Evaluation of a benchmark on dynamic reliability via Fluid Stochastic Petri Nets

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

Andrea Bobbio
Dipartimento di Informatica
Università del Piemonte Orientale
Via Bellini 25/G, 15100 Alessandria, Italy
bobbio@mfn.unipmn.it

Abstract

The paper presents the evaluation of a benchmark on dynamic reliability. Such system consists of a tank containing some liquid, two pumps and one valve to renew the liquid in the tank, a heat source warming the liquid, and a controller acting on the state of the components. Three failure conditions are possible: the dry out, the overflow or the high temperature of the liquid. Due to the presence of continuous variables, such as the liquid level and temperature, the system is modelled as a Fluid Stochastic Petri Net which is the object of simulation obtaining the unreliability evaluation of the system.

1 Introduction

The term *performability* was coined in [6] to account for the degradation of some performance index in a distributed redundant system when the failure of some of its parts reduces its capacity. However, in process industry performance and reliability may show a mutual influence in a different way through the common dependence on some process parameter. As an example, a temperature increase speeds up the chemical reactions through the Arrhenius law, but, at the same time, may have a detrimental effect on the component reliability. A hybrid system is a system whose behaviour is described by means of both discrete and continuous variables. In the dependability literature, the case in which the reliability characteristics vary continuously versus a process parameter is sometimes referred to as *dynamic reliability* [5]. The modelling and analysis of hybrid dynamic systems is an open research area.

Based on the example in [5], a benchmark was proposed to compare different methodologies [7]. The benchmark consists 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 of the liquid. Several versions of this system have been proposed and evaluated by means of Monte Carlo simulation in [5]. In this paper, we concentrate on the case in which a heat source is present to warm the liquid in the tank, and the component failure rates depend on the temperature (section 2).

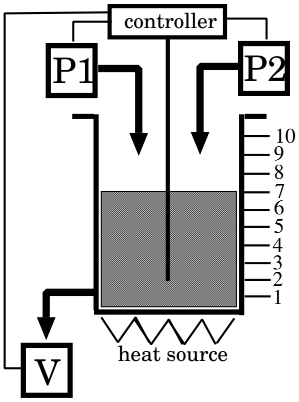

Figure 1. System scheme.

Due to the presence of discrete and continuous variables, in section 3 we model the dynamic behaviour of the system by means of a *Fluid Stochastic Petri Net* (FSPN) [3, 4]; the simulation of the FSPN model provides the system unreliability for each failure condition versus the mission times (section 4).

FSPNs are an extension of *Generalized Stochastic Petri Nets* (GSPN) [1]. With respect to GSPNs, FSPNs contain new primitives: fluid places, that contain a continuous level of fluid (instead of a discrete number of tokens), and fluid arcs that connect a timed transition to a fluid place (or viceversa). Flow rates are associated to fluid arcs to increase (or decrease) the level inside the fluid place while the timed transition is enabled. FSPNs extend the modelling power and flexibility of GSPNs, and are a useful modelling framework for hybrid systems.

2 The case study

The system [5] is composed by a tank containing some liquid, two pumps (P1 and P2) to fill the tank, one valve (V) to remove fluid 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 liquid level variation rate ($Q = 1.5m/h$) and can

Boundary	P1	P2	V
$L \leq HLA$	ON	ON	OFF
$L \geq HLB$	OFF	OFF	ON

Table 1. Control boundaries and laws.

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 ($HLA < L < HLB$).

Initially $L = 7$ 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 on a state transition towards the state stuck ON or stuck OFF, and causes a variation of L: Tab. 2 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 boundaries in Tab. 1, with the purpose of avoiding two failure conditions of the system: the liquid dry out ($L \leq HLV$) or overflow ($L \geq HLP$). If a component is stuck (ON or OFF), it does not respond to the controller orders, so it does not change its state.

Config.	P1	P2	V	effect on L
1	ON	OFF	OFF	↑
2	ON	ON	OFF	↑↑
3	ON	OFF	ON	=
4	ON	ON	ON	↑
5	OFF	OFF	OFF	=
6	OFF	ON	OFF	↑
7	OFF	OFF	ON	↓
8	OFF	ON	ON	=

Table 2. Variation of L for each configuration.

At the same time, a heat source (H) increases the temperature (T) of the liquid inside the tank which has a cross section area of $180m^2$ and is assumed to be filled with water. The heating power of H is $w = 753.48MJ/h = 1m°C/h$ [5]; we assume that there is no heat released outside the tank, and that the heat is uniformly distributed on the liquid. The initial temperature of the liquid inside the tank is $15.6667°C$; the temperature of the liquid introduced in the tank by the pumps, is $T_{in} = 15°C$, and we assume that it gets mixed instantaneously with the liquid in the tank. Assuming that a pump is activated at time t_0 and is still active at time $t > t_0$, we use the equations 1 and 2 to provide respectively the liquid level and temperature at time $t > t_0$, where L_0 is the the liquid level and T_0 is the liquid temperature at time t_0.

$$L(t) = L_0 + Q \cdot (t - t_0) \tag{1}$$

$$T(t) = T_0 \cdot \frac{L_0}{L(t)} + T_{in} \cdot \frac{Q}{L(t)} \cdot (t - t_0) \tag{2}$$

Component	λ_0 (h^{-1})
P1	0.004566
P2	0.005714
V	0.003125

Table 3. Failure rates for $T = 20°C$.

If we want to express the liquid temperature at time $t > t_0$ as $T(t) = T_0 - \theta(t)$, from equation 2 we can derive equation 3.

$$\theta(t) = (T_0 - T_{in}) \cdot \frac{Q}{L(t)} \cdot (t - t_0) \tag{3}$$

Another failure condition of the system occurs when T reaches $100°C$. The failure rates of the components P1, P2 and V are temperature dependent; λ_0 is the failure rate of the component for a temperature equal to $20°C$ (Tab. 3); the failure rate as a function of T, is given by equation 4 [5].

$$\lambda(T) = \lambda_0(0.2e^{0.005756(T-20)} + 0.8e^{-0.2301(T-20)}) \tag{4}$$

Moreover, we assume that the controller C has a probability of failure on demand (FOD) equal to $p = 0.2$; this means that the probability to fail of C when the liquid reaches a control boundary (Tab. 1), is p. If C fails, it does not execute the corresponding control rule on the component states.

3 The FSPN model

Fig. 2 shows the FSPN model of the system. The liquid level and temperature are represented by two fluid places, respectively L and T; fluid places graphically appear as double circles. L is initially set to 7, while T is initially set to 15.6667.

Component states. Let us consider the subnet modelling the states of P1; three discrete places (appearing as circles) are used: $P1on$, $P1off$ 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 also stuck. $P1on$ is initially marked. The component state variations due to a failure, are modelled by four timed transitions (they appear as white rectangles): $P1failONON$, $P1failONOFF$, $P1failOFFON$ and $P1failOFFOFF$. The transition $P1failONOFF$ for instance, 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 failure rate of P1 depends on the temperature, but it does not depend on the current state of P1; for this reason, the firing rate of such timed transitions is set to $\lambda(T)/2$, where $\lambda(T)$ is defined by equation 4, and T indicates the level inside the fluid place representing the temperature. The failure of P2 and V is modelled in the same way.

Variation of L and T. The action of P1, P2 and V on the liquid level is modelled by a set of transitions and fluid arcs (appearing as a pipe). 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 $\#P1on \cdot Q$, where $\#P1on$ is the current number of token 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 new 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.

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 on the liquid in the tank whose level is represented by the fluid place L.

Actions by C. The discrete place named $CORRECT$ indicates whether the liquid level is inside the region of correct functioning ($HLB < L < HLA$) or not; such place is initially marked because the liquid level is 7 at the begin. If the liquid level reaches HLA, the transition called $tooLOW$ fires, since its firing rate is set to $Dirac(L-6)$. The $Dirac$ delta function returns $+\infty$ if its argument is equal to 0, else it returns 0; so, the transition $tooLOW$ fires if $L = 6$. The effect of the firing of $tooLOW$ is moving the token from the place $CORRECT$ to the place $dangerLOW$, enablig the firing of two immediate transitions (graphically appearing as black rectangles): $LAW1$ and $FOD1$. The probability to fire of such transitions is ruled by their weights; the transition $LAW1$ models the correct functioning of the controller and its weight is $1-p$; the transition $FOD1$ models the failure on demand of the controller, and its weight is p (FOD probability). The effect of the firing of the transition $LAW1$ is moving the token from $dangerLOW$ to $ORDER1$. If such place is marked, several immediate transitions ($P1offon$, $P2offon$, $Vonoff$) representing the first control law in Tab. 1, fire changing the state of the components which are not stuck. The token is moved from the place $ORDER1$ to the place $CORRECT$ by means of the transition $enoughHIGH$, when the liquid level L comes back to the region of correct functioning. If the immediate transition $FOD1$ fires instead of $LAW1$, the token inside the place $dangerLOW$ is simply removed and no action on the state of the components is performed. The action of the controller when L reaches HLB (second control law in Tab. 1), is modelled analogously.

System failure. 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.

4 Unreliability evaluation

In order to evaluate the unreliability of the system, we computed via simulation of the FSPN model, the *cumulative distribution function* (cdf) for the dry out, the overflow and the high temperature failure condition; this means computing the probability that the system is in such conditions, as a function of the time. The dry out cdf has been computed as the mean number of tokens inside the place $DRYOUT$, at the given time; since such place can contain zero or one token, the mean number of tokens inside this place will be a value inside the continuous range (0,1). 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 [2]. The obtained cdf values for each failure condition and for a mission time varying between 0 and 1000 hours, are shown in Tab. 4 and in Fig. 3, where it is possible to compare them with the results obtained in the case with a null probability of FOD of C [5] (dashed lines).

5 Conclusions

In this paper, we have proposed FSPNs as a formalism suitable to model cases of hybrid and dynamic systems. The validity of FSPNs has been verified by comparing our results with those reported in [5] and returned by Monte Carlo simulation. The use of FSPN models can be extended from the analysis of the dynamic reliability to the analysis of the performability, when performance indices and reliability features are related to the variation of common process parameters.

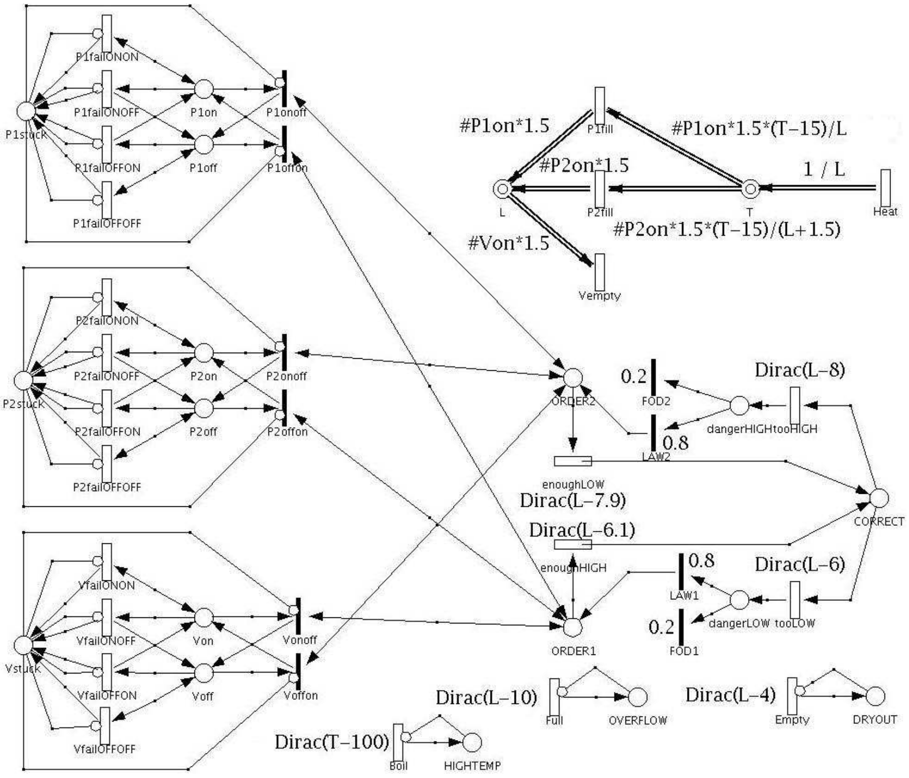

Figure 2. FSPN model of the system.

hours	dry out	overflow	high temp.
100	0.1178	0.3558	0.0002
200	0.1578	0.4722	0.0006
300	0.1724	0.5166	0.0008
400	0.1844	0.5372	0.0008
500	0.1892	0.5484	0.0008
600	0.1906	0.552	0.0194
700	0.1916	0.5528	0.0456
800	0.1916	0.553	0.065
900	0.1918	0.5534	0.0678
1000	0.1918	0.5534	0.0682

Table 4. cdf values for each failure condition.

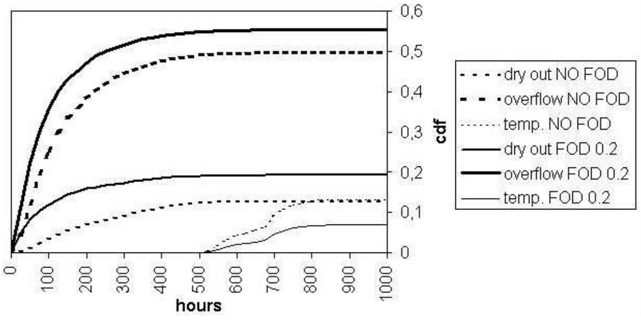

Figure 3. cdf of each failure condition

ACKNOWLEDGEMENTS. This work was supported by MIUR grant FIRB PERF RBNE019N8N, and was originated by the 3ASI [7] workgroup on dynamic reliability, coordinated by Enrico Zio (Politecnico di Milano).

References

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

[2] 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.

[3] M. Gribaudo, A. Bobbio, 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*, pages 81–85, 2001.

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

[6] J. F. Meyer. On evaluating the performability of degradable systems. *IEEE Transactions on Computers*, C-29:720–731, 1980.

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