

# Sûreté de Fonctionnement des systèmes informatiques

Walter SCHÖN

## Sûreté de Fonctionnement des systèmes informatiques

Évaluation quantitative des attributs de sûreté de fonctionnement  
(Évaluation ordinaire ou probabiliste de la Prévision des fautes)

# Évaluation probabiliste de la SdF : APR

3

- L'APR, comporte un volet **quantitatif** (taux d'occurrence : probabilité de l'événement indésirable par heure de fonctionnement du système).
- Ces valeurs sont **préliminaires** et sont en général des **objectifs**, dont l'atteinte devra être démontrée par les études détaillées.
- L'APR joue de ce point de vue le rôle d'outil **d'allocation des objectifs** et de **journal des situations dangereuses (Hazard Log)** : elles sont complétées en aval des études par les valeurs effectivement atteintes et les références des documents où figurent les calculs détaillés.

# Évaluation probabiliste de la SdF : AMDEC

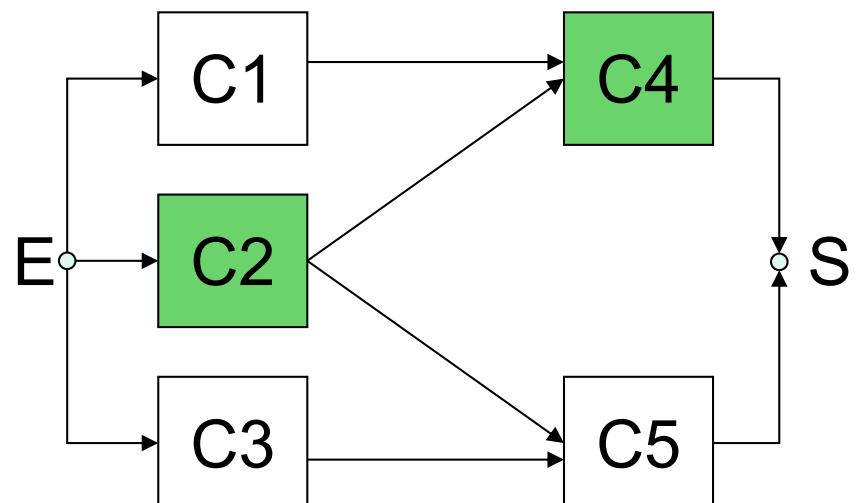
4

- Les valeurs de taux d'occurrence portées dans l'**AMDEC** sont précises (issues de bases de données de fiabilité ou de Retour d'Expérience).
- Il est donc théoriquement possible d'obtenir le taux d'occurrence de l'ensemble des scénarios AMDEC conduisant à des conséquences données.
- Mais la **limitation de l'AMDEC aux défaillances simples** rend l'exercice sans grand intérêt pratique
- Les évaluations probabilistes reposent donc de fait sur les diagrammes de succès, arbres de causes ou graphes de Markov.

# Diagrammes de fiabilité : chemins de succès et liens minimaux

5

- Chemin de succès : un ensemble de blocs rencontrés entre l'entrée et la sortie d'un diagramme.
  - Lien : un ensemble de blocs dont le bon fonctionnement assure le fonctionnement du système
  - Lien minimal : lien ne contenant aucun autre lien.
- Sauf en cas de blocs répétés (déconseillé en diagrammes de fiabilité) : Lien minimal  $\Leftrightarrow$  Chemin de succès.

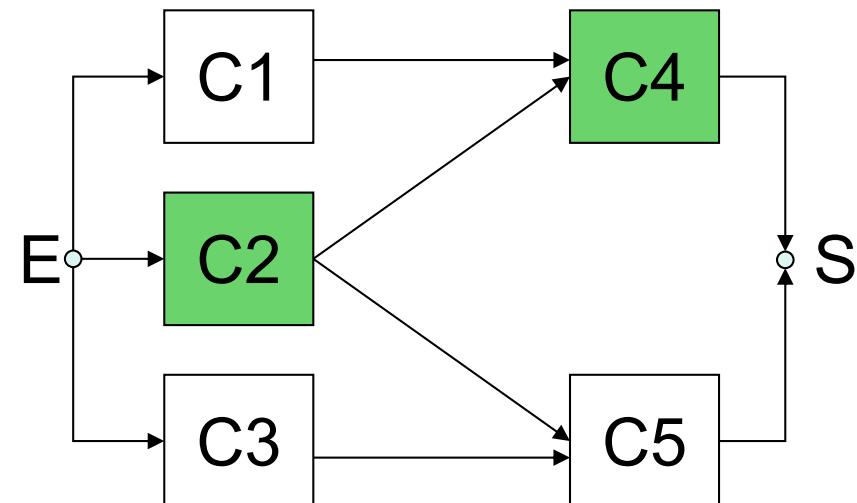


# Chemins de succès et liens minimaux

6

- La liste exhaustive des liens minimaux s'obtient alors par recherche de tous les chemins possibles. Notant simplement Ci l'événement bon fonctionnement du composant Ci, les liens minimaux sont dans l'exemple :

C1.C4  
C2.C4  
C2.C5,  
C3.C5



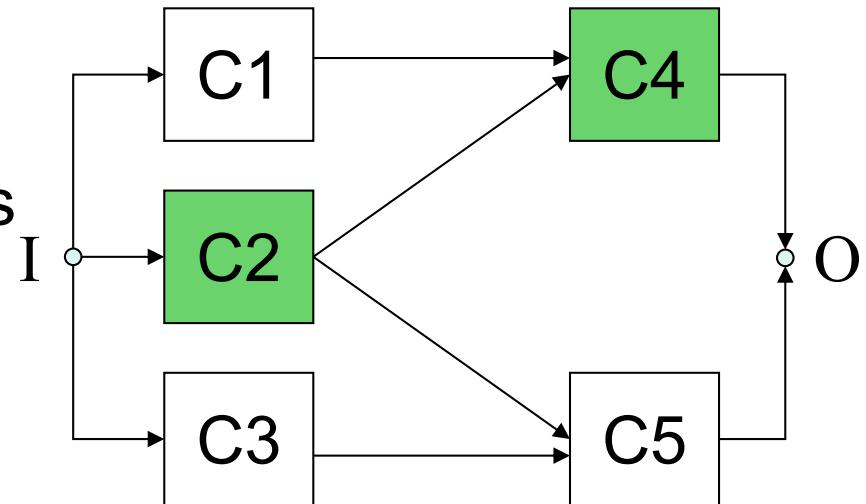
# Fonction Booléenne de succès

7

En notant  $S$  (resp.  $C_i$ ) une variable Booléenne indiquant que le système (resp. le composant  $C_i$ ) fonctionne sur  $[0, t]$  nous avons donc :

$$S = C_1 \cdot C_4 + C_2 \cdot C_4 + C_2 \cdot C_5 + C_3 \cdot C_5$$

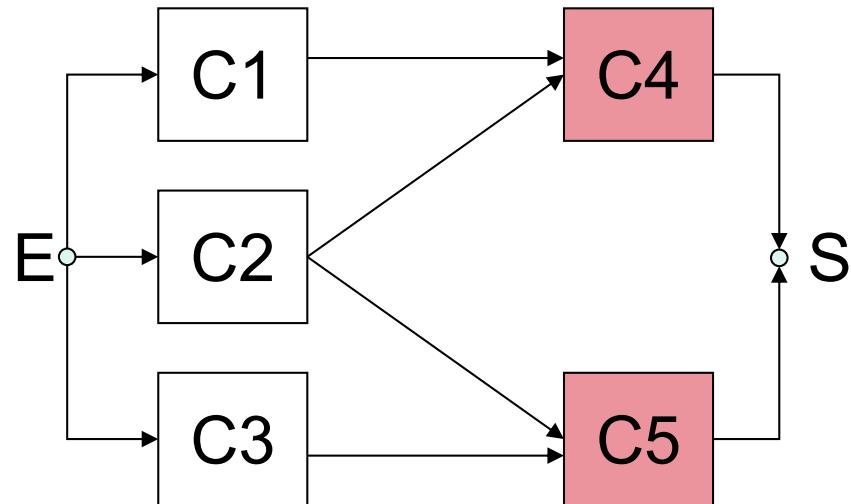
Cette fonction Booléenne de variables Booléennes sous forme de « somme de produits minimaux » (OU des chemins minimaux) est appelée la **fonction Booléenne de succès du système**



# Diagrammes de fiabilité : coupes minimales

8

- Coupe : un ensemble de blocs dont le dysfonctionnement entraîne le dysfonctionnement du système (il « coupe » donc tous les chemins de succès).
- Coupe minimale : coupe ne contenant aucune autre coupe.
- Ordre d'une coupe minimale : nombre de blocs de la coupe (ici une coupe minimale d'ordre 2).
- Les coupes minimales d'ordre le plus bas sont les éventuels « points faibles » du système.

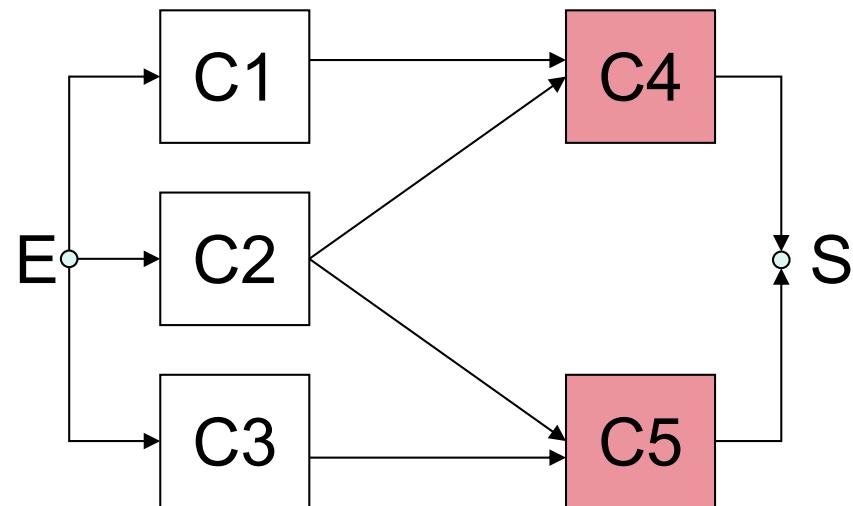


# Coupes minimales

9

- Sur les diagrammes simples, la liste exhaustive des coupes minimales s'obtient graphiquement par « lecture du diagramme ».
- Notant ici  $\overline{C_i}$  l'événement défaillance du composant i, les coupes minimales sont dans l'exemple :

$$\begin{array}{l} \overline{C_1}.\overline{C_2}.\overline{C_3} \\ \overline{C_4}.\overline{C_5} \\ \overline{C_1}.\overline{C_2}.\overline{C_5} \\ \overline{C_2}.\overline{C_3}.\overline{C_4} \end{array}$$



# Fonction Booléenne d'échec

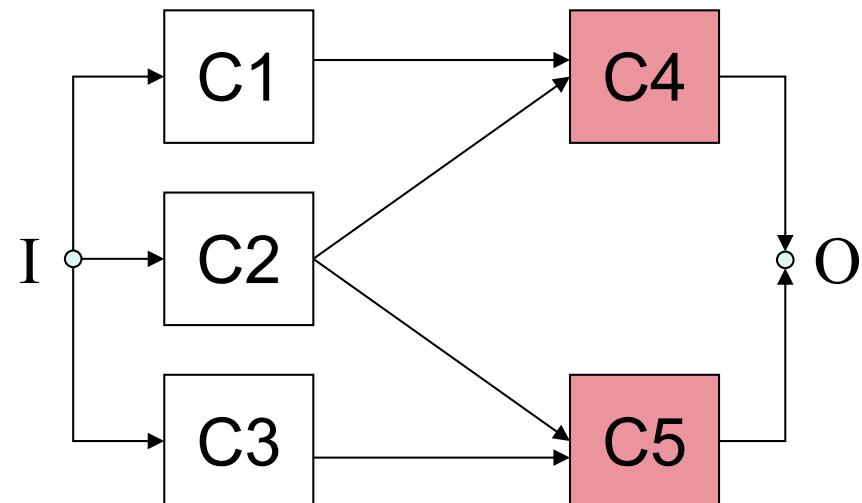
10

Notant  $\bar{S}$  une variable Booléenne indiquant que le système défaillle sur  $[0,t]$  nous avons donc :

$$\bar{S} = \overline{C_1 \cdot C_2 \cdot C_3} + \overline{C_4 \cdot C_5} + \overline{C_1 \cdot C_2 \cdot C_5} + \overline{C_2 \cdot C_3 \cdot C_4}$$

Cette fonction Booléenne « somme de produits minimaux » (OU des coupes minimales) est appelée **fonction d'échec du système**.

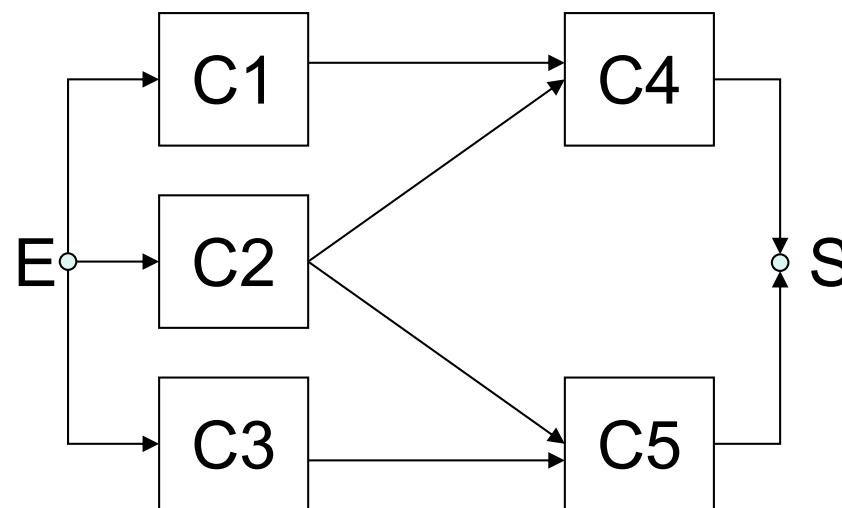
Bien sûr la fonction d'échec est le NOT Booléen de la fonction de succès ce qu'on pourrait vérifier par calcul algébrique.



# Coupes minimales : Recherche automatique

11

- Exemple ( très simple) d'algorithme facilement programmable :
- Première étape : recherche de tous les liens minimaux par parcours exhaustif de tous les chemins et construction d'une matrice d'incidence des blocs dans les liens :

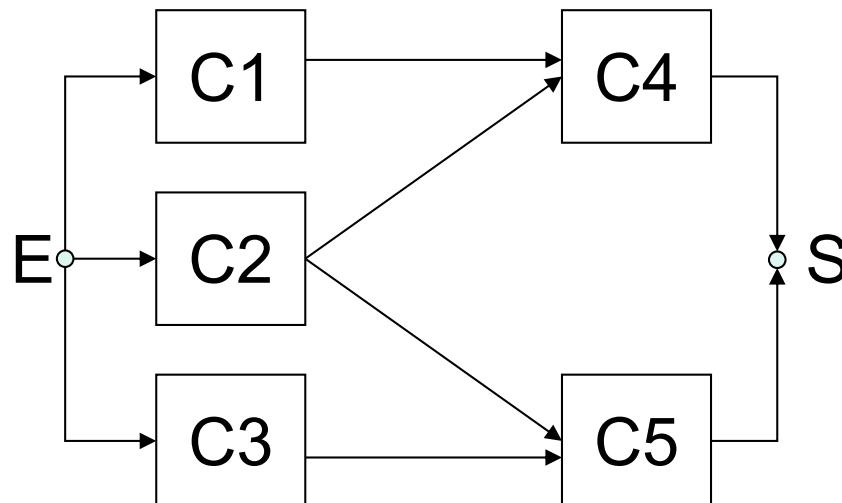


	C1	C2	C3	C4	C5
L1	1	0	0	1	0
L2	0	1	0	1	0
L3	0	1	0	0	1
L4	0	0	1	0	1

# Coupes minimales : recherche automatique

12

- Sur cette matrice, construite en lignes, on recherche d'éventuelles colonnes ne comportant que des 1.
- S'il y en a elles correspondent à des blocs figurant dans tous les liens donc coupes (forcément minimales) d'ordre 1 : dans l'exemple il n'y a pas de coupes d'ordre 1.



	C1	C2	C3	C4	C5
L1	1	0	0	1	0
L2	0	1	0	1	0
L3	0	1	0	0	1
L4	0	0	1	0	1

# Coupes minimales : recherche automatique

13

- On combine alors (en OU Booléen) les colonnes deux à deux, en éliminant les éventuelles colonnes identifiées comme coupe d'ordre 1 (qui ne donneraient que des surcoupes).
- Toute colonne ne comportant que des 1 correspond à des combinaisons figurant dans tous les liens (donc des coupes d'ordre 2, minimales puisqu'on a éliminé les coupes d'ordre 1)

1	2	3	4	5
1	0	0	1	0
0	1	0	1	0
0	1	0	0	1
0	0	1	0	1

12	13	14	15	23	24	25	34	35	45
1	1	1	1	0	1	0	1	0	1
1	0	1	0	1	1	1	1	0	1
1	0	0	1	1	1	1	0	1	1
0	1	0	1	1	0	1	1	1	1

# Coupes minimales : recherche automatique

14.

- Puis combinaisons de trois colonnes en éliminant les surcoupes des coupes d'ordres 1 et 2 (ici 145, 245 et 345)

1	2	3	4	5
1	0	0	1	0
0	1	0	1	0
0	1	0	0	1
0	0	1	0	1

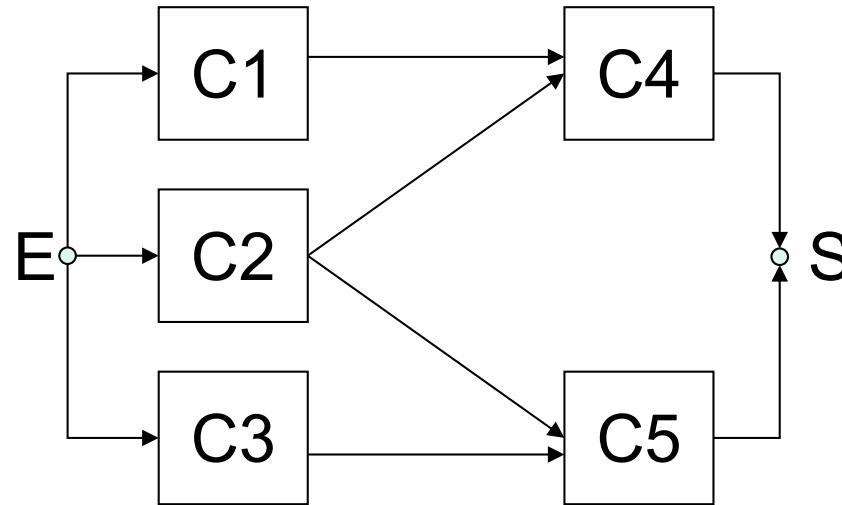
12	13	14	15	23	24	25	34	35	45
1	1	1	1	0	1	0	1	0	1
1	0	1	0	1	1	1	1	0	1
1	0	0	1	1	1	1	0	1	1
0	1	0	1	1	0	1	1	1	1

123	124	125	134	135	234	235
1	1	1	1	1	1	0
1	1	1	1	0	1	1
1	1	1	0	1	1	1
1	0	1	1	1	1	1

➤ On poursuit si nécessaire jusqu'aux combinaisons à N colonnes (ici toute combinaison à 4 est une surcoupe d'une coupe déjà identifiée)

# Coupes minimales : recherche automatique

15



12	13	14	15	23	24	25	34	35	45
1	1	1	1	0	1	0	1	0	1
1	0	1	0	1	1	1	1	0	1
1	0	0	1	1	1	1	0	1	1
0	1	0	1	1	0	1	1	1	1

123	124	125	134	135	234	235
1	1	1	1	1	1	0
1	1	1	1	0	1	1
1	1	1	0	1	1	1
1	0	1	1	1	1	1

# Arbres de causes et coupes minimales

16

Le traitement quantitatif des arbres de causes passe également par la recherche des coupes minimales (cas des arbres ne comportant que des portes ET et OU : si d'autres portes sont présentes des méthodes spécifiques doivent être mises en œuvre) :

- Une variable booléenne est associée à chaque événement.
- On recherche de proche en proche l'expression de l'événement sommet en fonction des événements de base.
- Comme l'arbre ne contient que des ET (« produits ») et des OU (« sommes »), le résultat est forcément une expression polynomiale que l'on développe entièrement.

# Arbres de causes et coupes minimales

17

- Après développement on obtient donc une somme de monômes (OU de ET) dont chacun est évidemment une coupe (comme ils sont en OU chacun d'eux est suffisant pour provoquer l'événement sommet).
- Ces coupes ne sont toutefois pas minimales : reste à les réduire par les règles d'absorption booléennes :

$$A + B = A \text{ si } B \subseteq A$$

$$A \cdot B = B \text{ si } B \subseteq A$$

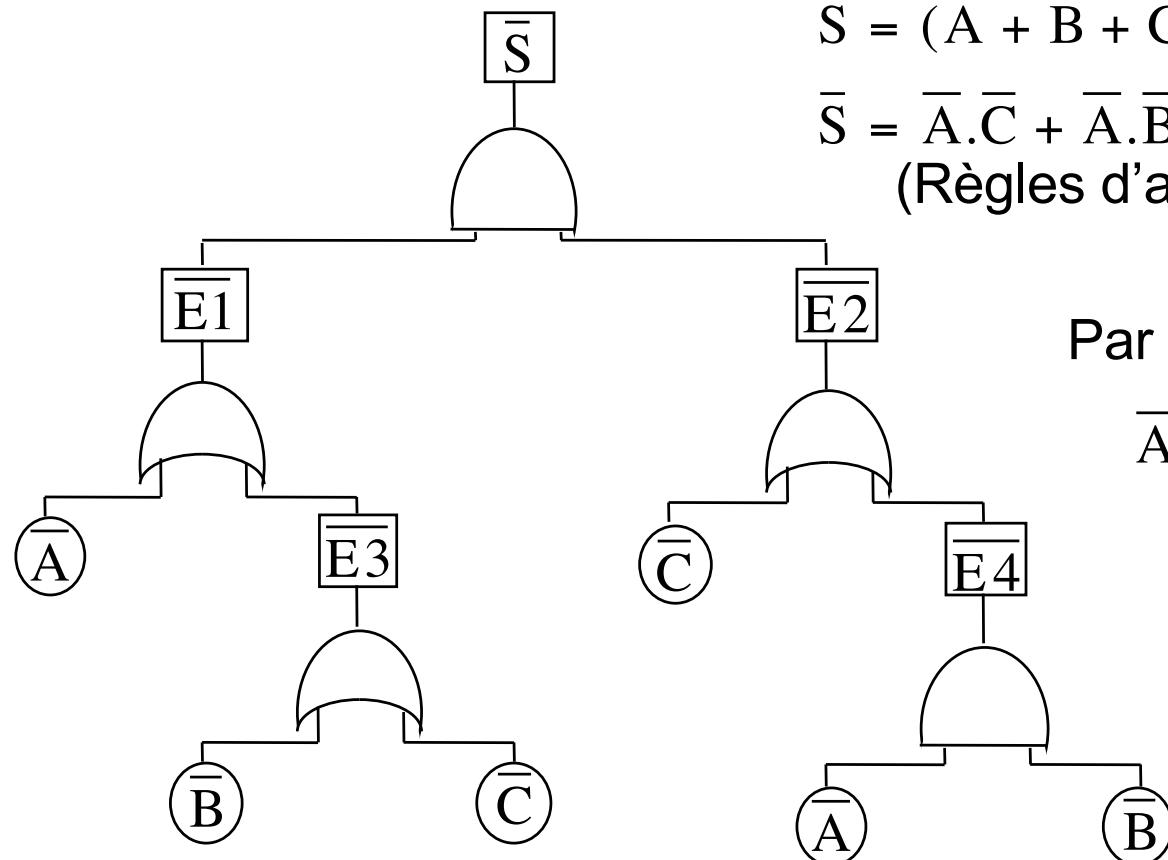


- L'expression finale est sous la forme :  $F = C_1 + C_2 + \dots + C_n$  où les  $C_i$  sont les coupes minimales.
- Chaque  $C_i$  est un ET d'événements de base :  $C_i = B_i^1 \cdot B_i^2 \cdots B_i^{n_i}$
- $n_i$  est l'ordre de la coupe minimale  $C_i$

# Arbres de causes et coupes minimales : exemple

18

Considérons l'arbre suivant:



$$\bar{S} = \bar{E}_1 \cdot \bar{E}_2 = (\bar{A} + \bar{E}_3) \cdot (\bar{C} + \bar{E}_4)$$

$$\bar{S} = (\bar{A} + \bar{B} + \bar{C}) \cdot (\bar{C} + \bar{A} \cdot \bar{B})$$

$$\begin{aligned} \bar{S} &= \bar{A} \cdot \bar{C} + \bar{A} \cdot \bar{B} + \bar{B} \cdot \bar{C} + \bar{A} \cdot \bar{B} + \bar{C} + \bar{A} \cdot \bar{B} \cdot \bar{C} \\ &\text{(Règles d'absorption } \bar{A} \cdot \bar{A} = \bar{A} \text{ etc.)} \end{aligned}$$

Par application des règles

$$\bar{A} \cdot \bar{B} + \bar{A} \cdot \bar{B} = \bar{A} \cdot \bar{B}$$

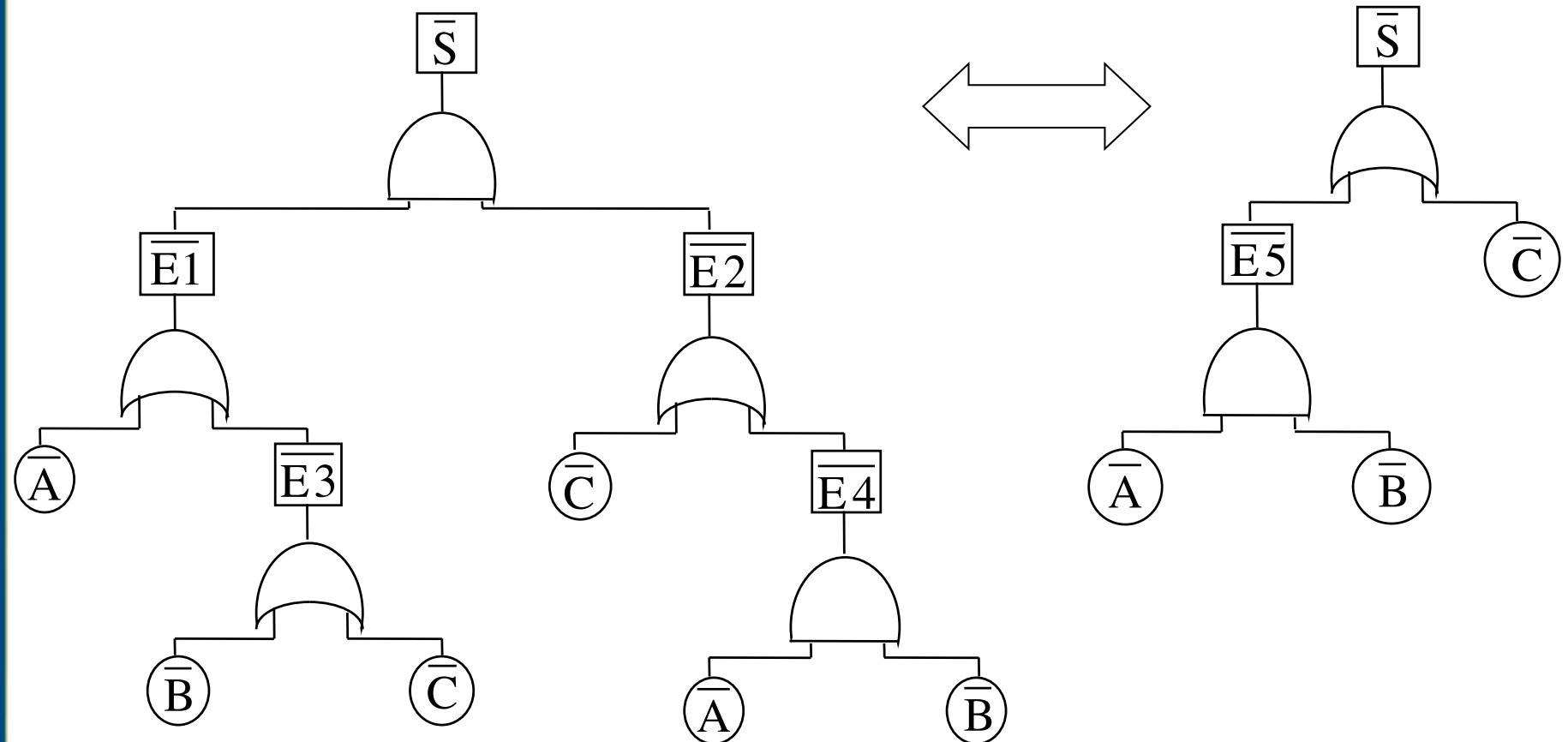
$$\bar{C} + \bar{A} \cdot \bar{C} = \bar{C} \quad \text{etc.}$$

$$\boxed{\bar{S} = \bar{A} \cdot \bar{B} + \bar{C}}$$

# Arbres de causes et coupes minimales : exemple

19

Par conséquent les deux arbres suivants sont équivalents :



# Utilisation des liens et coupes minimales

20

Outre leur intérêt qualitatif les liens et coupes minimales permettent les calculs de fiabilité dans le cas le plus général. En effet :

- Pas de défaillance sur  $[0,t]$   $\Leftrightarrow$  Au moins un lien minimal n'a pas de défaillance sur  $[0,t]$  soit en notations abrégées :  
 $R(t) = \text{Proba}(\text{OU(liens mini opérationnels)})$
- Défaillance sur  $[0,t]$   $\Leftrightarrow$  Au moins une coupe minimale a une défaillance sur  $[0,t]$  soit en notations abrégées :  
 $1-R(t) = \text{Proba}(\text{OU(coupes mini défaillantes)})$

# Liens et coupes minimales : calculs de fiabilité

21

- Selon les diagrammes l'une des deux méthodes précédentes est en général plus simple que l'autre.
- On développe alors la probabilité des OU de liens ou de coupes par le théorème de Poincaré :

$$P\left(\sum_i E_i\right) = \sum_i P(E_i) - \sum_{i \neq j} P(E_i \cdot E_j) + \sum_{i \neq j \neq k} P(E_i \cdot E_j \cdot E_k) + \dots + (-1)^{n+1} P\left(\prod_i E_i\right)$$

- Enfin **si les composants sont indépendants**, les probabilités des ET d'événements sont les produits des probabilités des événements élémentaires, ce qui fournit dans le cas général l'expression de la fiabilité (ou de la défiabilité) du diagramme en fonction des fiabilités (ou défiabilités) des composants.

# Chiffrage des arbres de causes

22

La méthode précédente est **systématique** pour le chiffrage des arbres de causes :

- La construction d'un arbre de causes par un expert est un processus intellectuel complexe qui conduit en général à des **arbres non réduits** (événements répétés dans l'arbre).
- La recherche des coupes minimales est donc **obligatoire**. Tenter de chiffrer directement sur l'arbre conduirait à considérer comme indépendants des événements qui ne le sont pas.
- Des approximations sont ensuite souvent utilisées pour limiter le nombre de combinaisons de coupes à prendre en compte.
- Pour les diagrammes de succès (répétition de blocs **déconseillée**) il existe des méthodes de chiffrages plus simples.

# Diagrammes de fiabilité : Exemple 1

23

Chemins de succès :

C1.C2, C3.C4

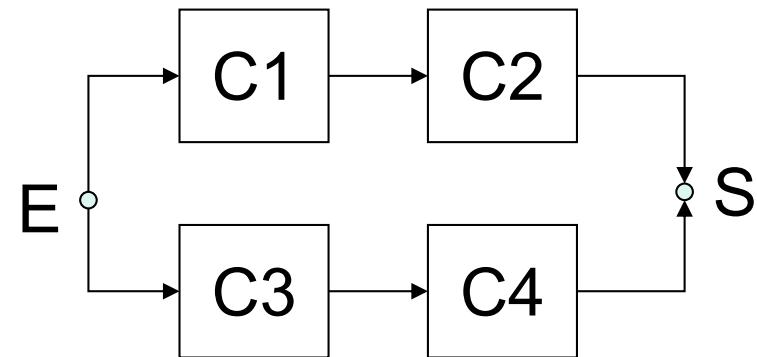
Coupes minimales :

$\overline{C1.C3}, \overline{C2.C4}, \overline{C1.C4}, \overline{C2.C3}$

$$R(t) = P(C1.C2 + C3.C4) = P(C1.C2) + P(C3.C4) - P(C1.C2.C3.C4)$$

$$R(t) = r_1.r_2 + r_3.r_4 - r_1.r_2.r_3.r_4$$

(si les composants sont indépendants)



# Diagrammes de fiabilité : Exemple 2

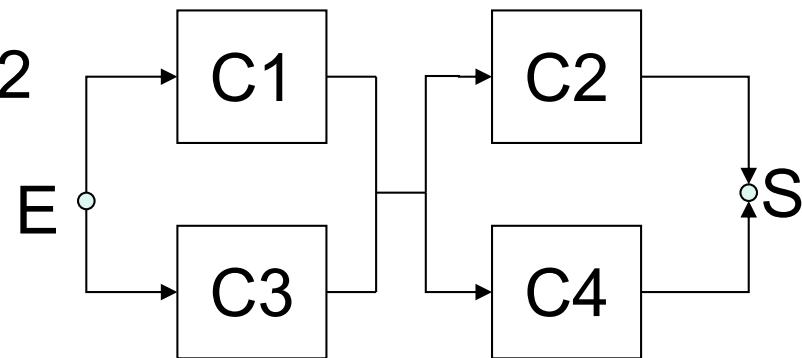
24

Chemins de succès :

C1.C2, C3.C4, C1.C4, C3.C2

Coupes minimales

$\overline{C1.C3}, \overline{C2.C4}$



$$1 - R(t) = P(\overline{C1.C3} + \overline{C2.C4})$$

$$1 - R(t) = (1 - r_1) \cdot (1 - r_3) + (1 - r_2) \cdot (1 - r_4) - (1 - r_1) \cdot (1 - r_3) \cdot (1 - r_2) \cdot (1 - r_4)$$

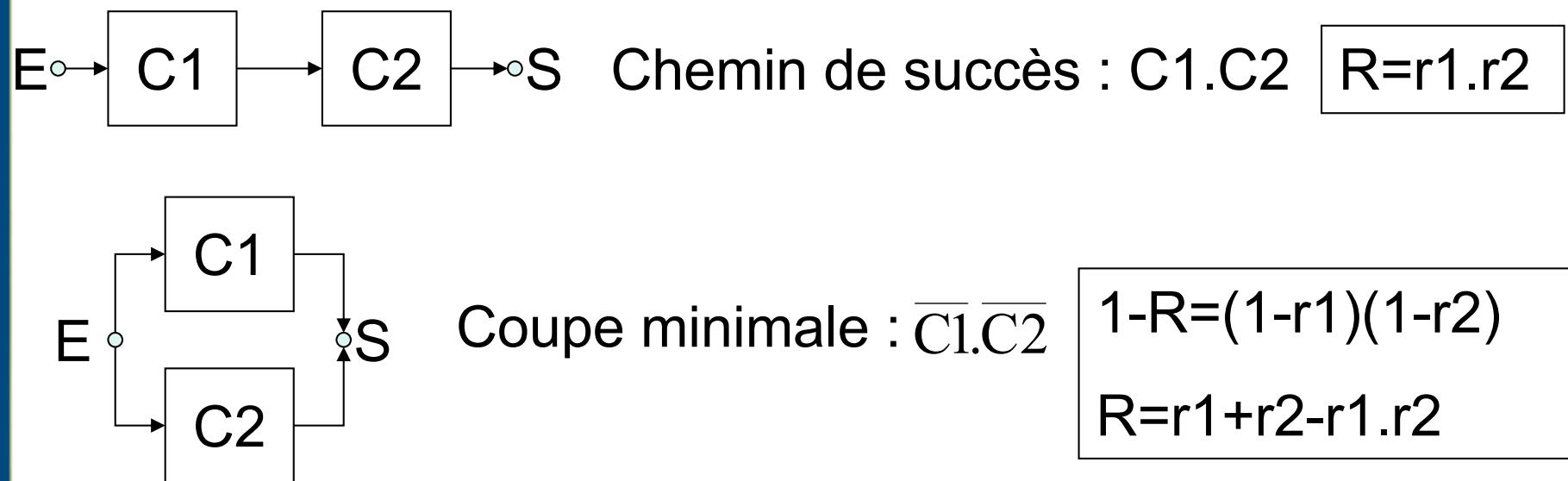
(si les composants sont indépendants)

# Calculs de fiabilité : Exemple 3

25

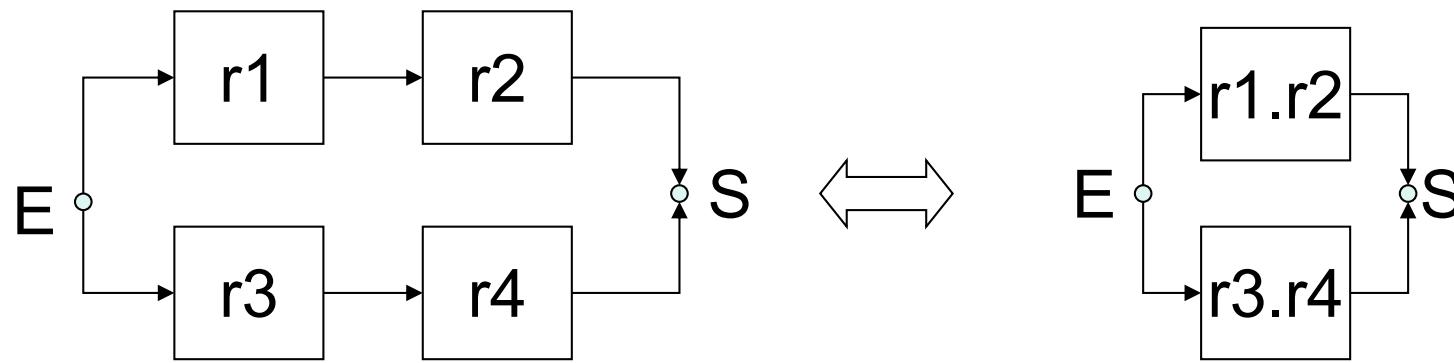
La méthode précédente est absolument générale et applicable à tous les types de diagrammes y compris complexes.

Pour les diagrammes série-parallèle et parallèle-série toutefois, une méthode directe plus simple est applicable. Commençons par deux résultats intermédiaires :



# Diagrammes de fiabilité : Exemple 4

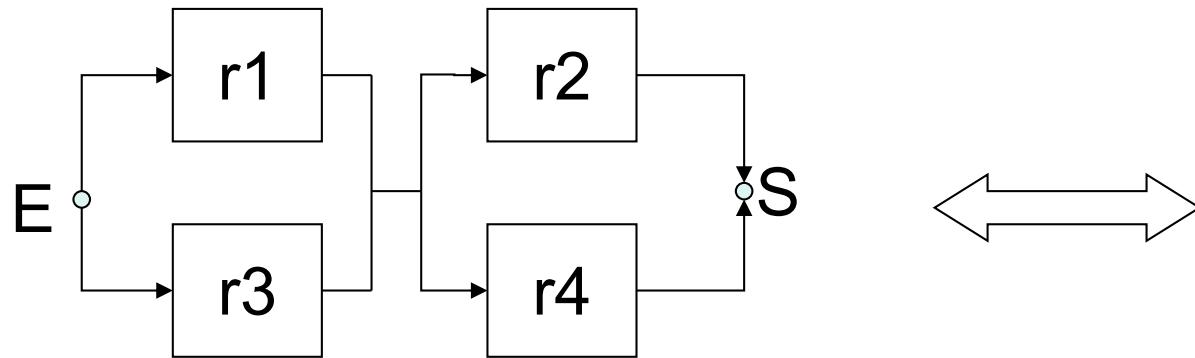
26



$$1-R(t)=(1-r_1.r2)(1-r_3.r4)$$

# Diagrammes de fiabilité : Exemple 5

27



$$E \rightarrow [1 - (1 - r_1)(1 - r_3)] \rightarrow [1 - (1 - r_2)(1 - r_4)] \rightarrow S$$

$$R(t) = [1 - (1 - r_1) \cdot (1 - r_3)][1 - (1 - r_2) \cdot (1 - r_4)]$$

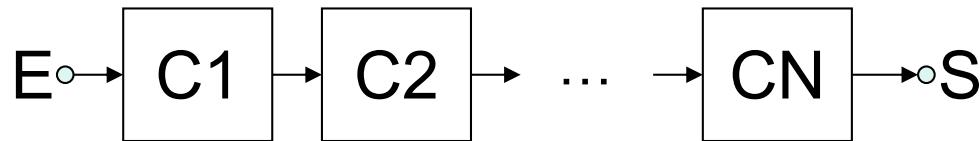
# Fiabilité des systèmes non réparables

28

- Tout ce qui précède suppose l'**indépendance des composants**.  
La fiabilité des systèmes réparables introduisant une dépendance nécessite un traitement spécifique (graphe de Markov ou autre).
- On traite donc dans cette partie la fiabilité des systèmes non réparables à composants indépendants :
  - Systèmes série
  - Systèmes parallèle à redondance active
  - Systèmes à voteur p/n
  - Combinaisons série-parallèle et parallèle série
  - Systèmes complexes (utilisation du théorème des probabilités totales)
  - Redondance passive (traitement spécifique car problème à composants dépendants)

# Systèmes série

29

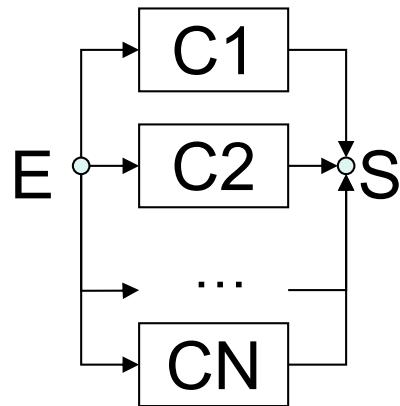


- Un seul lien minimal
- Proba(pas de défaillance sur [0,t])= Proba(tous composants sans défaillance sur [0,t])

$$R(t) = \prod_{i=1}^N r_i$$

➤ En série les fiabilités des composants se multiplient

# Redondance active



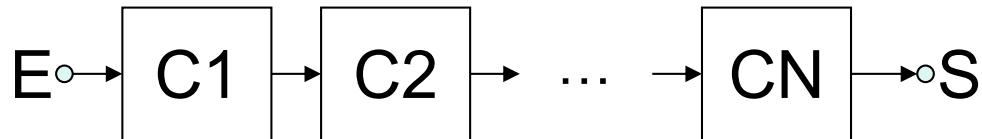
- Une seule coupe minimale
- Proba(défaillance sur  $[0,t]$ ) =  
Proba(tous composants défaillants sur  $[0,t]$ )

$$1 - R(t) = \prod_{i=1}^N (1 - r_i)$$

- En parallèle les défiabilités des composants se multiplient

# Systèmes série : taux de défaillance constants

31

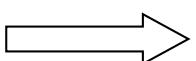


$$R(t) = \prod_{i=1}^N r_i$$

(formule générale)

- Si de plus les taux de défaillance  $\lambda_i$  des composants sont constants :

$$r_i(t) = e^{-\lambda_i t}$$



$$R(t) = e^{-\lambda_{\text{système}} t}$$

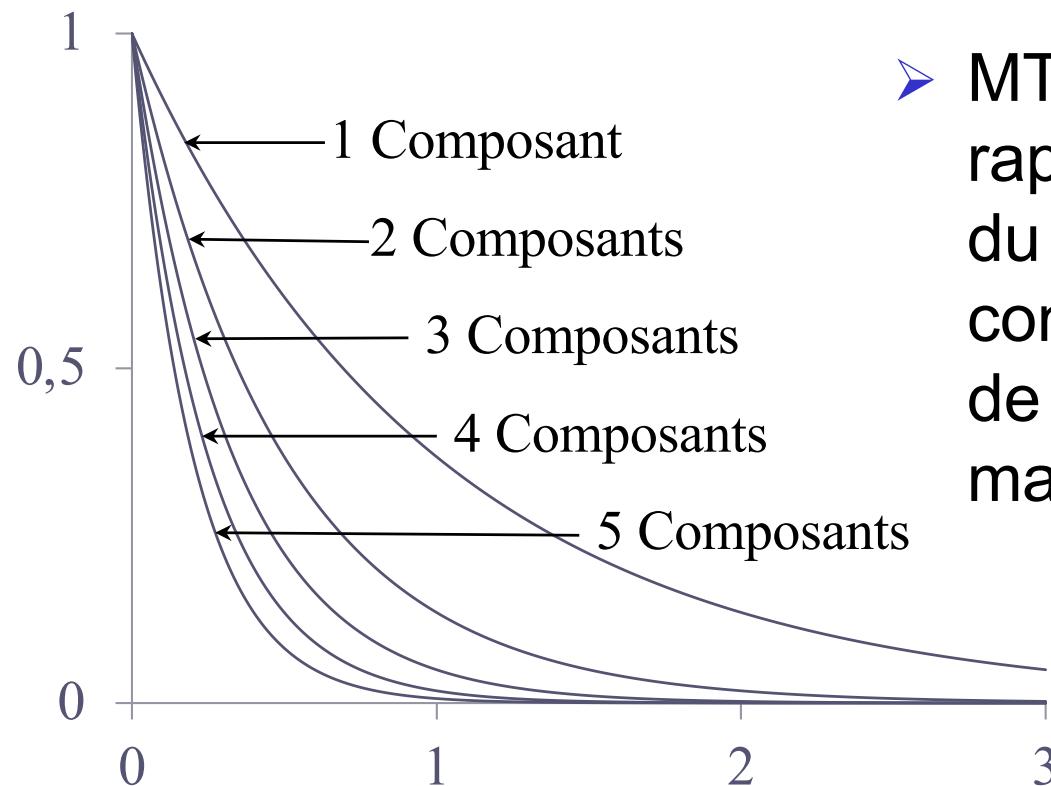
$$\text{ où } \lambda_{\text{système}} = \sum_i \lambda_i$$

- Un système série dont les tous les composants ont un  $\lambda$  constant a également un  $\lambda$  constant qui vaut la somme des  $\lambda$  des composants

# Systèmes série : taux de défaillance constants

32

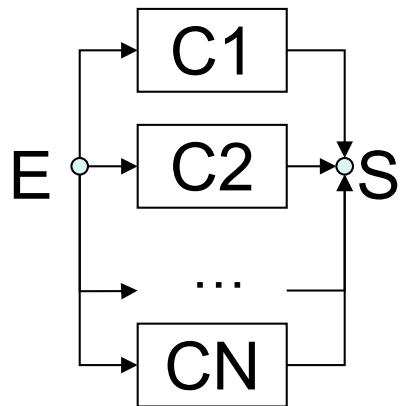
- La figure suivante illustre le cas de N composants identiques de même taux de défaillance constant  $\lambda$  pour N variant de 1 à 5 :



- $MTTF = 1/N\lambda$  décroît rapidement en fonction du nombre de composants (se souvenir de la fausse analogie du maillon faible)

# Redondance active : taux de défaillance constants

33



$$1 - R(t) = \prod_{i=1}^N (1 - r_i)$$

(formule générale)

- Si de plus les taux de défaillance  $\lambda_i$  des composants sont constants :

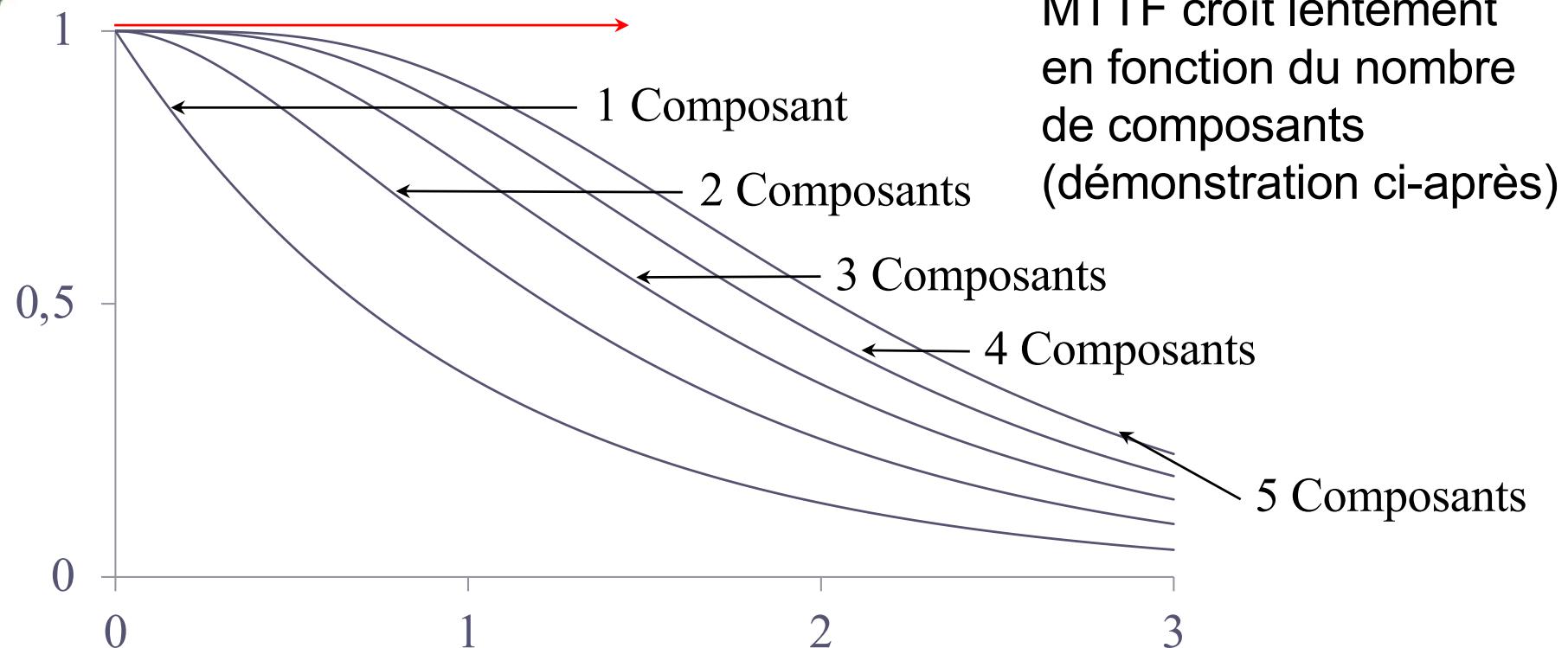
$$r_i(t) = e^{-\lambda_i t}$$

- $R(t)$  n'est plus une exponentielle décroissante => le taux de défaillance global du système **n'est plus constant**.
- Par conséquent : l'assemblage en parallèle de composants qui ne vieillissent pas donne un système qui vieillit !!!!!!

# Redondance active : taux de défaillance constants

34

La figure suivante illustre le cas de  $N$  composants identiques de même taux de défaillance constant  $\lambda$  pour  $N$  variant de 1 à 5 :



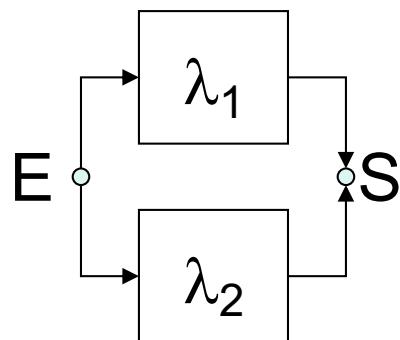
MTTF croît lentement  
en fonction du nombre  
de composants  
(démonstration ci-après)

A partir de  $N=2$  (véritable redondance) la décroissance de la fiabilité n'est plus exponentielle. En particulier la tangente à  $t=0$  est horizontale **propriété fondamentale des systèmes redondants** démontrée ci-après.

# Redondance active : taux de défaillance constants

35

Afin de mieux comprendre ce phénomène, considérons l'exemple suivant, dont on calcule facilement la fiabilité  $R$  puis après dérivation le taux de défaillance  $\Lambda$  :



$$R(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$$

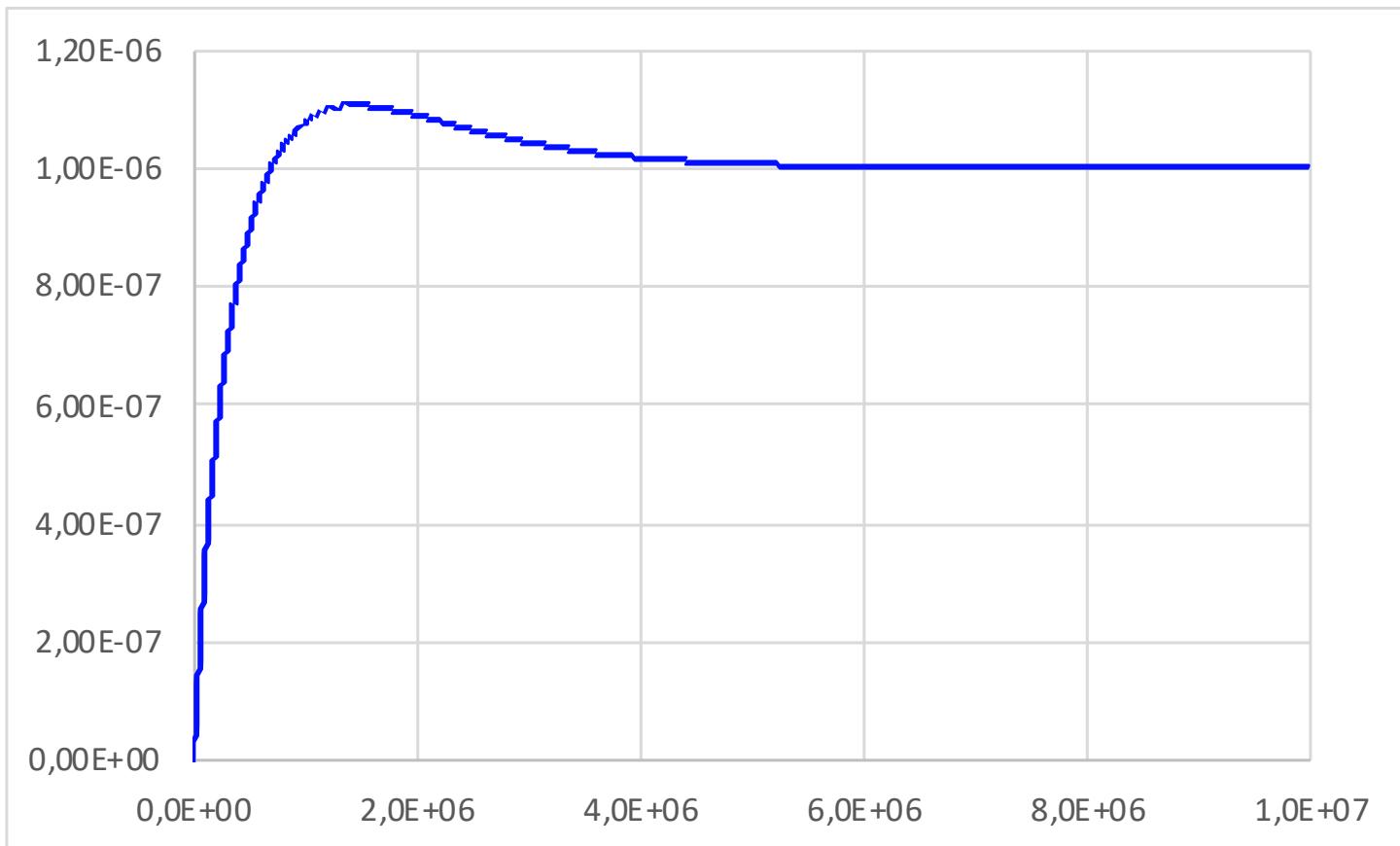
$$\Lambda(t) = \frac{\lambda_1 e^{-\lambda_1 t} + \lambda_2 e^{-\lambda_2 t} - (\lambda_1 + \lambda_2) e^{-(\lambda_1 + \lambda_2)t}}{e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}}$$

# Redondance active : taux de défaillance constants

36

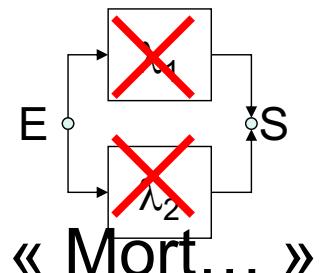
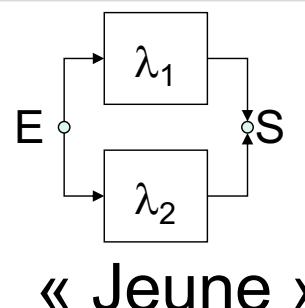
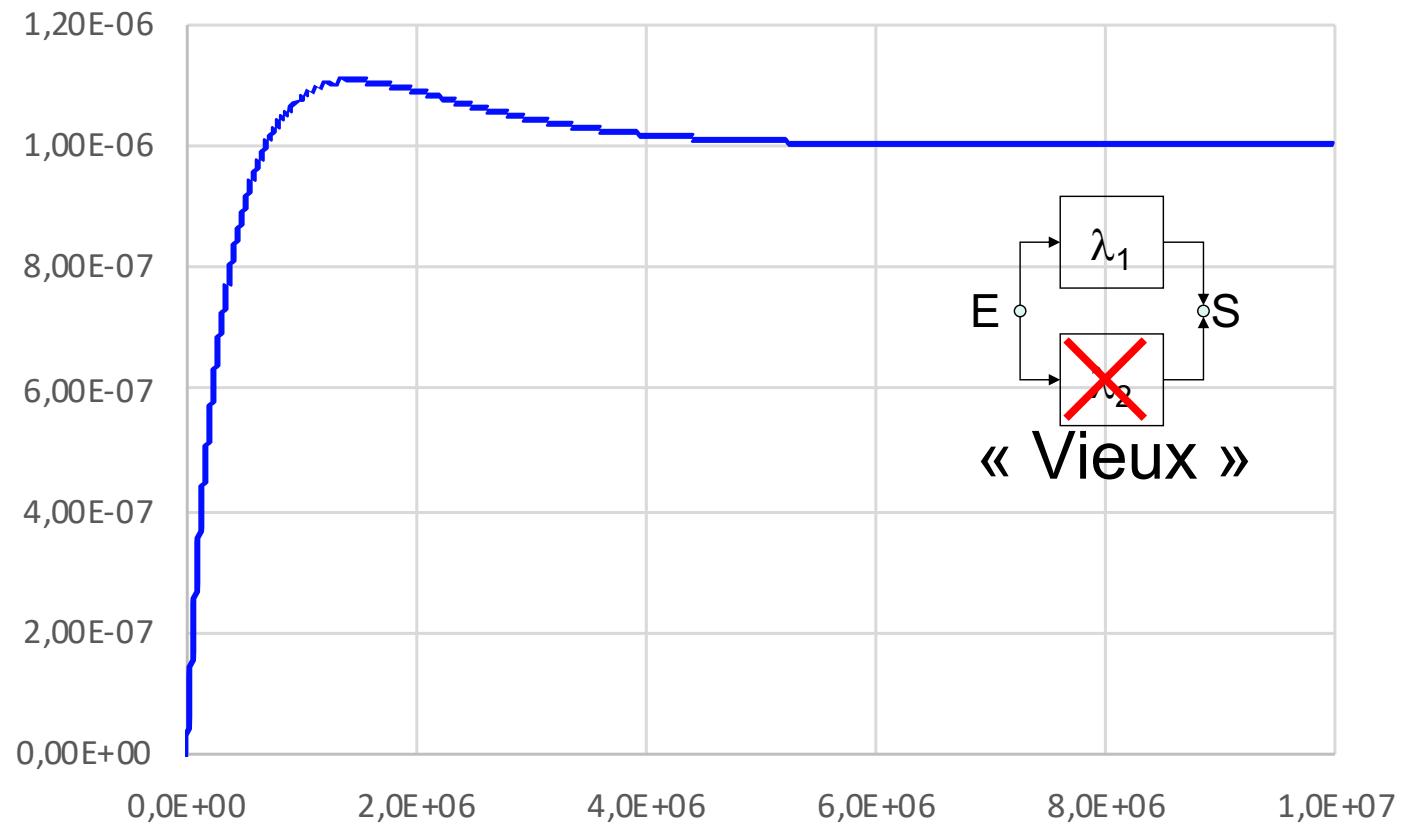
$$\Lambda(t) = \frac{\lambda_1 e^{-\lambda_1 t} + \lambda_2 e^{-\lambda_2 t} - (\lambda_1 + \lambda_2) e^{-(\lambda_1 + \lambda_2)t}}{e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}}$$

La courbe a l'allure suivante :



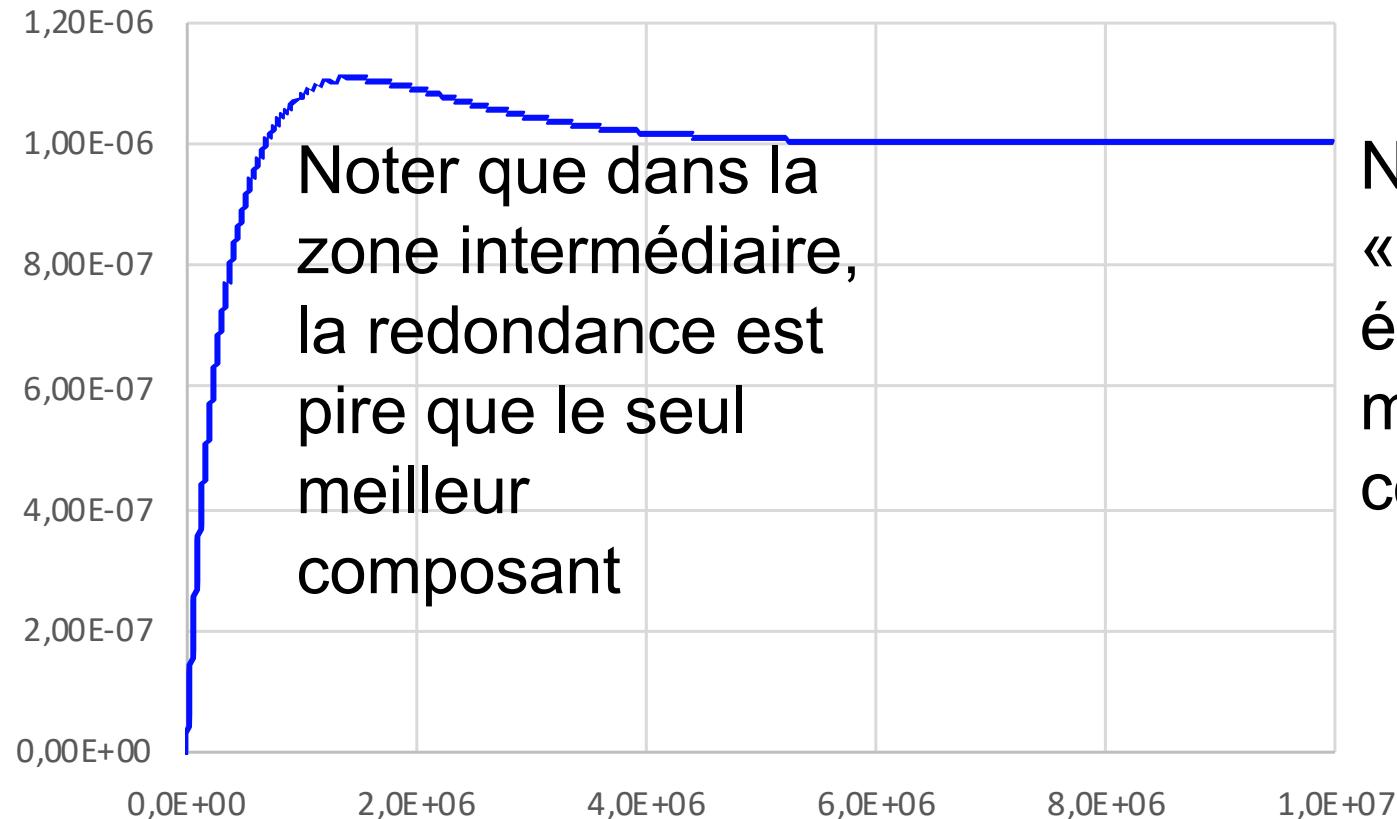
# Redondance active : taux de défaillance constants

37



# Redondance active : taux de défaillance constants

38



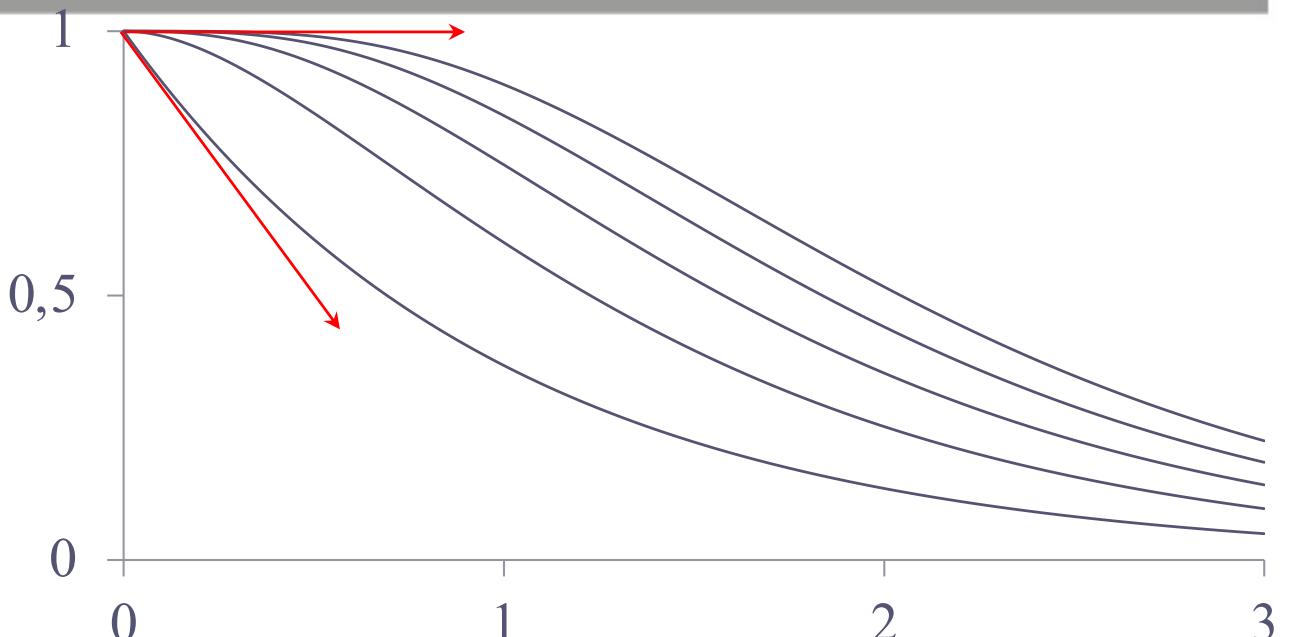
Noter que le « vieux » est équivalent au meilleur composant

Noter que le « jeune » a un taux de défaillance initialement nul (immortalité)

# Comportement aux temps courts

39

Le comportement aux temps courts (tous les  $\lambda_i t \ll 1$ ) est d'une importance fondamentale car c'est dans ce cas qu'apparaît l'intérêt essentiel des redondances



➤ Système série :  $R(t) = e^{-\lambda_{\text{système}} t} = 1 - \lambda_{\text{système}} \cdot t + O(t^2)$

où  $\lambda_{\text{système}} = \sum_i \lambda_i$  (Pente finie  $\lambda_{\text{système}} \cdot t$  à l'origine)

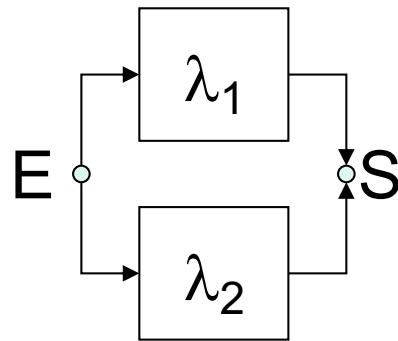
➤ Redondance active :  $1 - R(t) = \prod_{i=1}^N (1 - r_i)$   $r_i(t) = e^{-\lambda_i t} = 1 - \lambda_i \cdot t + O(t^2)$

$R(t) = 1 - \left[ \prod_{i=1}^N \lambda_i \right] \cdot t^N + O(t^{N+1})$  (tangente horizontale à l'origine si  $N > 1$ )

# Comportement aux temps courts

40

Exemple : pour le système parallèle à deux composants :



$$1 - R(t) = (1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t})$$
$$\lambda_1 t + O(t^2) \quad \lambda_2 t + O(t^2)$$
$$R(t) = 1 - \lambda_1 \lambda_2 t^2 + O(t^3)$$

Qui est bien le cas N=2 de la formule générale :

$$R(t) = 1 - \left[ \prod_{i=1}^N \lambda_i \right] t^N + O(t^{N+1})$$

Attention le développement de la fiabilité par la formule :

$$R(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$$

Donnerait aussi le résultat mais contraindrait à la formule de Taylor à l'ordre 2.

## Redondance active à $\lambda$ constants : MTTF

- 41 • Afin d'estimer quantitativement la faible croissance de MTTF avec le nombre de composants, on envisage le cas de N composants identiques de même  $\lambda$  constant :

$$\text{MTTF} = \int_0^{\infty} \left[ 1 - (1-r)^N \right] dt \quad \text{où} \quad r = e^{-\lambda t}$$

Posant  $u = 1-r$  donc  $du = \lambda \cdot r \cdot dt$  soit :  $dt = \frac{1}{\lambda} \frac{du}{1-u}$

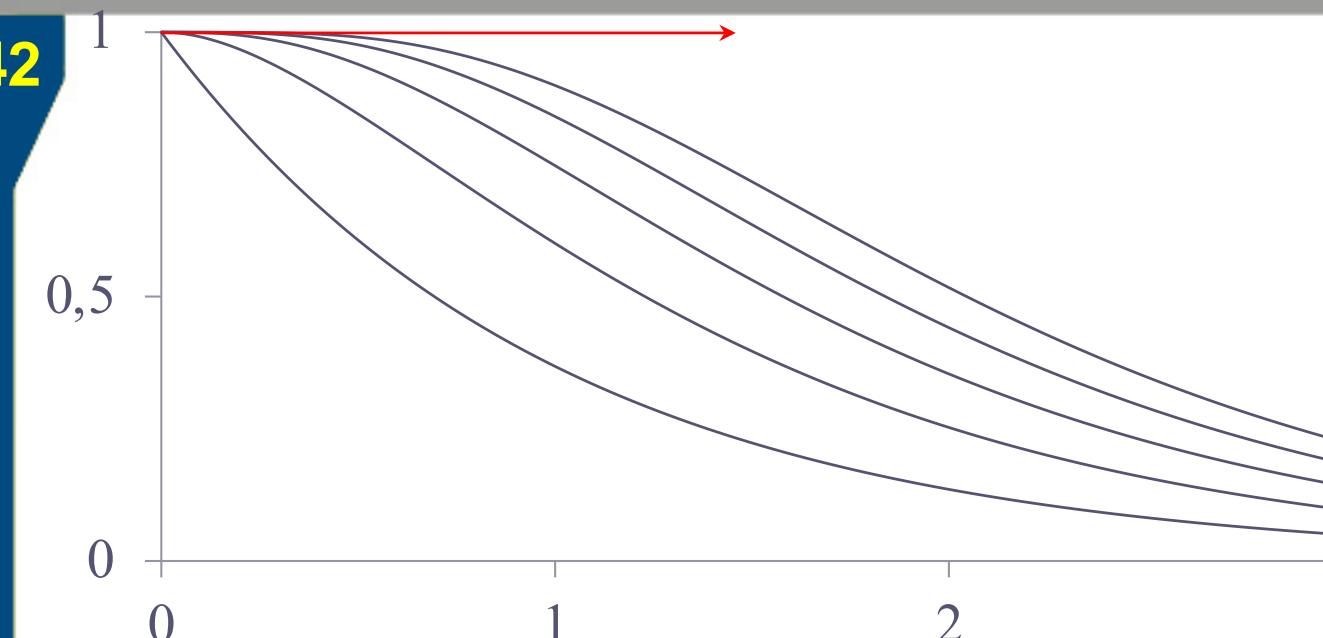
$$\text{MTTF} = \frac{1}{\lambda} \int_0^1 \left[ 1 - u^N \right] \frac{du}{1-u} = \frac{1}{\lambda} \sum_{k=0}^{N-1} \int_0^1 u^k du = \frac{1}{\lambda} \sum_{k=0}^{N-1} \frac{1}{k+1}$$

D'où enfin :

$$\boxed{\text{MTTF} = \frac{1}{\lambda} \sum_{i=1}^N \frac{1}{i}}$$

# Redondance active : taux de défaillance constants

42



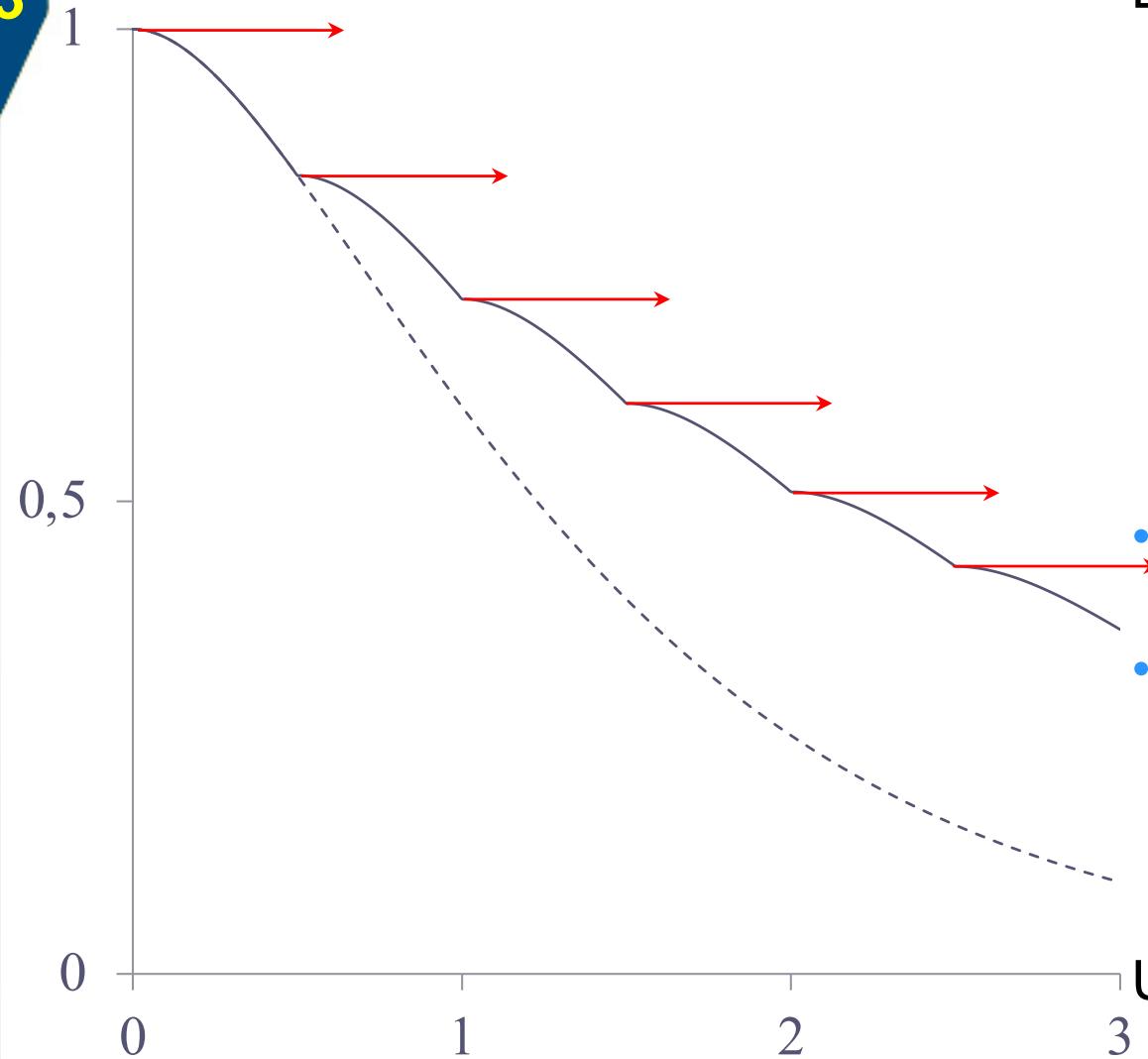
<b>N</b>	<b>Facteur de gain</b>	<b>N</b>	<b>Facteur de gain</b>
1	1	6	2,45
2	1,5	7	2,59
3	1,83	8	2,72
4	2,08	9	2,83
5	2,28	10	2,93

Par rapport à un composant unique (de MTTF=1/λ) le facteur de gain sur le MTTF avec  $N$  composants en redondance active vaut :

$$\sum_{i=1}^N \frac{1}{i}$$

# Sur l'utilisation des redondances

43



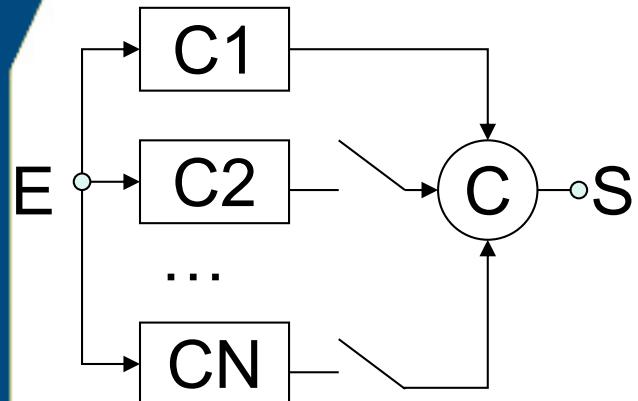
Les redondances ne doivent pas être utilisées sur des durées importantes. Il faut rester dans le domaine des « temps courts » (tous les  $\lambda t \ll 1$ ) où l'on exploite la **tangente horizontale** :

- Système de courte durée de vie  $T$  ( $\lambda T \ll 1$ )
- Système de longue durée de vie mais maintenu à intervalles réguliers  $T$  tels que  $\lambda T \ll 1$

Une redondance utilisée longtemps sans surveillance ne sert (presque) à rien

# Redondance passive

44



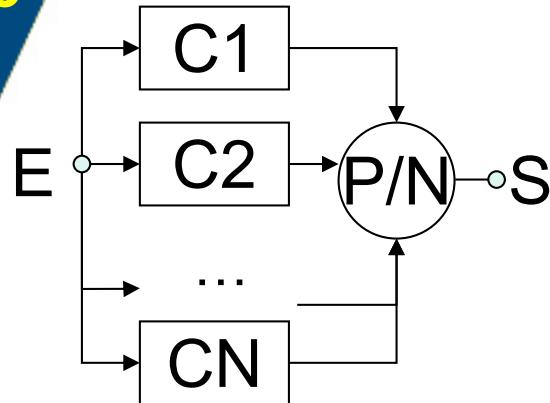
- Le cas de la redondance passive est un problème à **composants dépendants** (car la mise en marche d'un composant de secours n'a lieu que sur défaillance du composant principal), donc nécessite un traitement spécifique, esquissé en annexe.
- Le résultat essentiel concerne le comportement au temps courts dont on peut montrer qu'il est :

$$R(t) = 1 - \left[ \prod_{i=1}^N \lambda_i \right] \frac{t^N}{N!} + O(t^{N+1})$$

Interprétation intuitive : les défaillances doivent arriver dans un ordre précis (seul un ordre sur les  $N!$  possibles compte)

# Voteur P/N

45



- Traitable uniquement dans le cas de composants identiques de même fiabilité  $r$ .
- La fiabilité est alors une somme de valeurs de la loi binomiale :

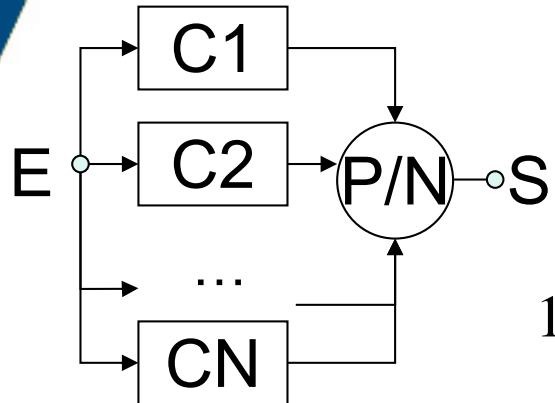
Au moins  $P$  fonctionnent      Exactement  $k$  fonctionnent

$$R = \sum_{k=P}^N \underbrace{C_N^k}_{\text{Choix de } k/N} r^k (1-r)^{N-k}$$

Les  $k$  choisis fonctionnent      Les  $N-k$  autres ne fonctionnent pas

# Voteur P/N

46



$$R = \sum_{k=P}^N C_N^k r^k (1-r)^{N-k} \quad (\text{Au moins } P \text{ fonctionnent})$$

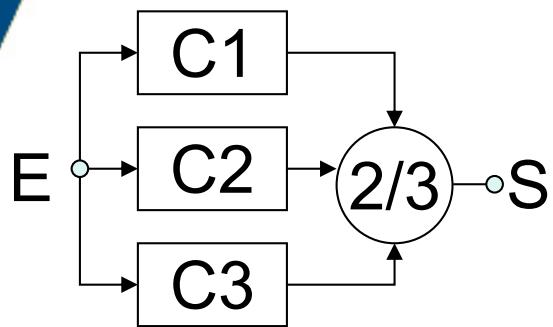
$$1 - R = \sum_{k=0}^{P-1} C_N^k r^k (1-r)^{N-k} \quad (\text{Moins de } P \text{ fonctionnent})$$

- Le voteur N/N = système série
- Le voteur 1/N = redondance active
- Si les taux de défaillances  $\lambda$  sont constants, en ne conservant que le terme d'ordre le plus bas en  $t$  de  $1-R$  on obtient le comportement aux temps courts (tangente horizontale sauf pour  $P=N$  qui est un système série)

$$R = 1 - C_N^{P-1} (\lambda t)^{N-P+1} + O(t^{N-P+2})$$

# Exemple du Voteur 2/3

47



- MTTF se calcule au cas par cas (pas de formule générale). Traitons par exemple le 2/3 (« vrai voteur » le plus simple), dans le cas où les taux de défaillance  $\lambda$  sont constants:

$$R = 3e^{-2\lambda t}(1-e^{-\lambda t}) + e^{-3\lambda t} = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

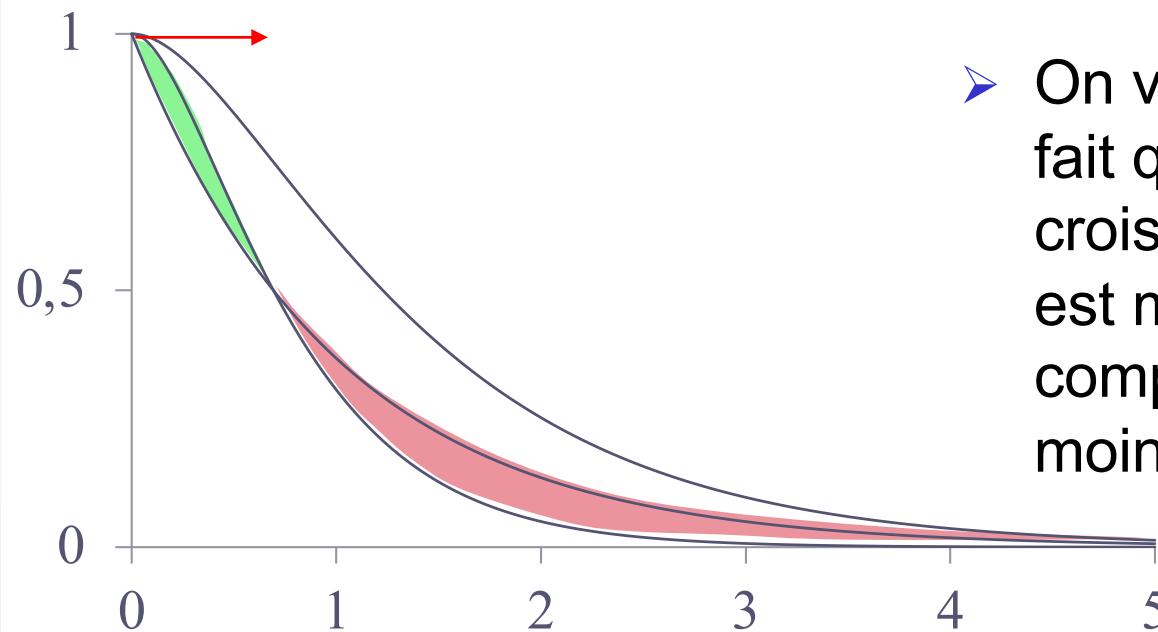
$$\text{MTTF} = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda}$$

- Par rapport au composant unique (de MTTF  $1/\lambda$ , le voteur 2/3 à un facteur de « gain » sur le MTTF de **5/6 !!!**)
- Comment s'explique ce paradoxe ?

## Exemple du voteur 2/3

48

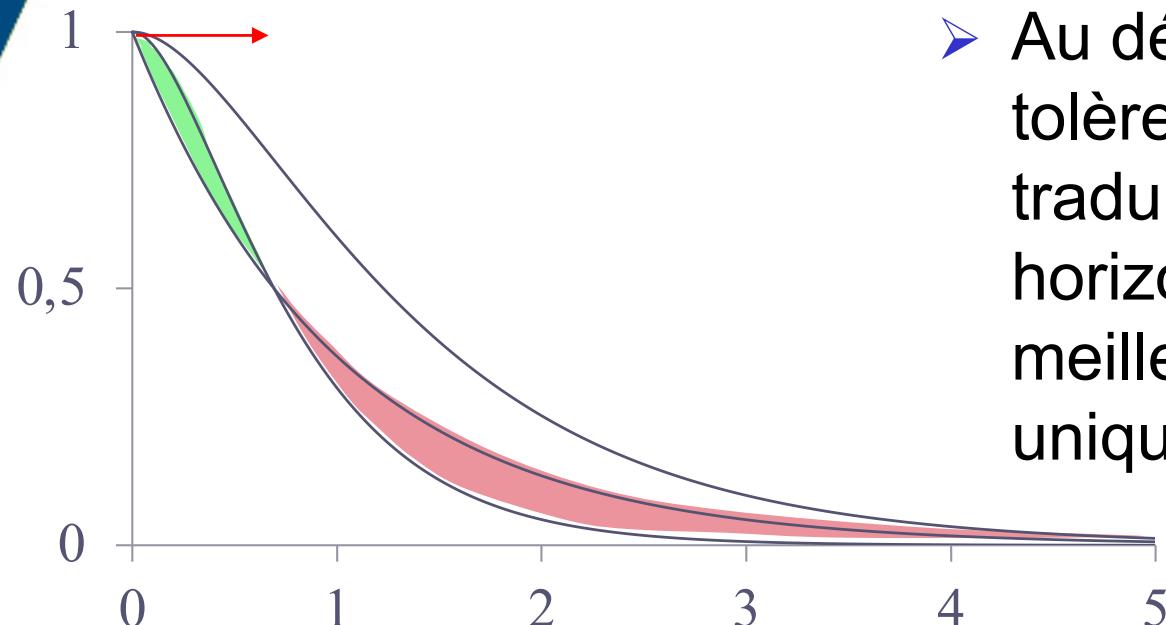
- Se souvenir que MTTF est une moyenne. En cas de paradoxe revenir à la fonction fiabilité :



- On voit que cela est dû au fait que les deux courbes se croisent : la fiabilité du voteur est meilleure que le composant unique au début, moins bonne à la fin...
- Ce que l'on **gagne au début** est plus faible que ce que l'on **perd à la fin**. Mais pourquoi les courbes se croisent elles ?

# Exemple du voteur 2/3

49

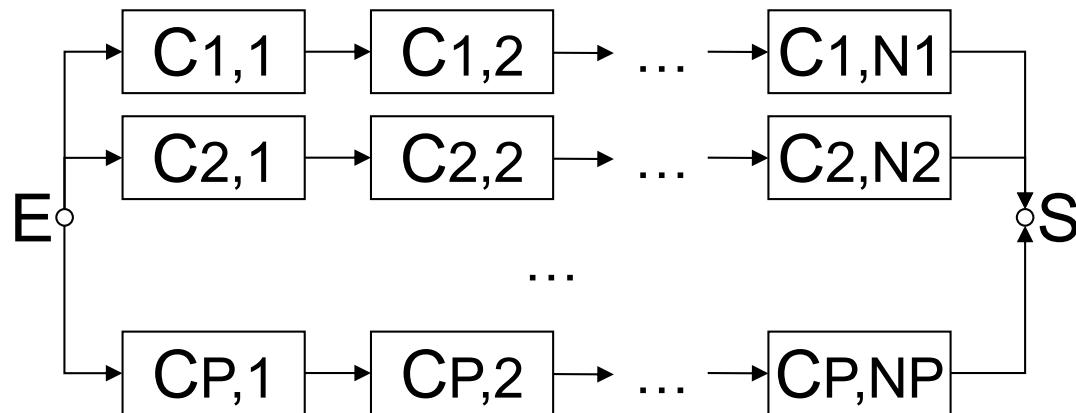


- Au départ le système tolère une panne ce que traduit la tangente horizontale (forcément meilleur que le composant unique)
- Après la première panne, le système devient **équivalent à un système série** à deux composants (forcément moins bon que le composant unique). Le point de croisement est une sorte d'instant moyen de la première panne.

# Systèmes série-parallèle

50

- Fiabilité d'un système série-parallèle (branches séries mises en parallèle) dans le cas général :

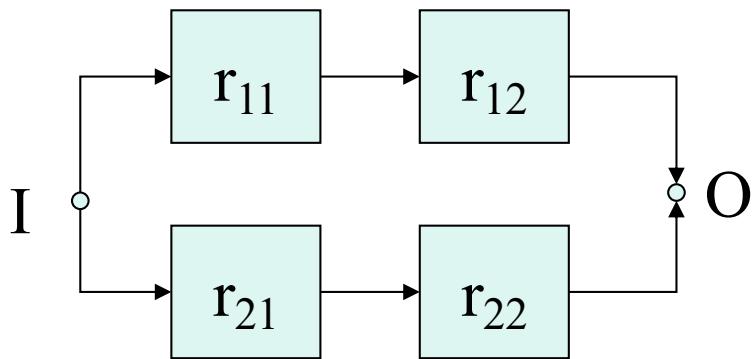


$$R = 1 - \prod_{i=1}^P \left( 1 - \prod_{j=1}^{N_i} r_{ij} \right)$$

- Où  $r_{ij}$  désigne la fiabilité du bloc  $C_{i,j}$  : on calcule la fiabilité de la branche  $j$  et on multiplie entre elles les défiabilités des branches pour obtenir la défiabilité du système.

# Système série-parallèle : exemple

51



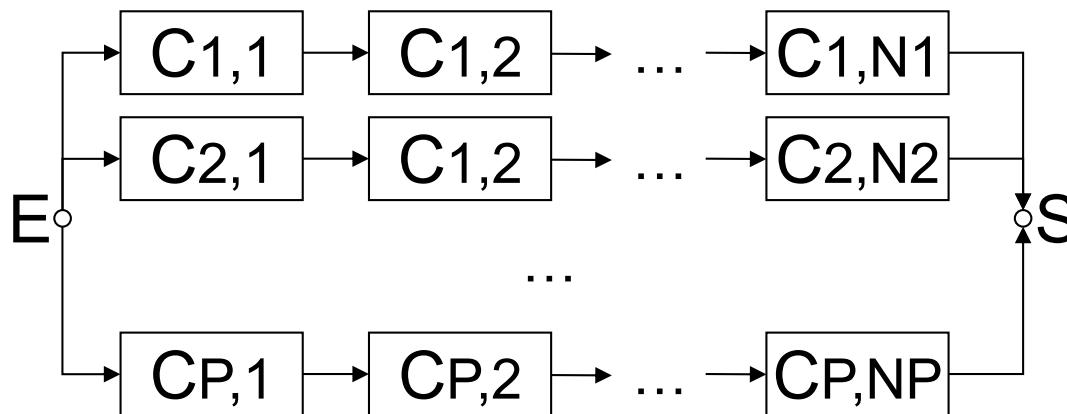
$$R = 1 - \prod_{i=1}^P \left( 1 - \prod_{j=1}^{N_i} r_{ij} \right)$$

$$R = 1 - (1 - r_{11} \cdot r_{12}) \cdot (1 - r_{21} \cdot r_{22})$$

# Systèmes série-parallèle

52

- Comportement aux temps courts si les taux de défaillance sont constants :



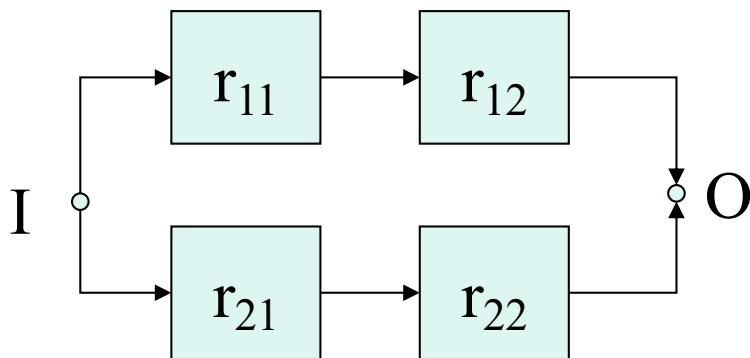
$$R = 1 - \prod_{i=1}^P \left( 1 - \prod_{j=1}^{N_i} r_{ij} \right)$$

$$R = 1 - \prod_{i=1}^P \left( \sum_{j=1}^{N_i} \lambda_{ij} \right) \cdot t^P + O(t^{P+1})$$

- Où  $\lambda_{ij}$  désigne le taux de défaillance du bloc  $C_{i,j}$ .

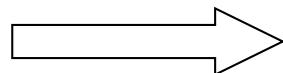
# Système série-parallèle : exemple

53



$$R = 1 - \prod_{i=1}^P \left( \sum_{j=1}^{N_i} \lambda_{ij} \right) \cdot t^P + O(t^{P+1})$$

$$R = 1 - (1 - r_{11} \cdot r_{12}) \cdot (1 - r_{21} \cdot r_{22})$$



$$R = 1 - (1 - \exp(-(\lambda_{11} + \lambda_{12})t)) \cdot (1 - \exp(-(\lambda_{21} + \lambda_{22})t))$$

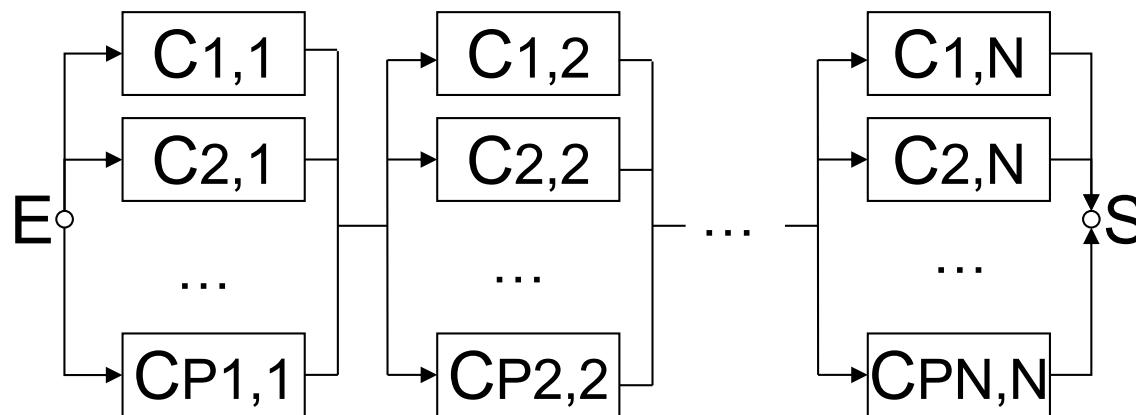


$$R = 1 - (\lambda_{11} + \lambda_{12}) \cdot (\lambda_{21} + \lambda_{22}) \cdot t^2$$

# Systèmes parallèle-série

54

- Fiabilité d'un système parallèle-série (étages parallèles mis en série) dans le cas général :

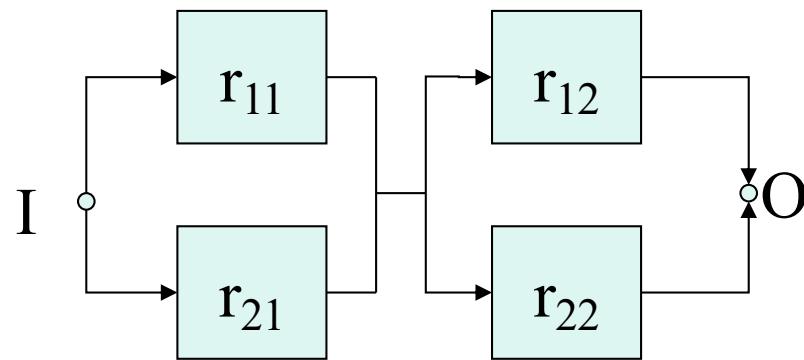


$$R = \prod_{j=1}^N \left( 1 - \prod_{i=1}^{P_j} (1 - r_{ij}) \right)$$

- On calcule la défiabilité de la branche l'étage  $i$  et on multiplie entre elles les fiabilités des étages pour obtenir la fiabilité du système.

# Systèmes parallèle-série : exemple

55



$$R = \prod_{j=1}^N \left( 1 - \prod_{i=1}^{P_j} (1 - r_{ij}) \right)$$

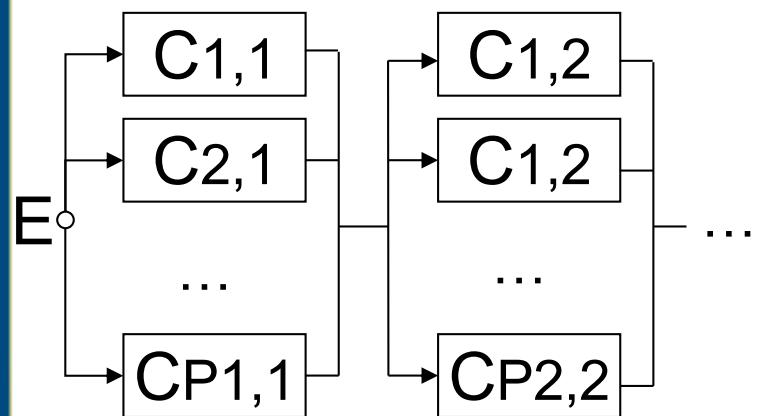
$$R = (1 - (1 - r_{11}) \cdot (1 - r_{21})) \cdot (1 - (1 - r_{12}) \cdot (1 - r_{22}))$$

# Systèmes parallèle série

56.

- Comportement aux temps courts si les taux de défaillance sont constants : imposé par le ou les étages ayant le  $P_j$  le plus petit (car  $R(\text{étage } j) = 1 - O(t^{P_j})$ )

Si tous les  $P_j$  sont égaux :



$$R = \prod_{j=1}^N \left( 1 - \prod_{i=1}^{P_j} (1 - r_{ij}) \right)$$

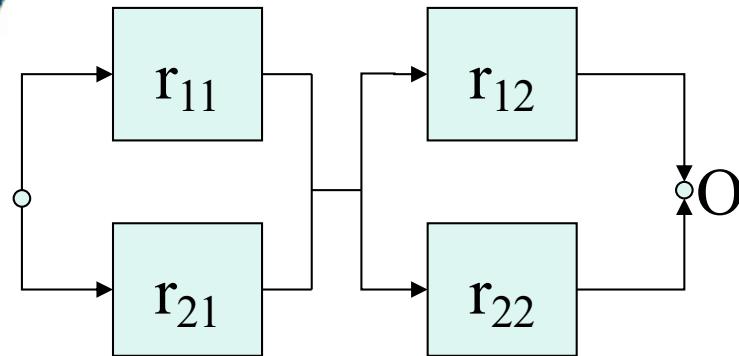
$$R = \prod_{j=1}^N \left( 1 - \left( \prod_{i=1}^P \lambda_{ij} \right) \cdot t^P + O(t^{P+1}) \right)$$

$$R = 1 - \left( \sum_{j=1}^N \prod_{i=1}^P \lambda_{ij} \right) \cdot t^P + O(t^{P+1})$$

# Système parallèle-série : exemple

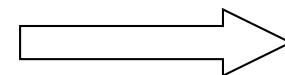
57

I

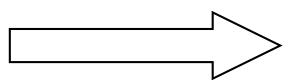


$$R = 1 - \left( \sum_{j=1}^N \prod_{i=1}^P \lambda_{ij} \right) \cdot t^P + O(t^{P+1})$$

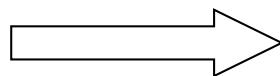
$$R = (1 - (1 - r_{11}) \cdot (1 - r_{21})) \cdot (1 - (1 - r_{12}) \cdot (1 - r_{22}))$$



$$R = [1 - (1 - \exp(-\lambda_{11} \cdot t)) \cdot (1 - \exp(-\lambda_{21} \cdot t))] \cdot [1 - (1 - \exp(-\lambda_{12} \cdot t)) \cdot (1 - \exp(-\lambda_{22} \cdot t))]$$



$$R = [1 - \lambda_{11} \cdot \lambda_{21} \cdot t^2] \cdot [1 - \lambda_{12} \cdot \lambda_{22} \cdot t^2]$$

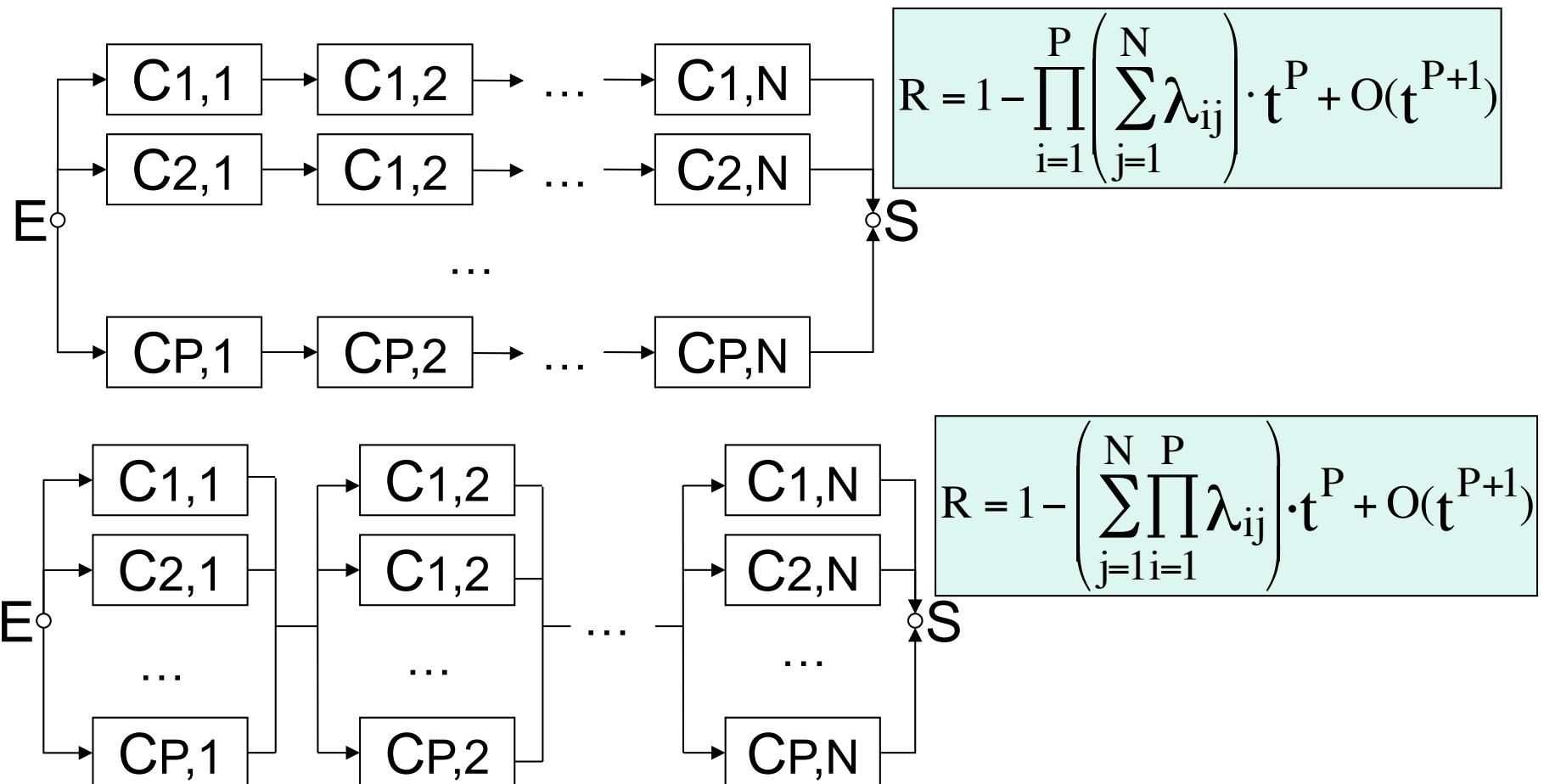


$$R = 1 - (\lambda_{11} \cdot \lambda_{21} + \lambda_{12} \cdot \lambda_{22}) t^2$$

# Sur la conception des redondances

58

- Deux systèmes comparables à N.P Composants lequel est le meilleur sur la fiabilité aux temps courts ?



# Sur la conception des redondances

59

$$\prod_{i=1}^P \left( \sum_{j=1}^N \lambda_{ij} \right)$$

Exemple:  $(\lambda_{11} + \lambda_{12}) \cdot (\lambda_{21} + \lambda_{22})$

Donne après développement NP termes  
 $\lambda_{1,j_1} \lambda_{2,j_2} \dots \lambda_{P,j_P}$  où chacune des P « cases »  
j<sub>1</sub>...j<sub>P</sub> peut être remplie par l'une quelconque  
des N valeurs de j (1 à N)

$$\left( \sum_{j=1}^N \prod_{i=1}^P \lambda_{ij} \right)$$

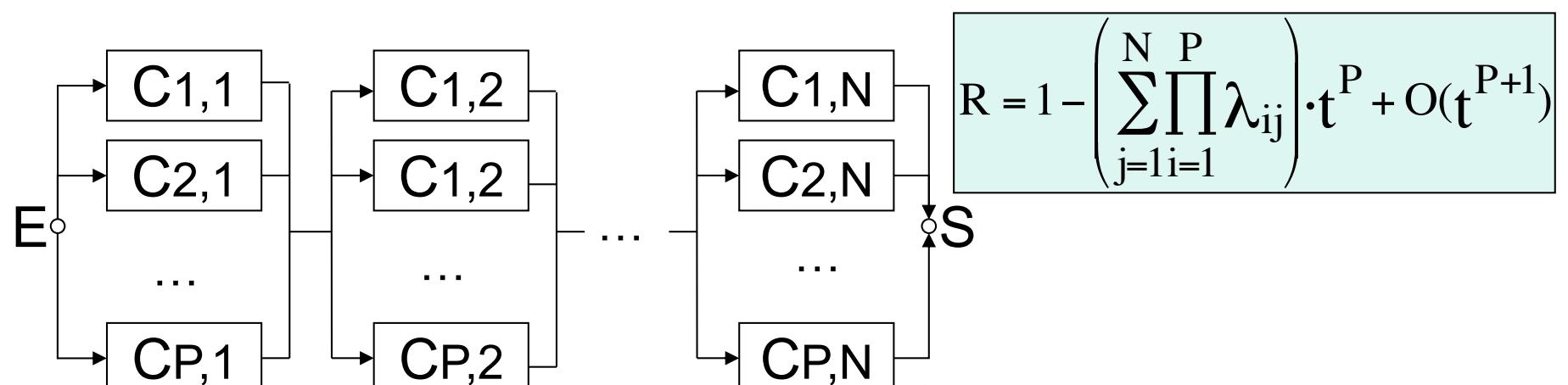
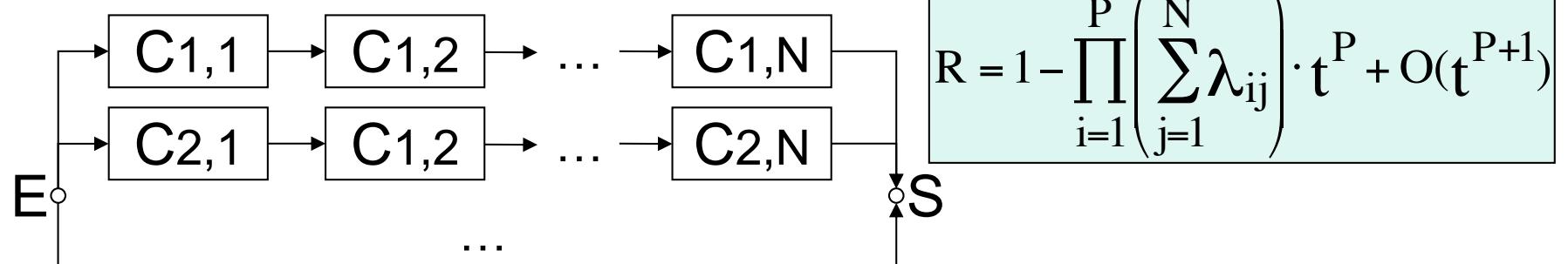
Exemple:  $\lambda_{11}\lambda_{21} + \lambda_{12}\lambda_{22}$

Ne contient que N termes du type  $\lambda_{1,j} \lambda_{2,j} \dots \lambda_{P,j}$   
(même j pour l'ensemble du terme) qui  
figurent parmi les NP termes précédents

Comme tous ces termes sont positifs, la somme de  
produits est plus petite que le produit de sommes.

# Sur la conception des redondances

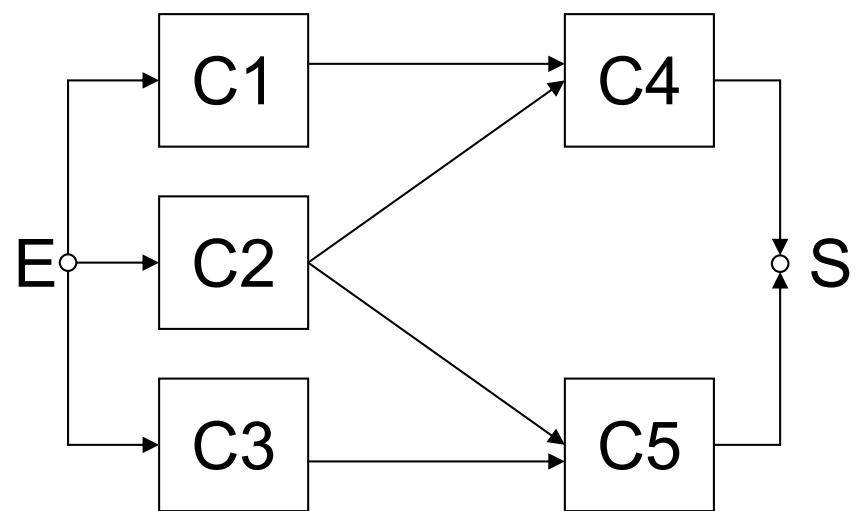
60. La conception parallèle-série (redondance « au plus bas niveau possible » : plus de liens et moins de coupes) est donc préférable à la conception série-parallèle (redondance à haut niveau)



# Systèmes complexes

61

- Face à un système complexe, existe toujours la méthodes par liens ou coupes, laborieuse mais certaine d'aboutir :



4 liens mini	4 coupes mini
C1.C4	$\overline{C_1} \overline{C_2} \overline{C_3}$
C2.C4	$\overline{C_4} \overline{C_5}$
C2.C5, C3.C5	$\overline{C_1} \overline{C_2} \overline{C_5}$ $\overline{C_2} \overline{C_3} \overline{C_4}$

$$R = P(C_1 C_4 + C_2 C_4 + C_2 C_5 + C_3 C_5)$$

# Systèmes complexes

62

- Supposant les composants indépendants, R se calcule alors par application du théorème de Poincaré :

$$R = P(C_1C_4 + C_2C_4 + C_2C_5 + C_3C_5)$$

4 liens :

$$r_1r_4 + r_2r_4 + r_2r_5 + r_3r_5$$

6 combinaisons à 2 liens :

$$-r_1r_2r_4 - \cancel{r_1r_2r_4}r_5 - r_1r_3r_4r_5$$

$$-r_2r_4r_5 - \cancel{r_2r_3}r_4r_5 - r_2r_3r_5$$

$$R = r_1r_4 + r_2r_4 + r_2r_5 + r_3r_5 - r_1r_2r_4 - r_2r_4r_5 - r_2r_3r_5 - r_1r_3r_4r_5 + r_1r_2r_3r_4r_5$$

4 combinaisons à 3 liens :

$$\cancel{r_1r_2r_4r_5} + \cancel{r_1r_2r_3r_4r_5}$$

$$+ r_1r_2r_3r_4r_5 + \cancel{r_2r_3r_4r_5}$$

1 combinaison à 4 liens :

$$\cancel{-r_1r_2r_3r_4r_5}$$

Fort heureusement dans bien des cas, il y a plus simple !

# Systèmes complexes : utilisation du théorème des probabilités totales

63

- Rappel : étant donné un ensemble complet d'événements  $A_i$  (événements deux à deux incompatibles dont l'union est l'événement certain), alors quel que soit l'événement  $B$  :

$$P(B) = \sum_i P(B|A_i) \cdot P(A_i)$$

Dans notre cas, l'ensemble complet d'événement va être :

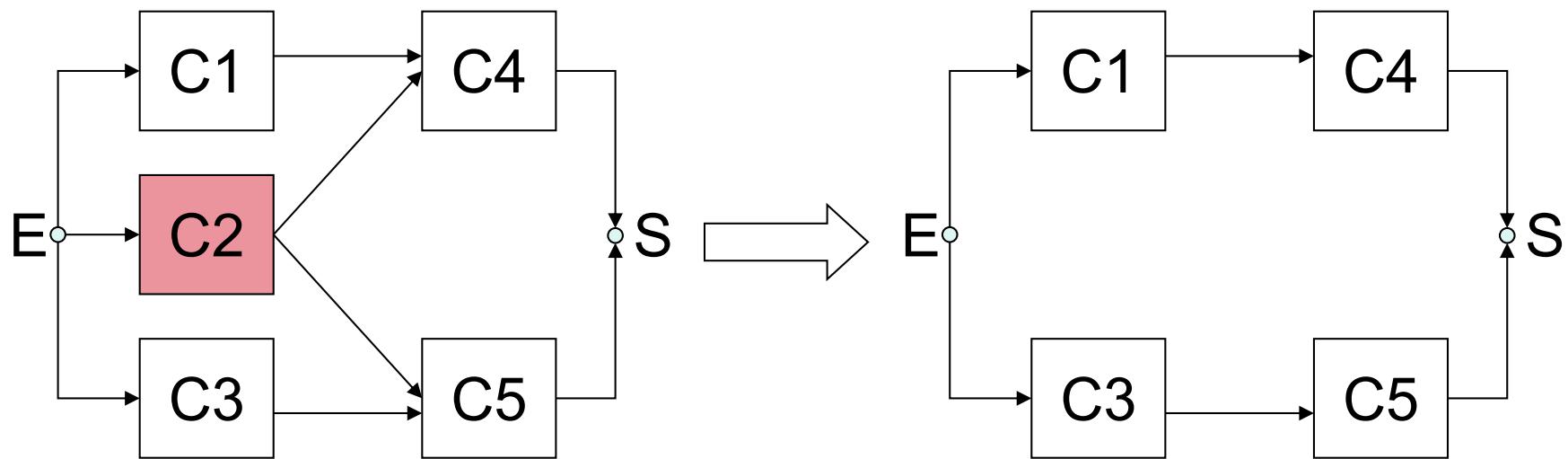
- Un composant (judicieusement choisi) fonctionne sur  $[0,t]$
- Ce même composant défaillle sur  $[0,t]$

Judicieusement choisi signifiant que le système se simplifie si l'on injecte l'hypothèse du fonctionnement ou non du composant en question !

# Systèmes complexes

64

- Particularisons C2 : Si C2 est défaillant le système se simplifie en :

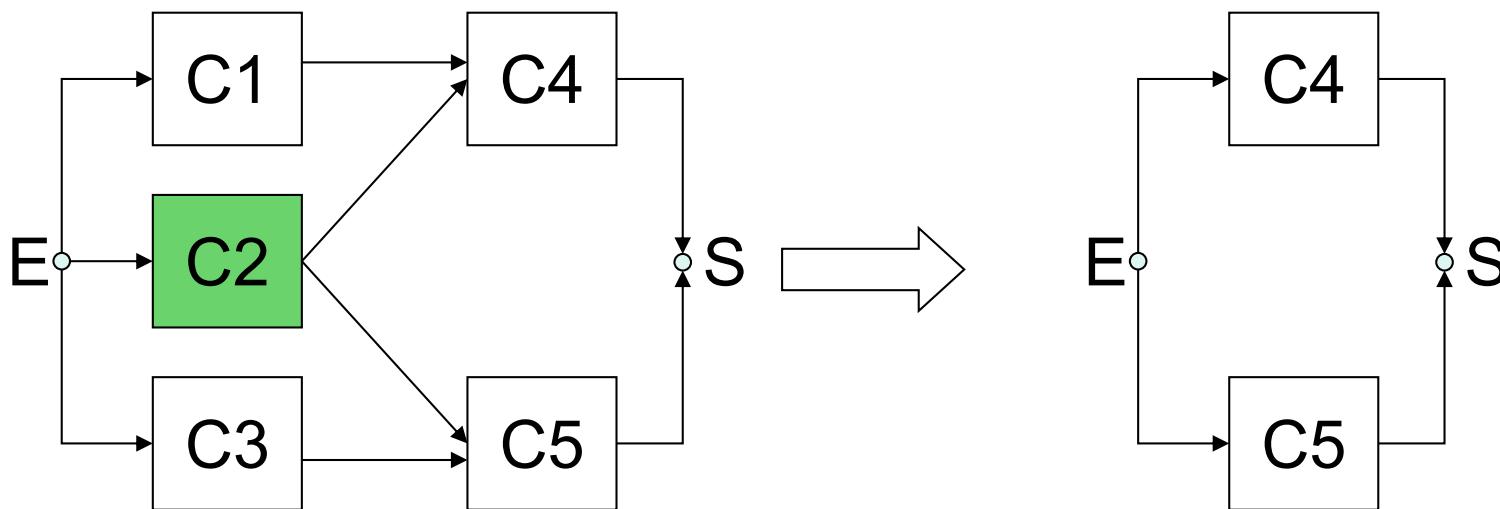


$$\text{Fiabilité : } 1 - (1 - r_1.r_4)(1 - r_3.r_5)$$

# Systèmes complexes

65

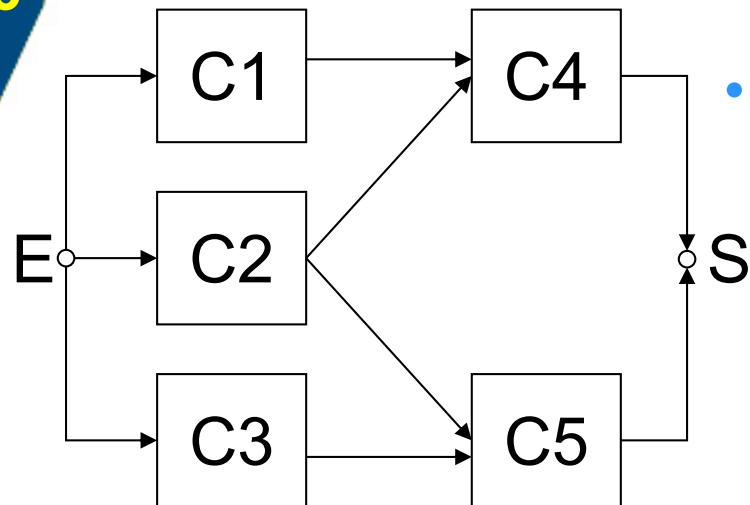
- Si au contraire C2 fonctionne C1 et C3 n'interviennent plus dans la fiabilité du système qui devient :



$$\text{Fiabilité : } 1 - (1 - r_4)(1 - r_5)$$

# Systèmes complexes

66



- Dans des cas plus compliqués on peut être amené à appliquer plusieurs fois le théorème des probabilités totales. Ici on trouve simplement si l'on résume graphiquement :

$$R(\text{█}) = R(\blacksquare) \cdot R(\text{█}) + [1 - R(\blacksquare)] \cdot R(\text{█})$$

$$R = r_2 \cdot [1 - (1 - r_4) \cdot (1 - r_5)] + (1 - r_2) \cdot [1 - (1 - r_1 \cdot r_4) \cdot (1 - r_3 \cdot r_5)]$$

$$R = r_2 \cdot (r_4 + r_5 - r_4 \cdot r_5) + (1 - r_2) \cdot (r_1 \cdot r_4 + r_3 \cdot r_5 - r_1 \cdot r_3 \cdot r_4 \cdot r_5)$$

(Expression équivalente à celle trouvée plus haut par les liens)

# Systèmes réparables

67

Pour traiter des systèmes réparables on peut :

- Construire et résoudre le graphe d'états : (relativement) simple uniquement dans le cas Markovien ( $\mu$  constants)
  - Certains (rares) problèmes de disponibilité sont à composants indépendants (suppose 1 réparateur par composant...) et peuvent donc utiliser les résultats précédents : en série les disponibilités se multiplient, en redondance active les indisponibilités se multiplient.
  - Dans les autres cas, il faut résoudre globalement le graphe du système (souvent résolution numérique).
- Alternativement on peut utiliser un modèle approché comme celui des maintenances périodiques à temps d'intervention négligeable proposé ci-après.

# Modèles à maintenances périodiques

68

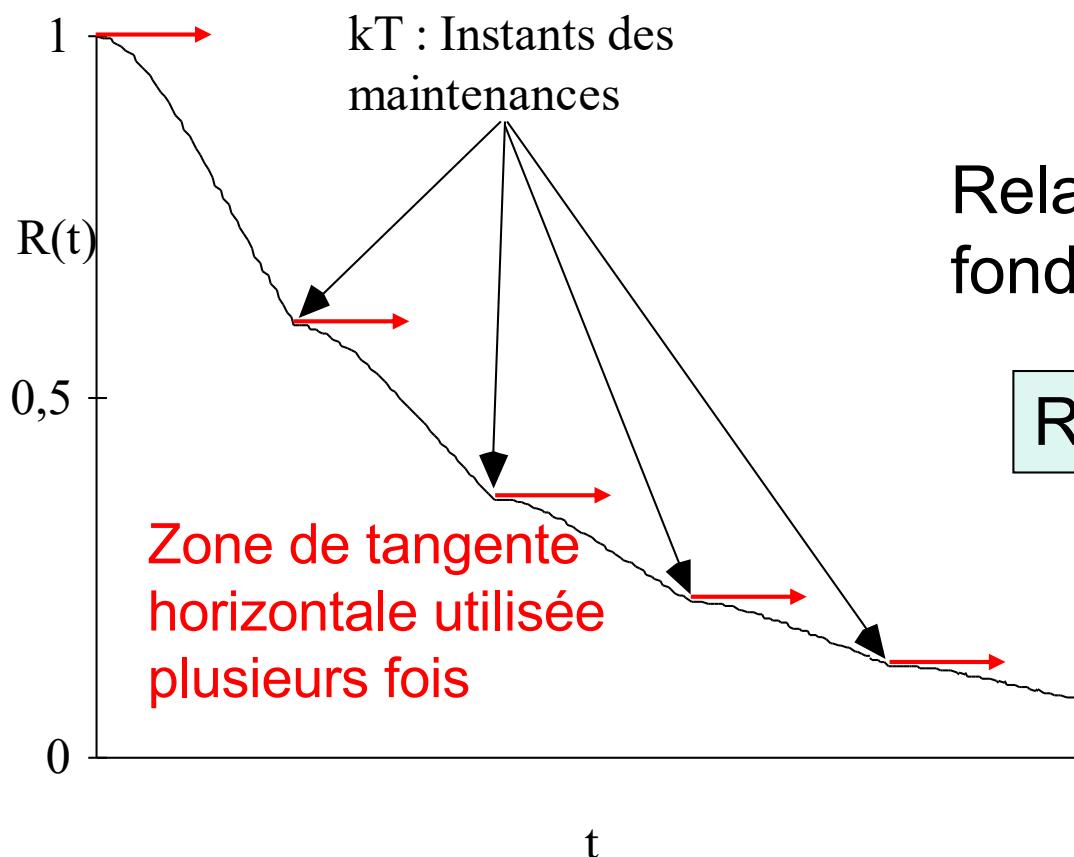
- Correspondent à des situations très fréquentes qu'il serait difficile de traiter autrement. Exemple :
  - Redondance à deux composants surveillée périodiquement.
  - Défaillance des deux composants entre deux maintenances => événement catastrophique.
  - Défaillance d'un seul composant constatée en maintenance => remplacement du composant (non catastrophique)
  - Durée moyenne jusqu'à événement catastrophique ?
- Problème typique de **fiabilité de système réparable**
- Sous certaines approximations maîtrisées (en particulier durée d'intervention négligeable) un modèle à maintenances périodique donne des résultats très simples, très fréquemment utilisés.

# Fiabilité d'un système redondant réparable avec maintenances périodiques

69

- $\text{Proba}(\text{pas de panne à } T+t) = \text{Proba}(\text{pas de panne à } T)^*$   
 $\text{Proba}(\text{pas de panne à } T+t | \text{pas de panne à } T)$

$=R(t)$  : remise en état du système s'il avait une défaillance



Relation fondamentale :

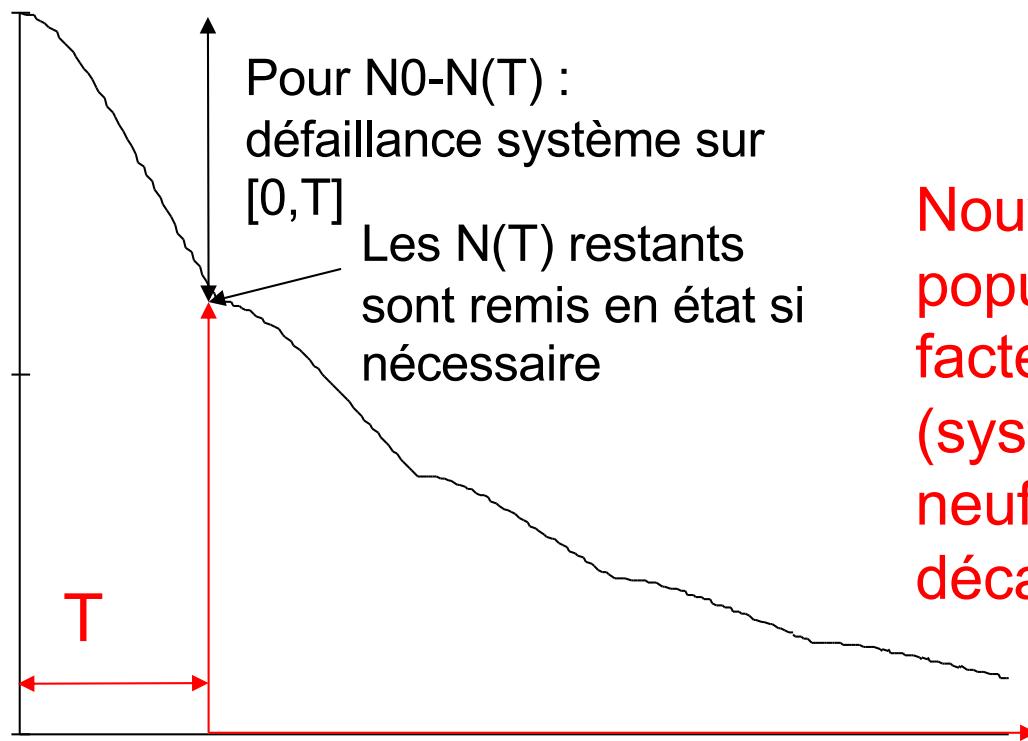
$$R(T+t) = R(T) \cdot R(t)$$

$$R(kT+t) = R^k(T) \cdot R(t)$$

# Maintenances périodiques : justification intuitive

70

Population initiale  $N_0$



Nouvelle expérience avec  
population réduite d'un  
facteur  $N(T)/N_0$   
(systèmes « remis à  
neuf ») et un temps  
décalé de  $T$  →

$$R(T+t) = R(T) \cdot R(t)$$

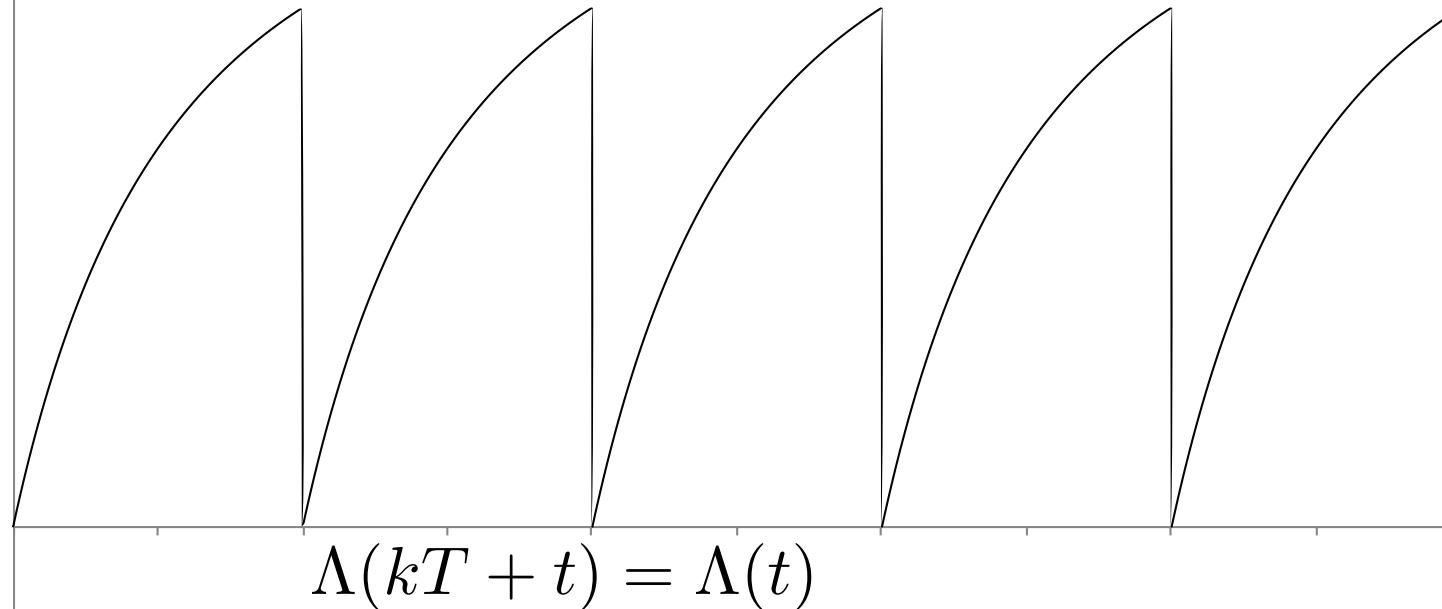
# Maintenances périodiques

71

Noter que le fait que la fiabilité dans tout intervalle  $[kT, (k+1)T]$  soit proportionnelle à la fiabilité sur  $[0, T]$  a pour conséquence que le taux de défaillance du système  $\Lambda$  est périodique de période  $T$  :

$\Lambda$

$$\Lambda(t) = -\frac{1}{R(t)} \frac{dR}{dt}(t)$$



# Maintenances périodiques

72

- Par intégration immédiate, on trouve MTTF durée moyenne jusqu'à événement catastrophique (beaucoup plus grand que MTTF sans maintenance)

$$MTTF = \left[ \sum_{k=0}^{\infty} R^k(T) \right] \cdot \int_0^T R(t) dt \quad \text{soit :}$$

$$MTTF = \frac{\int_0^T R(t) dt}{1 - R(T)}$$

Seule approximation jusqu'à présent : durée d'intervention négligeable. Si de plus tous les  $\lambda t \ll 1$  (maintenances fréquentes) :

$$\int_0^T R(t) dt \cong T \quad \text{d'où :}$$

$$MTTF = \frac{T}{1 - R(T)}$$

# Maintenances périodiques

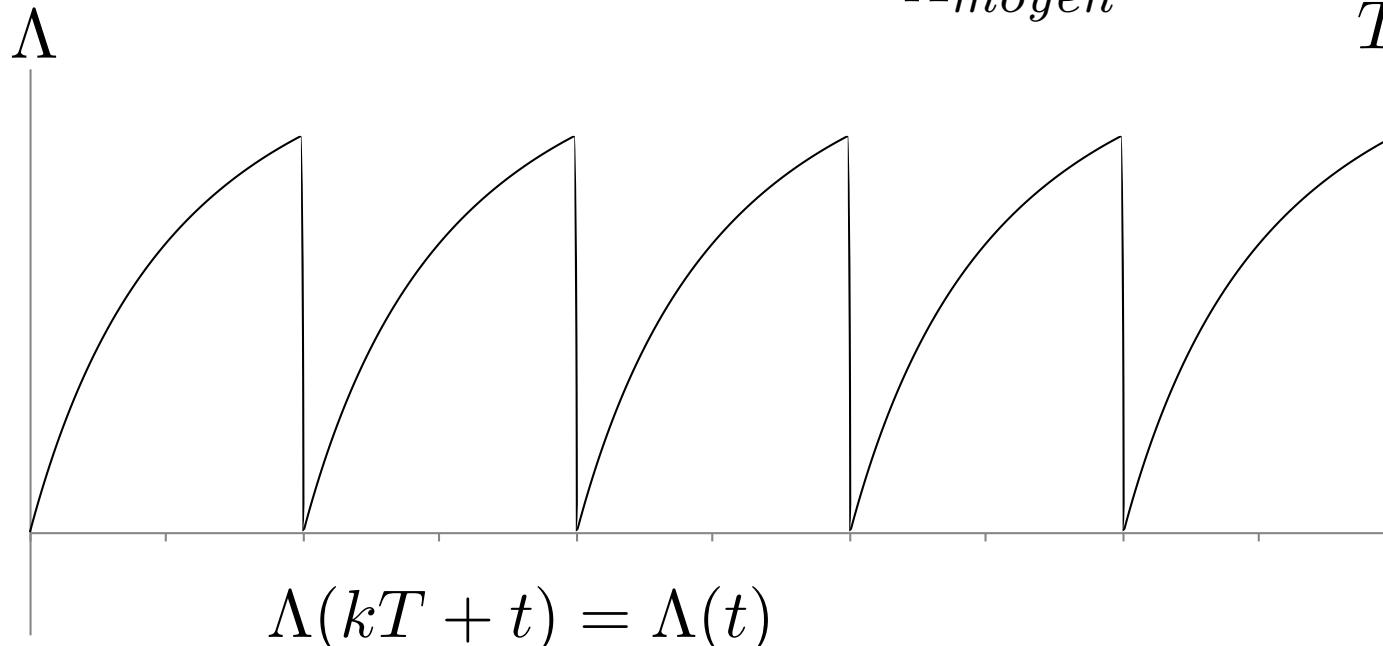
73

Le calcul du taux de défaillance système moyen donne quant à lui par intégration immédiate :

$$\int_0^T \Lambda(t)dt = -\ln(R(T)) \quad \text{soit : } \Lambda_{moyen} = -\frac{\ln(R(T))}{T}$$

et sous l'hypothèse des maintenances fréquentes qui a pour conséquence que  $(1-R(T) \ll 1)$

$$\Lambda_{moyen} = \frac{(1 - R(T))}{T}$$



# Maintenances périodiques fréquentes et rapides

74

Sous les deux hypothèses suivantes :

- Durées d'intervention négligeables (maintenances rapides)
- Périodicité de maintenance petite devant tous les  $1/\lambda$  (maintenances fréquentes)

MTTF est donc l'inverse du taux de défaillance moyen du système  $\Lambda_{moyen}$  :

$$\Lambda_{moyen} = \frac{1}{MTTF} = \frac{(1 - R(T))^{\text{maintenances}}}{T}$$

Probabilité de défaillance entre deux maintenances

Intervalle entre deux maintenances

# Maintenances périodiques fréquentes et rapides

75

Sous l'hypothèse des maintenances fréquentes on peut de plus utiliser les développements aux temps courts de  $R(T)$

$$\Lambda_{moyen} = \left[ \prod_{i=1}^N \lambda_i \right] T^{N-1}$$

Redondance active

$$\Lambda_{moyen} = \left[ \prod_{i=1}^N \lambda_i \right] \frac{T^{N-1}}{N!}$$

Redondance passive

$$\Lambda_{moyen} = \lambda C_N^{P-1} (\lambda T)^{N-P}$$

Voteur P/N

# Cas de deux composants redondants

76

- D'après les résultats précédents, on trouve pour deux composants redondants :

$$\Lambda_{moyen} = \lambda_1 \lambda_2 T$$

Redondance active (l'ordre n'importe pas)

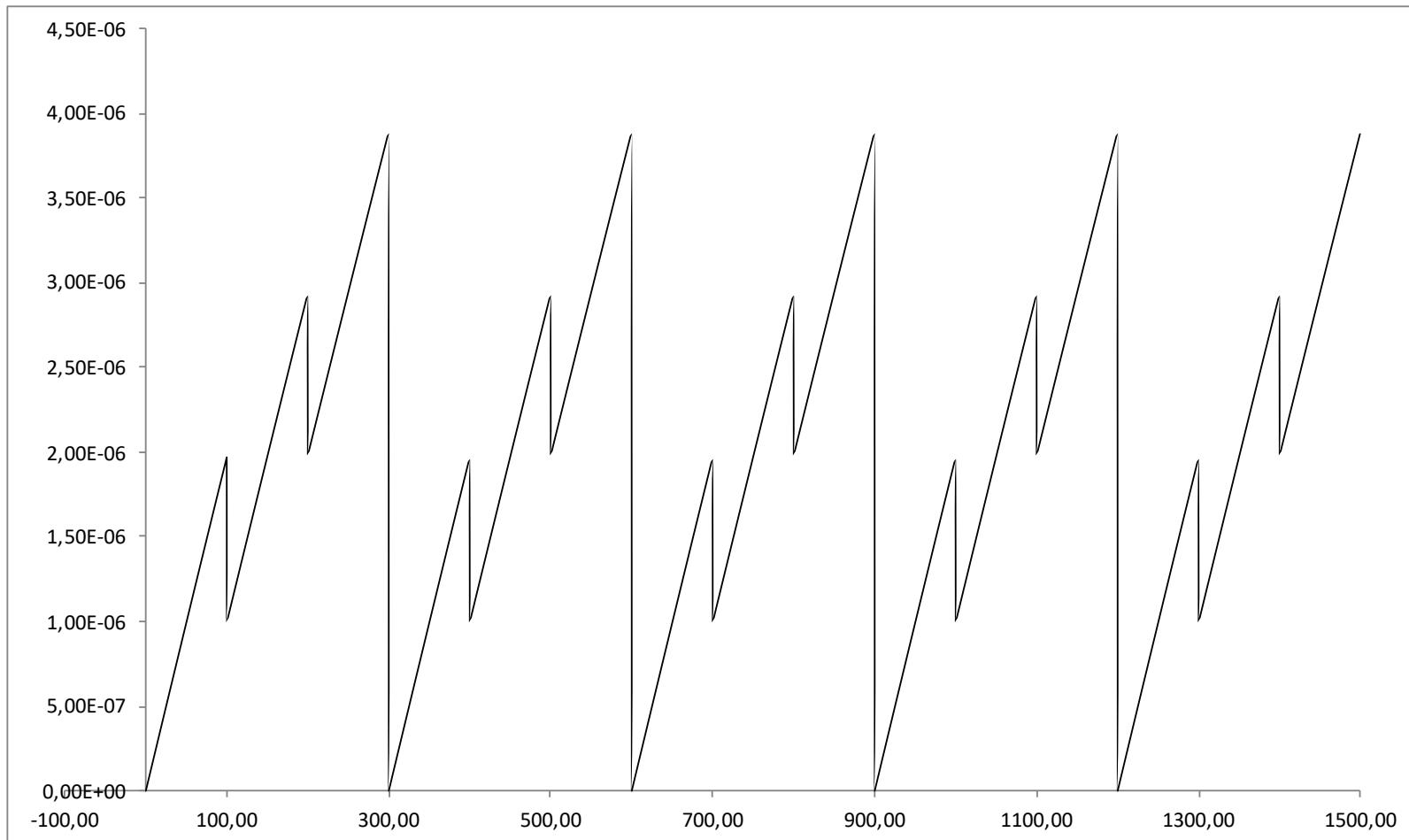
$$\Lambda_{moyen} = \frac{\lambda_1 \lambda_2 T}{2}$$

Redondance passive (l'ordre est imposé)

- Question : est il possible de généraliser ces résultats au cas où les périodicités de maintenance ne sont pas les mêmes pour les deux composants ?

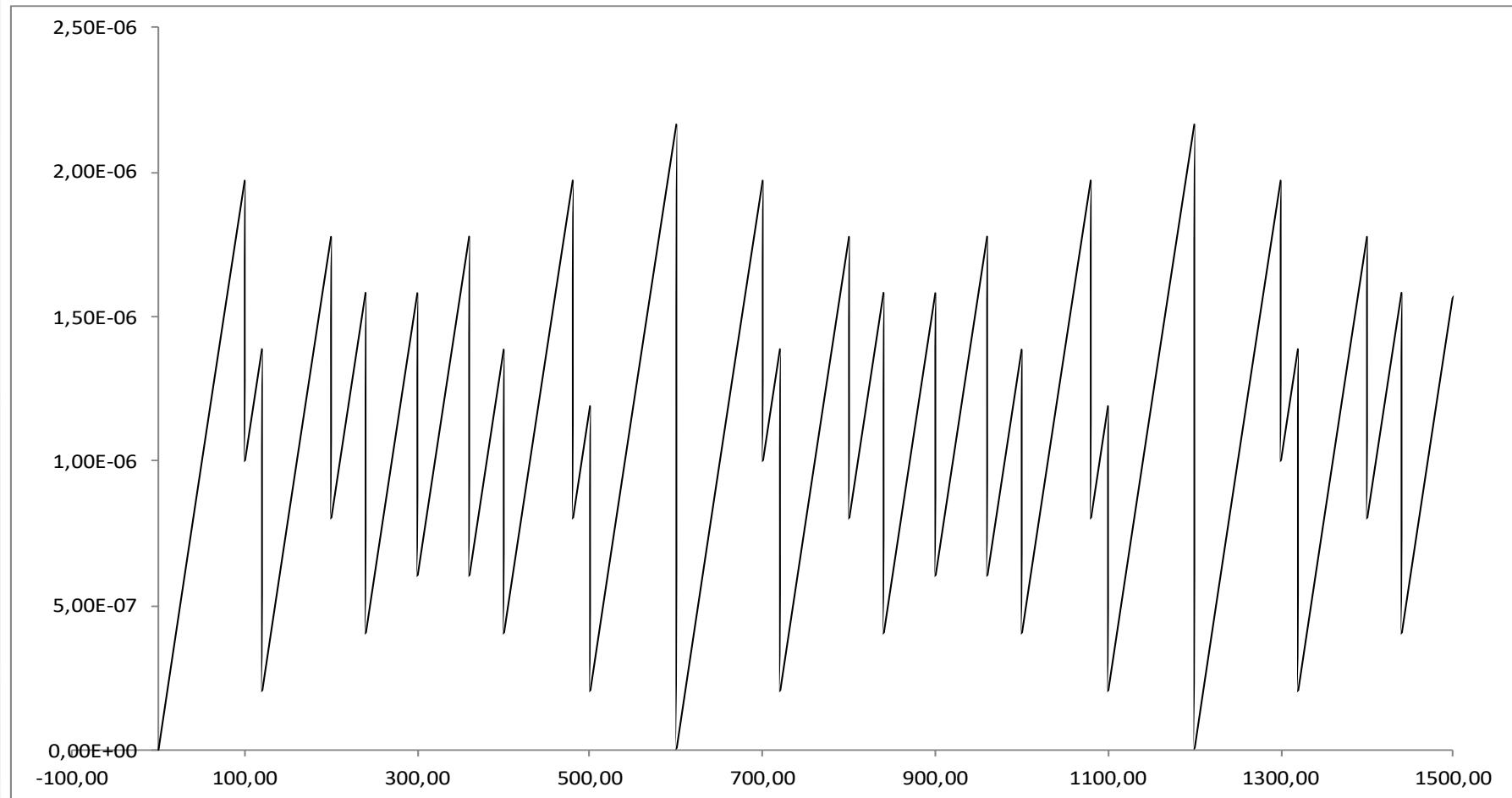
# Cas de deux composants redondants

77 Lorsque les périodes sont multiples l'une de l'autre (ici un exemple avec  $T_1=100\text{h}$  et  $T_2=300\text{h}$ ), le taux de défaillance système est périodique de période  $T_2$



# Cas de deux composants redondants

78 Lorsque les périodes ne sont pas multiples l'une de l'autre (ici un exemple avec  $T1=100h$  et  $T2=120h$ ), le taux de défaillance système est périodique de période  $\text{ppcm}(T1, T2)$



# Cas de deux composants redondants

79

Dans les deux cas, on parvient à démontrer la formule suivante (voir démonstrations en annexe)

$$\Lambda_{moyen} = \lambda_1 \lambda_2 \frac{T_1 + T_2}{2}$$

Sachant que la valeur maximale est, quant à elle :

$$\Lambda_{max} = \Lambda(ppcm(T_1, T_2)) = \lambda_1 \lambda_2 (T_1 + T_2)$$

## Cas de trois composants redondants

80

Pour trois composants, on parvient à démontrer par des techniques analogues le résultat suivant valable dans le cas général :

$$\Lambda_{max} = \Lambda(ppcm(T_1, T_2, T_3)) = \lambda_1 \lambda_2 \lambda_3 (T_1 T_2 + T_1 T_3 + T_2 T_3)$$

Ainsi (laborieusement) que le résultat suivant, valable uniquement si  $T_3$  est multiple de  $T_2$  lui-même multiple de  $T_1$ .

$$\Lambda_{moyen} = \lambda_1 \lambda_2 \lambda_3 \frac{2T_1^2 + T_2^2 + 3T_1 T_2 + 3T_1 T_3 + 3T_2 T_3}{12}$$

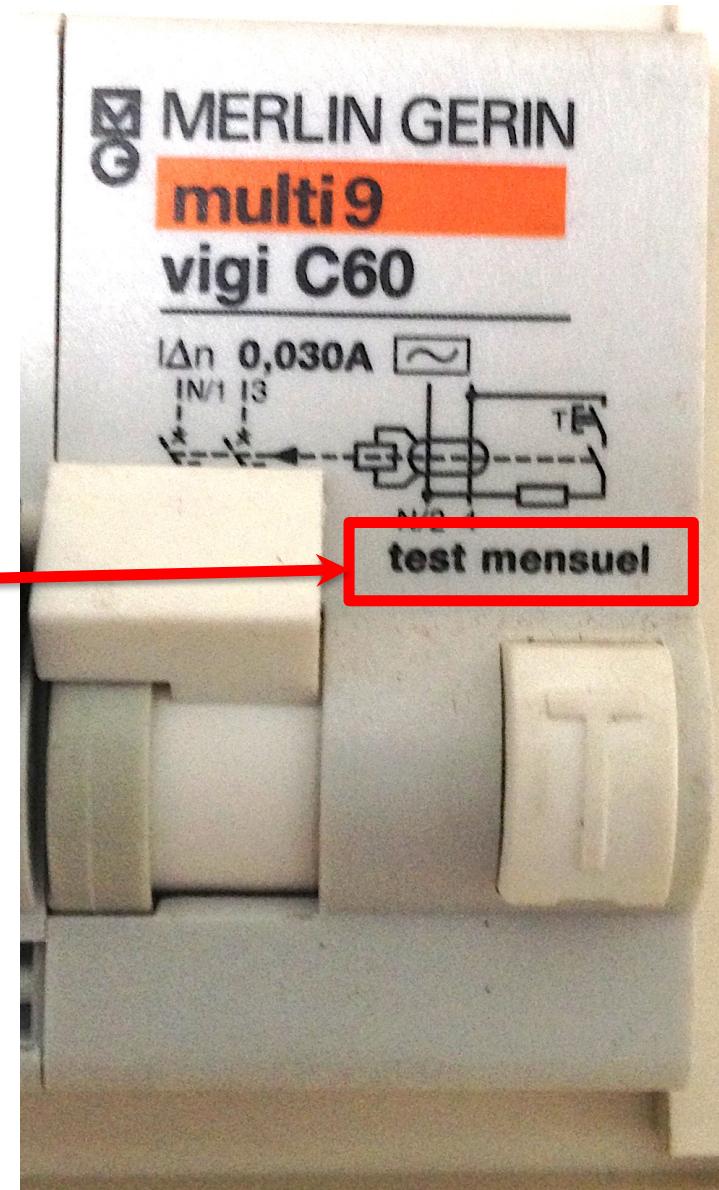
Il n'existe pas de formule générale si les périodicités ne sont pas multiples l'une de l'autre (encore moins dans le cas général à plus de trois composants).

Ces calculs sont de toutes façons généralement effectués numériquement grâce aux outils de sûreté de fonctionnement.

# Moralité concernant les redondances

81

- Pour être utile un système redondant doit rester **jeune**
- Si tel n'est pas le cas le gain lié à la redondance peut être faible, voire être en fait une **perte** (voteurs...)
- La jouvence de la redondance est la **maintenance** qui passe par la **surveillance** (tests...) et la remise en état de redondances ayant vieilli.
- C'est par cette surveillance que les temps de latence potentiellement exagérément élevés (typiques entre autres des organes de protection) peuvent être maîtrisés.



## Annexe1 : Démonstrations pour deux composants

82

Avec des périodicités de maintenance différentes  $T_1$  et  $T_2$  en considérant que  $T_2$  est multiple de  $T_1$  ( $T_2=NT_1$ ), N pouvant être égal à 1 :

Si l'on se place après la maintenance k (qui n'a lieu que si la double défaillance n'est pas survenue avant) dans l'intervalle  $[kT_1,(k+1)T_1]$  au temps t ( $kT_1 < t < (k+1)T_1$ ), la probabilité que le système soit défaillant est (compte tenu de la maintenance du composant 1 à  $kT_1$ ) :  $(1 - e^{-\lambda_1(t-kT_1)})(1 - e^{-\lambda_2 t})$

Dans l'approximation des temps courts, cela signifie que la probabilité de défaillance sur l'intervalle  $[kT_1,(k+1)T_1]$  est :

$$(k + 1)\lambda_1 \lambda_2 T_1^2$$

## Annexe 1 : Démonstrations pour deux composants

83

Les scénarios de défaillance sur les intervalles  $[k.T_1, (k+1)T_1]$  étant mutuellement exclusifs, la probabilité de défaillance sur  $[0, NT_1]$  est :

$$(1 + 2 + \dots + N)\lambda_1\lambda_2 T_1^2 = \frac{N(N+1)}{2}\lambda_1\lambda_2 T_1^2$$

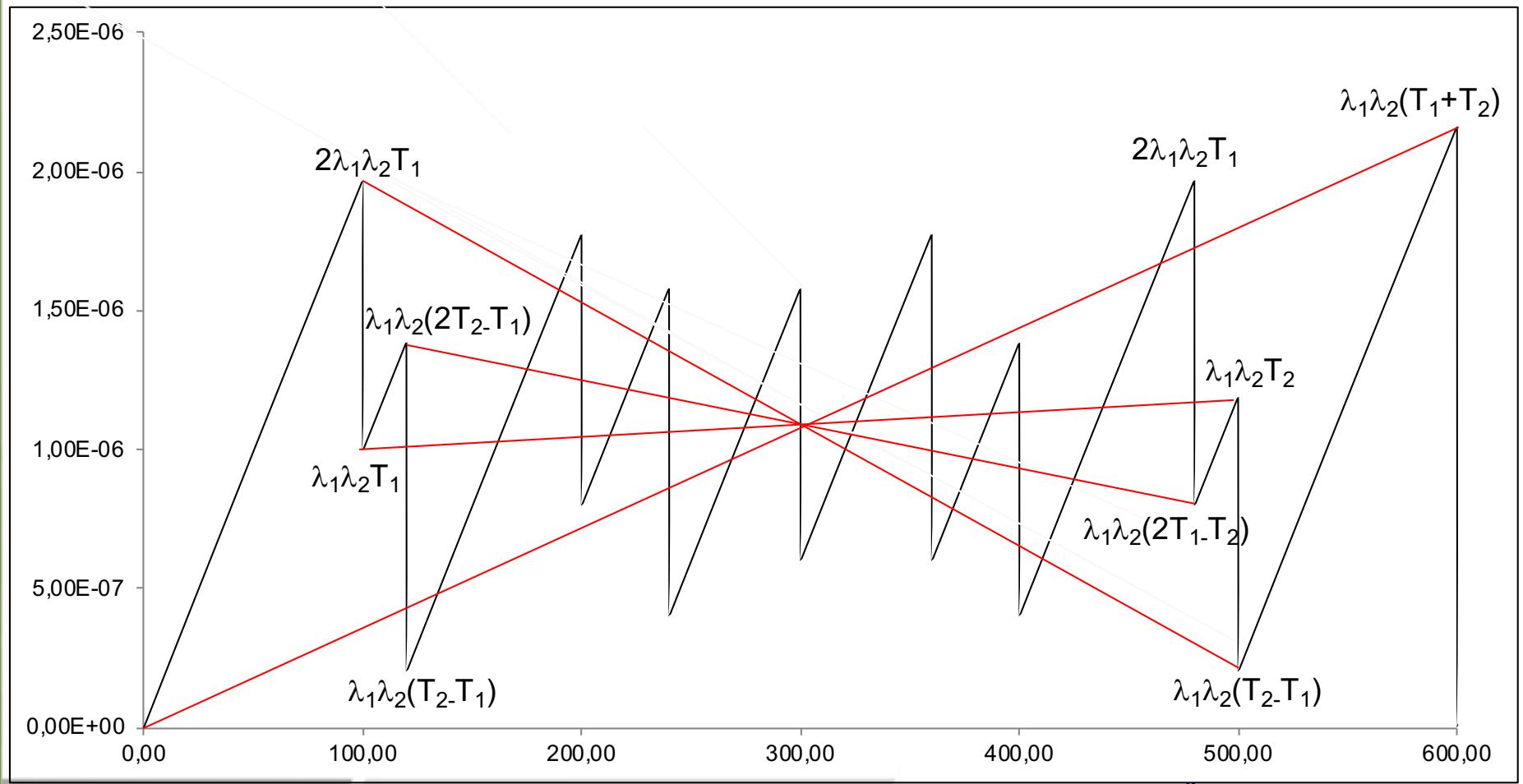
Soit :  $1 - R(T_2) = \frac{(N+1)}{2N}\lambda_1\lambda_2 T_2^2$

D'où :  $\Lambda_{moyen} = \frac{N+1}{2N}\lambda_1\lambda_2 T_2 = \frac{\lambda_1\lambda_2}{2}\left(\frac{T_2}{N} + T_2\right) = \lambda_1\lambda_2 \frac{T_1 + T_2}{2}$

Cela justifie donc, quand les périodicités sont multiples l'une de l'autre, d'en faire la moyenne arithmétique. Ce résultat est généralisable, en calculant dans chaque intervalle, une approximation de  $R(t)$  puis de  $\Lambda(t)$  :

## Annexe 1 : Démonstrations pour deux composants

84 Sous l'hypothèse des temps courts on peut de plus démontrer la remarquable propriété de symétrie suivante :  
 $\Lambda(t) + \Lambda(ppcm(T_1, T_2) - t) = \Lambda_{max} = \lambda_1 \lambda_2 (T_1 + T_2)$



## Annexe 1 : Démonstrations pour deux composants

**85** En effet ultérieurement à une maintenance du composant 1 à l'instant  $k_1 T_1$  (expressions tout à fait analogues après une maintenance du composant 2), une approximation de la fiabilité est :

$$R(t) \approx R(k_1 T_1)[1 - \lambda_1 \lambda_2 (t - k_1 T_1)(t - k_2 T_2)]$$

Avec :  $k_2 = \lfloor \frac{k_1 T_1}{T_2} \rfloor$

D'où :  $\Lambda(t) \approx \lambda_1 \lambda_2 (2t - k_1 T_1 - k_2 T_2)$

=> ensemble de droites de pente  $2\lambda_1 \lambda_2$  avec discontinuités de

- $-\lambda_1 \lambda_2 T_1$  si maintenance composant 1
- $-\lambda_1 \lambda_2 T_2$  si maintenance composant 2

## Annexe 1 : Démonstrations pour deux composants

86

De plus on calcule facilement à partir de la formule :

$$\Lambda(t) \approx \lambda_1 \lambda_2 (2t - k_1 T_1 - k_2 T_2)$$

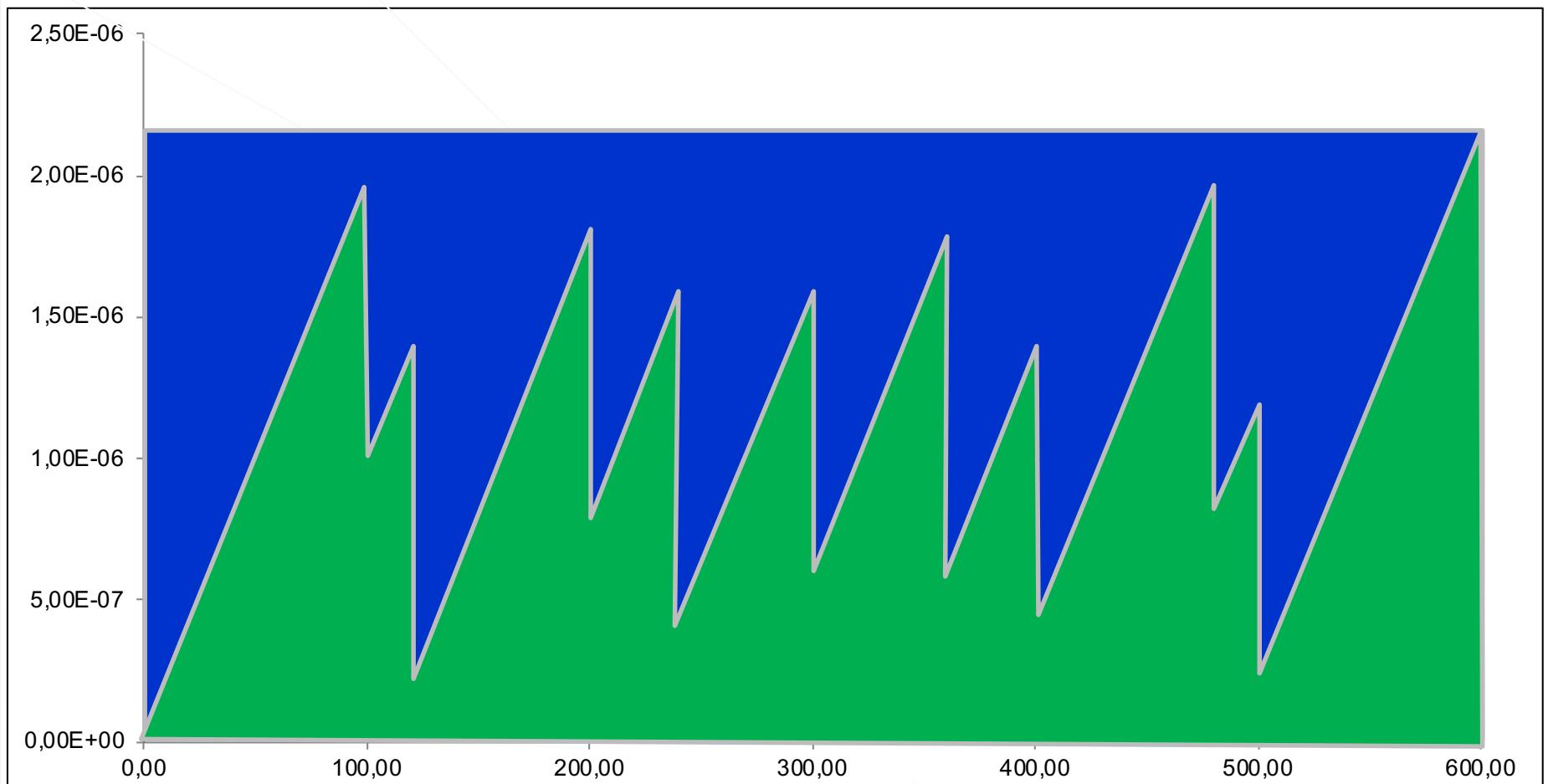
en se plaçant à  $t = \text{ppcm}(T_1, T_2) = n_1 T_1 = n_2 T_2$ , ( $n_1$  et  $n_2$  entiers) :

$$\Lambda_{max} = \Lambda(\text{ppcm}(T_1, T_2)) = \lambda_1 \lambda_2 (T_1 + T_2)$$

# Annexe 1 : Démonstrations pour deux composants

87 Cela a pour conséquence que :

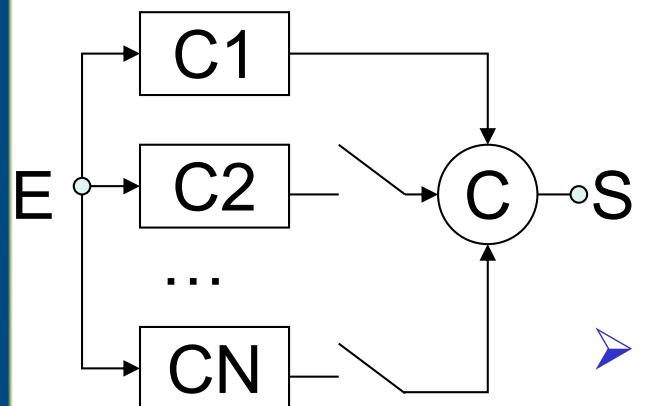
$$\Lambda_{moyen} = \frac{\Lambda_{max}}{2} = \frac{\lambda_1 \lambda_2 (T_1 + T_2)}{2}$$



## Annexe 2 : Systèmes à éléments de secours

88

- Parfois appelé **redondance passive ou froide** : C2 est mis en marche sur défaillance de C1, C3 sur défaillance de C2...
- Il s'agit donc clairement d'un problème à **composants dépendants** qui pourrait être traité par graphes de Markov



Dans ce qui suit on traite (vu son importance) ce problème de manière spécifique **par récurrence**, considérant le taux de défaillance à l'arrêt comme nul :

- Dans le cas où les taux de défaillance  $\lambda_i$  sont constants
- Dans le cas particulier où ils sont de plus tous égaux

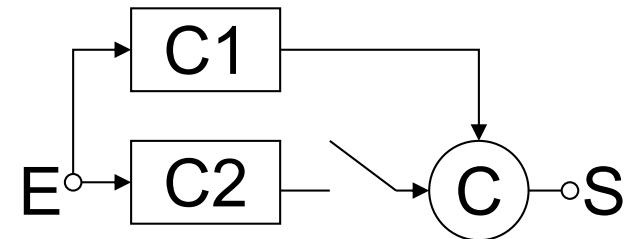
# Redondance passive

89

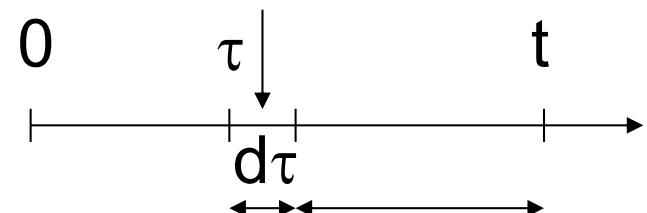
- Commençons par le cas du système à deux éléments : on calcule la défiabilité en envisageant tous les scénarios possibles de défaillance système : on somme sur l'instant t de la défaillance de C1 :

$$1 - R(t) = \int_0^t -\frac{dr_1}{d\tau}(\tau) d\tau (1 - r_2(t - \tau))$$

$$1 - R(t) = \int_0^t \lambda_1 e^{-\lambda_1 \cdot \tau} (1 - e^{-\lambda_2 \cdot (t - \tau)}) d\tau$$



Un scénario de défaillance système : la défaillance de C1 arrive ici :



C2 défaillie dans cet intervalle

# Redondance passive

90

- Par intégration immédiate on trouve :

$$R(t) = \frac{\lambda_2}{\lambda_2 - \lambda_1} e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 - \lambda_2} e^{-\lambda_2 t} \quad \text{Si } \lambda_1 \text{ et } \lambda_2 \text{ sont différents}$$

$$R(t) = (1 + \lambda t) e^{-\lambda t} \quad \text{Si } \lambda_1 = \lambda_2 = \lambda$$

Ces résultats se généralisent en :

$$R(t) = \sum_{i=1}^N B_{i,N} e^{-\lambda_i t} \text{ où } B_{i,N} = \frac{\prod_{k \neq i} \lambda_k}{\prod_{k \neq i} (\lambda_k - \lambda_i)} \quad \text{Si tous les } \lambda_i \text{ sont différents}$$

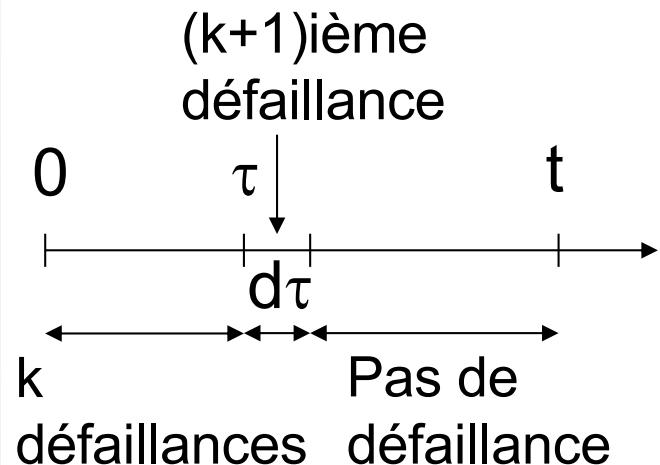
$$R(t) = e^{-\lambda t} \sum_{k=0}^{N-1} \frac{(\lambda t)^k}{k!} \quad \text{Si tous les } \lambda_i \text{ sont égaux à } \lambda \\ (\text{démonstration ci-après dans ce cas})$$

# Redondance passive

91

- On considère un composant de  $\lambda$  constant que l'on remplace par un composant identique à chaque défaillance.
- Dans ce cas : proba( $k$  défaillances sur  $[0,t]$ ) =  $\frac{(\lambda t)^k}{k!} e^{-\lambda t}$

(Loi de Poisson). En effet : Proba(0 défaillances sur  $[0,t]$ ) =  $e^{-\lambda t}$   
La propriété est vraie pour  $k=0$ . La supposant vraie pour  $k$  on obtient par sommation sur l'instant  $\tau$  de la  $(k+1)$ ième défaillance :



proba( $k+1$  défaillances sur  $[0,t]$ )

$$= \int_0^t \frac{(\lambda \tau)^k}{k!} e^{-\lambda \tau} \cdot \lambda d\tau \cdot e^{-\lambda(t-\tau)}$$
$$= \frac{(\lambda t)^{k+1}}{(k+1)!} e^{-\lambda t}$$

# Redondance passive

92

- Fiabilité d'un système composé de N éléments en redondance passive de même  $\lambda$  constant = probabilité(0 à N-1 défaillances) dans l'expérience précédente :

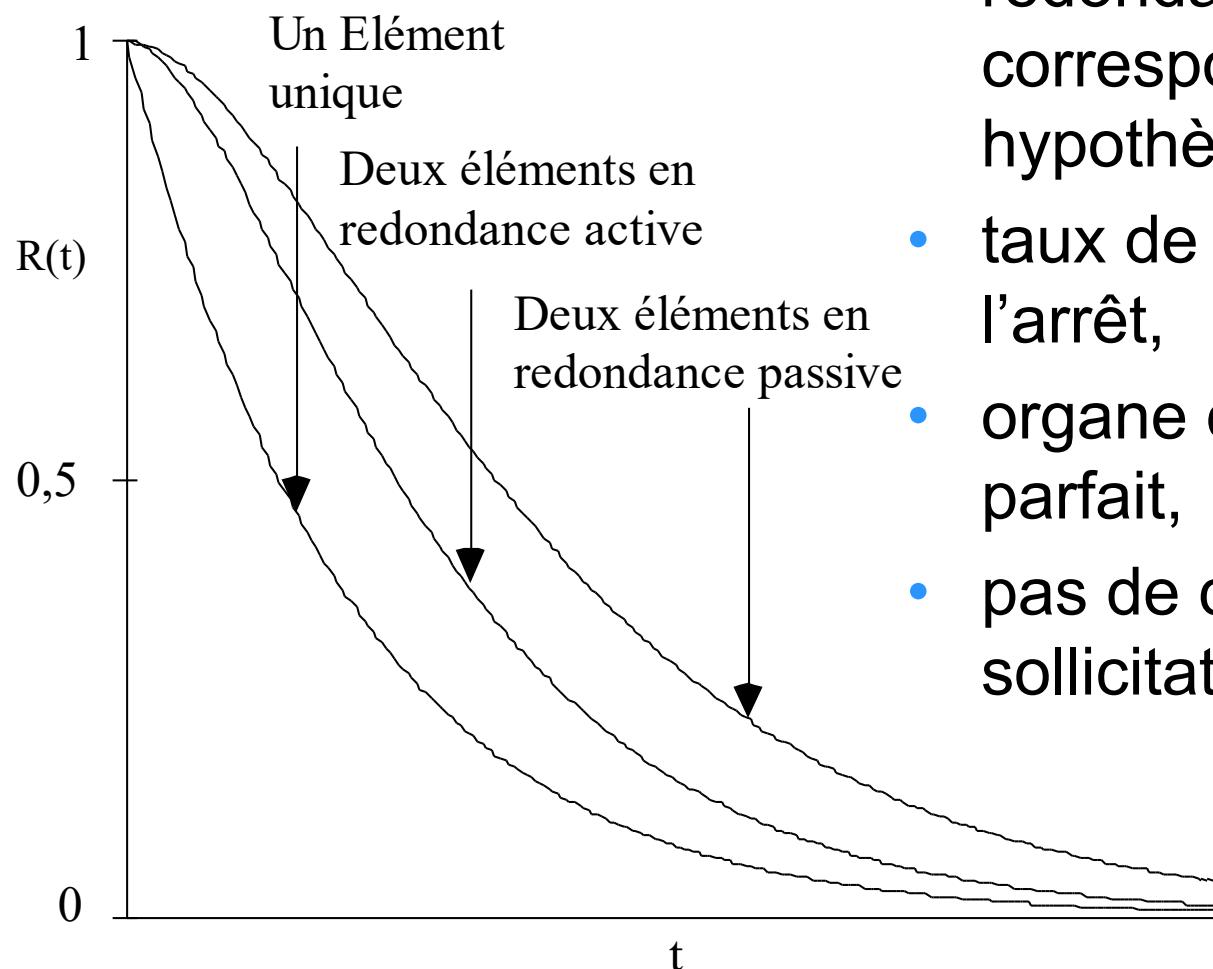
$$R(t) = e^{-\lambda t} \sum_{k=0}^{N-1} \frac{(\lambda t)^k}{k!}$$

$$\prod_{i=1}^N \lambda_i$$

- Comportement aux temps courts :  $R(t) = 1 - \frac{\prod_{i=1}^N \lambda_i}{N!} t^N + O(t^{N+1})$
- Valable y compris si les  $\lambda_i$  sont différents
- Démonstration facile par récurrence à partir des définitions
- Interprétation intuitive : les défaillances doivent arriver dans un ordre précis (seul un ordre sur les  $N!$  possibles compte)

# Redondance passive

93



La redondance passive est donc meilleure que la redondance active correspondante, sous les hypothèses sous-jacentes :

- taux de défaillance nul à l'arrêt,
- organe de commutation parfait,
- pas de défaillance à la sollicitation.