# Evaluation de performances

# Sûreté de fonctionnement

Phuc Do

phuc.do@univ-lorraine.fr

**TELECOM Nancy – Université de Lorraine** 



# Sûreté de fonctionnement (SdF)

- Généralités sur le SdF
- Grandeurs de fiabilité
- Calcul de fiabilité au niveau systèm



# Pour quoi sûreté de fonctionnement ?

 Probabilité qu'une ressource fonctionne correctement à un instant d onné ou pendant une intervalle de temps donnée n'est pas égale à 1

#### Causes:

- Défaillance/dysfonctionnement de programmes/logiciels embarques
  - Ex: un programmeur professionnel fait en moyenne 6 fautes pour 1000 lignes de codes, ...
- Défaillance de matériels, ...
  - Dégradations, choc, ...
- Exemple: ordinateurs, smart phones, ...

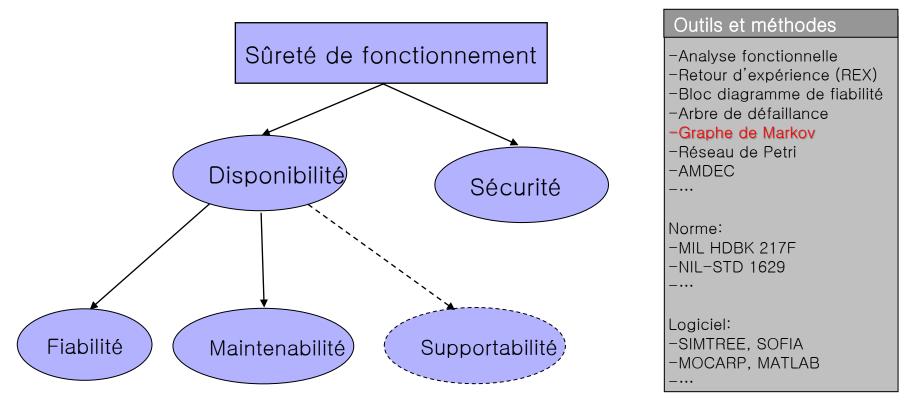
Quelques accidents provoqués par défaillance

29 bugs informatiques aux conséquences catastrophiques

Systèmes informatiques ou réseaux de télécommunication comportent des ressources



Sûreté de fonctionnement: ensemble des aptitudes (fiabilité, maintenabilité, supportabilité, disponibilité, sécurité) d'un produit (composant/système) qui lui permettent de disposer des performances fonctionnelles spécifiques, au moment voulu, pendant la durée prévue et sans dommage pour lui-même et son environnement.





 Disponibilité: Aptitude d'un produit à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné

- Une grande disponibilité implique:
  - que le système tombe peu souvent en panne: grande fiabilité
  - qu'il nécessite peu d'entretien (temps d'indisponibilité)
  - > que le temps de réparation soit le plus faible possible

$$Disponibilit\'e = \frac{Temps\ d'utilisation\ possible}{Temps\ total}$$

■ Remarque: Disponibilité  $\neq$  Taux d'utilisation =  $\frac{Temps d'utilisation réelle}{Temps d'utilisation possible}$ 



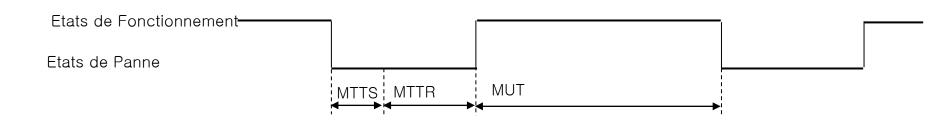
 Fiabilité: Aptitude d'un produit à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné

#### La fiabilité dépend:

- du niveau de qualité des composants et de leur quantité
- de la structure du système
- de l'environnement dans lequel l'équipement est utilisé ou stocké.
- des paramètres mécaniques (vibration, secousses, chocs,...) ou thermiques (pour des composants électroniques)
- modes de fonctionnement (nominal, sous-charge, surchargé, ...)



- Maintenabilité: Aptitude d'un produit à être maintenu ou établi, pendant un intervalle de temps donné, dans un état dans lequel il peut accomplir une fonction requise, lorsque l'exploitation et la maintenance sont accomplies dans des conditions données, avec des procédures et des moyens prescrits
- On définit l'efficacité de la maintenabilité par le temps moyen de réparation MTTR (Mean Time To Repair)
  - Ex: En moyenne 12 heures de travail pour détecter et corriger une faute logiciel



Disponibilité moyenne = 
$$\frac{MUT}{MUT + MTTR + MTTS}$$

MTTS = Mean Time to Support, cas idéal MTTS=0 MUT = Mean Up Time



Supportabilité: Aptitude d'une organisation de maintenance à mettre en place les moyens de maintenance appropriés à l'endroit voulu en vue d'exécuter l'activité de maintenance demandée à un instant donné ou durant un intervalle de temps donné

#### La supportabilité dépend:

- des moyens en personnel: qualification, formation, bonne définition des tâches, ...
- des moyens en en matériel: appareils de mesure, outillages, pièces de rechanges, fournitures, ...
- des procédures d'intervention: définition et description dans la documentation,...
- On définit l'efficacité de la supportabilité par le temps moyen de soutien MTTS (Mean Time To Suport)

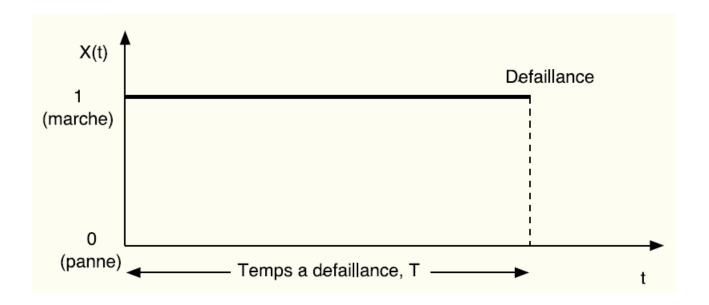


# Grandeurs de fiabilité pour un système

- Fiabilité (ou fonction de survie) R(t)
- Taux de défaillance z(t)
- Temps moyen à la (première) défaillance MTTF
- Durée de vie résiduelle moyenne MRL



#### Variable d'état



$$X(t) = \begin{cases} 1 & \text{si le système est en marche} \\ 0 & \text{si le système est en panne} \end{cases}$$

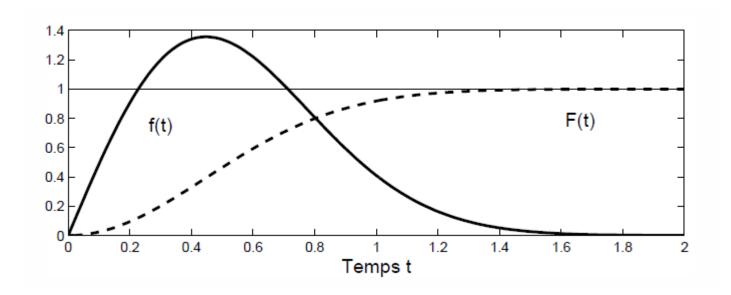
L'état du système X(t) et la date de panne T sont des variable aléatoire



#### Fonction de distribution de T

Fonction de distribution de T est

$$F(t) = \mathbb{P}(T \le t) = \int_0^t f(u)du \text{ pour } t > 0$$



F(t) est la probabilité que le système tombe en panne sur ]0, t]



# Densité de probabilité de T

■ La densité de probabilité de *T* (densité de panne) est

$$f(t) = \frac{d}{dt}F(t) = \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} = \lim_{\Delta t \to 0} \frac{\mathbb{P}(t < T \le t + \Delta t)}{\Delta t}$$

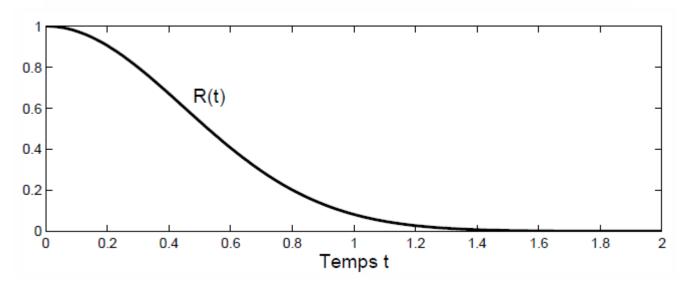
• Lorsque  $\Delta t$  est petit

$$\mathbb{P}(t < T \leq t + \Delta t) \simeq f(t).\Delta t$$



#### **Fiabilité**

$$R(t) = \mathbb{P}(T > t) = 1 - F(t) = \int_{t}^{\infty} f(u)du$$



- Arr R(t) = probabilité que le système ne tombe pas en panne sur ]0, t]
- R(t) = probabilité que le système fonctionne jusqu'à l'instant t
- $\blacksquare$  R(t) est aussi appelée fonction de survie du système



## Taux de défaillance

On s'intéresse à la probabilité conditionnelle

$$\mathbb{P}(|T \le t + \Delta t|T > t) = \frac{\mathbb{P}(t < T \le t + \Delta t)}{\mathbb{P}(T > t)} = \frac{F(t + \Delta t) - F(t)}{R(t)}$$

Le taux de défaillance du système est donné par

$$z(t) = \lim_{\Delta t \to 0} \frac{\mathbb{P}(T \le t + \Delta t | T > t)}{\Delta t}$$
$$= \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} \cdot \frac{1}{R(t)} = \frac{f(t)}{R(t)}$$

• Lorsque  $\Delta t$  est petit

$$\mathbb{P}(T \le t + \Delta t | T > t) \simeq z(t).\Delta t$$



# Taux de défaillance (suite)

On a

$$f(t) = \frac{d}{dt}F(t) = \frac{d}{dt}(1 - R(t)) = -R'(t)$$

■ ďoù

$$z(t) = -\frac{R'(t)}{R(t)} = -\frac{d}{dt} \ln R(t)$$

■ Comme *R(0)*=0, on a

$$\int_0^t z(u)du = -\ln R(t)$$

$$R(t) = \exp\left(-\int_0^t z(u)du\right)$$

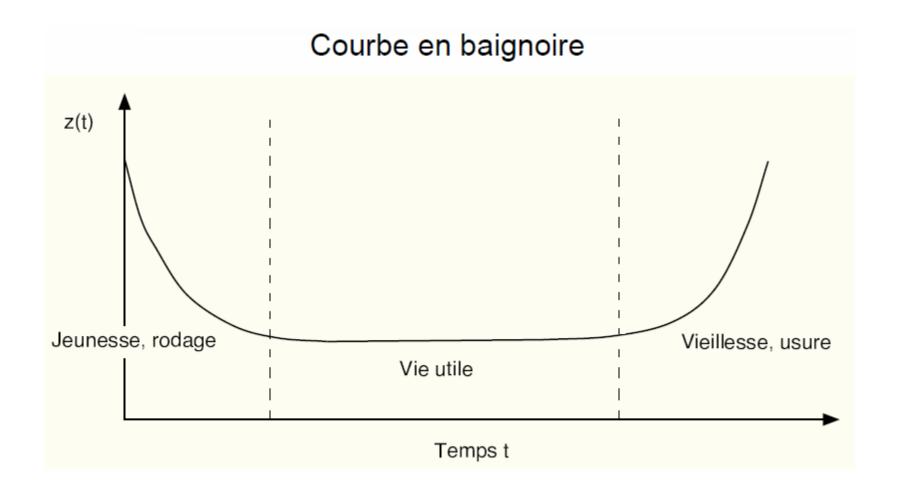
$$f(t) = z(t) \cdot \exp\left(-\int_0^t z(u)du\right)$$
 pour  $t > 0$ 



R(t), F(t), f(t) sont déterminés uniquement par z(t)

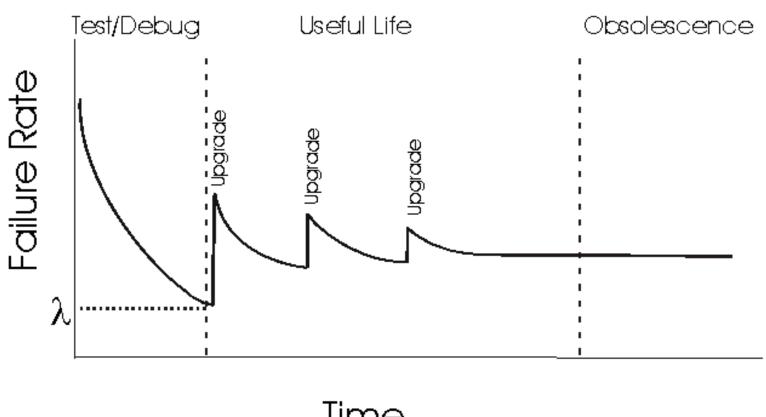


#### Taux de défaillance: matériels





# Taux de défaillance: logiciels





# Temps moyen à la défaillance

Temps moyen à la défaillance d'un système est donné par

$$MTTF = \mathbb{E}(T) = \int_0^\infty t f(t) dt$$

- Comme f(t) = -R'(t), on a donc  $MTTF = -\int_0^\infty tR'(t)dt$ ,
- En intégrant par partie:

$$MTTF = -\left[tR(t)\right]_0^\infty + \int_0^\infty R(t)dt$$

■ Si  $MTTF < \infty$ , on peut montrer que  $-[tR(t)]_0^\infty = 0$  et

$$MTTF = \int_0^\infty R(t)dt$$

#### Duré de vie résiduelle



Un système mis en marche à l'instant t = 0 fonctionne encore à l'instant t. La probabilité que ce système d'âge t fonctionne encore pendant une durée x est

$$R(x|t) = \mathbb{P}(T > x + t|T > t) = \frac{\mathbb{P}(T > x + t)}{\mathbb{P}(T > t)} = \frac{R(x + t)}{R(t)}$$

R(x|t) est la fiabilité conditionnelle du système à la âge t

La durée de vie résiduelle moyenne du système à la âge *t* est

$$MRL(t) = \int_0^\infty R(x|t)dx \quad \textcircled{F} \quad MRL(t) = \frac{1}{R(t)} \int_t^\infty R(x)dx$$

A l'instant initial (t=0), le système est neuf. On a donc:

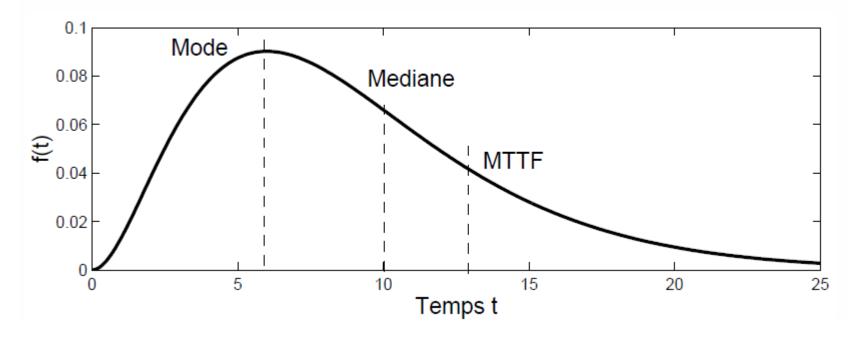
$$MRL(0) = MTTF$$





#### Durée de vie médiane et mode

- La durée de vie médiane  $t_m$  est définie par  $R(t_m) = 0.5$
- Le mode de la loi de durée de vie correspond à la durée de vie la plus probable:  $f(t_{mode}) = \max_{0 \le t \le \infty} f(t)$



• A mémoire:  $MTTF = \mathbb{E}(T) = \int_0^\infty t f(t) dt$ 

## Quelques lois particulières



Densité de probabilité de 
$$\mathit{T:}\quad f(t)=\left\{ egin{array}{ll} \lambda e^{-\lambda t} & \mathrm{pour}\ t>0, \lambda>0 \\ 0 & \mathrm{sinon} \end{array} \right.$$

- Fonction de survie/fiabilité:  $R(t) = \mathbb{P}(T > t) = \int_0^\infty f(u) du = e^{-\lambda t}$
- Moyenne (*MTTF*) et variance de *T*:

$$MTTF = \int_{0}^{\infty} R(t)dt = \frac{1}{\lambda}$$
 et  $var(T) = \frac{1}{\lambda^2}$ 

Taux de défaillance:

$$z(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

Taux de défaillance constant, indépendant du temps

- Fonction de survie conditionnelle:  $R(x|t) = \mathbb{P}(T > t + x|T > t) = \frac{\mathbb{P}(T > t + x)}{\mathbb{P}(T > t)}$   $= \frac{e^{-\lambda(t+x)}}{e^{-\lambda t}} = e^{-\lambda x} = \mathbb{P}(T > x) = R(x)$
- Absence de mémoire : un système qui fonctionne (même depuis longtemps) est aussi bon qu'un système neuf



# Evaluation quantitative de fiabilité au niveau système

- > Terminologies
- Diagramme de fiabilité
- Fonction structure du système
- Méthode 1: Calcul de fiabilité par la fonction de structure
- Méthode 2: Calcul de fiabilité par une chaine de Markov à temps continu



# Systèmes à composants multiples

- Soit un système composé de n indépendants composants
  - La défaillance d'un composant n'affecte pas le comportement des autres composants du système
  - Cette hypothèse n'est souvent pas réaliste, ... mais tellement pratique!

#### Chemin de succès:

- Un chemin de succès est un ensemble de composants qui en fonctionnant tous assurent le fonctionnement du système.
- Un chemin de succès est minimal s'il ne peut pas être réduit sans cesser d'être un chemin de succès.

## Coupes:

- Une coupe est un ensemble de composants qui en devenant tous défaillants entraînent la panne du système.
- Une coupe est minimale si elle ne peut pas être réduite sans cesser d'être une coupe



# **Exemple**

Soit un système suivant

Arrivée des clients

File d'attente 2

Quels sont les chemins de succès, les chemins de succès minimaux ?

Quelles sont les coupes, les coupes minimales ?



## Diagramme de fiabilité

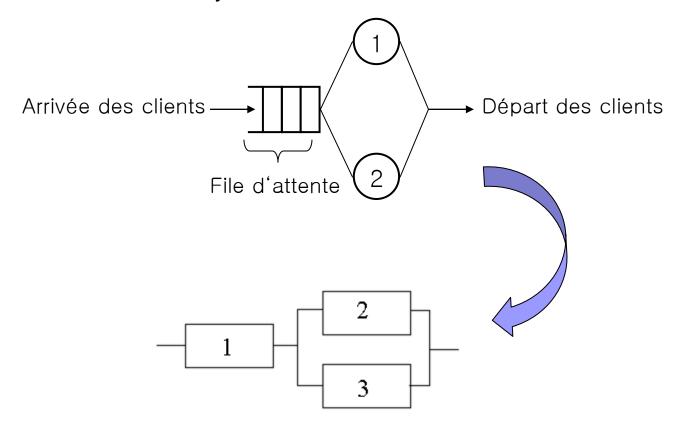
- Une représentation graphique du système et de la fiabilité.
- Chaque composant est représenté par un bloc.
- Sert a déterminer si le système est en marche ou panne en fonction des états de ses composants.
- Idée intuitive : un bloc peut être vu comme un switch qui est fermé quand le composant est en marche et ouvert quand le composant est en panne
- C'est un modèle reposant sur la logique et non pas sur les états.
- Modèle statique: pas de représentation du temps ni de l'ordre entre des évènements successifs.
- Pas de pannes arrivant conjointement ou de pannes provoquées par la panne d'un autre composant.

Le comportement du système par rapport à la panne est modélisé par les connexions entre blocs.



# **Exemple:**

Exemple: considérons un système suivant





#### Variables d'états

- La variable d'état d'un composant i est une variable aléatoire dépendant du temps X<sub>i</sub>(t):
- Le vecteur d'état du système est :  $X(t) = (X_1(t), X_2(t), \dots, X_n(t))$
- L'état du système est donné par  $\phi(X(t))$ :

$$\phi(\mathbf{X}(t)) = \begin{cases} 1 \text{ si système en marche} \\ 0 \text{ si système en panne} \end{cases}$$

Lorsque n composants sont indépendants,  $X_1(t)$ ,  $X_2(t)$ , . . . ,  $X_n(t)$ ) sont donc des variables aléatoires indépendantes

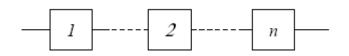
## Fonction de structure





#### Fonction de structures

Structure série:



$$\phi(\mathbf{X}(t)) = \prod_{i=1}^{n} X_i(t)$$

Structure parallèle:

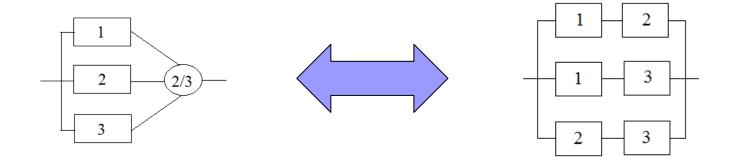
$$\phi(\mathbf{X}(t)) = \prod_{i=1}^{n} X_i(t) = 1 - \prod_{i=1}^{n} (1 - X_i(t))$$

Structure k/n:

$$\widehat{k/n} \longrightarrow \phi(\mathbf{X}(t)) = \begin{cases}
1 \text{ si } \sum_{i=1}^{n} X_i(t) \ge k \\
0 \text{ si } \sum_{i=1}^{n} X_i(t) < k
\end{cases}$$



# Exemple: système 2/3



Fonction de structure:

$$\phi(\mathbf{X}(t)) = X_1(t)X_2(t) + X_1(t)X_3(t) + X_2(t)X_3(t) - 2X_1(t)X_2(t)X_3(t)$$

# Méthode 1: Calcul de fiabilité par fonction de structure

# re.

#### Calcul direct à partir de la fonction de structure

#### Probabilité de fonctionnement

Probabilité de fonctionnement du composant i à l'instant t.

$$p_i(t) = \mathbb{P}(X_i(t) = 1) = \mathbb{E}[X_i(t)] =$$
  
=  $0.\mathbb{P}(X_i(t) = 0) + 1.\mathbb{P}(X_i(t) = 1)$ 

Probabilité de fonctionnement du système à l'instant t.

$$p_s(t) = \mathbb{P}(\phi(\mathbf{X}(t)) = 1) = \mathbb{E}[\phi(\mathbf{X}(t))]$$
$$= 0.\mathbb{P}(\phi(\mathbf{X}(t)) = 0) + 1.\mathbb{P}(\phi(\mathbf{X}(t)) = 1)$$

Sous l'hypothèse d'indépendance,  $p_s(t)$  est une fonction des  $p_i(t)$  seuls:

$$p_s(t) = h(\mathbf{p}(t)) = h(p_1(t), p_2(t), \dots, p_n(t))$$

# M

#### Calcul direct à partir de la fonction de structure

# Probabilité de fonctionnement (suite)

Structure série:

$$h(\mathbf{p}(t)) = \mathbb{E}\left[\int_{i=1}^{n} X_i(t)\right]$$
$$= \prod_{i=1}^{n} \mathbb{E}\left[X_i(t)\right] = \prod_{i=1}^{n} p_i(t)$$

Structure parallèle:

$$h(\mathbf{p}(t)) = \mathbb{E}[\phi(\mathbf{X}(t))] = 1 - \prod_{i=1}^{n} (1 - \mathbb{E}[X_i(t)])$$
$$= 1 - \prod_{i=1}^{n} (1 - p_i(t))$$

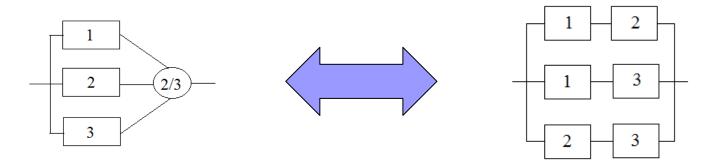
■ Structure k/n (cas n composants sont identiques,  $p_i(t) = p(t) \ \forall \ i = 1 ... n$ ):

$$p_s(t) = \sum_{y=k}^{n} C_n^y p(t)^y (1 - p(t))^{n-y}$$



#### Calcul direct à partir de la fonction de structure

# Exemple: système 2/3



Fonction de structure:

$$\phi(\mathbf{X}(t)) = X_1(t)X_2(t) + X_1(t)X_3(t) + X_2(t)X_3(t) - 2X_1(t)X_2(t)X_3(t)$$

Fiabilité du système:

$$R_s(t) =$$

- Si les composants sont identiques et le taux de défaillance est constant
  - Fiabilité:

$$R_s(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

> MTTF:

$$MTTF = \int_0^\infty R_s(t)dt = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda}$$



Calcul de fiabilité par une chaîne de Markov à temps continu

#### Evaluation par processus de Markov

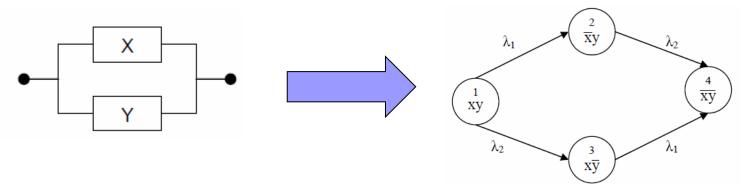


- Identification des "états" du système ou de ses composants: états nominaux, états dégradés, états de panne
- Discrétisation des états du système:
  - $E = \bigcup_i \{e_i\}$  = Espace des états du système
  - L'état du système à l'instant *t* est une variable aléatoire
- Description basée sur les probabilités d'occupation  $P_i(t)$  des états  $e_i$  et des transitions entre états  $P_{ij}(t)$  (de l'état  $e_i$  vers  $e_j$ :
  - > construction d'un graphe des états du système
  - construction d'équations d'état du système
- Avantages de l'approche markovienne: systèmes à composants dépendants
- Inconvénients:
  - assez compliqué à mettre en place
  - taux de défaillance constants



# **Exemple 1:**

 Un système non réparable de 2 composants (X, Y) en parallèle (le taux de défaillance λ1, λ2)



- Les états du système:
  - L'état 1 : tous les composants sont en marches et le système est en marche
  - L'état 2,3 : un composant est défaillant et le système est en marche
  - L'état 4 : tous les composants sont défaillants et le système est en panne

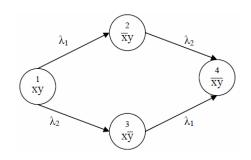




# Exemple 1:

Matrice des taux de transition

$$\mathbf{M} = \begin{bmatrix} -(\lambda_1 + \lambda_2) & 0 & 0 & 0 \\ \lambda_1 & -\lambda_2 & 0 & 0 \\ \lambda_2 & 0 & -\lambda_1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$



Equations de Chapman-Kolmogorov

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{P}(t)\mathbf{M},$$

Solution:

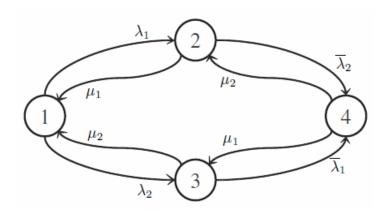
$$\begin{cases} \mathbf{P}_{1}(t) = e^{-(\lambda_{1} + \lambda_{2})t} \\ \mathbf{P}_{2}(t) = e^{-\lambda_{2}t} - e^{-(\lambda_{1} + \lambda_{2})t} \\ \mathbf{P}_{3}(t) = e^{-\lambda_{1}t} - e^{-(\lambda_{1} + \lambda_{2})t} \\ \mathbf{P}_{4}(t) = 1 - \mathbf{P}_{1}(t) + \mathbf{P}_{2}(t) + \mathbf{P}_{3}(t) \end{cases}$$

Fiabilité du système: 
$$\mathbf{R}(t) = \mathbf{P}_1(t) + \mathbf{P}_2(t) + \mathbf{P}_3(t)$$



# **Exemple 2: Partage de charge**

- Considérons un système formé de 2 composants élémentaires C1 et C2 en parallèle.
  - Le taux de réparation du composant Ci est  $\mu_i$ . Le taux de défaillance du composant Ci est  $\lambda_i$  en fonctionnement normal (c'est-à-dire si l'autre composant est en fonctionnement).
  - Par contre si un composant est en réparation, le composant restant est plus "sollicité" et son taux de défaillance est  $\overline{\lambda_i}$  ( $\overline{\lambda_i} > \lambda_i$ )
- Graphe de transition:



Disponibilité:

$$\mathbf{R}(t) = \mathbf{P}_1(t) + \mathbf{P}_2(t) + \mathbf{P}_3(t)$$

# w

## Proposition d'actions en réduction de défaillance

# Corrective

- Diminution du MTTR
- Meilleure gestion des pièces de rechange
- □ Développement d'un systèm

е

d'aide au diagnostic

# Préventive

- Optimisation des opérations de maintenance préventive
- ☐ Mise en oeuvre de nouvelles opérations



# **Prédictive**

- □ Augmentation de la SdF
- □ Augmentation du MTBF
- Amélioration de la sécurité des opérateurs



# Optimiser et développer la maintenance

# Prognostics & Health Management

