MODELLING DYNAMIC RELIABILITY VIA FLUID PETRI NETS

DANIELE CODETTA-RAITERI,

Dipartimento di Informatica, Università di Torino Italy

ANDREA BOBBIO

Dipartimento di Informatica, Università del Piemonte, Orientale, Italy

Combinatorial models for reliability analysis (like fault-trees or block diagram) are static models that cannot include any type of component dependence. In the CTMC (*Continuous Time Markov Chain*) framework, the transition rates can depend on the state of the system thus allowing the analyst to include some dependencies among components. However, in more general terms, the system reliability may depend on parameters or quantities that vary continuously in time (like temperature, pressure, distance, etc.). Systems whose behavior in time can be described by discrete as well as continuous variables, are called hybrid systems. In the dependability literature, the case in which the reliability characteristics vary continuously versus a process parameter, is sometimes referred to as *dynamic reliability* [1]. The modelling and analysis of hybrid dynamic systems is an open research area. The present paper discusses the evaluation of a benchmark on dynamic reliability proposed in [1] via a modelling framework called *Fluid Stochastic Petri Net* (FSPN).

Key Words: Dynamic Reliability, Fluid Stochastic Petri Nets.

1. INTRODUCTION

Combinatorial models for reliability modelling and evaluation (like fault-trees or block diagram) are static models that cannot include any type of statistical dependence among components. In the CTMC (*Continuous Time Markov Chain*) framework, the random variables (failure and repair times) are exponentially distributed and have a time independent failure rate. However, the failure rates can depend on the state of the system, thus allowing the analyst to model the dependence of one component on the up or down state of the others. In more general terms, the system reliability may depend on some parameter or quantity that vary continuously in time (like temperature, pressure, distance, etc.). Systems whose behavior in time can be described by discrete as well as continuous variables are called *hybrid* systems [2]. In the dependability literature, the case in which the reliability characteristics vary continuously versus a process parameter is sometimes referred to as *dynamic reliability* [1]. The modelling and analysis of hybrid dynamic systems is an open and challenging research area. The present paper discusses the evaluation of a benchmark on dynamic reliability proposed in [1] via a modelling framework called *Fluid Stochastic Petri Net* (FSPN) [3] [4].

FSPNs are an extension of GSPNs (Generalized Stochastic Petri Nets) since they contain new primitives: fluid places, that contain a continuous level of fluid (instead of a discrete number of tokens), and fluid arcs with the aim of increasing or decreasing the fluid level inside fluid places. FSPNs extend the modelling power and flexibility of GSPNs, and are a useful modelling framework for hybrid systems [3] [5] [6].

Based on the example discussed in [1], a benchmark was proposed (Section 2) consisting of a hybrid dynamic system composed by a tank containing some liquid whose level is influenced by a controller acting on two pumps and one valve with the aim of avoiding the dry out or the overflow condition of the liquid. The controller influences the system configuration by switching on or off the pumps or the valve according to the current liquid level. Several versions of this system have been proposed and evaluated by means of Monte Carlo simulation in [1].In this paper, we concentrate on two hybrid situations:

1. The value of the failure rates of the pumps and of the valve, depends on the current state (ON or OFF) of these components. The level of the liquid in the tank varies continuously, and the unreliable condition is related to the attainment of an upper (overflow) or a lower (dry-out) boundary.
2. A heat source is present to warm the liquid in the tank, and the component failure rates depend on the liquid temperature that vary continuously as a balance of the heat source and of the fresh water pumped into the tank; besides the liquid overflow and dry-out, the system failure occurs also if the liquid temperature reaches a certain boundary.

In Section 4, we model the attainment of an unsafe liquid level (case I) by using a conventional GSPN [7] and discretizing the level in the tank. The GSPN model is solved analytically. Then, we show how the system reliability can be modelled resorting to FSPN and comparing the simulative results with the GSPN case (Section 4.3). The effect of the temperature variation on the failure rates (case II) is considered in Section 5. Due to the presence of discrete and continuous variables, we model the dynamic behavior of the system by means of a FSPN [4]; the simulation of the FSPN model provides the system unreliability for each failure condition versus the mission times (Section 5.2).

2. THE CASE STUDY

The system [1] is composed by a tank containing some liquid, two pumps (P1 and P2) to fill the tank, one valve (V) to remove liquid from the tank, and a controller (C) monitoring the fluid level (L) and turning on or off the pumps or the valve, if L is too low or too high. P1, P2 and V have the same flow rate Q, measured as a linear variation of the liquid level (m/h), and can be in one of these four states: ON, OFF, stuck ON, stuck OFF. Fig. 1 shows the system scheme: the system is working correctly if L is inside the region of correct functioning (6 m < L < 8 m).

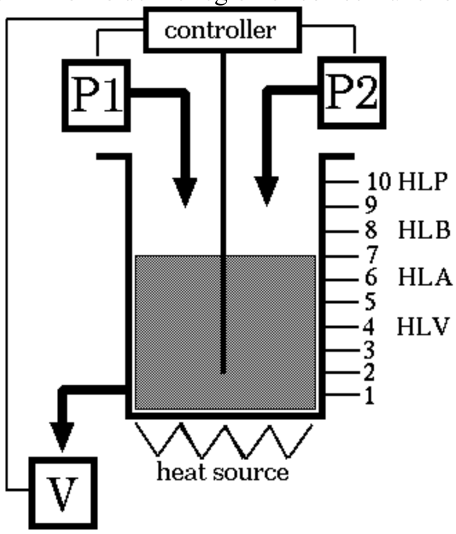

Fig. 1: System scheme

Initially L = 7 m, with P1 and V in state ON, and P2 in state OFF; in this situation, the liquid is renewed, but L does not change. The failure of P1, P2 or V consists of a state transition towards the state stuck ON or stuck OFF (see Fig. 2), and causes a variation of L. Table 1 indicates how L changes according to the current state of the components.

The controller orders the components to change their state if L is not inside the region of correct functioning, according to the control rules in Tab. 2, with the purpose of avoiding two failure conditions of the system: the liquid dry out (L ≤ 4 m) or overflow (L ≥ 10 m). If a component is stuck (ON or OFF), it does not respond to the controller orders, so it maintains its state.

Table 1: Variation of L for every system configuration.

P1	P2	V	effect on L	variation rate
ON	OFF	OFF	↑	Q
ON	ON	OFF	↑↑	2 Q
ON	OFF	ON	=	
ON	ON	ON	↑	Q
OFF	OFF	OFF	=	
OFF	ON	OFF	↑	Q
OFF	OFF	ON	↓	Q
OFF	ON	ON	=	

Table 2: Control boundaries and laws

Boundary	P1	P2	V
L ≤ 6 m	ON	ON	OFF
L ≥ 8 m	OFF	OFF	ON

3. GSPN vs FSPN

GSPNs are an extension of Petri nets including timed transitions whose firing delay is a random variable. Their composing elements are places, timed transitions, immediate transitions, directed arcs and inhibitor arcs. Places (graphically denoted by circles) can contain a discrete number of tokens; immediate transitions (black rectangles) fire as soon as they are enabled, while timed transitions (white rectangles) fire after a random period of time which is ruled by a negative exponential distribution. Directed arcs are used to move tokens when a transition fires, while inhibitor arcs (ending with a small circle) can connect a place to a transition in order to disable the transition if the place is not empty.

FSPNs are a new extension of Petri nets including the same elements of GSPNs with the addition of fluid places and fluid arcs; fluid places are represented as double circles, contain a continuous fluid level, and are suitable to represent continuous variables such as the temperature and the pressure. A fluid place can be connected to a timed transition by means of a fluid arc (with the shape of a pipe); while the timed transition is enabled to fire, some fluid is moved through the fluid arc, from or to the fluid place with respect to the flow rate associated with the fluid arc. Moreover, the firing of a timed transition may depend on the fluid level inside a fluid place: the Dirac delta function is used to make a transition fire when the fluid level reaches a certain value. The Dirac delta function returns 0 if its argument differs from 0, while it returns $+\infty$ if its argument is equal to 0. So, if we want a transition T to fire as soon as the fluid inside the place P reaches the level x, we have to set the firing rate of T to Dirac(P-x).

4. UNRELIABILITY VERSUS LEVEL

In this version of the system (case I), the failure rate of a component (P1, P2, V) depends on its current state. The level variation rate of P1, P2 and V is Q = 0.6 m/h. The whole system fails in two conditions: the liquid overflow and the liquid dry-out. Tab. 3 shows the failure rates for every component and for every state transition due to the component failure.

In conventional discrete-state models the (un)reliability is evaluated as the probability of being in some unsafe state. In this case, we account for an hybrid reliability condition, caused by a continuous variable (the liquid level) to hit an unsafe barrier.

The use of a discrete model such as GSPN, to represent the system, requires the discretization of the continuous variables; in this case, the liquid level has been discretized considering eight intermediate levels. The use of FSPN instead, allows to deal directly with continuous variables.

Table 3: Failure rates for every state of a component.

Component	from state	to state	failure rate
P1	ON	stuck ON	0.002283 1/h
P1	ON	stuck OFF	0.002283 1/h
P1	OFF	stuck ON	0.045662 1/h
P1	OFF	stuck OFF	0.456621 1/h
P2	ON	stuck ON	0.057142 1/h
P2	ON	stuck OFF	0.571429 1/h
P2	OFF	stuck ON	0.002857 1/h
P2	OFF	stuck OFF	0.002857 1/h
V	ON	stuck ON	0.001562 1/h
V	ON	stuck OFF	0.001562 1/h
V	OFF	stuck ON	0.031250 1/h
V	OFF	stuck OFF	0.312500 1/h

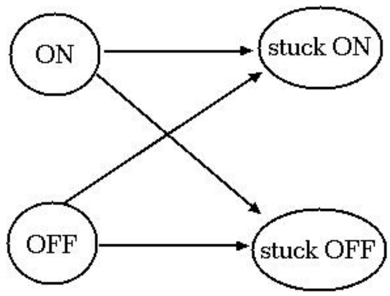

Fig. 2: State transitions of a component due to a failure.

4.1. GSPN model of the system

The system has been modelled as a GSPN (Fig. 3) with the purpose of performing the reliability evaluation of the system with an analytical approach. The state of a component, for instance P1, is modelled by three places: P1on, P1off and P1stuck; when P1on contains one token, P1 is ON; when P1off contains one token, P1 is OFF; if P1stuck contains one token, P1 is stuck.

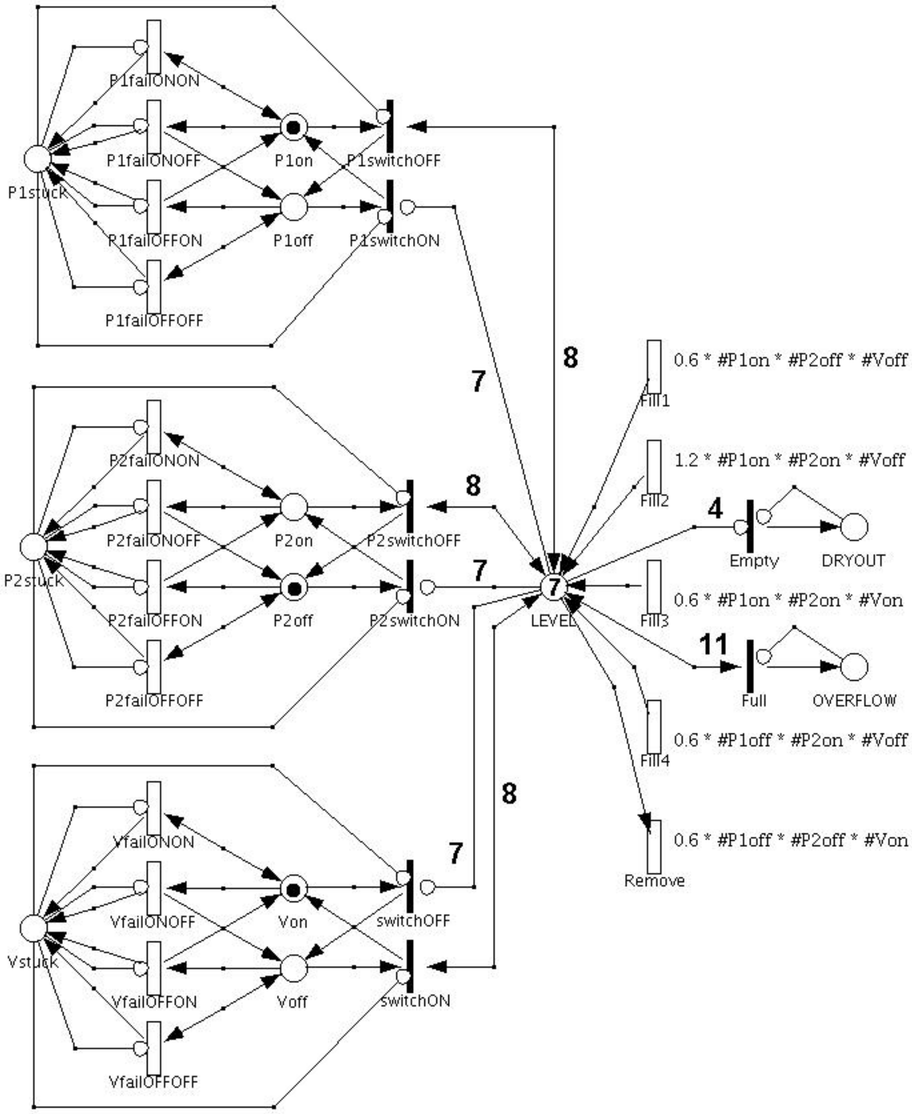

Fig. 3: GSPN model of the system.

The component state variations due to a failure, are modelled by four timed transitions: P1failONON, P1failONOFF, P1failOFFON and P1failOFFOFF. For instance, P1failONOFF models the transition from the state ON to the state stuck OFF by moving the token from P1on to P1off and putting one token in P1stuck. The firing rate of the timed transition P1failONOFF is the failure rate of P1 for the state transition from ON to stuck OFF (Table 3). The failure of P2 and V is modelled in the same way.

Table 4: Correspondence between the number of tokens in the place LEVEL and the liquid level L.

#tokens	Tank Level (L)	Condition
11	> 10 m	overflow
10	10 m	
9	9 m	
8	8 m	control boundary
7	7 m	correct functioning
6	6 m	control boundary
5	5 m	
4	4 m	
3	< 4 m	dry-out

The liquid level has been discretized: eight intermediate levels have been modelled by a set of tokens inside the place named LEVEL; Tab. 4 shows the correspondence between the number of tokens in the place LEVEL and the level of the fluid in the tank. The liquid level variations are modelled by five timed transitions: Fill1, Fill2, Fill3, Fill4, Remove; they correspond to the four state configurations leading to the fluid level increase, and to the unique state configuration leading to the fluid level decrease (Tab. 1). The firing rate of these transitions differs from 0 while the relative state configuration holds; in this period, the firing rate is equal to the level variation rate of the relative state configuration. The effect of their firing is the addition (or the removal) of one token in LEVEL; in this way, we model the increase (or the decrease) of L.

In the initial marking of the GSPN, P1on, P2off and Von are marked with one token, while LEVEL contains 7 tokens, corresponding to the correct functioning level (Tab. 4); all the other places are empty.

The controller action on the component state with respect to L, is modelled by two immediate transitions for each component, connected to the place LEVEL. In the case of P1, we have P1switchON and P1switchOFF; the first one fires when LEVEL contains less than seven tokens, i. e. $L \leq 6$ m (see Tab. 4), with the effect of moving the token from P1off to P1on if P1 is currently OFF. Similarly, P1switchOFF fires when LEVEL contains at least eight tokens ($L \geq 8$ m), and moves the token from P1on to P1off if P1 is currently ON. Both transitions are disabled if P1stuck is marked.

The dry-out and the overflow conditions are detected by two specific immediate transitions: Empty and Full, respectively; the first one fires when LEVEL contains less than four tokens ($L < 4$ m), and puts one token inside the place DRYOUT meaning that the dry out has occurred; the second one fires when LEVEL contains 11 tokens ($L > 10$ m), and puts one token inside OVERFLOW, meaning that the overflow has occurred.

4.2. FSPN model of the system

In order to verify the correctness of the results obtained through the fluid level discretization in the GSPN model, we have built the FSPN model relative to the same system, in Fig. 4.

The fluid level in the tank is represented by the fluid place L. The three fluid arcs connected to L, model the action of the two pumps and of the valve on L. If we consider for instance pump P1, the fluid variation rate of the relative fluid arc is $0.6 \cdot \#P1on$, where #P1on is the number of tokens inside the place P1on; in other words, some fluid is moved to L only while P1 is ON.

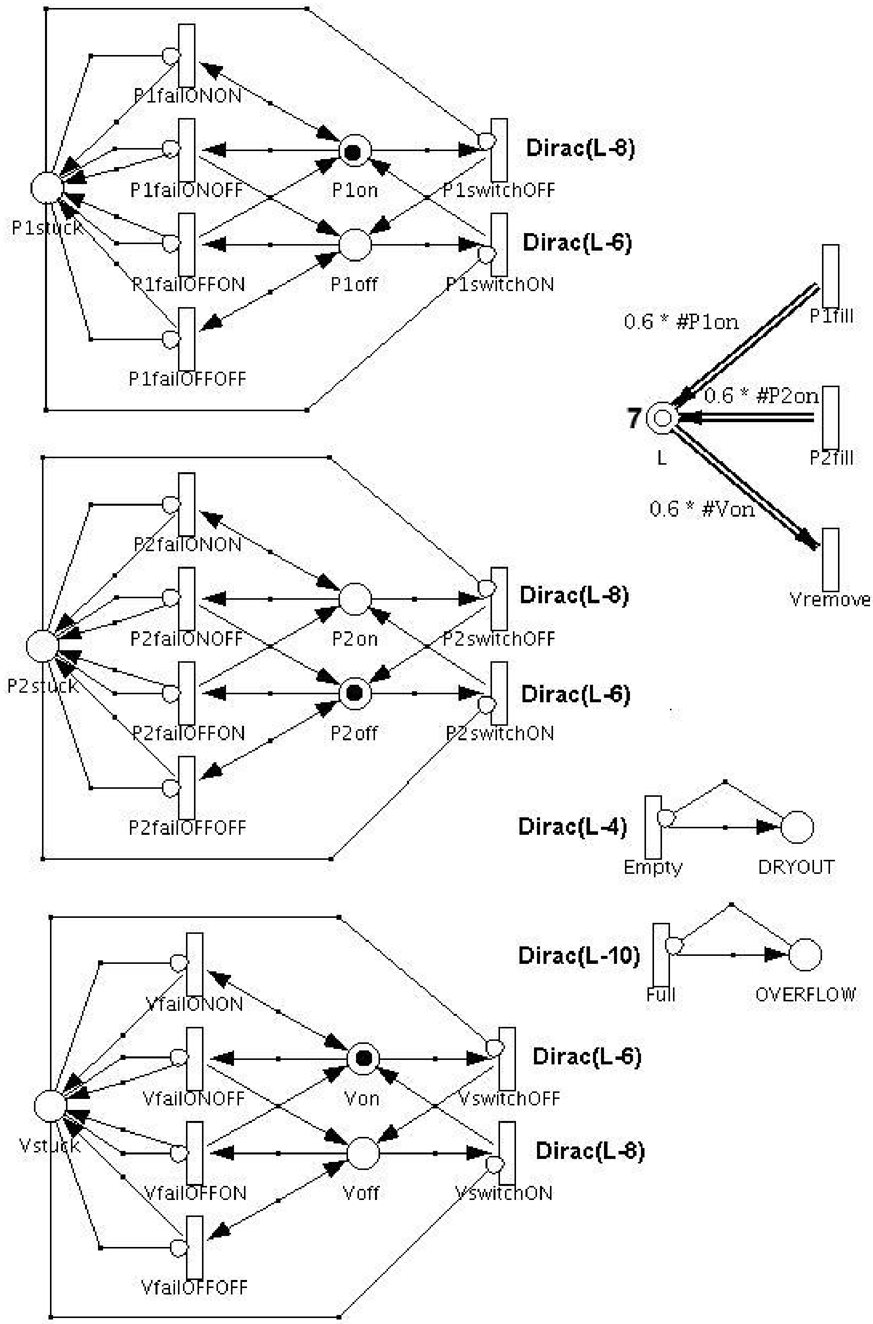

Fig. 4: FSPN model of the system.

The current state and the failure of a component are modelled in the same way as in the GSPN; the controller action on the components is now modelled by two timed transitions for each component. In the case of P1, they are P1switchON and P1switchOFF; the first one must fire when L reaches 6 m, so its firing rate is the function Dirac(L-6), and it switches P1 to ON if P1 is currently OFF. The second transition must fire when L reaches 8 m, so its firing rate is Dirac(L-8) and it switches P1 to OFF if P1 is currently ON. Both transitions are disabled if P1 is stuck.

Two timed transitions named Empty and Full, detect the dry out and the overflow condition respectively; the transition Empty must fire when L reaches 4 m, so the firing rate of this transition is Dirac(L-4). The transition Full must fire when L reaches 10 m, so its firing rate is Dirac(L-10).

4.3. Comparison of results

In order to evaluate the reliability of the system, we calculated the dry out and the overflow *cumulative distribution function* (cdf) on both the GSPN and the FSPN model; this means computing the probability that the system is in such conditions, as a function of the time. The cdf has been computed as the probability of the presence of one token in the place DRYOUT and in the place OVERFLOW respectively, as a function of the time. Since these places can contain zero or one token, the mean number of tokens inside each of these places, will be a value inside the continuous range (0,1).

The GSPN model has been drawn and analyzed by means of the GreatSPN tool [8]; the analytical results obtained in this way, are validated by comparison with the results returned by the FSPN simulation which is executed by means of the FSPNedit tool [9].

The cdf is computed for a mission time varying from 0 to 1000 hours. The results obtained on both the GSPN and the FSPN models are reported in Tab.5 (dry out) and in Tab. 6 (overflow). For each time value, the result given by the GSPN analysis is inside the range of values between the lower and the upper confidence levels returned for the cdf by the FSPN simulation; this is shown in Fig. 5 (dry out) and in Fig. 6 (overflow). Our analytical results are also quite similar to those reported in [1], obtained by Monte Carlo simulation.

Table 5: cdf values for the dry-out failure condition.

time	cdf (GSPN)	min (FSPN)	max (FSPN)
100 h	0.019585	0.016763	0.022237
200 h	0.039143	0.038078	0.046122
300 h	0.053337	0.048871	0.057929
400 h	0.063036	0.058176	0.068024
500 h	0.069508	0.064140	0.074460
600 h	0.073770	0.068957	0.079643
700 h	0.076553	0.071754	0.082646
800 h	0.078357	0.073877	0.084923
900 h	0.079520	0.074649	0.085751
1000 h	0.080267	0.075518	0.086682

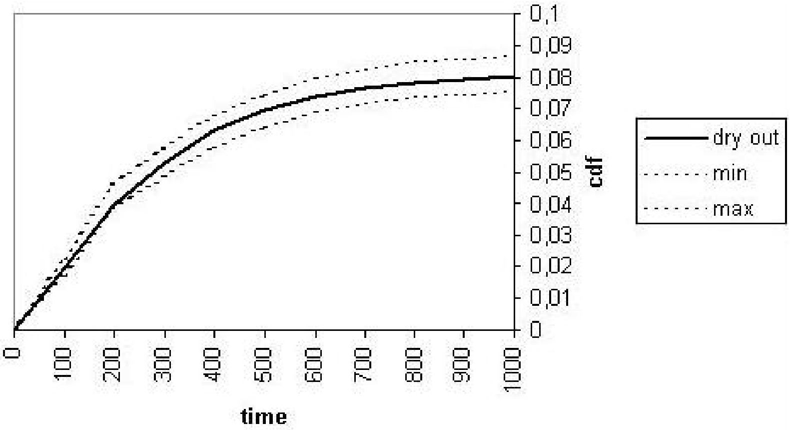

Fig. 5: Dry-out cdf. The solid line indicates the GSPN analytical results.

Table 6: cdf values for the overflow failure condition.

hours	cdf (GSPN)	min (FSPN)	max (FSPN)
100 h	0.077879	0.070307	0.081093
200 h	0.167562	0.160161	0.176239
300 h	0.234353	0.221677	0.240523
400 h	0.280056	0.265212	0.285788
500 h	0.310778	0.295452	0.317148
600 h	0.331513	0.316283	0.338717
700 h	0.345659	0.331619	0.354581
800 h	0.355426	0.340273	0.363527
900 h	0.362243	0.345387	0.368813
1000 h	0.367048	0.350502	0.374098

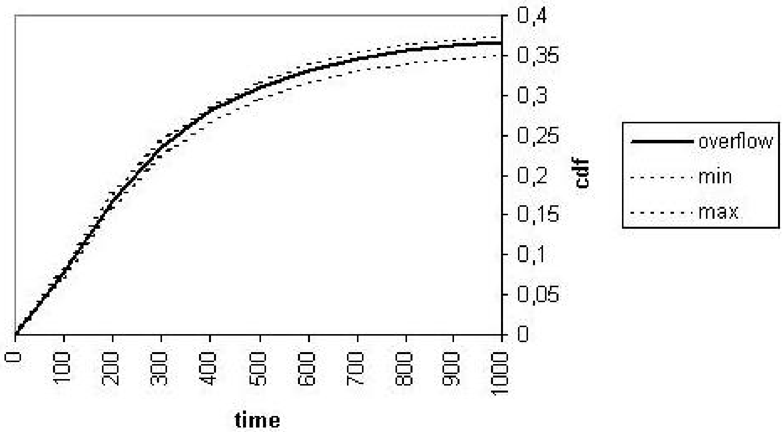

Fig. 6: Overflow cdf. The solid line indicates the GSPN analytical results.

5. THE DEPENDENCE ON THE TEMPERATURE

In this version of the system, a heat source (H) is present with the aim of increasing the temperature (T) of the liquid inside the tank. The liquid level variation rate of the pumps and of the valve is now Q = 1.5 m/h.

The tank is assumed to be filled with water and has a cross section area of 180 m^2. The heating power of H is w=753.48 MJ/h = 1m°C/h [1]; we assume that there is no heat released outside the tank, and that the heat is uniformly distributed in the liquid. The initial temperature of the liquid inside the tank is 15.6667°C; the temperature of the fresh liquid pumped in the tank is T_in=15°C, and we assume that the pumped liquid gets mixed instantaneously with the liquid in the tank. Besides the dry-out and the overflow conditions, the system failure occurs if the temperature T reaches a threshold of 100°C. Assuming that a pump is activated at time t0 and is still active at time t > t0, we use the equations 1 and 2 to provide respectively the liquid level and temperature at time t > t0, where L0 is the the liquid level and T0 is the liquid temperature at time t0.

$$L(t) = L0 + Q \cdot (t - t0) \qquad (1)$$

$$T(t) = T0 \cdot L0 / L(t) + T\_in \cdot Q \cdot (t - t0) / L(t) \qquad (2)$$

If we want to express the liquid temperature at time t > t0 as T(t) = T0 - θ(t), from equation 2 we can derive equation 3.

$$\theta(t) = (T0 - T\_in) \cdot Q \cdot (t - t0) / L(t) \qquad (3)$$

The failure rates of the components P1, P2 and V are temperature dependent; λ0 in Tab. 7 is the failure rate of the component for a temperature equal to 20°C; the failure rate as a function of T, is given by equation 4 [1].

$$\lambda(T) = \lambda0 \cdot (0.2\exp(0.005756(T-20)) + 0.8\exp(-0.2301(T-20))) \qquad (4)$$

Table 7: Failure rates for T=20°C

Component	Failure rate λ0
P1	0.004566 1/h
P2	0.005714 1/h
V	0.003125 1/h

5.1. The FSPN model

Fig. 7 shows the FSPN model of the system. The liquid level and temperature are represented by two fluid places L and T, respectively. L is initially set to 7, while T is initially set to 15.6667.

The component states and failure conditions are modelled as in the previous case. The failure rates of P1, P2 and V depend on the temperature, but do not depend on the current state of the component; moreover, the failure of P1 or P2 leads the component to the state stuck ON or stuck OFF with the same probability. For this reasons, the firing rate of such timed transitions is set to λ(T)/2, where λ(T) is defined by equation 4, and T is the current temperature, represented by the level inside the fluid place representing the temperature.

The action of P1, P2 and V on the liquid level is modelled by a set of transitions and fluid arcs. The addition of liquid in the tank by P1, is modelled by a fluid arc drawn from the transition P1fill to the fluid place L; the flow rate of such arc is #P1on · Q, where #P1on is the current number of tokens inside the discrete place P1on (0 or 1). In other words, while P1 is on, it injects some liquid in the tank according to its level variation rate. The action of P2 is modelled in the same way (transition P2fill), while the removal of liquid from the tank by the valve V, is modelled by a fluid arc drawn from the fluid place L to the transition Vremove.

The transitions P1fill and P2fill are connected by means of other fluid arcs, also to the fluid place T representing the current liquid temperature. In this way, we model the variation of the temperature of the liquid inside the tank, due to the injection of some fresh liquid by the pumps. We use θ (equation 3) as the flow rate of the fluid arcs drawn from the fluid place T to the transitions named P1fill and P2fill, respectively.

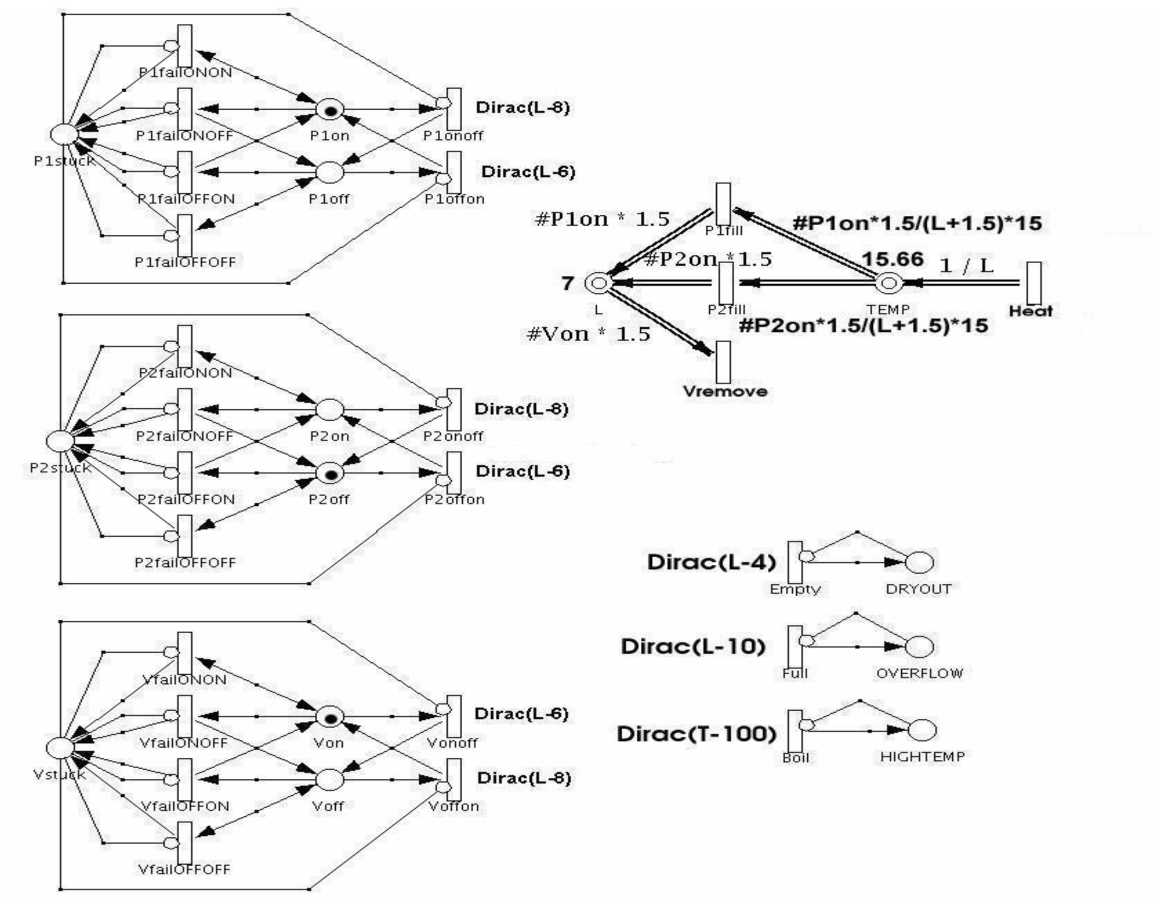

Fig. 7: FSPN model of the system.

The temperature of the liquid in the tank is also influenced by the presence of the heat source which is modelled in the FSPN as the fluid arc drawn from the transition Heat to the fluid place T, in order to represent the increase of the temperature due to the heat source. The flow rate of such fluid arc is 1/L, since the heat power is uniformly distributed in the liquid in the tank whose level is represented by the fluid place L.

For each component, two timed transitions model the action of C on the component state. In the case of P1, the timed transition P1offon switches P1 on if P1 is OFF and is not stuck, by moving the token inside the place P1off, to the place P1on. Such transition must fire when L reaches 6 m, so its firing rate is Dirac(L-6). The timed transition P1onoff instead, models the other control law (Tab. 2); its aim is switching P1 on when L reaches 8 m, so its firing rate is Dirac(L-8). The action of C on the state of P2 and V, is modelled analogously.

The detection of the system failure conditions (dry out, overflow, high temperature) is achieved by means of three transitions. The transition Empty detects the dry out condition (L=4), so its firing rate is Dirac (L-4); if this transition fires, one token appears in the place DRYOUT, in order to represent the dry out state of the system. The overflow condition (L=10) is detected by the transition Full whose firing rate is Dirac (L-10); this transition puts one token inside the place OVERFLOW to represent the overflow state. Finally, the transition Boil fires when the temperature of the liquid inside the tank reaches 100°C, so its firing rate is Dirac(T-100); the effect of its firing is the presence of one token inside the place HIGHTEMP in order to model the failure of the system due to the condition of high temperature.

5.2. Unreliability evaluation

In order to evaluate the unreliability of the system, we computed via simulation on the FSPN model, the cdf for the dry out, the overflow and the high temperature failure condition. The dry out cdf has been computed as the mean number of tokens inside the place DRYOUT, at the given time. Analogously, the overflow cdf is computed as the mean number of tokens inside the place OVERFLOW, while the high temperature cdf is computed as the mean number of tokens inside the place HIGHTEMP.

The FSPN model has been drawn and simulated by means of the FSPNedit tool [9]. The obtained cdf values for each failure condition and for a mission time varying between 0 and 1000 hours, are shown in Tab. 8 and in Fig. 8.

Table 8: cdf values for every failure condition.

time	dry-out	overflow	high temperature
100	0.0334	0.2537	0
200	0.0684	0.3855	0
300	0.0910	0.4451	0
400	0.1107	0.4757	0
500	0.1225	0.4911	0
600	0.1254	0.4956	0.0424
700	0.1261	0.4967	0.0912
800	0.1261	0.4967	0.1276
900	0.1261	0.4968	0.1315
1000	0.1261	0.4968	0.1320

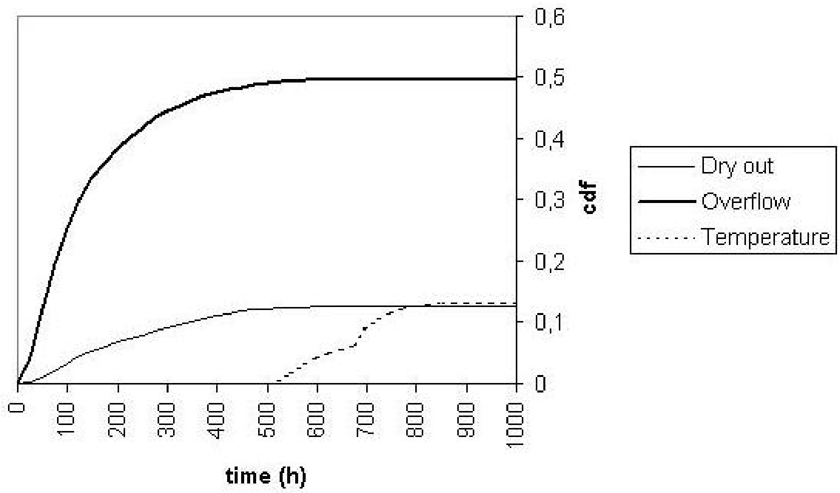

Fig. 8: cdf values for each failure condition.

6. CONCLUSIONS

In this paper, we propose the use of Petri Nets for the evaluation of hybrid and dynamic systems. When the continuous variables describing the system behavior can be discretized with a not relevant loss of precision in the system evaluation, the GSPN formalism is suitable for the modelling and the analysis of the system. The case I (Section 4) of the benchmark examined in this paper, has been modelled and analyzed as a GSPN. The analytical results obtained on such model have been validated by comparison with the results returned by the simulation of the FSPN model of the same version of the benchmark, and with the results returned by Monte Carlo simulation and reported in [1].

When the discretization of the continuous variables describing the system behavior, becomes unpracticable, as in the case II (Section 5) of the benchmark, the FSPN formalism is a valid framework to evaluate the system, though simulative results can be computed on FSPN models.

ACKNOWLEDGEMENTS

This work was supported by MIUR grant FIRB PERF RBNE019N8N, and was originated by the 3ASI [10] workgroup on dynamic reliability.

REFERENCES

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

[2]. R. Alur, T. A. Henzinger, and P. H. Ho. Automatic symbolic verification of embedded systems. IEEE Transaction on Software Engineering, 22:181--201, 1996.

[3]. H. Alla and R. David. Continuous and hybrid Petri nets. Journal of Systems Circuits and Computers, 8(1):159--188, Feb. 1998.

[4]. 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.

[5]. B. Tuffin, D. S. Chen, and K. Trivedi. Comparison of hybrid systems and fluid stochastic Petri nets. Discrete Event Dynamic Systems, 11 (1/2):77-95, January 2001.

[6]. M. Gribaudo, A. Horvath, A. Bobbio, E. Tronci, E. Ciancamerla, and M. Minichino. Fluid Petri nets and hybrid model-checking: A comparative case study. Reliability Engineering and System Safety, 81:239-257, 2003.

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

[8]. 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.

[9]. M.Gribaudo. FSPNEdit: a Fluid Stochastic Petri Net Modeling and Analysis Tool. In Proceedings of the International Conference on Measuring, Modeling and Evaluation of Computer and Communication Systems, pages 24-28, Aachen, Germany, 2001.

[10].http://www.3asi.it - web page of the 3ASI Association.