immediate transitions start_VALVE is enabled when $H \geq HLB$ (there are at least 5 tokens in LEVEL) and forces the components to change their state according to the second control law in Tab. 1.

To model the initial configuration, P1_ON, P2_OFF and V_ON are marked with one token, while LEVEL contains 4 tokens, corresponding to $H = 0$ (Tab. 4).

The subnet in Fig. 5 models the variation of H by changing the number of tokens in LEVEL according to the components state: four timed transition with the same firing rate, equal to the common fluid level variation





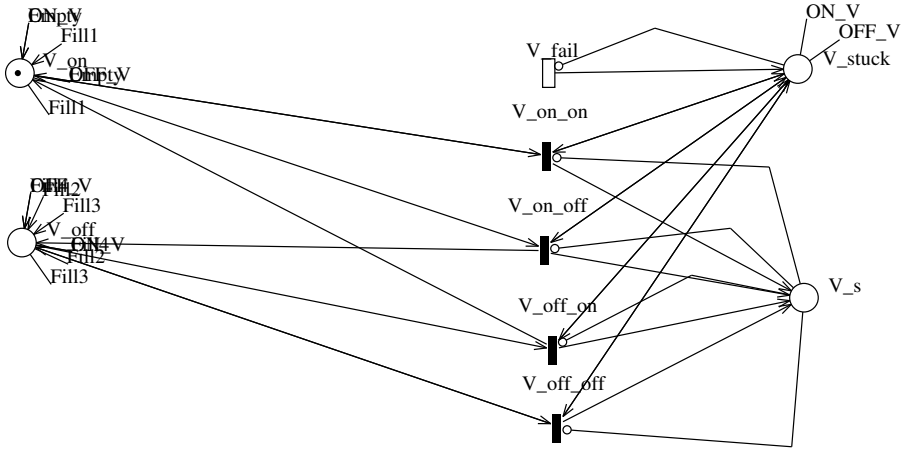


Figure 3: GSPN modelling the component failures

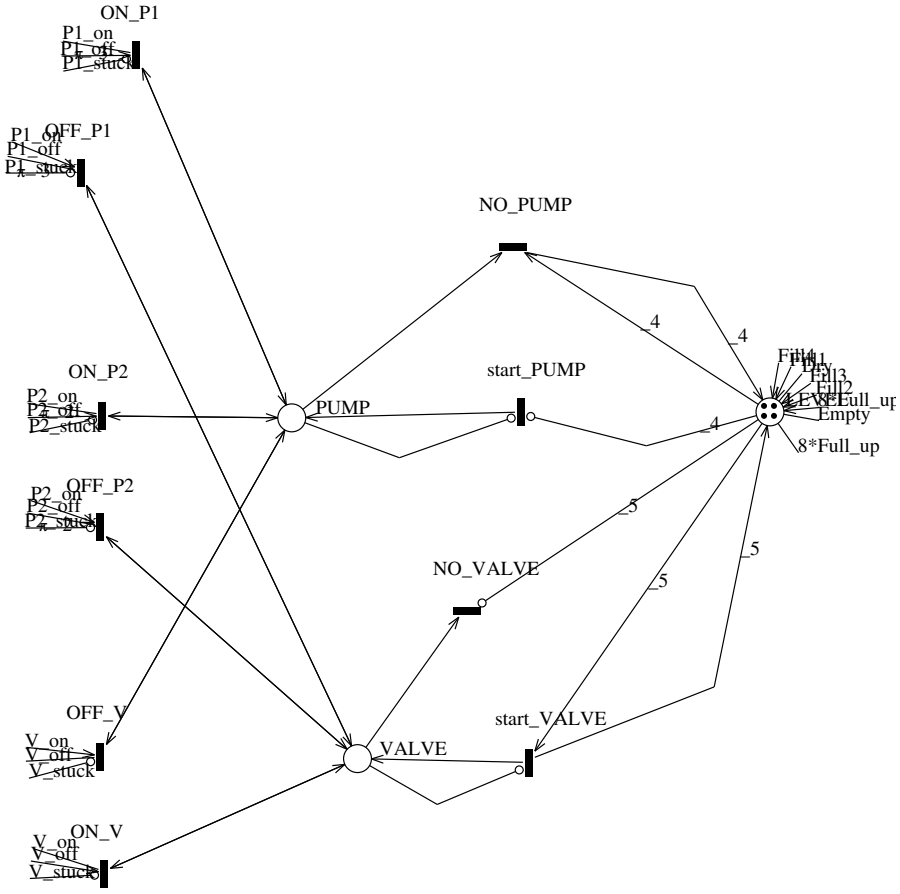


Figure 4: GSPN modelling the controls on the components

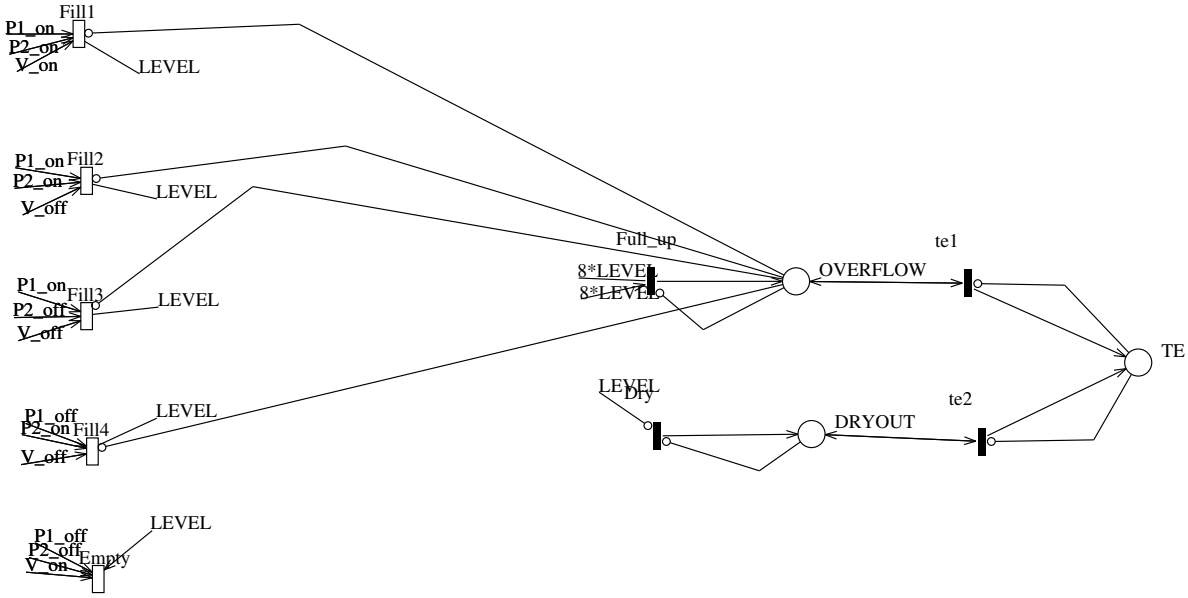


Figure 5: GSPN modelling the fluid level variation and the overflow or dry out of the system

#tokens	H	Region	Condition
8	$> +3$		overflow
7	$+3$	3	HLP
6	$+2$	3	
5	$+1$	3	HLB
4	0	2	correct functioning
3	-1	1	HLA
2	-2	1	
1	-3	1	HLV
0	< -3		dry out

Table 4: Correspondance between the number of tokens in LEVEL and H

rate, model the increase of H in the four configurations of component states determining such variation (Tab. 2); in the case where both pumps are ON and the valve is OFF, the output arc of the corresponding transition has a double multiplicity to represent a faster increase of H. There is a unique timed transition to model the decrease of H since there is only one configuration of the component states determining such variation, when both pumps are OFF and the valve is ON (Tab. 2). This subnet contains two immediate transitions to detect the failure of the whole system: the dry out condition is verified when LEVEL is empty, while the overflow happens when LEVEL contains 8 tokens (Tab. 4).

1.2 Preliminary results

We have calculated on the GSPN the dry out and overflow cumulative distribution function (*cdf*) in the analytical way as the probability of the presence of a token in the places DRYOUT and OVERFLOW respectively, at the mission time; the model has been drawn and analyzed by means of the *GreatSPN* tool [3]. The results calculated for a mission time varying from 0 to 1000, are numerically reported in Tab. 5, and graphically in Fig. 6 and Fig. 7.

hours	dry out	overflow
100	0.004557	0.075193
200	0.022258	0.196118
300	0.045038	0.292837
400	0.065992	0.360354
500	0.082696	0.405700
600	0.095110	0.435912
700	0.104009	0.456106
800	0.110277	0.469702
900	0.114659	0.478933
1000	0.117715	0.485253

Table 5: dry out and overflow cdf

2 System variations and their modelling

This section is about some of the variations to the system proposed in [1] and their reliability analysis; every variation proposed in the following subsections must be related to the initial case, explained in the previous section.

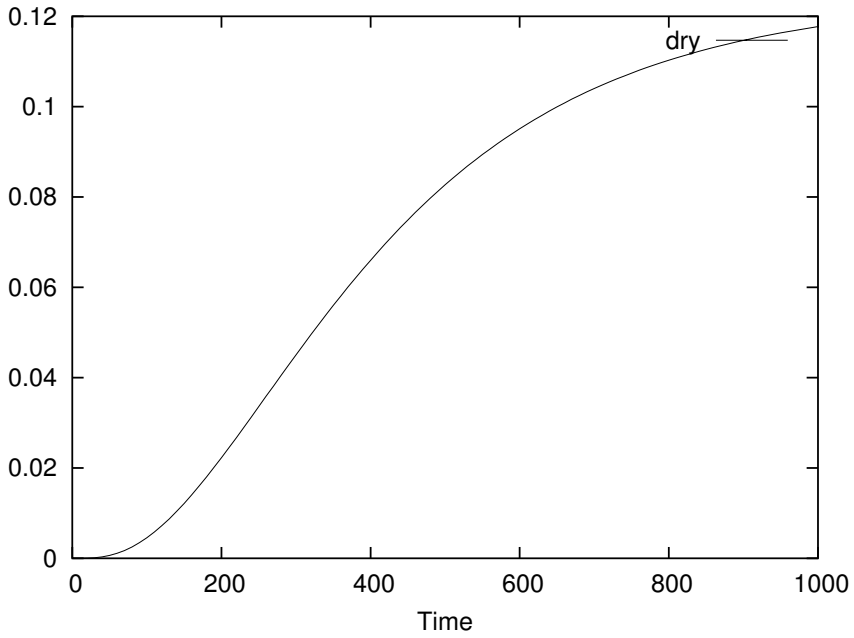


Figure 6: dry out cdf in the initial case

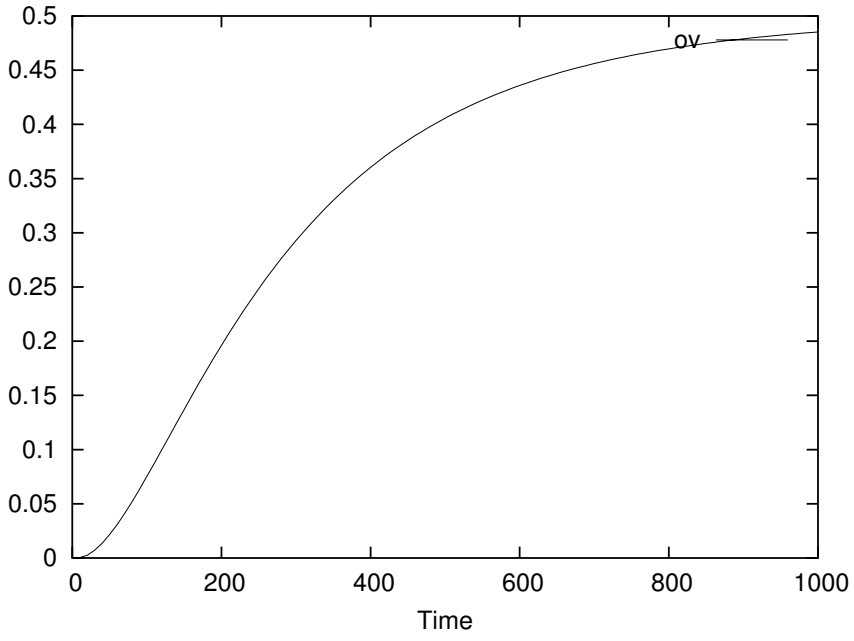


Figure 7: overflow cdf in the initial case

2.1 Different failure rates for the ON and OFF states

In this version of the system, the components have several failure rates, depending on the current state and the possible state transitions; such situation is shown in Tab. 6 providing the failure rates for each component in each state.

Component	from	to	failure rate
P1	ON	stuck (ON or OFF)	0.004566
P1	OFF	stuck ON	0.045662
P1	OFF	stuck OFF	0.456621
P2	ON	stuck ON	0.057142
P2	ON	stuck OFF	0.571429
P2	OFF	stuck (ON or OFF)	0.005714
V	ON	stuck (ON or OFF)	0.003125
V	OFF	stuck ON	0.031250
V	OFF	stuck OFF	0.312500

Table 6: Failure rates for each component in each state

For P1 in state ON, P2 in state OFF and V in state ON, the state transition respects the scheme in Fig. 2; for P2 in state ON, the situation is shown in Fig. 8.a, for P1 in state OFF and V in state OFF, in Fig. 8.b.

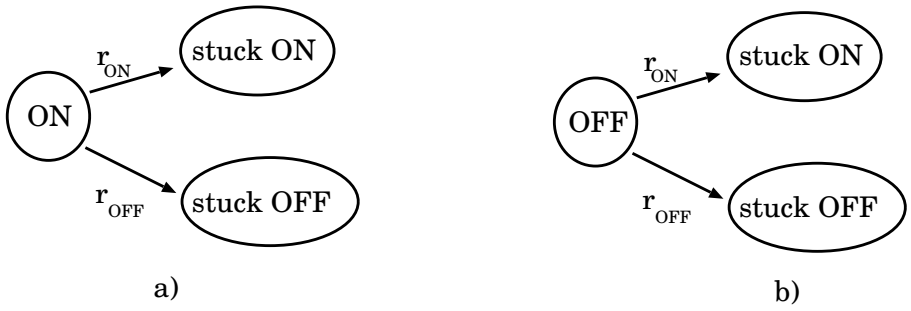


Figure 8: The states of a component; r_{ON} and r_{OFF} are its failure rates

In order to model this version of the system as a GSPN, we have only to replace the subnet related to the component failures, with a new one considering such situation (Fig. 9): for the cases respecting Fig. 8, two new timed transitions have been added for each component to represent the change of the failure rate when changing the component state, while the rest of the model has not been modified.

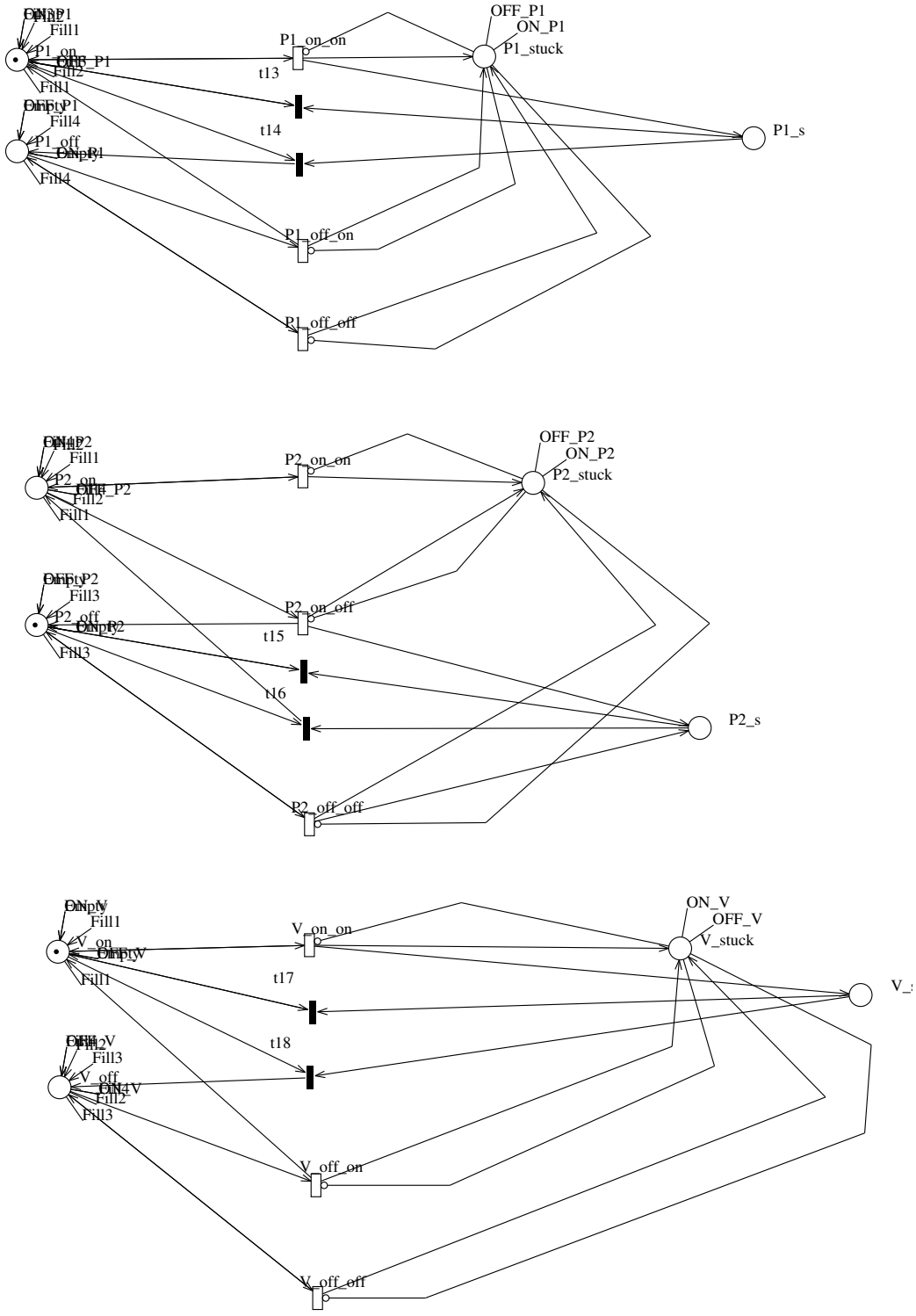


Figure 9: GSPN modelling the component failures with different failure rates

As for the initial version of the system, we calculated the dry out and overflow *cdf*; the results are reported in Tab. 7, in Fig. 10 and in Fig. 11.

hours	dry out	overflow
100	0.011260	0.107120
200	0.024957	0.208382
300	0.036410	0.279633
400	0.044960	0.327547
500	0.050977	0.359611
600	0.055065	0.381254
700	0.057782	0.396045
800	0.059562	0.406277
900	0.060717	0.413434
1000	0.061461	0.418485

Table 7: dry out and overflow cdf when failure rates depending on the component state

2.2 The components may not respond to controller orders

In this version of the system, a component may not respond to the controller orders; in other words, a component modifies its state obeying to the controller order with a 0.9 probability. This situation has been modeled as the controller could fail and be repaired; we added to the GSPN of the initial case, a small subnet (Fig. 12) composed by two timed transitions representing the failure and repair events of the controller while the place C_dn indicates the controller state; the firing rates of the transitions has been set in order to cause the working state of the controller in about the 90% of the mission time, and the failed state in about the 10% (the failure rate of the controller is 0.111111, the repair rate is 1.0). When the controller is down, the immediate transitions start_PUMP and start_VALVE are disabled even if H would allow their firing.

We calculated the dry out and overflow *cdf* in the analytical way; the results are reported in Tab. 8, in Fig. 13 and in Fig. 14.

2.3 The components are repairable

In this version, the pumps and the valve are repairable if failed; the controller detects the failures by observing the fluid level: if H is in region 1 or 3,

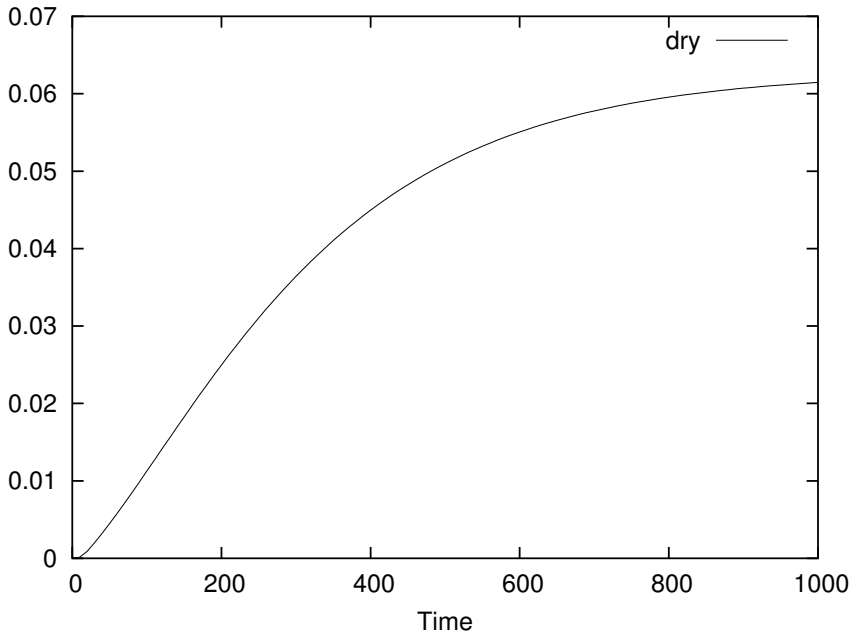


Figure 10: dry out cdf when failure rates depending on the component state

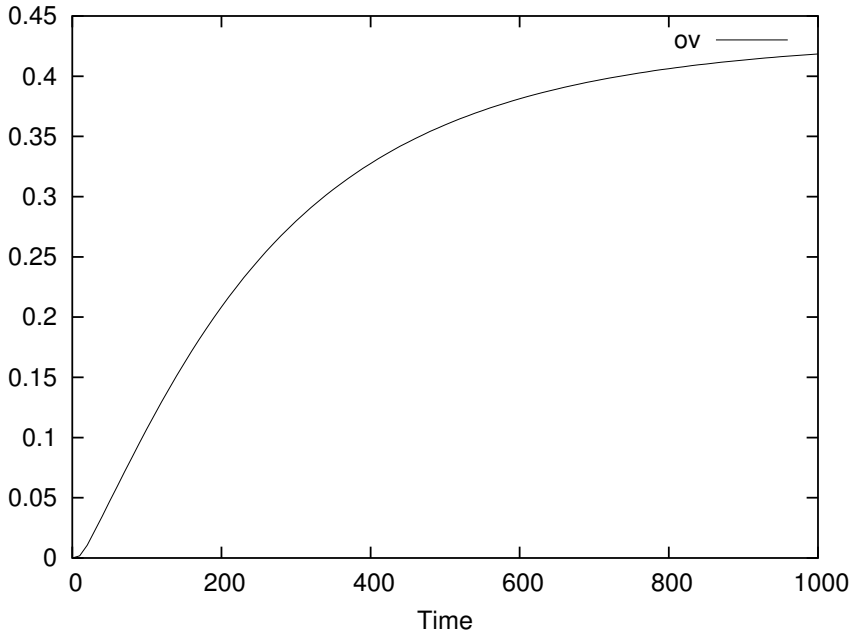


Figure 11: overflow cdf when failure rates depending on the component state

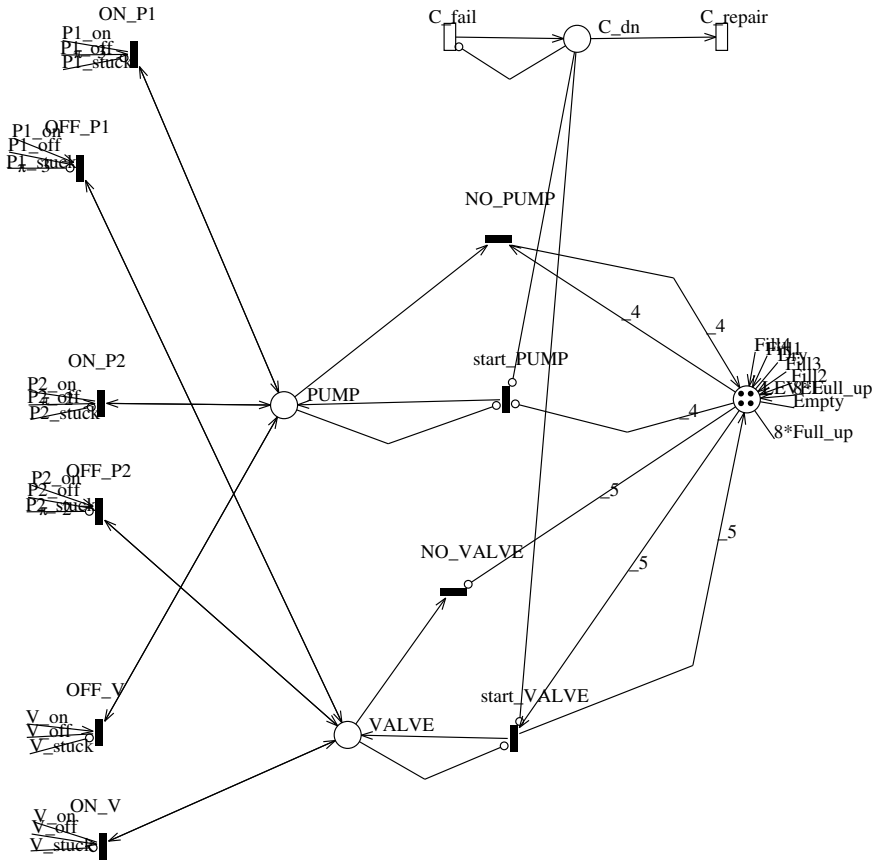


Figure 12: GSPN modelling the controls on the components where the components may not respond to the controller orders

hours	dry out	overflow
100	0.008539	0.080414
200	0.030281	0.205360
300	0.054889	0.303744
400	0.076327	0.371612
500	0.092949	0.416775
600	0.105112	0.446663
700	0.113755	0.466543
800	0.119809	0.479884
900	0.124026	0.488922
1000	0.126962	0.495102

Table 8: dry out and overflow cdf when the components may not respond to the controller orders

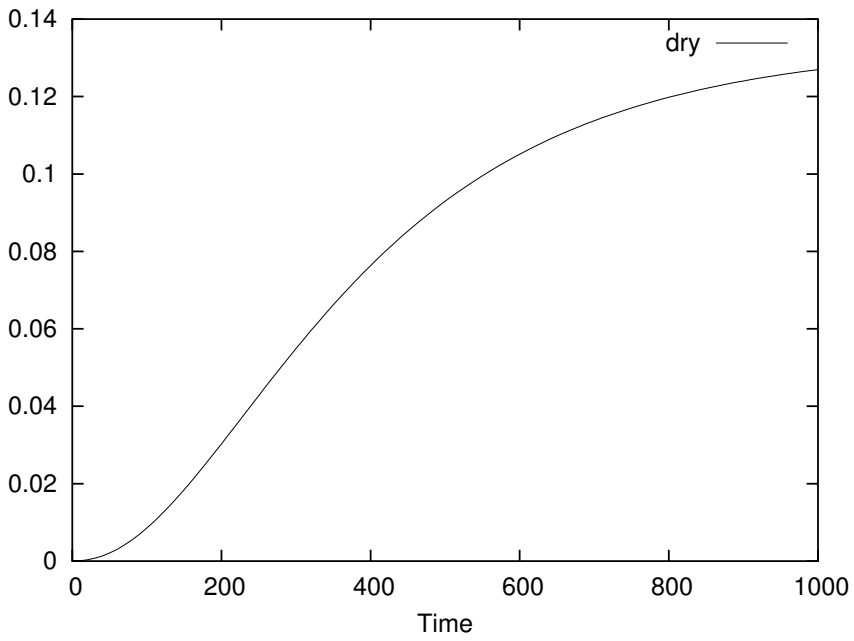


Figure 13: dry out cdf when the components may not respond to the controller orders

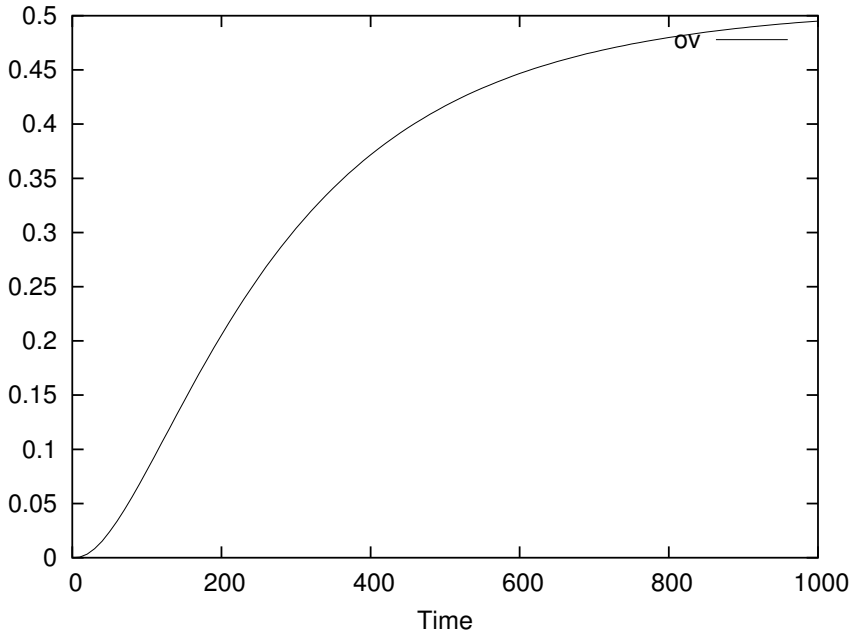


Figure 14: overflow cdf when the components may not respond to the controller orders

there must be a failure; so, only when H is in such regions the repair can be performed. All the components have the same repair rate (0.2) and we assume that the repair of each component is performed indipendently from the repair of the others; in other words, the repair of a component may begin or end at a different time from the others.

In this case, the thresholds for the overflow and the dry out have been changed; Tab. 9 shows the correspondance between the number of tokens in LEVEL and the new tresholds. The GSPN has been modified in this way (Fig. 15 and Fig. 16): the new thresholds have been considered; the immediate transition start_PUMP is enabled when $H < HLA$ (there are less than 5 tokens in LEVEL), while start_VALVE is enabled when $H > HLB$ (there are at least 8 tokens in LEVEL); a new timed transition whose firing rate is equal to the repair rate, has been added for each component in order to remove the token from the place representing its stuck condition; such transitions are all enabled when H is in a dangerous region (1 or 3); this is modeled with the place named DANGER.

The results of the analytical solution, for a mission time varying from 1 to 500 hours, are reported in Tab. 10, in Fig. 17 and in Fig. 18.

#tokens	H	Region	Condition
12	$> +5$		overflow
11	$+5$	3	HLP
10	$+4$	3	
9	$+3$	3	
8	$+2$	3	
7	$+1$	2	HLB
6	0	2	initial condition
5	-1	2	HLA
4	-2	1	
3	-3	1	
2	-4	1	
1	-5	1	HLV
0	< -5		dry out

Table 9: Correspondance between the number of tokens in LEVEL and H

hours	dry out	overflow
50	0.000023	0.001702
100	0.000142	0.005554
150	0.000363	0.010670
200	0.000655	0.016609
250	0.000987	0.023066
300	0.001332	0.029828
350	0.001673	0.036741
400	0.001998	0.043695
450	0.002303	0.050611
500	0.002584	0.057431

Table 10: dry out and overflow cdf when components are repairable

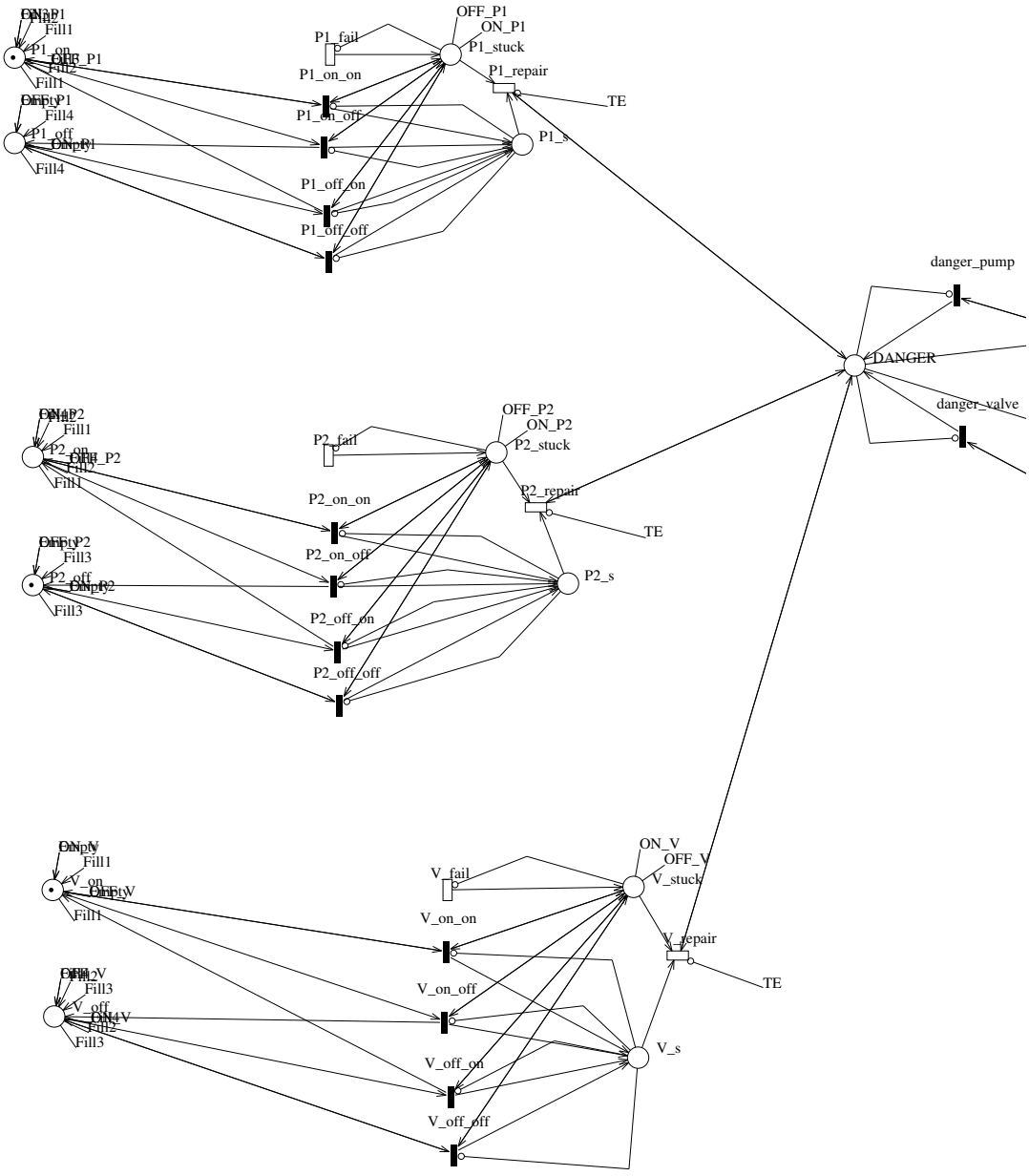


Figure 15: GSPN modelling the failure and the repair of the components

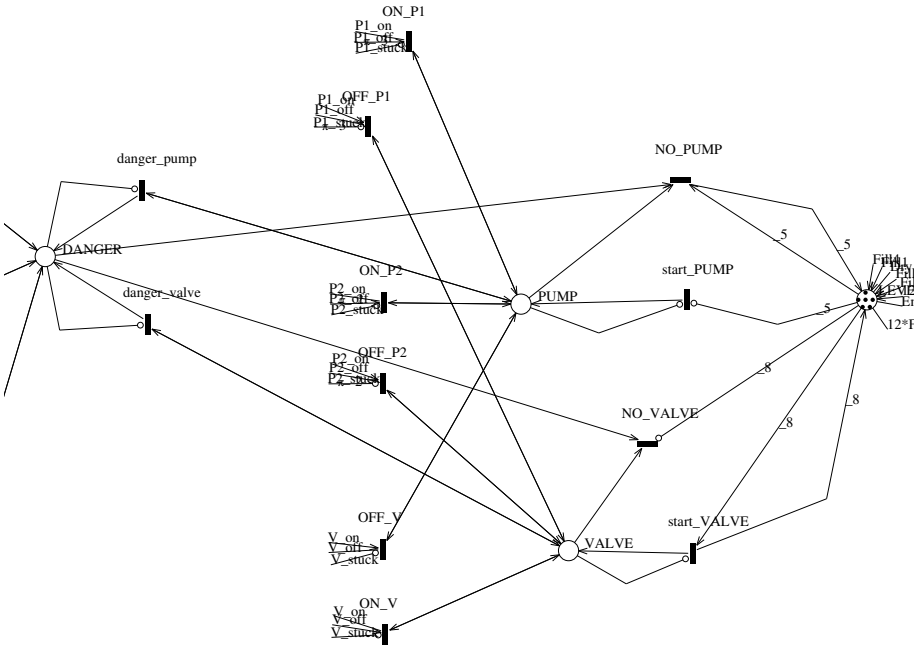


Figure 16: GSPN modelling the controls on the components when they are repairable

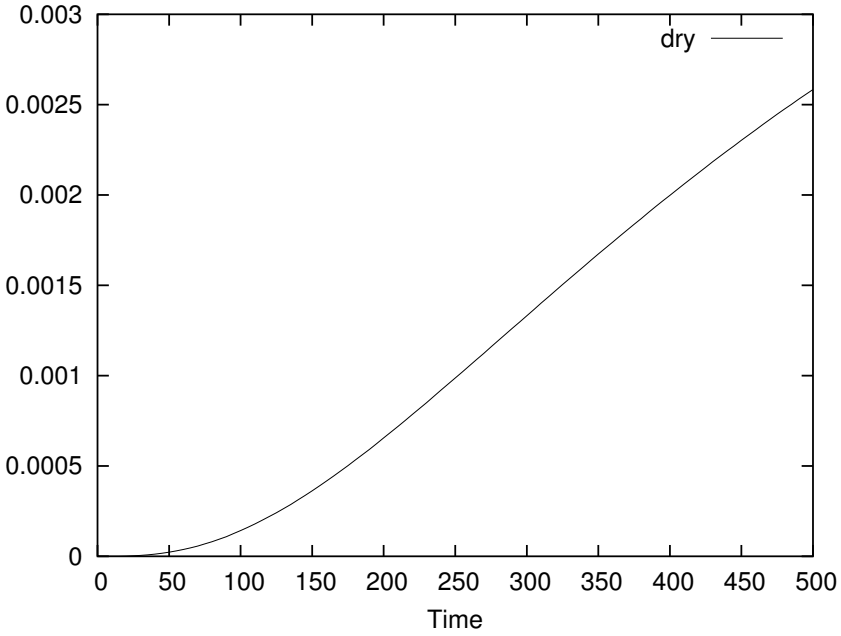


Figure 17: dry out cdf when components are repairable

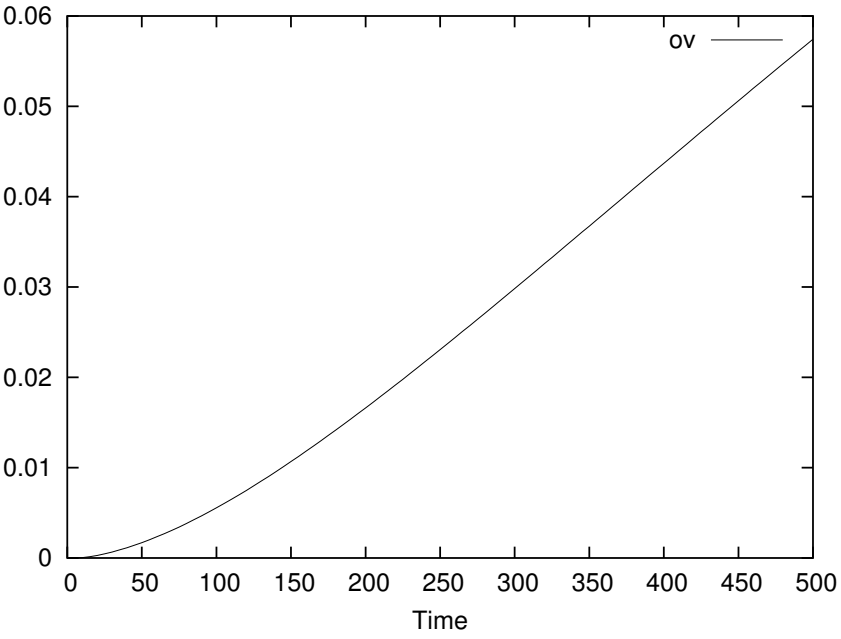


Figure 18: overflow cdf when components are repairable

3 Conclusions and future works

In the initial case and in the first two variations, we obtained results for the *cdf* that are similar to those reported in [1]; in the case with repairable components, we obtained different results, especially for the dry out condition.

The other cases proposed in [1] has not been yet faced; future works on this benchmark will consider the use of *Fluid Stochastic Petri Nets* (FSPN) [4][5] instead of GSPN; this would lead to more precise results in the reliability analysis considering that in FSPN, fluid places can be present; instead of tokens, a fluid place contains some fluid whose level is a continuous variable; this is useful to represent more precisely the continous measures such as the fluid level in the tank or the temperature of the fluid.

References

[1] M. Marseguerra and E. Zio. Monte Carlo Approach to PSA for dynamic process system. *Reliability Engineering and Safety System*, 52:227–241, 1996.

[2] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis. *Modelling with Generalized Stochastic Petri Nets.* Wiley Series in Parallel Computing, 1995.

[3] G. Chiola, G. Franceschinis, R. Gaeta, and M. Ribaudo. GreatSPN 1.7: Graphical Editor and Analyzer for Timed and Stochastic Petri Nets. *Performance Evaluation*, 24:47–68, November 1995.

[4] A. Bobbio M. Gribaudo and M. Sereno. Modeling physical quantities in industrial systems using fluid stochastic petri nets. In *Proceedings 5-th International Workshop on Performability Modeling of Computer and Communication Systems (PMCCS5)*, pages 81–85, September 2001.

[5] M. Gribaudo, M. Sereno, A. Horvath, and A. Bobbio. Fluid stochastic petri nets augmented with flush-out arcs: Modelling and analysis. *Discrete Event Dynamic Systems*, 11(1/2):97–117, 2001.