Sûreté de fonctionnement

Diagrammes de fiabilité ou diagrammes de succès (Reliability block diagram)

Nicolae Brînzei

Introduction

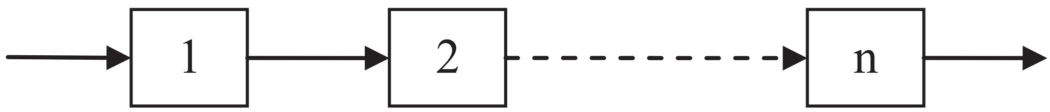
- c'est la méthode la plus anciennement connue pour le calcul de la fiabilité des systèmes non réparables
- bien qu'elle puisse aussi s'appliquer aux systèmes réparables, son usage y reste limité

- le diagramme de fiabilité représente les conditions de réalisation de la fonction d'un système composé de sous systèmes caractérisés par leur fiabilité
- on appelle chemin de succès, un chemin permettant d'aller de l'extrémité gauche à l'extrémité droite du diagramme, symbolisant ainsi que la fonction du système est réalisée
- c'est par analogie avec les circuits électriques que cette méthode a été proposée ; la perte d'un composant dans un circuit électrique empêche le passage du courant
- par analogie, la défaillance d'un composant interrompt le chemin de succès

Systèmes série

Cas général

Un système composé d'au moins 2 sous-systèmes, tel que l'événement E_i, la défaillance d'un d'entre eux, entraîne l'événement E, la défaillance du système.



$$R(t) = P\left[\overline{E}\right] = P\left[\overline{E_1 \mathrm{ou} E_2 \mathrm{ou} \ldots \mathrm{ou} E_n}\right]$$

$$R(t) = P\left[\overline{E_1} \mathrm{et} \overline{E_2} \mathrm{et} \ldots \mathrm{et} \overline{E_n}\right]$$

Si les sous systèmes sont indépendants du point de vue de leurs défaillances :

$$R(t) = \prod_{i=1}^{n} P[\overline{E_i}] = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} \exp\left(-\int_0^t \lambda_i(x)dx\right) = \exp\left(\sum_{i=1}^{n} -\int_0^t \lambda_i(x)dx\right)$$

Systèmes série

Cas général

La fiabilité du système est donc le produit des fiabilités des sous ensembles :

$$R = \prod_{i=1}^{n} (R_i)$$

- pour une série de composants de même type, on peut rechercher des expressions analytiques équivalents pour le taux de défaillance ou le MTTF
- lorsque les composants ne sont pas de même type, seul le recours au calcul numérique permettra de calculer les $R_S(t)$, $\lambda_S(t)$ et $MTTF_S$ équivalents du système

Systèmes série

Taux de défaillance constant

Si le taux de défaillance est constant pour chaque sous ensemble :

$$R = \exp\left(-\left(\sum_{i=1}^{n}\lambda_i\right)t\right)$$

Par identification, le taux de défaillance du système est donc :

$$\lambda = \sum_{i=1}^{n}\lambda_i$$

et le MTTF du système : $\mathrm{MTTF} = \dfrac{1}{\sum_{i=1}^{n}\lambda_i}$

Si les composants sont tous identiques : $\mathrm{MTTF} = \dfrac{1}{n\lambda}$

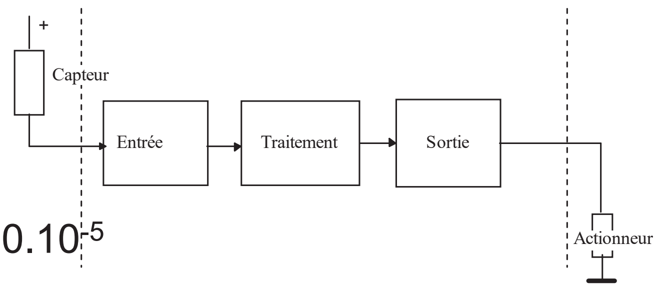
Il est n fois plus petit que celui de chaque composant.

Systèmes série

Exemple

La société SdF produit des systèmes d'automatisme embarqués constitués d'une carte d'entrée (reliée à des capteurs qui fournissent les mesures), d'une unité de traitement et d'une carte de sortie (reliée à des actionneurs pour transmettre les consignes). Chacun de ces composants est caractérisé par un taux de défaillance constant (λ_{In} = 4.10^{-5} h^{-1}, λ_T= 3.10^{-5} h^{-1} et λ_{Out} = 10.10^{-5} h^{-1}).

La défaillance d'un des trois composants entraînera automatiquement la défaillance du système entier.



Le taux de défaillance du système sera donc égal à :

$\lambda_S = \lambda_{In} + \lambda_T + \lambda_{Out}$ = $4.10^{-5} + 3.10^{-5} + 10.10^{-5}$ = 17.10^{-5} h^{-1}

$$\mathrm{MTTF} = \frac{1}{\lambda_S} = 5882 \text{ h}$$

Nous pouvons également estimer la fiabilité à 1000 h de fonctionnement à :

$$R_{1000} = e^{-1000\lambda_S} = 0.84$$

Systèmes série

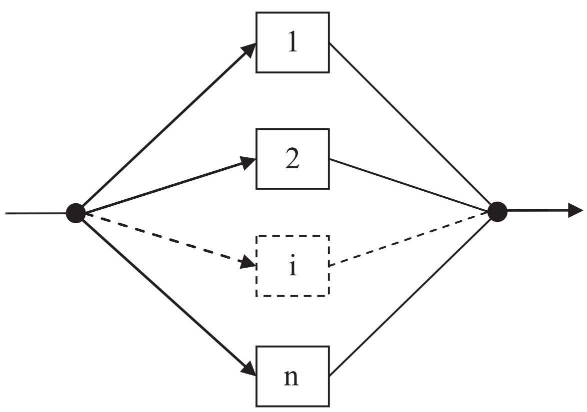
Exercice

L'entreprise SdF décide d'améliorer la fiabilité de ce système pour obtenir une durée moyenne de fonctionnement avant défaillance d'une année (utilisation 24h/24, 7j/7). Pour cela elle décide de concentrer ses efforts seulement sur un des trois composants.

1. Sur quel composant l'entreprise doit elle porter son étude ?
2. Que deviens la valeur de R_{1000} ?
3. Quel sera le taux de défaillance du composant modifié ?

Systèmes parallèle

Cas général



Le système fonctionne dès que l'un au moins des sous-systèmes fonctionne, sa défaillance implique la défaillance de tous les sous-ensembles.

1 - R (t) = P [E1 et E2 et ... et En]

Si les sous systèmes sont mutuellement indépendants :

1 - R (t) = P [E1] . P [E2] … P [En]
= [1 - R1 (t)] . [1 - R2 (t)] … [1 - Rn (t)]

$$R(t) = 1 - \prod_{i=1}^{n}\left(1 - R_i(t)\right)$$

$$R(t) = 1 - \prod_{i=1}^{n}\left[1 - \exp\left(-\int_0^t \lambda_i(x)dx\right)\right]$$

Systèmes parallèle

Cas du taux de défaillance constant

$$R(t) = 1 - \prod_{i=1}^{n} \left[1 - e^{-\lambda_i t}\right] \quad *$$

$$= \sum_{i=1}^{n} e^{-\lambda_i t} - \sum_{i} \sum_{j \neq i} e^{-(\lambda_i + \lambda_j)t} + \sum_{i} \sum_{j \neq i} \sum_{k \neq j \neq i} e^{-(\lambda_i + \lambda_j + \lambda_k)t} + \ldots.. + (-1)^n e^{-\sum_{i=1}^{n} \lambda_i t} \quad **$$

Le taux de défaillance du système est obtenu par la relation $\lambda(t) = -\frac{\frac{dR(t)}{dt}}{R(t)}$

en dérivant * considérée sous la forme $R(t) = 1 - \left[1 - e^{-\lambda_j t}\right] \prod_{i=1; i \neq j}^{n} \left[1 - e^{-\lambda_i t}\right]$

et en itérant on obtient :

$$\lambda(t) = \frac{-R'}{R} = \frac{1}{R} \sum_{i=1}^{n} \lambda_i e^{-\lambda_i t} \prod_{j=1; j \neq i}^{n} \left(1 - e^{-\lambda_j t}\right)$$

En intégrant chacun des termes de R (t) dans **, le $MTTF = \int_0^\infty R(t).dt$ est alors:

$$MTTF = \sum_{i=1}^{n} \frac{1}{\lambda_i} - \sum_{i} \sum_{j \neq i} \frac{1}{\lambda_i + \lambda_j} + \sum_{i} \sum_{j \neq i} \sum_{k \neq j \neq i} \frac{1}{\lambda_i + \lambda_j + \lambda_k} + \ldots. + (-1)^{n+1} \frac{1}{\sum_{i} \lambda_i}$$

Dans le cas où tous les éléments ont le même λ :

$$MTTF = \frac{1}{\lambda} \sum_{i=1}^{n} \frac{1}{i}$$

LORRAINE INP Ensem

Systèmes parallèle

Exemple

Dans le cas simple de deux sous systèmes en parallèle

$$R(t) = 1 - (1 - R_1)(1 - R_2) = R_1 + R_2 - R_1 R_2$$

$$MTTF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

Si les 2 éléments ont même taux λ de défaillance et même fiabilité :

$$R(t) = 2R_1 - R_1^2$$

$$R(t) = R_1(2 - R_1)$$

$$MTTF = \frac{1,5}{\lambda}$$

Systèmes parallèle

Exemple

L'entreprise SdF découvre qu'il est impossible d'améliorer le taux de défaillance des composants constituant le système embarqué pour des raisons techniques. Elle évalue donc la possibilité de mettre une seconde ligne L_2 (identique à la première L_1) en parallèle.

Le MTTF devient donc :

$$MTTF = \frac{1}{\lambda_{L_1}} + \frac{1}{\lambda_{L_2}} - \frac{1}{\lambda_{L_1} + \lambda_{L_2}}$$ avec $\lambda_{L_1} = \lambda_{L_2} = \lambda_s$

$$MTTF = \frac{3}{2 * \lambda s} = 8824h$$

$$R_{1000} = 1 - (1 - e^{-1000\lambda_{L1}}).(1 - e^{-1000\lambda_{L2}}) \approx 0.98$$

LORRAINE INP Ensem

Systèmes parallèle

Exercice

Compte tenu du coût de production du système embarqué constitué de deux lignes de traitement parallèles, l'entreprise s'interroge sur l'opportunité d'étudier d'autres configuration en mettant en parallèle, seulement un des trois composants pour atteindre l'objectif désiré : MTTF d'une année. On considèrera pour la suite que les taux de défaillances des trois composants restent inchangés. Pour des considérations de gestion de stock de pièces de rechange, il est décidé de mettre en redondance uniquement la carte d'entrée ou l'unité de traitement ou la carte de sortie.

1. Sur quel composant l'entreprise doit elle porter son étude ?
2. Combien faut-il mettre des composants du même type en parallèle ? Conclusion ?

Remarques sur la nature des RBD

- supposons que la défaillance redoutée (le risque) d'un relais est de **ne pas se fermer**, on en placera alors **un second en parallèle réalisant ainsi une redondance parallèle**

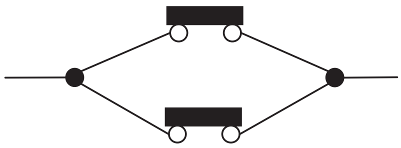


Schéma électrique

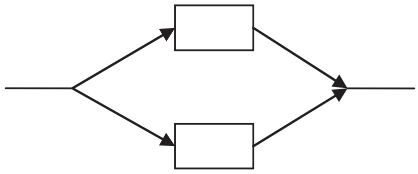


Diagramme de fiabilité

- supposons maintenant que la défaillance redoutée d'un relais est de **ne pas s'ouvrir ; on place alors un deuxième relais en série**

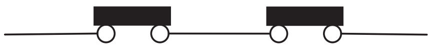


Schéma électrique

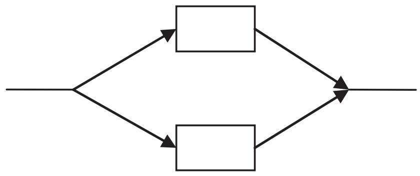


Diagramme de fiabilité

Electriquement, les deux relais sont en série, mais fonctionnellement, du point de vue fiabiliste, ils sont en parallèle. **On a réalisé une redondance parallèle.**

Remarques sur la nature des RBD

- supposons maintenant que deux relais sont en série pour réaliser une **fonction logique ET**, si la défaillance redoutée de ces relais est **le refus de se fermer**, les deux relais sont également **en série du point de vue de la fiabilité** de la fonction logique réalisée, car le refus de se fermer de l'un ou l'autre des deux composants entrave la réalisation de la fonction

Schéma électrique

Diagramme de fiabilité

- de même, les 2 relais en parallèle réalisant une **fonction logique OU**, **le refus de se fermer** de l'un ou l'autre des relais empêche la fonction de se réaliser ; les deux relais sont alors **en série du point de vue de la fiabilité** de la fonction logique

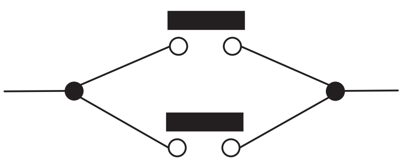


Schéma électrique

Diagramme de fiabilité

Remarques sur la nature des RBD

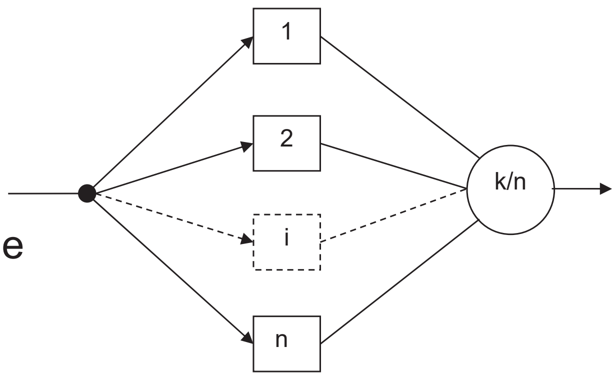
On conçoit donc aisément que pour augmenter la fiabilité de systèmes on soit amené à mettre des sous-systèmes en parallèle ou en série, selon la nature des défaillances redoutées de ces derniers.

La mise en parallèle de sous systèmes du point de vue fiabilité peut se confondre avec la notion de redondance à laquelle on recourt pour améliorer la fiabilité. Il faut cependant faire remarquer que parfois des sous-systèmes se trouvent naturellement en redondance ou qu'il peut y avoir dans un système des redondances cachées. Il est donc important de faire précéder l'établissement du diagramme de succès (fiabilité) par une analyse fonctionnelle précise du système, tout au moins lorsqu'on cherche à évaluer à posteriori la SdF d'un système déjà conçu.

L'idéal, bien sûr, consiste à intégrer l'analyse de la SdF lors de la conception du système.

Redondance k/n

- représente le cas où on exige qu'au moins k éléments parmi les n placés en parallèle soient non défaillants pour que le système fonctionne



- il existe deux cas dégénérés : k=1 (système en parallèle) et k=n (système en série)

- si tous les n éléments sont identiques :

  R(t) = P(au moins k éléments parmi n fonctionnent)

- le nombre d'éléments en fonctionnement suit une loi binomiale de paramètres n et $R_e(t)$ (fiabilité d'un élément)

  Rappel. Loi binomiale de paramètres (n,p) : la v.a. X représente le nombre de réalisations de l'événement A avec la probabilité p au cours de n expériences

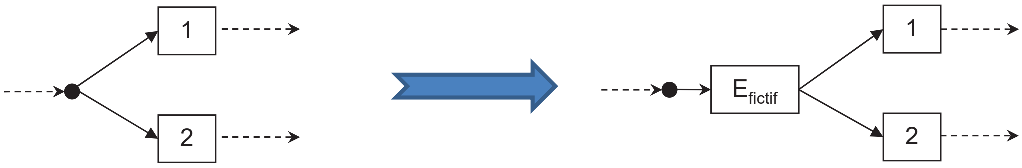
$$P(X=i)=C_n^i p^i (1-p)^{n-i} \quad 0 \le i \le n,\ n \in \mathcal{N}^*,\ p \in [0,1]$$

Fiabilité du système : $R(t)=\sum_{i=k}^{n} C_n^i R_e(t)^i \left(1-R_e(t)\right)^{n-i}$

Extensions

Pour tenir compte de certaines conditions plus complexes, on sera amené à définir quelques extensions :

• pour tenir compte d'**un mode (cause) commun(e) de défaillance** de deux éléments (pannes de mode commun), on introduit dans le RDB **un bloc fictif** pour le représenter



C'est le cas par exemple de deux sources d'alimentation en énergie électrique d'un système qui peuvent tomber en panne pour une raison commune, tel qu'un fort orage.

Extensions

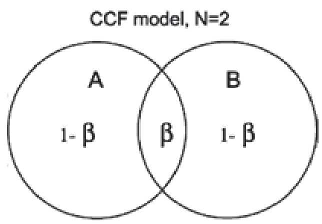
Défaillance de cause commune (DCC) - modèle du facteur β

Ce modèle suppose qu'un certain pourcentage de toutes les défaillances de composants sont des DCC. Plus précisément, on considère qu'un composant peut être défaillant à cause :

- de circonstances qui ne concernent que ce composant en particulier ;
- de l'occurrence d'événements externes qui conduisent à la défaillance simultanée de plusieurs composants.

Le taux de défaillance d'un composant λ_{total} s'écrit alors comme la somme de deux taux de défaillance :

$$\lambda_{total} = \lambda_{ind} + \lambda_{DCC}$$



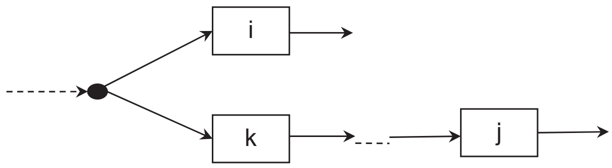
Le facteur β, appelé aussi le facteur de cause commune, est défini par :

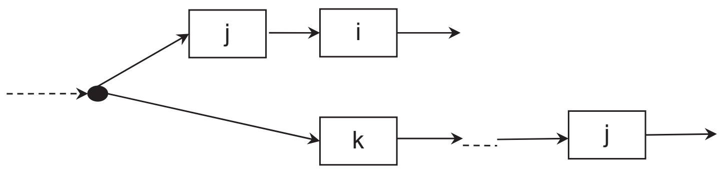
$$\beta = \frac{\lambda_{DCC}}{\lambda_{ind} + \lambda_{DCC}} = \frac{\lambda_{DCC}}{\lambda_{total}}$$

Ce modèle est particulièrement performant dans le cas où le nombre de composants est supérieur ou égal à 2 et que tous les composants sont identiques, c'est-à-dire issus du même fabricant mais aussi exploités dans les mêmes conditions.

Extensions

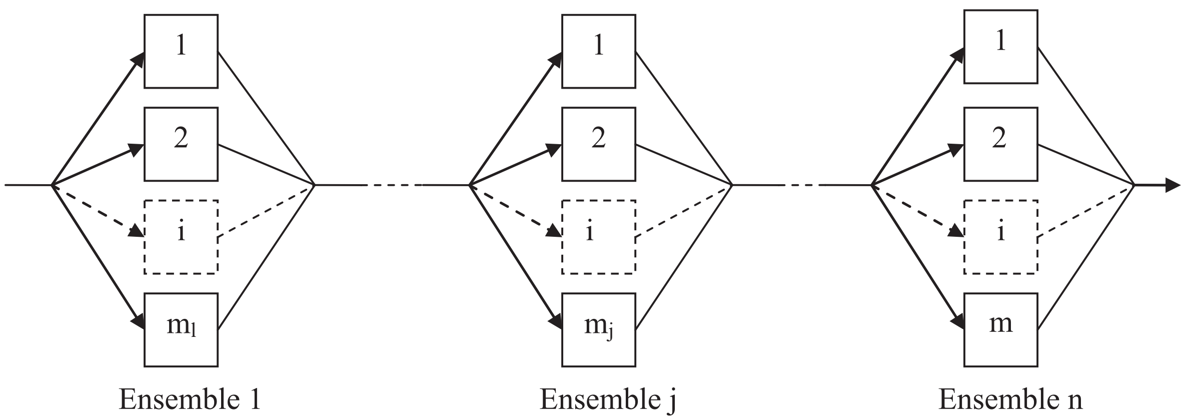
- lorsqu'il y a certaines dépendances entre la défaillance d'un élément i qui est provoquée par la défaillance d'un élément j situé en aval de l'élément i dans le RBD, on **dédouble** le bloc j de façon à tenir compte de cette condition





Systèmes mixtes

Systèmes parallèle-série



Fiabilité d'un ensemble j :

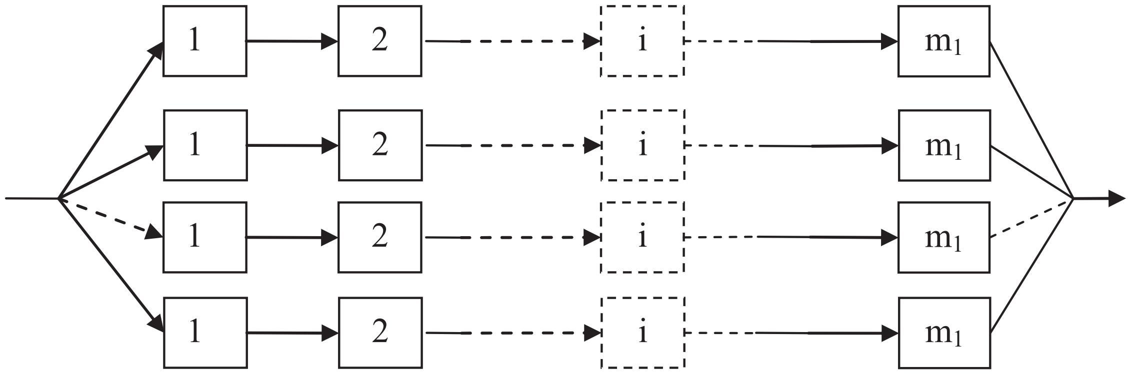
$$R_j = 1 - \prod_{i=1}^{m_j} \left(1 - R_{ij}\right)$$

R_{ij} : fiabilité de l'élément i du $j^{ième}$ ensemble

Fiabilité du système : $$R = \prod_{j=1}^{n} \left[1 - \prod_{i=1}^{m_j} \left(1 - R_{ij}\right)\right]$$

Systèmes mixtes

Système série parallèle



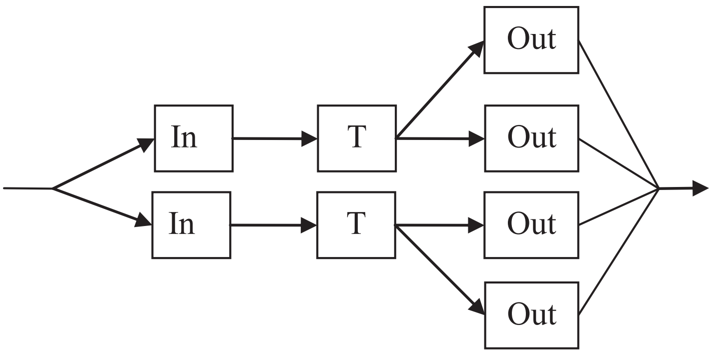
Fiabilité d'une branche série : $R = \prod_{i=1}^{m_j} \left(R_{ij}\right)$

Fiabilité de l'ensemble : $R = 1 - \prod_{j=1}^{n} \left[1 - \prod_{i=1}^{m_j} \left(R_{ij}\right) \right]$

Systèmes mixtes

Exercice

Finalement après différentes études de disponibilité, coût, criticité de l'installation…, la direction de la société SDF a décidé de valider la configuration suivante :

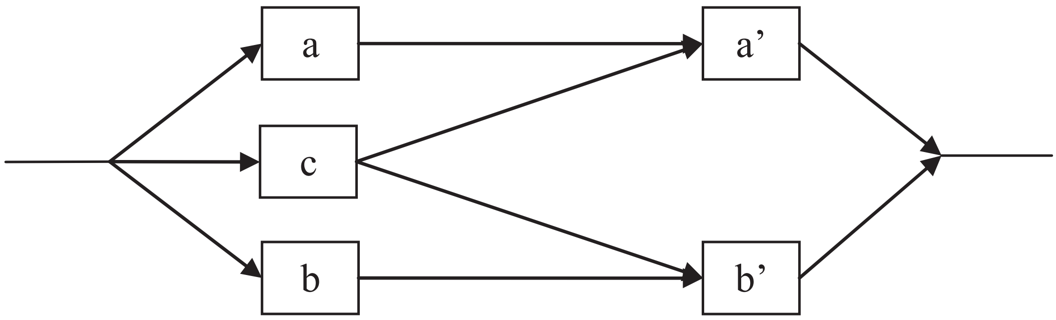


1. Quelle est la fiabilité de ce nouveau système d'automatisme ? Evaluer R_{1000}.
2. L'objectif du MTTF = 1 an est-il respecté ?

Systèmes plus complexes

Exemple

Système avec redondance partagée : dans les chemins aa' et bb', on a constaté que a et b ont une fiabilité insuffisante. On a alors ajouté le composant c en redondance partagée ; il permet de rajouter les chemins de succès ca' ou cb'.



Systèmes plus complexes

Exemple

- soit S l'événement le système s fonctionne et $\overline{S}$ l'événement le système s est défaillant
- soit C l'événement le sous système c fonctionne

Appliquons le théorème des probabilités totales en considérant comme système complet d'événements, les événements suivants :

- le composant c fonctionne
- ce même composant est défaillant

$$P[\overline{S}] = P[\overline{S}/C].P[C] + P[\overline{S}/\overline{C}].P[\overline{C}]$$
$$1 - R_{Sys} = P[\overline{S}/C]R_c + P[\overline{S}/\overline{C}][1 - R_c]$$

- si on sait que c fonctionne, cela revient à dire qu'il y a une connexion directe entre l'extrémité gauche du diagramme et les composants a' et b'. La probabilité que s soit défaillant, sachant que c fonctionne, correspond donc à celle de la défaillance simultanée de a' et b' qui sont en parallèle, soit

$$P[\overline{S}/C] = [1 - R_{a'}][1 - R_{b'}]$$

Systèmes plus complexes

Exemple

- si on sait que c ne fonctionne pas alors il peut être retiré du diagramme qui est réduit aux composants a, b, a', b'. La probabilité que s soit défaillant sachant que c est défaillant correspond donc à celle de la défaillance simultanée des voies aa' et bb', soit

$$P[\bar{S}/C] = [1 - R_{aa'}][1 - R_{bb'}]$$

où $R_{aa'} = R_a.R_{a'}$ et $R_{bb'} = R_b.R_{b'}$

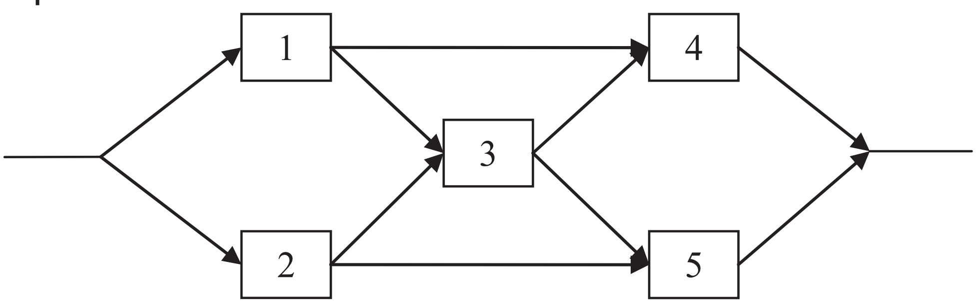
Conséquence

$$1 - R_{Sys} = [1 - R_{a'}]\,[1 - R_{b'}]\,R_c + [1 - R_a.R_{a'}]\,[1 - R_b.R_{b'}]\,[1 - R_c]$$

Systèmes plus complexes

Exercice

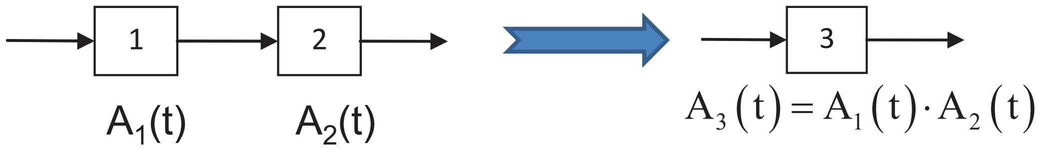
Afin d'augmenter le nombre de chemins de succès et donc la fiabilité du système, on intercale un commutateur (composant 3) ayant lui-même une fiabilité propre.



Calculer la fiabilité équivalente du système.

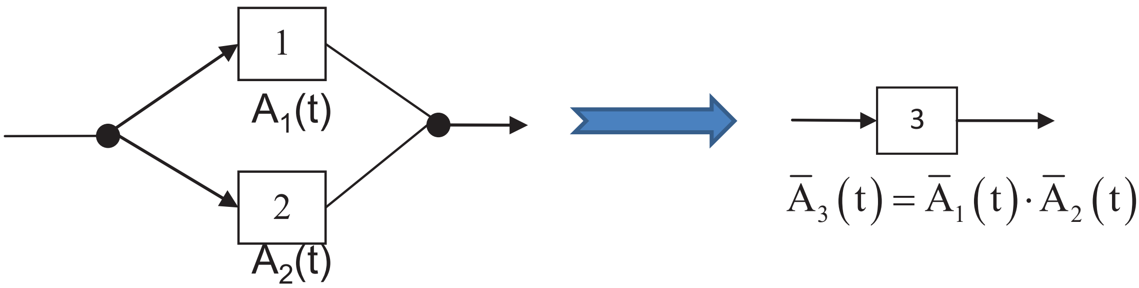
Évaluation de la disponibilité

- on considère des systèmes dont les éléments sont indépendants et sont placés soit *en série*, soit *en parallèle*
- dans le RDB on peut alors remplacer chaque ensemble en série E_1E_2 par :



un seul élément E_3 dont la disponibilité est : $A_3(t) = A_1(t).A_2(t)$

- dans le RDB on peut alors remplacer chaque ensemble en parallèle E_1E_2 par:



un seul élément E_3 dont la disponibilité est : $A_3(t) = 1 - (1 - A_1(t)) \cdot (1 - A_2(t))$

Évaluation de la disponibilité

- en appliquant **successivement** ces réductions on obtient directement la disponibilité du système

- en général $A_i(t)$ est proche de 1, donc $\bar{A}_i(t) << 1$ les calculs se font très simplement en utilisant les indisponibilités
  - systèmes en série

$$\bar{A}_3(t) = 1 - A_1(t) \cdot A_2(t) = 1 - (1 - \bar{A}_1(t)) \cdot (1 - \bar{A}_2(t)) \cong \bar{A}_1(t) + \bar{A}_2(t)$$

  - systèmes en parallèle

$$\bar{A}_3(t) = \bar{A}_1(t) \cdot \bar{A}_2(t)$$

Conclusion

Cette méthode permet de calculer la fiabilité d'un système à partir de l'étude de sa structure fonctionnelle qui permet de définir le diagramme de fiabilité. Elle devient difficile à appliquer pour les structures non simples. On peut également l'utiliser pour le calcul des autres composants de la SdF (maintenabilité, disponibilité).

Il faut noter qu'elle exige certaines hypothèses (sous systèmes indépendants, taux constants, etc.), mais elle présente également des avantages : méthode très répandue et mature, modélisation graphique intuitive et facile, des méthodes de calcul relativement standard et éprouvées.