Sureté de fonctionnement

Simon Chabot

20 mai 2013

1 Un peu de terminologie

Définition 1.1 (Safety) *il s'agit de la sécurité technique. C'est-à-dire du fait qu'il n'y ait pas de panne.*

Définition 1.2 (Security) *il s'agit de la sécurité réglementaire (code du travail, règlement, etc).*

Définition 1.3 (Défaillance) *Une* défaillance *est une altération temporaire ou permanente du service délivré.*

Définition 1.4 (Erreur) *Une* erreur *est l'origine d'une défaillance.*

Définition 1.5 (Faute) *Une* faute *est l'origine d'une erreur.*

Il existe différents moyens de classifications :
- Tolérance aux fautes
- Élimination des fautes
- Prévention des fautes

Une faute peut être :

Passive : c'est à dire qu'elle existe, mais ne perturbe pas le fonctionnement du produit.

Active : son activation produit une erreur de l'un des composant du produit.

Une erreur peut être effacée avant de provoquer une défaillance, par *redondance* par exemple.

2 Fiabilité, maintenabilité, MTTF, MUT, MDT, MTBF et autres joyeusetés

Définition 2.1 (Fiabilité) *Soit $X(t)$ une variable aléatoire dénotant l'état du système S à l'instant t. Si le système est défaillant au temps t, alors $X(t) = 0$ sinon $X(t) = 1$. On pose*

$$R(t) = P\{X(i) = 1, \forall i \in [0; t]\} \tag{1}$$

$R(t)$ est la fonction donnant, par définition, la fiabilité *du système.*

Définition 2.2 (Maintenabilité) *On appelle maintenabilité la fonction $M(t)$ définit comme étant la probabilité que la réparation du système soit achevée sur $[0; t]$; le système étant supposé dans un état défaillant à $t = 0$.*

- *$M(0) = 0$, par hypothèse*
- *$M'(t) > 0$, plus la durée augmente et plus la probabilité de réparation augmente.*
- *$M(\infty) = 1$*

Définition 2.3 (Défiabilité) *On a simplement :*

$$U(t) = 1 - R(t) \tag{2}$$

Définition 2.4 (MTTF − Mean Time To Failure) *Il s'agit de la durée moyenne de fonctionnement. On a :*

$$MTTF = \int_0^{+\infty} R(t)\,\mathrm{d}\,t \tag{3}$$

Définition 2.5 (Taux de défaillance instantanée) *L'événement E est défini par : S est défaillant entre t et $t + \Delta t$ sachant que S n'a pas eu de défaillance sur $[0; t]$.*

$$\Lambda(t) = \lim_{\Delta t \to 0} \frac{P(E)}{\Delta t} \tag{4}$$

D'où :

$$R(t) = \exp\left(-\int_0^t \Lambda(u)\,\mathrm{d}\,u\right) \tag{5}$$

En supposant que le taux de défaillance[1] *soit constant, on le note $\Lambda(t) = \lambda$. On a alors :*

$$R(t) = e^{-\lambda t} \tag{6}$$

$$MTTF = \frac{1}{\lambda} \tag{7}$$

1. ou *taux de panne*

Définition 2.6 (MTTR − Mean Time To Repair) *Le taux de réparation μ est défini ainsi :*

$$\mu = \frac{1}{1-M}\frac{\mathrm{d}\,M}{\mathrm{d}\,t} \tag{8}$$

On peut donc calculer la durée moyenne jusqu'à la réparation. Et on a :

$$MTTR = \int_0^\infty (1 - M(t))\,\mathrm{d}\,t \tag{9}$$

Dans le cas où μ est constant, on a :

$$M(t) = 1 - e^{-\mu t} \qquad\qquad MTTR = \frac{1}{\mu}$$

Définition 2.7 (MUT − Mean Up Time) *Durée moyenne de bon fonctionnement après réparation.*

Définition 2.8 (MDT − Mean Down Time) *Durée moyenne de réparation après défaillance.*

Définition 2.9 (MTBF − Mean Time Between Failures) *Durée moyenne entre défaillances.*

Définition 2.10 (Disponibilité) *La disponibilité $A(t)$ est la probabilité que le système soit disponible au temps t. Dans le cas où μ et λ sont constants, il est possible d'obtenir une expression analytique :*

$$A(t + \mathrm{d}\,t) = A(t)(1 - \lambda\,\mathrm{d}\,t) + (1 - A(t))\mu\,\mathrm{d}\,t \tag{10}$$

Par intégration on trouve :

$$A(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t} \qquad \textit{Si disponible à } t = 0$$

$$A(t) = \frac{\mu}{\lambda+\mu} - \frac{\mu}{\lambda+\mu}e^{-(\lambda+\mu)t} \qquad \textit{Si indisponible à } t = 0$$

On obtient alors une disponibilité asymptotique valant $\frac{\mu}{\lambda+\mu}$.

3 Association série et parallèle

3.1 Série

Soit S un système formé de n composants C_k de loi de fiabilité $R_k(t)$. Le système cesse de fonctionner si *un* des composants tombe en panne. On a donc :

$$R(t) = \prod_{k=1}^{n} R_k(t) \tag{11}$$

$$MTTF = \frac{n}{\lambda} \qquad \text{si } \lambda \text{ est constant} \tag{12}$$

3.2 Parallèle

Soit S un système formé de n composants C_k de loi de fiabilité $R_k(t)$. Le système cesse de fonctionner si *tous* les composants tombent en panne. On a donc :

$$R(t) = 1 - \prod_{k=1}^{n} (1 - R_k(t)) \tag{13}$$

$$MTTF = \frac{1}{\lambda} \sum_{k=1}^{n} \frac{1}{k} \qquad \text{si } \lambda \text{ est constant} \tag{14}$$

4 Redondance M parmi N

Définition 4.1 (Degré de redondance) *Le* degré de redondance *mesure la quantité de redondance présente dans la configuration d'un système. Cette mesure varie de 0 à 1. 0 signifie que le système n'est pas du tout redondant (série) et 1 signifie qu'il s'agit d'un système pur parallèle ($m = 1$).*

$$\eta = \frac{n - m}{n - 1} \tag{15}$$

4.1 Fiabilité et MTTF

En supposant que les N composants soient actifs dès le début, on a :

$$R(t) = \sum_{k=m}^{n} \binom{n}{k} \left(e^{-\lambda t}\right)^k \left(1 - e^{-\lambda t}\right)^{n-k} \tag{16}$$

$$MTTF = \frac{1}{\lambda} \sum_{k=m}^{n} \frac{1}{k} \tag{17}$$

4.1.1 Redondance parallèle active

Voir 3.2.

4.1.2 Redondance parallèle passive

En supposant que les N composants soient actifs dès le début, on a :

$$R(t) = e^{-\lambda t} \sum_{k=1}^{n} \frac{(\lambda t)^{k-1}}{(k-1)!} \tag{18}$$

$$MTTF = \frac{n}{\lambda} \qquad \text{si } \lambda \text{ est constant} \tag{19}$$

5 Système série-parallèle et parallèle-série

5.1 Série-parallèle

La fiabilité d'un système série-parallèle (P branches séries, de longueur N_j, mises en parallèle) est donnée par :

$$R = 1 - \prod_{i=1}^{P} \left(1 - \prod_{j=1}^{N_i} r_{ij} \right) \tag{20}$$

Si les taux de fiabilité sont constants, le comportement aux temps courts est donné par :

$$R = 1 - \prod_{i=1}^{P} \left(\sum_{j=1}^{N_i} \lambda_{ij} \right) t^P + O\left(t^{P+1}\right) \tag{21}$$

5.2 Parallèle-série

La fiabilité d'un système parallèle-série (N étages, de hauteur P_j, parallèles mise en série) est donnée par :

$$R = \prod_{j=1}^{N} \left(1 - \prod_{i=1}^{P_j} (1 - r_{ij}) \right) \tag{22}$$

Si les taux de fiabilité sont constants, le comportement aux temps courts est donné par :

$$R = 1 - \left(\sum_{j=1}^{N} \prod_{i=1}^{P} \lambda_{ij} \right) t^P + O(t^{P+1}) \tag{23}$$

5.3 Systèmes complexes

Soit le système complexe donné en exemple par la figure 1, on s'intéresse alors à sa fiabilité.

- On suppose le composant C_2 défaillant. On obtient alors un système série-parallèle et donc une fiabilité donnée par :

$$r_a = 1 - (1 - r_1 r_4) \times (1 - r_3 r_5)$$

- Si *au contraire* C_2 fonctionne, alors C_1 et C_3 deviennent inutiles et on obtient donc un système parallèle simple dont la fiabilité est donnée par :

$$r_b = 1 - (1 - r_4) \times (1 - r_5)$$

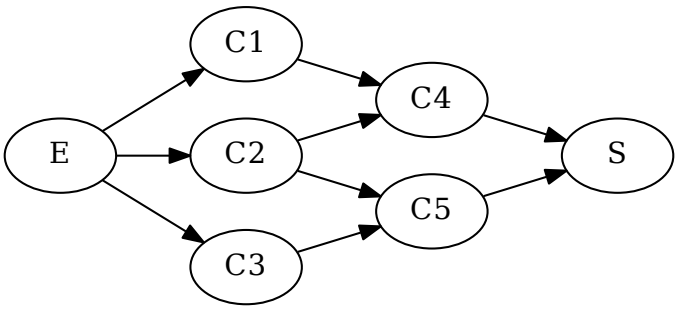

FIGURE 1: Système complexe

– *In fine* on obtient la fiabilité totale du système :

$$\begin{aligned} R &= (1-r_2)r_a + r_2 r_b \\ &= (1-r_2)[1-(1-r_1r_4)(1-r_3r_5)] + r_2[1-(1-r_4)(1-r_5)] \end{aligned}$$

6 Diagrammes de fiabilité

Définition 6.1 (Diagramme de fiabilité) *Un diagramme de fiabilité consiste à visualiser la* logique *de fonctionnement d'un système avec la règle suivante :*

Le système fonctionne s'il existe un chemin[2] *entre l'état et la sortie du diagramme qui ne traverse pas un bloc défaillant.*

Définition 6.2 (Coupe) *Un ensemble de blocs dont le dysfonctionnement entraîne le dysfonctionnement du système.*

– *Une* coupe minimale *est une coupe qui n'en contient aucune autre.*
– *L'*ordre *d'une coupe est le nombre de blocs qu'elle contient.*

6.1 Recherche automatique de coupe minimale

1. On se donne un diagramme de fiabilité.
2. On recherche alors tous les liens minimaux par un parcours exhaustif de tous les chemins et l'on construit une matrice d'incidence des blocs dans les liens.

2. alors appelé chemin de succès.

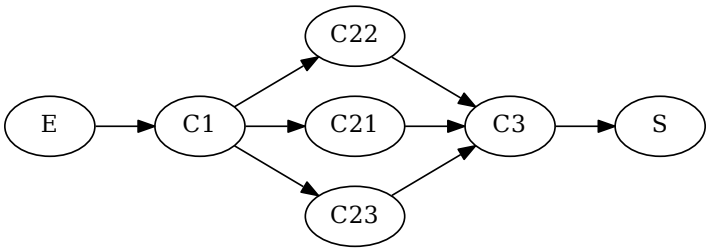

FIGURE 2: Exemple de diagramme de fiabilité

3. Pour trouver les coupes d'ordre 1, on recherche les lignes n'ayant que des uns.
4. On supprime ensuite ces colonnes, qui correspondent aux coupes d'ordre 1. On combine toutes les colonnes deux à deux (avec un OU booléen). Les colonnes n'ayant que des uns sont les coupes minimales d'ordre 2.
5. On supprime les colonnes ainsi trouvées et on recommence pour obtenir les coupes d'ordre 3. Etc.

Exemple 6.1 *Soit le diagramme de fiabilité donné par la figure 3, sur avec lequel on applique la méthode sus-citée.*

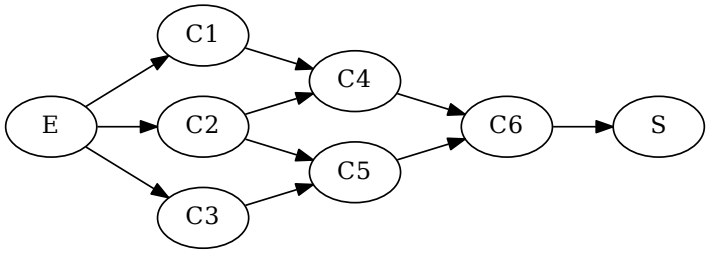

FIGURE 3: Recherche automatique de coupes minimales d'ordre 1

On obtient alors la matrice suivante :

C_1	C_2	C_3	C_4	C_5	C_6
1	0	0	1	0	1
0	1	0	1	0	1
0	1	0	0	1	1
0	0	1	0	1	1

On constate alors que $\bar{C}_6$ constitue une coupe minimale d'ordre 1. On recherche maintenant les coupes minimales d'ordre 2.

C_1C_2	C_1C_3	C_1C_4	C_1C_5	C_2C_3	C_2C_4	C_2C_5	C_3C_4	C_3C_5	C_4C_5
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

On constate alors que $\bar{C}_4\bar{C}_5$ est une coupe minimale d'ordre 2. On peut voir également d'un rapide coup d'œil qu'il y a de nombreuses coupes minimales d'ordre 3 ($\bar{C}_1\bar{C}_2\bar{C}_3$ par exemple).

7 Principe d'inclusion-exclusion

On a :

$$\mathcal{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{S\in[1;n],S\neq\emptyset} (-1)^{-1+\|S\|}\mathcal{P}\left(\bigcap_{i\in S} A_i\right) \tag{24}$$