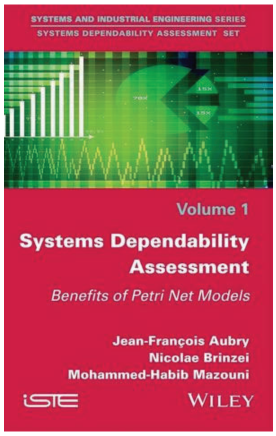
Sûreté de fonctionnement

Approches par l'espace d'états.
Réseaux de Petri Stochastiques (RdPS)

Nicolae Brînzei

Introduction



Ce chapitre est basé sur plusieurs chapitres du livre suivant :

Aubry Jean-François, Brinzei Nicolae, Mazouni Mohamed Habib, *Systems dependability assessment. Benefits of Petri net models*, ISTE-Wiley, 2016.

Ce livre est disponible :
- à la bibliothèque :
  - ✓ en version papier : côte **511.3 AUB**
  - ✓ en version électronique téléchargeable :

https://www-dawsonera-com.bases-doc.univ-lorraine.fr/search?q=Systems+Dependability+Assessment&sType=ALL&searchFrom=0&sortBy=0&infinityOffset=1

Il faudra ensuite :
  - Vous identifier (*identifiant* et *mdp Sésame*)
  - Accepter les conditions générales d'utilisation
- auprès de l'éditeur :

http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1848219911.html

Introduction

Exemple

Considérons un calculateur qui doit réaliser deux tâches. Les requêtes pour ces tâches sont soumis au calculateur qui le traite une par une et qui élabore un résultat pour chaque tâche. Cependant, le calculateur peut tomber en panne mais il peut être réparée. Le réseau de Petri ci-dessous modélise cet ensemble avec 4 places et 3 transitions :

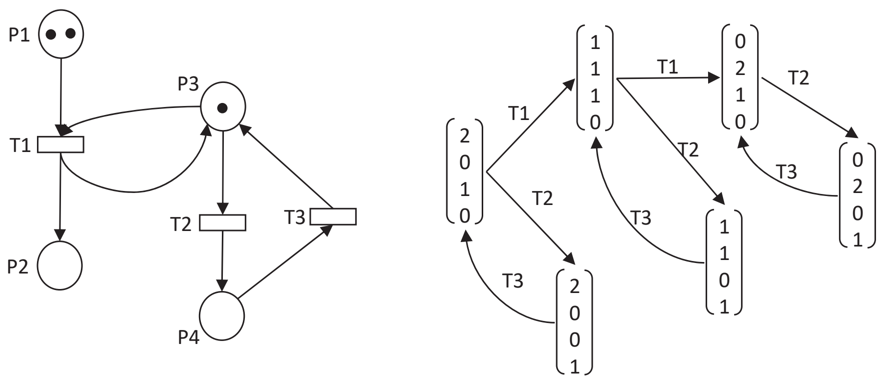


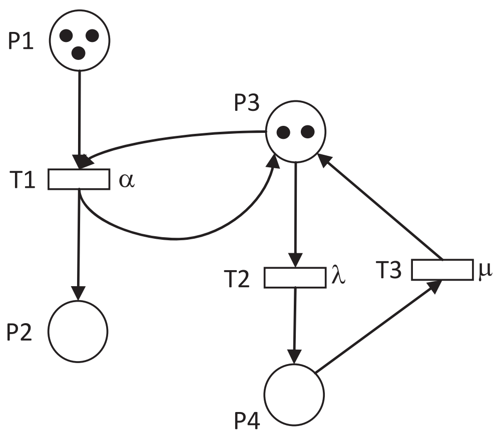
Figure 1 : exemple de RdP et de son graphe de marquage.

- P1 représente les requêtes en attente
- P2 représente les requêtes traitées ou les résultats élaborés pour ces requêtes
- P3 représente l’état de disponibilité du calculateur
- P4 représente son état d’indisponibilité (panne)
- T1 représente l’opération de traitement de la requête
- T2 représente la défaillance du calculateur
- T3 représente sa réparation

Introduction

Exemple

La figure ci-dessous reprend le RdP précédent avec un marquage initial tel qu’il y ait 3 requêtes et deux calculateurs disponibles pour réaliser les tâches.



A ce modèle, on doit ajouter le fait que les changements d’état provoqués par l’occurrence des événements (franchissement des transitions) sont aléatoires.

Le modèle RdP stochastiques associe à chaque transition d’un RdP autonome un taux de franchissement λ tel que λ.dt soit la probabilité de franchir la transition entre les instants t et t+dt, sachant que la transition est validée à l'instant t.

En considérant que ces taux α, λ et μ sont constants (distributions exponentielles), ils seront égaux respectivement à l’inverse du temps moyen de traitement de la requête, à l’inverse du MTTF et à l’inverse du MTTR.

Introduction

Les réseaux de Petri stochastiques ont été définis pour répondre à des problèmes informatiques liés à la sûreté de fonctionnement.

Une transition n'est ainsi plus franchie immédiatement dès sa validation, mais on lui associe une durée de franchissement qui est une variable aléatoire θ avec une distribution de probabilité exponentielle :

$$P(\theta < t) = 1 - e^{-\lambda t}$$

La fonction $P(\theta < t)$ décrit la probabilité que le franchissement ait lieu avant t.

La valeur moyenne de la durée de franchissement est :

$$\bar{\theta} = \int_0^\infty (1 - P(t))dt = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda}$$

λ est appelé taux de franchissement.

Définition et évolution des RdPS

Un réseau de Petri stochastique (RdPS) est un doublet $R_S = < R, \Lambda >$ **tel que :**

- $R = < \mathcal{P}, \mathcal{T}, \text{Pré}, \text{Post}, M_0 >$ **est un réseau de Petri généralisé**
- $\Lambda : \mathcal{T} \to \mathbb{R}^+$ **est l'application qui à chaque transition** $T_j \in \mathcal{T}$ **associe un taux de franchissement :** $\Lambda(T_j) = \lambda_j$

Définition et évolution des RdPS

Notion de n-validation

Dans un RdP généralisé, une transition T_j est n-validée si :

$$n \leq \min (M(P_i)/Pré(P_i, T_j)) < n+1, \qquad P_i \in °T_j$$

où :

- $M(P_i)$ est le marquage de P_i,
- $°T_j$ l'ensemble de places d'entrées de T_j,
- $Pré(P_i, T_j)$ la valuation de l'arc (P_i, T_j).

Dans le cas où tous les arcs sont mono-valués la condition s'écrit :

$$\min (M(P_i)) = n, \qquad P_i \in °T_j$$

Dans le cas du RdP de l'exemple précédent, la transition T_1 est 2-validée car ici $°T_1=\{P_1, P_3\}$, $M(P_1)=3$ et $M(P_3)=2$.

La transition T_2 est également 2-validée car $°T_2=\{P_3\}$ et $M(P_3)=2$.

Définition et évolution des RdPS

Notion de n-validation

On s'intéresse uniquement au cas où le RdPS est borné. Soient :

- M un marquage accessible pour le réseau autonome sous jacent à un RdPS
- $\lambda_j(M)$ le taux de franchissement associé à la transition T_j pour le marquage M

Si T_j a un taux de franchissement λ_j et qu'elle est n-validée pour le marquage M, alors le taux de franchissement de la transition T_j dans le marquage M est :

$$\lambda_j(M) = n\,\lambda_j$$

Définition et évolution des RdPS

Notion de n-validation

La durée de séjour D_j dans l'état M entre le moment où la transition T_j est validée et le moment où elle sera franchie, a une fonction de répartition :

$$H_j(t) = 1 - e^{-\lambda_j(M)\cdot t}$$

et une densité de probabilité :

$$h_j(t) = \lambda_j \cdot e^{-\lambda_j(M)\cdot t}$$

En clair, lorsque n entités concourent ensemble à la réalisation d'une même tâche, le temps d'exécution moyen de cette tâche est divisé par n, c.à.d. que dans un RdPS le taux de franchissement de la transition associée à cette tâche est multiplié par n. Dans notre exemple, le taux de défaillance d'une entité parmi les deux est doublé.

Définition et évolution des RdPS

Notion de n-validation

Soit $\mathcal{T}(M)$ l'ensemble des transitions validées par le marquage M.

Si $T_k \in \mathcal{T}(M)$, alors la probabilité conditionnelle de franchissement de cette transition à partir de M est :

$$\Pr(T_k / M) = \frac{\lambda_k(M)}{\sum_{T_j \in \mathcal{T}(M)} \lambda_j(M)}$$

et la durée du séjour dans l'état M suit une loi exponentielle de paramètre :

$$\lambda(M) = \sum_{T_j \in \mathcal{T}(M)} \lambda_j(M)$$

Par conséquent, le temps de séjour moyen dans le marquage M est égal à :

$$\eta(M) = \frac{1}{\lambda(M)}$$

Définition et évolution des RdPS

Evolution du marquage

Pour **représenter le fonctionnement** du système, le marquage du RdPS va évoluer de la manière suivante :

- pour un marquage donné, plusieurs transitions peuvent être validées. Pour chacune d'elles, on réalise un tirage aléatoire de la durée d_j associée (suivant la loi exponentielle de paramètre λ_j). Pour une transition n-validée, si le taux de franchissement associé à T_j est λ_j, alors le tirage se fait en considérant un taux $n.\lambda_j$.
- au bout d'un temps égal à la plus courte de ces durées, on franchit la transition correspondante, ce qui nous amène à un nouveau marquage et un nouvel ensemble de transitions validées sur lequel on réalise un nouveau tirage et ainsi de suite.

Les transitions $T_j \in \mathcal{T}(M)$ validées dans le marquage M sont en **compétition**, *la transition franchie sera celle qui correspondra au événement qui se produit en premier* (fin de traitement de la requête ou l'occurrence de la défaillance, dans l'exemple considéré).

Chaîne de Markov à temps continu équivalente au RdPS

Dans le cas d'un RdPS borné, **le graphe des marquages** (n valeurs différentes du vecteur de marquage) **est isomorphe à une chaîne de Markov à temps continu** de dimension n, que l'on obtient en associant à chaque arc un taux de transition qui dépend du taux de la transition franchie et du marquage des places en amont de la transition (transition n-validée).

On peut déterminer alors la matrice des taux de transition A de la chaîne de Markov.

Soit $\mathcal{P}(t) = [\mathbb{P}_1(t)\,\mathbb{P}_2(t) \ldots \mathbb{P}_n(t)]$ le vecteur ligne de dimension n où le $i^{ème}$ composant $\mathbb{P}_i(t) = \mathbb{P}(M_i)$ représente la probabilité d'être dans le marquage M_i (état *i*).

Alors la distribution des probabilités d'états $\mathcal{P}(t) = [\mathbb{P}_1(t)\,\mathbb{P}_2(t) \ldots \mathbb{P}_n(t)]$ est donnée par la solution de l'équation fondamentale de la chaîne de Markov :

$$\dot{\mathcal{P}}(t) = \mathcal{P}(t) \cdot \mathbf{A}$$

Cette solution est donnée par la relation suivante : $\mathcal{P}(t) = \mathcal{P}(0) \cdot e^{\mathbf{A}t}$

Chaîne de Markov à temps continu équivalente au RdPS

Si la chaîne de Markov isomorphe au RdPS est ergodique, alors dans son comportement asymptotique le système tend vers une distribution limite unique, indépendante des conditions initiales :

$$\boldsymbol{\pi} = \mathbb{P}(\infty) = \lim_{t\to\infty} \mathbb{P}(t)$$

Le vecteur π représente la distribution de probabilités d'états en régime permanent et est appelé **distribution stationnaire des probabilités**.

En régime stationnaire $(t \to \infty)$, l'équation fondamentale dévient :

$$\boldsymbol{0} = \boldsymbol{\pi} \cdot \mathbf{A}$$

et permet de déterminer la distribution stationnaire π, en tenant compte que :

$$\boldsymbol{\pi} \cdot \bar{\boldsymbol{1}} = 1$$

où $\bar{1}$ est un vecteur de 1 uniquement.
Les composants du vecteur $\boldsymbol{\pi} = [\pi_1, \pi_2, ..., \pi_n]$ représentent les probabilités moyennes d'être dans les différents états de la chaîne de Markov, c.à.d. les différents marquages du RdPS.

Performances des RdPS

En connaissant les probabilités moyennes des marquages du RdPS données par le vecteur π, plusieurs indicateurs de performance peuvent être définis :

- **les marquages moyens des places** $P_i \in \mathcal{P}$

$$M^*(P_i) = \sum_{k=1}^{n} M_k(P_i) \cdot \pi_k$$

- **les fréquences moyennes de franchissement des transitions** $T_i \in \mathcal{T}$

$$f^*(T_j) = \sum_{k=1}^{n} \lambda_j(k) \cdot \pi_k$$

k tels que T_j est franchissable à partir de M_k, $\lambda_j(k)$ dépendant de M_k

Performances des RdPS

- **les temps moyens de séjour des marques dans les places $P_i \in \mathcal{P}$ en régime stationnaire donnés par la formule de Little**

$$D^*(P_i) = \frac{M^*(P_i)}{Post_i \cdot F^*}$$

où :

$Post_i$ est la i-ème ligne de la matrice d'incidence arrière W^+ et

$F^* = \left[f^*(T_1), f^*(T_2), \dots f^*(T_m) \right]^T$ est le vecteur des fréquences moyennes de franchissement des transitions

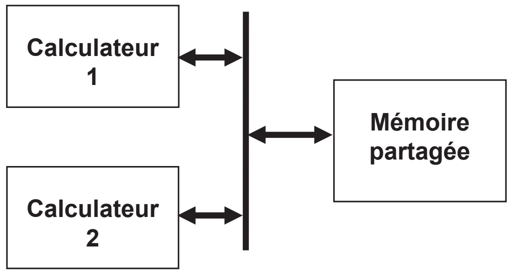
Le temps de séjour moyen est égal au rapport du marquage moyen de cette place en régime permanent sur la somme pondérée par les incidences des arcs des fréquences moyennes de transition en amont de la place.

Exercice

Exercice

Deux calculateurs partagent une mémoire commune.

On note λ_c et μ_c les taux de défaillance et de réparation des calculateurs et λ_m et μ_m ceux de la mémoire partagée. On suppose que le bus de communication est exempt d'erreurs (ce n'est qu'un exemple bien sûr, la réalité peut être toute autre).



Exercice

Exercice

RdP Stochastique

Chaîne de Markov équivalente

Exercice

Exercice

La matrice des taux de transitions de la CdM est :

$$A = \begin{bmatrix} -(\lambda_m + 2\lambda_c) & 2\lambda_c & 0 & \lambda_m & 0 & 0 \\ \mu_c & -(\lambda_c + \mu_c + \lambda_m) & \lambda_c & 0 & \lambda_m & 0 \\ 0 & 2\mu_c & -(2\mu_c + \lambda_m) & 0 & 0 & \lambda_m \\ \mu_m & 0 & 0 & -(\mu_m + 2\lambda_c) & 2\lambda_c & 0 \\ 0 & \mu_m & 0 & \mu_c & -(\mu_c + \lambda_c + \mu_m) & \lambda_c \\ 0 & 0 & \mu_m & 0 & 2\mu_c & -(\mu_m + 2\mu_c) \end{bmatrix}$$

Avec les données numériques suivantes (non réalistes, mais pour la simplicité des calculs) : λ_c=1, μ_c=2, λ_m=1, μ_m=3, on obtient :

π_1 = 1/3, π_2 = 1/3, π_3 = 1/12,
π_4 = 1/9, π_5 = 1/9, π_6 = 1/36

$$A(\infty) = \pi_1 + \pi_2 = 2/3$$

$$\overline{A}(\infty) = \pi_3 + \pi_4 + \pi_5 + \pi_6 = 1/3$$

π_1 = 1/3 est la probabilité d'avoir un fonctionnement normal,
π_2 = 1/3 est la probabilité d'avoir un fonctionnement dégradé,
$\pi_3 + \pi_4 + \pi_5 + \pi_6$ = 1/3 est la probabilité d'avoir un fonctionnement arrêté

Exercice

Exercice

On peut ensuite calculer les performances suivantes :

- *les fréquences moyennes de franchissement*

- *les marquages moyens*

Exercice

Exercice

On peut ensuite calculer les performances suivantes :

- *les temps moyens de séjour dans les places*

où la matrice d'incidence arrière du RdPS est :

Réseaux de Petri Stochastiques Généralisés

- **Les RdPS sont très bien adaptés pour modéliser des processus dont les durées sont variables.** *Par exemple, le temps de bon fonctionnement entre deux défaillances, le temps de réparation ou dans certains cas la durée d'exécution d'une tâche sont des durées plus ou moins grandes pouvant être modélisées par des variables aléatoires.*
- **La modélisation des systèmes nécessite parfois de prendre en compte des événements de durées nulles.** *On peut donner comme exemple, le début et la fin d'une tâche par un contrôleur.* Ce type d'événement nécessite pour sa modélisation une transition ayant une durée nulle.
- Besoin d'une extension des RdPS : **les réseaux de Petri stochastiques généralisés (GSPN)**. Ils autorisent l'utilisation simultanée de transitions ayant des durées nulles et des durées variables non nulles (distribuées exponentiellement).

Réseaux de Petri Stochastiques Généralisés

Un réseau de Petri stochastique généralisé (RdPSG) est un doublet

$\mathrm{R}_{SG} = < \mathrm{R}, \Lambda >$ **tel que :**

- $\mathrm{R} = < \mathcal{P}, \mathcal{T}, \text{Pré}, \text{Post}, M_0 >$ **est un réseau de Petri généralisé**
- $\mathcal{T} = \mathcal{T}_i \cup \mathcal{T}_t, \mathcal{T}_i \cap \mathcal{T}_t = \varnothing$ **, l'ensemble de transitions $\mathcal{T}$ est composé de deux sous-ensembles $\mathcal{T}_i$ et $\mathcal{T}_t$ non vides et disjoints**
- $\Lambda : \mathcal{T}_t \rightarrow \mathbb{R}^+$ **est l'application qui à chaque transition $\mathrm{T}_j \in \mathcal{T}_t$ associe un taux de franchissement :** $\Lambda(\mathrm{T}_j) = \lambda_j$

Réseaux de Petri Stochastiques Généralisés

- les transitions $T_j \in \mathcal{T}_i$ de durée nulle de franchissement sont appelées **transitions immédiates**
- les transitions $T_j \in \mathcal{T}_t$ ayant une durée de franchissement aléatoire sont appelées **transitions temporisées**

Les deux types de transitions génèrent deux types de marquage :

- **les marquages immédiats** ou **instables** pour lesquels au moins une transition immédiate est validée
- **les marquages tangibles** ou **stables** ne validant que des transitions temporisées

Le graphe des marquages accessibles par un RdPSG peut être considérablement simplifié. En effet, puisque les transitions immédiates sont franchies dès leur validation, il va de soi que le système ne fera que traverser les états instables sans s'y arrêter.

D'un point de vue probabiliste, la probabilité d'occupation des états instables sera nulle et on pourra les supprimer du graphe des marquages accessibles sans modifier les résultats d'une analyse quantitative.

Réseaux de Petri Stochastiques Généralisés

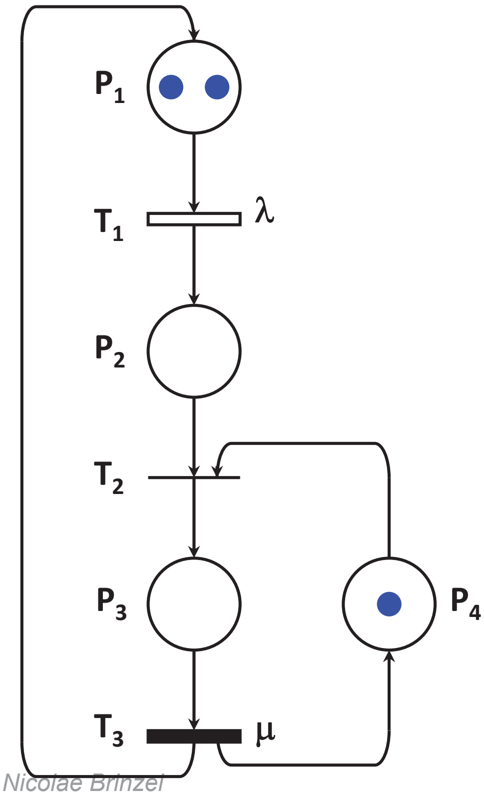
Exemple

On considère un système formé de deux composants identiques caractérisées par un taux de défaillance λ constant.

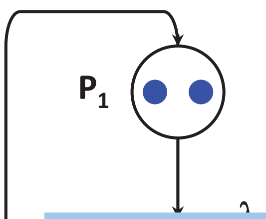
L'équipe de maintenance est composé d'un seul opérateur humain qui est en état de repos lorsque les composants sont en état de fonctionnement.

Lorsqu'un composant tombe en panne la réparation commence tout de suite si l'opérateur de maintenance est disponible, sinon on attend que l'opérateur finisse la réparation en cours. La durée des réparation est une variable aléatoire caractérisée par un taux de réparation μ constant.

Exemple

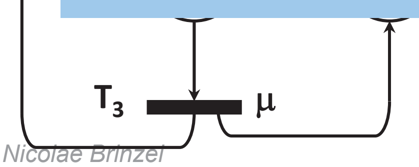


Exemple



Comment modéliser un système constitué de 10 composants et une équipe de maintenance constituée de 2 opérateurs, chacun travaillant indépendamment ?

Réponse: La structure du modèle RdPS ne change absolument pas.
Ce sera juste le marquage initiale de places P_1 et P_4 qui sera modifié.
La chaîne de Markov sera ensuite déduite de manière automatique en utilisant la procédure de génération du graphe de marquages d'un RdP.



Simulation des RdPS

les RdPS ou les RdPSG associent aux transitions temporisées $\mathrm{T_j} \in \mathcal{T}_t$ des taux de franchissement

$$\Lambda\left(\mathrm{T_j}\right) = \lambda_j = \mathrm{ct.}$$

(lois exponentielles)

→ Graphe de marquages réduit aux états tangibles

|||

Chaîne de Markov à temps continu

↓

Solution analytique pour obtenir :

- les probabilités d'états
- les indicateurs de SdF (fiabilité, disponibilité, MTTF, MTTR, …)

Si les hypothèses nécessaires au passage au modèle markovien ne sont pas vérifiées → **Recours à la Simulation de Monte-Carlo**

Simulation des RdPS

Algorithme de simulation

On associe à chaque transition T_j une temporisation aléatoire d_j de distribution connue.

L'évolution du RdP se conforme à l'algorithme suivant :

- *pas 1 :* initialisation du marquage. L'échéancier contient t=0.

- *pas 2 :* soit X = { T_1, T_2, ... , T_j, ...} l'ensemble des transitions validées.

- *pas 3 :* pour chaque transition T_j de l'ensemble X, faire un tirage aléatoire de la durée d_j. Si le taux de franchissement associé à T_j est λ_j, alors le tirage se fait en considérant un taux $n.\lambda_j$ pour une transition n-validée.

- *pas 4 :* soit d_m = min (d_1, d_2, ... , d_j, ...), et T_m la transition correspondante. Remplacer t par t+dm dans l'échéancier.

- *pas 5 :* franchir la transition T_m à l'instant t. Aller au pas 2.

Simulation des RdPS

On peut évaluer ensuite les marquages moyens, les fréquences moyennes et les temps moyens de séjour dans les places du réseau par statistique en faisant évoluer le modèle sur une durée suffisante. Si le RdPS est bloquant, il faut répéter plusieurs histoires menant à ce blocage.

Le critère d'arrêt peut être lié à la précision voulue sur les moyennes et à une probabilité d'obtention de cette précision.

Références bibliographiques

[1] Aubry Jean-François, Brinzei Nicolae, Mazouni Mohamed Habib, *Systems dependability assessment. Benefits of Petri net models*, ISTE-Wiley, 2016, côte bibliothèque **511.3 AUB**.
https://www-dawsonera-com.bases-doc.univ-lorraine.fr/search?q=Systems+Dependability+Assessment&sType=ALL&searchFrom=0&sortBy=0&infinityOffset=1
http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1848219911.html
[2] Bause Falko, Kritzinger Pieter, *Stochastic Petri Nets. An introduction to the theory*, 2^{nd} edition, Vieweg Verlag, 2002.
[3] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli and G. Franceschinis, *Modelling with Generalized Stochastic Petri Nets, Wiley, 1995.*